Command Reference

Digi

Connectware™

Device and Terminal Servers

www.digi.com

Making DEVICE NETWORKING easy™

Contents

Chapter 1 Introduction to Commands

Chapter 2 Commands

Chapter 1 Introduction to Commands

Navigation and Editing Keys

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

Action	Keys
Moves the cursor back one space	Ctrl b
Moves the cursor forward one space	Ctrl f
Deletes the character to the left of the cursor	Back space or Ctrl h
Deletes the character under the cursor	Delete
Scrolls back through commands	Ctrl p
Scrolls forward through commands	Ctrl n
Executes the command	Enter

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 ? **Example:** info ? **Example:** 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 chose 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.

Chapter 2 Commands

This chapter provides a description of each command.

admin

Use the admin command to temporarily access commands reserved for administrators (root) when logged in as a normal (non-root) user.

About the admin Command

After issuing the admin command, the following occurs:

1. A prompt requesting the root password appears.
2. The user types in the root password.
3. If the password is
   - Accepted, the device displays the root prompt, indicating that the user can issue commands reserved for administrators.
   - Not accepted, the device displays the following message: “Incorrect password”

Required Privileges

Only normal users can use the admin command.

Related Information

For information on ending temporary root sessions, see the following commands:

- exit on page 17
- quit on page 28

Syntax

```
admin
```

Example

```
admin
```

boot

Use the boot command to do the following:

- Reboot
- Restore the configuration to defaults
- Load new POST code from a TFTP server
- Load a new firmware into flash ROM from a TFTP host

Note: 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: (1) Attempt to boot from a remote firmware image before issuing the boot load command. See set config on page 44 for more information. (2) After issuing the boot load command, ensure that you receive the message “The image in flash now appears valid.” If you do **not** receive this message, do **not** reboot. Call technical support for instructions on what to do next.

Required Privileges

Root privileges are required to use this command.

Related Information

See the following commands:

- cpconf on page 12 for information on saving the current configuration to a host prior to restoring the configuration to defaults
- revert on page 31 for information on restoring configuration defaults to the latest configuration stored in NVRAM

Syntax: Rebooting

Here is the syntax to reboot the device server:

```
boot action=reset
```

Syntax: Restoring Configuration Defaults

Here is the syntax to restore the configuration to defaults:

```
boot action={eewrite | factory | reset} switch={factory | user}
```

Syntax: Loading New Firmware

Here is the syntax to load a firmware into flash ROM from a TFTP host:

```
boot load={host-ip-address | host-name}:[load-file]
```

Syntax: Loading New POST Code (Digi One and PortServer TS 2/4 only)

```
boot load-post=tftp-server-ip:filename
```

Syntax: Loading New Boot Code (PortServer TS 8/16 only)

```
boot load-post=tftp-server-ip:filename
```

Fields

action={eewrite | factory | reset}

eewrite
resets all but the network-related parts of the configuration to defaults. Ports, users, passwords, and most other features are reset. This option does **not** apply to the PortServer TS 8/16.

factory
resets the entire configuration to defaults

reset
reboots the device

load={*host-ip-address* | *host-name*}:[*file*]

{*host-ip-address* | *host-name*}
is 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*]
is the firmware file

load-post=*tftp-server-ip:post-filename*

tftp-server-ip
is the IP address of a server running TFTP

post-file-name
is the file that holds the new POST or Boot code

switch={factory | user}
determines the firmware to use on reboot. This option applies to PortServer TS 8/16 only.

factory
is the firmware that shipped with the device

user
is the most recent firmware upgrade

Example: Restoring Configuration Defaults

The command reloads the firmware stored in flash ROM and resets the configuration to defaults.

```
boot action=factory
```

Example: Resetting All-But the Network-Related Parts of the Configuration

The command resets all but the network-related parts of the configuration to defaults. This example does **not** apply to PortServer TS 8/16.

```
boot action=eewrite
```

Example: Using the Current OS and Configuration

The command reboots the device and uses the current firmware and configuration stored in flash ROM.

```
boot action=reset
```

Example: 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
```

close

Use the close command to close active Telnet, Rlogin, and connect sessions.

About the close Command

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.

Related Information

See the following commands:

- set user on page 134 for information on defining escape keys for Telnet, Rlogin, and connect sessions

status on page 152 for information on displaying status information on active sessions

Syntax

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

Fields

*

closes all active sessions

connection-number

identifies the session to close

Note: When you issue the close command without options, the current connection is closed.

Example: Closing a Session Identified by Number

```
close 1
```

Example: Closing the Current Session

```
close
```

connect

Use the connect command to initiate a local connection on a port.

About the connect Command

Here is some information on 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.

Note: 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.

Related Information

See the following related commands:

- close on page 10 for information on ending a session
- reconnect on page 29 for information on reestablishing a port connection
- set user on page 134 for information on defining an escape character

Syntax

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

Fields

serial_port
specifies the number of the port on which to establish a connection

id-name
specifies the name (defined on the set ports command) of the port on which to establish a connection

hunt_group
specifies a hunt group, defined with the set ports group command

Example: Connecting to Port 1

```
connect 1
```

cpconf

Use the cpconf command to do the following:

- 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.

Related Information

None

Syntax

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

Fields

fromhost=*host*[:*file*]

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

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

tohost=*host*[:*file*]

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

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

Note: 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

Example: Copying the Configuration From a Host

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

Example: Copying the Configuration To a Host

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

Example: Copying to a Terminal

```
cpconf term
```

display

Use the display command 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

Required Privileges

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

Related Information

None

Syntax: Displaying Information

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

Syntax: Clearing 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 configuration information for the ports specified on the range option. There is only 1 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
is a range of ports. There is only 1 port on the SP/IA.

switches
displays dip switch settings for devices supporting MEI

Example: Displaying Configuration Information on a Port

```
display port range=1
```

Example: Displaying Configuration Information on a Range of Ports

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

Example: Displaying a List of Errors

```
display error
```

Example: Displaying Information on Dip Switch Settings

```
display switches
```

Example: Displaying Power Information

```
display power
```

Example: Clearing Errors

```
display error clear
```

display buffers

Use the display buffers command 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.

Related Information

See the following commands:

- set buffers on page 40
- set wlan on page 145

Syntax

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

Fields

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

range=*range*
is the port or ports to which the command applies

screen
displays the port buffer contents on the screen

tail=*number*
defines the number of lines in the buffer that will be displayed in total. The

number is calculated from the end of the buffer counting back.

tftp=*server:filename*

*serve*r
is the IP address or DNS name of a server running TFTP to which buffer information should be transferred.

filename
is the name to use for the file that will be transferred to the TFTP server

Example: Displaying Buffers

The command displays port buffering information on the screen:

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

Example: Outputting Buffering Information to a TFTP Server

The command transfers port buffering information to a TFTP server:

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

exit

Use the exit command to terminate the following:

- 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.

Related Information

See the following commands:

- admin on page 7 for information on starting a temporary root session
- quit on page 28 for an alternate method of ending a root session

Syntax

```
exit
```

Example

```
exit
```

help

Use this command for information commands.

Required Privileges

Anyone can use this command.

Related Information

None

Syntax

```
help
```

Example

```
help
```

info

Use the info command to do the following:

- Display protocol, interface, IA, serial, and UDP over serial statistics
- Clear statistics

About Statistics Tables

The statistics in these tables are those gathered since the tables were last cleared.

Required Privileges

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

Related Information

None

Syntax: Clear Statistics

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

Syntax: Display Statistics

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

Fields

info clear
clears all the statistic tables

info {*protocol* | network | serial:*port* | ia:*protocol* | sou*:range*}
displays one or more statistics tables, depending on the option specified. Use the following table to clarify how the command works

Syntax	Result	Example
info clear	All statistics are cleared.	info clear
info *protocol* where *protocol* 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:*port* where *port* the port number	Port statistics are displayed.	info serial:1
info ia:*protocol* where *protocol* is one of the following: Compoway/F, df1fullduplex, df1halfduplex, fins, hostlink, modbus, userdefined	IA protocol statistics are displayed.	info ia:fins

Syntax	Result	Example
info sou:*range* where *range* is the port or ports	Serial over UDP statistics associated with a serial port are displayed.	info sou:2

Example: Displaying the IP Table

```
info ip
```

Example: Displaying Information on Modbus

```
info ia:modbus
```

Example: Displaying Serial over UDP Statistics for Port 1

```
info sou:1
```

Example: Clearing All Network Statistics Tables

```
info clear
```

kill

Use the kill command to clear or reset sessions on ports.

Required Privileges

Root privileges are required to use this command.

Related Information

See who on page 158 for information on determining current users.

Syntax

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

Fields

tty=*tty-number*
specifies a port on which to clear a session. Number = 1.

tty=*tty-range*
specifies a range of ports on which to clear sessions. Range = 1.

tty-number
is an alternate method of specifying the number of the port on which to clear a session. Number = 1.

tty-range
is an alternate method of specifying a range of ports on which to clear sessions. Range = 1.

Example: Killing a Session on a Specific Port

```
kill tty=1
```

Example: Killing a Session on a Range of Ports

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

mode

Use the mode command to change or display the operating options for a current Telnet session.

Required Privileges

Anyone can use this command.

Related Information

None

Syntax: Changing Telnet Options

```
mode [bin={on|off}][crmod={on|off}][crlf={on|off}]
```

Syntax: Displaying Telnet Options

```
mode
```

Fields

bin

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

off
turns binary mode off for this Telnet session

The default is off.

crmod

on
means that line feeds are added to received carriage returns

off
means that line feeds are **not** added to received carriage returns

The default is off.

crlf

on
means line feed characters are added to transmitted carriage returns

off
means line feed characters are **not** added to transmitted carriage returns

The default is off.

Example: Turning Binary Mode On

```
mode binary=on
```

Example: Adding Line Feed Characters

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

Example: Displaying Operating Options

```
mode
```

newpass

Use the newpass command 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)

Required Privileges

Anyone can change his or her own password. Root privileges are required to change someone else's password or the root password.

About the newpass Command

When you enter the newpass command, a series of prompts guide you through the process of changing a password.

Related Information

See set user on page 134 for information on configuring users.

Syntax

```
newpass [name=username]
```

Field

name=*username*

is 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 command initiates a dialog that changes the user's password.

```
newpass
```

ping

Use the ping command to test if a host or other device is active and reachable.

Required Privileges

Anyone can use this command.

Related Information

None

Syntax

```
ping [continuous][fill=char] {hostname | ip-addr} [intv=msec]
[loose_sroute=ip-addr,ip-addr...] [npkts=num] [pksiz=bytes]
[record_route] [strict_sroute=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
is the interval in milliseconds between pings

The range is -1 to 60,000, and the default is 1000 milliseconds (one second). -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_sroute
specifies that the ping pass through the routers indicated on its way to the target host. These routers are identified by their IP addresses.

npkts
is the number of packets to include with each ping

The range is 1 to 30,000, and the default is 1.

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

record_route
specifies that routers handling the ping include their IP addresses in the echo reply

strict_sroute
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

Example: Specifying a Simple Ping

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

```
ping 199.150.150.10
```

Example: Specifying Loose Source Routing

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

```
ping 199.150.150.10 loose_sroute=199.150.160.10,190.150.161.10
```

Example: Specifying Strict Source Routing

The command specifies that the ping pass through the routers identified on the strict_sroute 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_sroute=199.150.160.10,190.150.161.10
```

power

Use the power command to:

- 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

Note: This command is context sensitive. The action specified will determine whether it applies to a power unit or to 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

Here is the form of the power command to configure the operating parameters:

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

Outlet can be specified either by entering an outlet number or by using "id" and /or "group" options.

Fields

action

used in conjunction with range, outlet, port or id fields

clear

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

- on means that the outlet(s) configured to the device will receive power
- off means that the outlet(s) configured to the device will not receive power
- reboot means that the outlet(s) 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 outlet(s) is/are already receiving power.
- show displays the status of the unit and/or devices connected for the specified range.

id

performs an action on device unit with specified id, must be used with the action field.

group

performs an action on an outlet with specified group number

range
performs an action on power unit with specified index.

outlet
performs an action on device with specified index

Example: Displaying Status of the Outlets

In this example, the power command displays the status of the outlet including whether they are on/off, id, and the group number.

```
power action=show range=2 outlets=3 (or just "power range=2 outlet=3")
```

Example: Displaying Status of Power Units

In this example, the power command displays the status of two remote power control devices connected to PortServer. Among 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
```

Example: Controlling the Power to a Port

In this example, the power to all outlets affiliated with group 3 will be turned off.

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

Example: Clearing the Maximum Current Detected

In this example, the power command clears the maximum current detected variable for the power unit on port 8.

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

Example: Controlling a Device with a Device Range

In this example, the power to the device on the unit 2 connected to the outlet 3 will be turned on.

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

Example: Controlling 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

Use the quit command to end

- 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.

Related Information

See admin on page 7 for information on temporarily accessing commands reserved for the administrator.

Syntax

```
quit
```

Example

```
quit
```

reconnect

Use the reconnect command to reestablish a connection previously established.

Required Privileges

Anyone can use this command.

Related Information

See the following related commands:

- connect on page 11 for information on establishing a connection on a selected port
- close on page 10 for information on ending a connection
- status on page 152 for information on gathering status on current connections

Syntax

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

Fields

serial-port
specifies the serial port to which this command applies

p=*serial-port* | s=*session*
specifies a serial port or session to which this command applies

Example: Reconnecting to the Last Port Used

```
reconnect
```

remove

Use this command to remove entries from configuration tables.

Required Privileges

Root privileges are required to use this command.

Related Information

None

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
: is one of the following configuration tables:

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

Example: Removing an Entry By Name

The command removes a user from the user table.

```
remove user name=martymertz
```

Example: Removing an Entry By IP Address

The command uses a IP address to identify and remove an entry from the altip table.

```
remove altip ip=143.191.2.120
```

Example: Removing an Entry By Index Number

The command uses an index number to identify and remove an entry from the altip table.

```
remove altip range=3
```

revert

Use this command to restore the configuration to defaults or to the latest configuration stored in NVRAM.

Required Privileges

Root privileges are required to use this command.

Related Information

None

Syntax

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

Fields

option={factory | nvram}

sets one of the configuration options listed in the following table to either the factory defaults or to the latest version of the configuration stored in NVRAM. Here are the options you can specify:

If you specify ...	Then this part of the configuration reverts ...
all	Entire configuration
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
network	altip, arp, host, route, snmp, tcpip, and telnetip configuration

If you specify ...	Then this part of the configuration reverts ...
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

defines a range of ports to which the command applies. This option is valid when used with serial, port, line, flow, keys and login.

Example: Resetting the Port Configuration

The command resets port 1 configuration to defaults.

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

Example: Resetting Network-Related Settings

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

```
revert config=nvram
```

rlogin

Use the rlogin command to log into a remote system from the command line.

Required Privileges

Anyone can use this command.

Related Information

See set user on page 134 for information on configuring a user-specific Rlogin escape character

Syntax

```
rlogin [esc=(char)] {hostname|host-ip-addr}
[{user=user-name | -1 user-name}]
```

Fields

esc

is 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

is the name of a host to log into

host-ip-addr

is the IP address of a host to log into

user=*user-name* | -1 *user-name*

is 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 -1 user-name option is for compatibility with the UNIX rlogin command.

Example: Using a Host Name

The rlogin command establishes an Rlogin session using a host name.

```
rlogin host1
```

Example: Using an IP Address

The rlogin command establishes an Rlogin session using an IP address.

```
rlogin 192.192.150.28
```

Example: 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
```

send

Use the send command to send a control command to a Telnet peer.

Required Privileges

Anyone can use this command.

Related Information

See telnet on page 153 for information on establishing Telnet sessions.

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

Example: Sending the Interrupt Process Signal

The send command transmits an interrupt process signal.

```
send ip
```

Example: Sending an Are You There Signal

The send command transmits an “are you there” signal.

```
send ayt
```

set altip

Use the set altip command to

- Configure a serial port or group of serial ports with an IP address
- Display current entries in the altip table

About the set altip Command

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.

Related Information

See set tcpip on page 119 (the sockets option) for information on configuring the base option.

Syntax: Configuration

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

Syntax: Display

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

Fields

group
  is 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
  specifies a range of index entries in the altip table

mode
  is either raw or Telnet, which is used to determine a connection type for reverse Telnet connections

Example: Displaying the Entire Altip Table

```
set altip
```

Example: Displaying Several Entries

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

Example: Configuring an Entry

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

set arp

Use the set arp command to

- Manually configure an entry in the Address Resolution Protocol (ARP) Table
- Display the contents of the ARP table

About the ARP Table

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.

Required Privileges

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

Related Information

None

Syntax: Configuring ARP Entries

```
set arp ether=etaddr ip=ipaddr [tim2liv=time]
```

Syntax: Displaying ARP Entries

```
set arp [range=range]
```

Fields

ether
: specifies the Ethernet address of a device

ip
: specifies the IP address of a device

range
: specifies a range of table entries, which are identified by the index field in the ARP table

tim2liv
: specifies 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.

Example: Displaying a Range of Entries

```
set arp range=1-4
```

Example: Displaying All Entries

```
set arp
```

Example: Configuring an Entry

```
set arp ip=198.150.150.10 ether=08:00:20:05:0b:da tim2liv=900
```

set auth

Use the set auth command to

- Configure access permissions to serial ports for LAN users.
- Display permission levels

About set auth

The set auth command is a very powerful tool for limiting LAN users' access to ports. Here are a few principles for you to understand in order to use this powerful tool to produce the configuration results you intend:

- 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.

Related Information

See the following commands:

- set ports on page 91 for information on defining ports
- set user on page 134 for information on configuring a user for outbound port access

Syntax: Configuration

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

Syntax: Display

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

Fields

ip

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

login={*range* | none}

requires that users of the IP address specified log in. 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 some 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={*range* | none}

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={*range* | none}
configures unrestricted access for the IP address specified to the range of ports specified

Example: Displaying the Entire Auth Table

```
set auth
```

Example: Displaying Setting for a Range of Entries

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

Example: Configuring No Access for an IP Address

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

Example: Configuring 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
```

Example: Configuring 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 rmauth=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
```

Example: Using the Mask 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
```

set buffers

Use the set buffers command on Digi devices to:

- Configure buffering parameters on a port
- Display the port buffer configuration on all ports

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.

Related Information

See the following commands:

- display buffers on page 15.
- set wlan on page 145

Syntax: Configuring Port Buffering

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

Syntax: Displaying the Port Buffering Configuration

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

Fields

clear
clears the contents of the specified buffer

range=*number*
is the port or ports to which the command applies

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

state

on
means that the data will be buffered

off
means the data will not be buffered and all data will be cleared from the buffer

pause
means the data will not be buffered, but data in the buffer will not be cleared

Example: Displaying Buffer Attributes

In this example, the set buffer command displays the port buffer configuration for all ports.

```
set buffer
```

Example: Configuring 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
```

set chat

Use the set chat command to

- Configure entries in the chat table
- Display chat table entries
- Remove entries
- Rename entries

About the Set Chat Command

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.

Related Information

See set script on page 104 for information on creating scripts that use telephone string translation.

Syntax: Configuration

Here is the form of the set chat command used to configure chat table entries:

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

Syntax: Display

Here is the form of the set chat command used to display chat table entries:

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

Syntax: Remove

Here is the form of the set chat command used to remove a chat table entry:

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

Syntax: Rename

Here is the form of the set chat command used to rename a chat table entry:

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

Fields

delay
: is 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
: is 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
is 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
is a string of up to 24 characters to substitute into telephone numbers in place of the wait character

Example: Displaying the Entire Chat Table

In this example, the set chat command displays the entire chat table.

```
set chat
```

Example: Configuring a Table Entry

In this example, the set chat command configures a new entry.

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

Example: Removing An Entry

In this example, the set chat command removes a chat table entry from the chat table.

```
set chat rmchat=chat1
```

Example: Renaming a Chat Table Entry

In this example, the set chat command renames the chat table entry.

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

set config

Use the set config command to configure or display entries in the network parameters configuration table, which holds

- 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.

Related Information

None

Syntax: Configuration

```
set config [bootfile=file] [boothost=host-ipaddr] [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}]
[circuitbreaker=reset]
```

Syntax: Display

```
set config
```

Fields

bootfile

is 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

is 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

specifies the IP address of a domain name server. This parameter cannot be changed if dhcp=on.

domain

is the name of device server's domain

gateway

is the IP address of the default gateway

ip
is the device server’s IP address

myname
is the device server’s DNS name

nameserv
is 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={latency | throughput}
configures how the Digi device handles network latency. Choose latency if the Digi device will handle delay-sensitive data and 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

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

ignore
means discard ICMP routing redirect messages

The default is ignore.

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

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

sockets
sets the base TCP socket service, which 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. Here is the formula for issuing commands:

- For Telnet connections, the formula is base socket + port number.
- For raw connections, the formula is base socket + 100 + port number.
- For SSH connections, the formula is base socket + 500 + port number.

- For SSL/TLS connections, the formula is base socket + 600 + port number.

The examples that follow in the table illustrate how this works

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

submask

is 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. This is the default. Example: `set config tbreak=std`

any

configures tbreak so any keystroke will break a Telnet connection.

Example: `set config tbreak=any`

none

configures tbreak so no keystoke will break a Telnet connection

Example: `set config tbreak=none`

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

yes

means always boot from the TFTP host identified on the boothost field

smart
means that 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
means boot the device server from internal flash ROM

The default is no.

Example: Displaying the Complete Table

In this example, the set config command displays the network parameter configuration table.

```
set config
```

set device

Use the set device command 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.

Related Information

See the following related commands:

- set chat on page 42
- set line on page 78
- set script on page 104
- set user on page 134

Syntax: Configuration

```
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]
```

Syntax: Display

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

Fields

baud

no
means the baud rate specified on the set line command will be used

rate
is 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, and the default is no.

chat

no
means that a chat table entry is **not** associated with this device

index-num
is a chat table entry (index number) associated with this device

chat-name
is the name of a chat table entry

The default is no.

dialer

no
means that a dialer script is not associated with this device

index-num
is a script table entry (index number) associated with this device

script-name
is the name of a script

The default is no.

name
is a user-defined name for the device

newname
is a new name for a previously defined device

p{1-9}
are integers (1-9) that can be used in the variable fields of login or dialer scripts

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

range
is a device table entry or range of entries (identified by their index numbers)

Example: Displaying the Device Table

```
set device
```

Example: Displaying a Range of Entries in the Device Table

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

Example: Configuring 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
```

set dhcp

Use the set dhcp command 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.

Related Information

See set config on page 44 for information on configuring the IP address manually.

Syntax: Configuration

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

Syntax: Display

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

```
set dhcp
```

Fields

client_identifier=*string*
is 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 \x*n*, where *n* is a hexadecimal value (0- F). To use the backslash character as the string, use two consecutive backslashes (\\).

client_id_type=*type*
is 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={accept | ignore}
determines which TCP keep-alive attributes are used, those set by the DHCP server or those specified on the set tcpip command.

accept
means that the DHCP server settings are used, and the set tcpip settings are not used.

ignore
means that 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={on | off}
turns DHCP on or off. The default is on.

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

renew
renews the IP address of the device server

Example: Enabling DHCP

```
set dhcp run=on
```

Example: Renewing the IP address

```
set dhcp renew
```

set ethernet

Use this command to set and adjust Ethernet communications parameters.

Required Privileges

Root privileges are required to use this command.

Related Information

See "set config" on page 44.

Syntax

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

Fields

duplex={half | full | auto}

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

- half to communicate in half-duplex mode
- full to communicate in full-duplex mode
- auto to sense the mode used on the network and adjust automatically

The default is half-duplex. 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={10 | 100 | auto}

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 to operate at 10 megabits per second (Mbps) only
- 100 to operate at 100 Mbps only
- auto to configure the Digi device to sense 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.

Example: Configuring 100 Mbps Throughput

```
set ethernet speed=100
```

Example: Configuring Full-Duplex Mode

```
set ethernet duplex=full
```

set filter

Use the set filter command to manage 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: An Overview

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

Here are some rules for creating filters:

- 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.

- 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.

About the Filter Table

The filter table holds a maximum of 64 entries.

Required Privileges

Root privileges are required to use this command.

Related Information

See set user on page 134 for information on associating a filter with a particular user.

Syntax: Creation

Use this form of the set filter command to create filters and add stanzas to them or to rename filters.

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

Syntax: Display Filter Table Entries

Use this form of the set filter command to display entries in the filter table.

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

Syntax: Display Filter Stanzas

Use this form of the set filter command to display all the stanzas of a filter.

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

Fields

name
is a name for the filter

newname
is a new name for a previously defined filter

range
is an entry or range of entries in the filters table

show

on
means that stanzas from the filter identified on the name field will be displayed

off
means that stanzas from the filter identified on the name field will **not** be displayed

The default is off.

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

#
is the number of a stanza, which can be from 1 to 32

token/token/token...
are 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:

- *servicename*, which means filter criterion is a name in the service table that identifies a particular process, such as Telnet (see set service on page 112)
- *hostname*, which means filter criterion is the name of a host defined in the host table (see set host on page 63)
- *protocol-number*, which means filter criterion is 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.
- *ip-addr*, which means filter criterion is an IP address
- *ip-mask*, which is an IP mask that modifies the meaning of the ip-addr field
- *port-num*, which means filter criterion is a TCP or UDP port number
- *port-num-port-num*, which means filter criterion is a range of TCP or UDP port numbers
- rcv, which means filter criterion is incoming packets
- send, which means filter criterion is outgoing packets
- dst, which means filter criteria will be found in destination IP packet fields within the IP packet, such as destination IP addresses, ports, and host names
- src, which means filter criteria will be found in source IP packet fields, such as IP addresses, ports, or host names
- syn, which means 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, which means 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, which means filter criterion is TCP packets
- udp, which means filter criterion is UDP packets
- icmp, which means filter criterion is ICMP packets. Note: You can also specify a type of ICMP packet. Here is how: s1=*type*/icmp. *type* is the type of ICMP packet, which can be any of the following listed in the following table:

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

- ! (exclamation), which means that 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

Example: Displaying the Filter Table

```
set filter
```

Example: Displaying Filter Stanzas

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

Example: Removing a Filter from the Filter Table

```
set filter rmfilter=filter1
```

Example: Filtering on a Source IP Address

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

Example: Filtering 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
```

set flow

Use the set flow command to configure or display 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.

Related Information

See the following commands:

- set keys on page 76
- set line on page 78
- set ports on page 91

Syntax: Configuration

```
set flow [aixon={on|off}][altpin={on|off}] [cts={on|off}]
[dcd={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}]
```

Syntax: Display

```
set flow [range=range]
```

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

Fields

aixon={on | off}

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

- on means that they are.
- off means that they are not.

The default is off.

altpin={on | off}

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 means that the altpin option is used.
- off means that the altpin option is **not** used.

The default is off.

cts={on | off}

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

- on means CTS is used for output flow control.
- off means CTS is **not** used for output flow control.

The default is off.

dcd={on | off}
determines whether DCD (data carrier detect) is used for output flow control:

- on means that DCD is used for output flow control.
- off means that DCD is **not** used for output flow control.

The default is off.

dsr={on | off}
determines whether DSR (data set ready) is used for output flow control:

- on means that DSR (data set ready) is used for output flow control.
- off means that DSR is **not** used for output flow control.

The default is off.

dtr={on |off}
determines whether DTR (data terminal ready) is used for input flow control:

- on means that DTR is used for input flow control
- off means that DTR is **not** used for input flow control

The default is off.

forcedcd={on | off}
determines whether the port acts as though DCD were always high. The primary implications 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={on | off}
is used only with software flow control (XON\XOFF) and only if ixany=on:

- on means that the character that resumes output is discarded.
- off means that the character that resumes output is **not** discarded.

The default is off.

ixany={on | off}
is used only with software flow control:

- on means 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 means output will resume only when the XON character is received.

The default is off.

ixoff={on | off}
determines whether to use input software flow control:

- on means use input software flow control
- off means do **not** use input software flow control

The default is on.

ixon={on | off}
determines whether to use output software flow control:

- on means use output software flow control
- off means do **not** use output software flow control

The default is on.

pre-delay=*milliseconds*
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=*milliseconds*
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
is a port or range of ports to which this set flow command applies

ri={on | off}
determines whether RI (ring indicator) is used for output flow control:

- on means use RI for output flow control.
- off means do **not** use RI for output flow control.

The default is off.

rts={on | off | toggle}
determines whether RTS (request to send) is used for output flow control:

- on means use RTS for output flow control.
- off means do not use RTS for output flow control.
- toggle means that RTS is turned on when transmitting. This option does not apply to PortServer TS 8/16 devices.

The default is off.

show=rtstoggle
displays settings related to the RTS toggle feature, which includes information on rts=toggle, post-delay, and predelay

Example: Displaying Flow Control Settings

```
set flow range=1
```

Example: Configuring Flow Control Settings

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

set forwarding

Use the set forwarding command to

- Configure device server to
  - — Function as an IP router using Routing Information Protocol (RIP) to dynamically maintain routes
  - — Perform Proxy ARP services
  - — Handle various ICMP-related functions
- Display IP routing options

Required Privileges

Root privileges are required to use this command.

Related Information

See set route on page 102 for information on creating static routes.

Syntax: Configuration

```
set forwarding [advertise=time] [breakoutsubnets={on | off}]
[icmpdiscovery={on | off}] [icmpsendredirects={on | off}]
[icmpmaskserver={on | off}] [igmp={on | off}]
[poisonreverse={on | off}] [proxyarp={on | off}]
[save={on|off}][state={off | passive | active}]
[splithorizon={on | off}] [timeout=time]
```

Syntax: Display

```
set forwarding
```

Fields

advertise

is 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, and the default is 30 seconds.

icmpdiscovery

on
means send and answer ICMP Router Discovery packets

off
means do **not** send and answer ICMP Router Discovery packets

The default is off.

icmpmaskserver

on
means act as an ICMP mask server

off
means do **not** act as an ICMP mask server

The default is off**.**

icmpsendredirects

on
means 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
means do **not** send ICMP redirect messages

The default is off.

igmp

on
means that 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
means that 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

on
means that poisonreverse 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
means that the poisonreverse option is off

The default is off.

proxyarp

on
means provide proxy ARP services. 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.

off
means do **not** provide proxy ARP services

The default is off.

splithorizon

on
means 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
means the splithorizon option is off

The default is on.

save
on means the configuration will be saved, and off means that 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

off
limits routing to static routes defined in the route table. See set route on page 102.

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
is 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, and the default is 180 seconds.

Example: Displaying the IP Routing Table

```
set forwarding
```

Example: Configuring Proxy ARP

```
set forwarding proxyarp=on
```

Example: Configuring 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
```

set host

Use the set host command to

- Configure the host table, which contains host name-to-IP address mappings
- Display entries in the host table

About the Host Table and DNS

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.

This 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

- 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.

Related Information

See set config on page 44 for information on configuring device server to use a DNS server.

Syntax: Configuration

```
set host name=host-name ip=ip-addr
```

Syntax: Display

```
set host
```

Fields

ip

is the IP address that is to be mapped to the name specified on the name field

name

is the name that is to be mapped to the IP address specified on the ip field

range

is one or a range of index numbers that identify entries in the host table

Example: Displaying the Entire Host Table

```
set host
```

Example: Displaying an Entry in the Host Table

```
set host range=1
```

Example: Configuring a Name-to-IP Address Mapping

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

set ia

Use this command to configure Digi devices for industrial automation (IA) protocols.

Device Support

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

This device ...	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: Serial Port-Connected Devices

Use this discussion for information on configuring serial port-connected master or slave 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}] [rtutimeout=time-out]
[start=start] [type={master | slave}]
```

Fields : Serial Port-Connected Devices

Use this discussion for information on configuring serial port-connected master or slave devices.

set ia serial
: specifies that this command configures a serial port-connected master or a slave

acktimeout=*time-out*
: applies to the DF1 Full-Duplex, DF1 Half-Duplex, FINS, and Hostlink protocols and is 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 default is 250

milliseconds, and the range is 0 to 60000 milliseconds.

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

addextfunc={(*range of functions*) | all}
applies to the Modbus RTU and Modbus Ascii protocols and is 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={on | off}
applies to the user defined protocol and it is 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 accidently recognized as the end of the message.

broadcast={on | off | replace}
applies to the Modbus RTU and Modbus ASCII protocols and specifies how to handle an incoming Modbus request with a unit id equal to 0 (the Modbus broadcast address). A value of “on” will tell the Digi device to send requests to the destination device and not expect a response message in return. A value of “off” tells the Digi device to throw away the broadcast request. A value of “replace” will change a broadcast request to a normal request by replacing the unit id 0 with a value of 1. The default setting is “replace”.

checksum={bcc | crc}
applies to the DF1 Full-Duplex and DF1 Half-Duplex protocols and is the error checking method to use on this serial connection. Choose the method required by the device connected to the serial port.

duplicatedetection={on | off}
applies to the DF1 Full-Duplex and DF1 Half-Duplex protocols and setting this parameter to “on” filters out consecutive requests that have identical command, source, and tns bytes. This behavior is necessary for compliance with the DF1 specification. The default setting is “on”.

end=*end*
applies to the user defined protocol and is the character string that tells the Digi One IA RealPort that the protocol message is complete. Here are some rules and tips for specifying this string:

- 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, \x*hh*, 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 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={on | off}
applies to the DF1 Full-Duplex, DF1 Half-Duplex, Modbus RTU, and Modbus ASCII protocols. This parameter specifies if 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={*0-65535ms*}
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 is typically used to accommodate Modbus requests with functions that take a long time to complete. The addextfunc and rmextfunc commands 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={auto | (1-255)}
applies to the Modbus RTU and Modbus Ascii protocols and is 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=*milliseconds*
applies to all the serial IA protocols and is the period to wait for a response to a request before discarding the message. The default is 1000 milliseconds, and the range is 0 to 60000 milliseconds.

naktimeoutlimit=*retries*
applies to the DF1 Full-Duplex protocol and is 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 default is 3, and the range is 0 to 255.

polltimeout
applies to the DF1Half-Duplex protocol and is the period a master waits for a response to a poll before either polling again (see the polltimeoutlimit option) or giving up on getting a response. The default is 250 milliseconds, and the range is 0 to 60000 milliseconds.

polltimeoutlimit
applies to the DF1 Half-Duplex protocol and is the number of polltimeouts

allowed before the master gives up on getting a response to a poll. The default is 3, and the range is 0 to 255.

protocol=*serial-protocol*

is 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, if the connected device requires the Omron Compowayf protocol
- df1fullduplex, if the connected device requires the Allen-Bradley DF1 Full-Duplex protocol
- df1halfduplex, if the connected device requires the Allen-Bradley DF1 Half-Duplex protocol
- fins, if the connected device requires the FINS protocol
- hostlink, if the connected device requires the Hostlink protocol
- modbusascii, if the connected device requires the Modbus ASCII protocol
- modbusrtu, if the connected device requires the Modbus RTU protocol
- userdefined, if 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=*range*

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

rmextfunc={(*range of functions*) | all}

applies to the Modbus RTU and Modbus ASCII protocols and is used to remove from the list of Modbus functions that will use the exttimeout instead of the messagetimeout. See the exttimeout command for more details.

rtutimeout=*time-out*

applies to the Modbus RTU protocol and is the period 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=*start*

applies to the user defined protocol and is the character string that tells the Digi device that the protocol message has started. Here are some rules and tips for specifying this string:

- 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, \x*hh*, 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={master | slave}
defines whether the serial entity configured with this command is a master or a slave device

Syntax: Network-Based Masters

Use this discussion to configure a network-based master, which is required only if you want to deactivate a class of network masters.

```
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}]
```

Fields: Network-Based Masters

Use this discussion to do the following:

- Configure one of the timeout values that will be used for communication with a network master (usually the defaults work)
- Want to deactivate all masters that use a specific protocol

set ia netmaster
specifies that this command configures a master that is located on the network

protocol
is one of the following:

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

active={on | off}
determines whether this network master accepts incoming connections. The default is on.

addextfunc={(*range of functions*) | all}
applies to the Modbus TCP protocol and is 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.

broadcast={on | off | replace}
applies to the Modbus TCP protocol and specifies how to handle an incoming Modbus request with a unit id equal to 0 (the Modbus broadcast address). A value of “on” will tell the Digi device to send requests to the destination device and not expect a response message in return. A value of “off” tells the Digi device to throw away the broadcast request. A value of “replace” will change a broadcast request to a normal request by replacing the unit id 0 with a value of 1. The default setting is “replace”.

connectiontimeout
defines the time in seconds 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={on | off}
applies to the Allen-Bradley Ethernet and Modbus TCP protocols. This parameter specifies if 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={*0-65535ms*}
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 commands are used to add and remove from the list of Modbus functions that will use the exttimeout setting. 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={(*range of functions*) | all}
applies to the Modbus TCP protocol and is used to remove from the list of Modbus functions that will use the exttimeout instead of the messagetimeout. See the exttimeout command for more details.

Syntax: Network-Based Slaves

Use this discussion for information on configuring a network-based slave.

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

Fields: Network-Based Slaves

Use this discussion for information on configuring a network-based slave.

active={on |off}
determines whether this network slave is active. The default is on.

encoding={tcp | udp}
determines the transport service--either TCP or UDP--for communication with the network slave. Use this option only when the `protocol=socket` is also specified. Use TCP for connection-oriented

service and UDP for connectionless service. If you choose UDP, packet delivery is not guaranteed. The default is TCP.

ip=*ip-address*
is the IP address of a network slave

port=*num*
is 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={abethernet | ethernetip | modbustcp | socket}
is 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, if the network slave uses the Allen-Bradley Ethernet protocol
- modbustcp, if the network slave uses the Modbus/TCP protocol
- socket, if the network slave uses TCP or UDP socket communication
- ethernetip, for communication with a network-based device that communicates using Ethernet/IP

range=*range*
is an identifying number for this slave. Use numbers 1 through 8.

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

Syntax: Serial Master Routes

Use this discussion for information on configuring either a network or serial route for a serial master.

```
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}]
```

Fields for Routes

protaddr=*protocol-address*
is 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:

- For Modbus RTU or Modbus ASCII, the range is 0 to 255.

- For DF1 Full-Duplex and Half-Duplex, the range is 0 to 255.
- For Omron Hostlink and FINS, the range is 0 to 99.

CompoWay/F does not support protocol addressing.

range=*range*
identifies the route being configured. Use numbers 1 through 12.

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

type={network **|** serial **|** empty}
specifies the type of route to configure. Use network to configure a route to a network based device. Use serial for routes to a serial based device. Use empty to remove a route entry from the route table.

Fields for Network-Based Routes

Use this discussion for information on configuring a network-based route.

active={on |off}
determines whether a network route is active. When active is set to on, messages will be forwarded to this route. When active is set to off, messages will not 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.

encoding={tcp **|** udp}
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. Use TCP for connection-oriented service and UDP for connectionless service. If you choose UDP, packet delivery is not guaranteed. The default is TCP.

fixedaddress={auto | (*1-255*)}
applies to the Modbus TCP protocol and is 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=*ip-address*
specifies the IP address of the network route

port=*num*
is 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={abethernet **|** ethernetip **|** modbustcp **|** socket}
is 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, if the network slave uses the Allen-Bradley Ethernet (sometimes called CSP) protocol
- modbustcp, if the network slave uses the Modbus/TCP protocol
- socket, if the network slave uses TCP or UDP socket communication
- ethernetip, for communication with a network-based device that communicates using Ethernet/IP

reconnecttime=*time*

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 default is 4000 milliseconds, and the range is 0 to 60000 milliseconds. Specifying 0 means that the Digi device does not wait between attempts to establish a connection.

Field: Serial-Based Routes

Use this discussion for information on configuring a serial-based route.

port=*num*

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

Example: 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
`set ia serial protocol=modbusrtu type=master range=1`	`set ia serial protocol=modbusrtu type=slave range=1`
`set ia route ip=192.1.1.2 protocol=socket active=on range=1 table=1 protaddr=0-255`	

Example: 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
```

Example: 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
```

Example: 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
```

set ippool

Use the set ippool command to create a pool of IP addresses for serial ports

Required Privileges

Root privileges are required to use this command.

Related Information

For information on linking a user to the IP address pool, see set user on page 134.

Syntax

```
set ippool count=num-ip-addr ip=1st-ip-addr
```

Fields

count

is the number of IP addresses in the pool. The count can be from 1 to 64.

ip

is the first IP address in the pool

Example

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.

```
set ippool ip=190.175.175.20 count=4
```

set keys

Use the set keys command to

- Change the key or key sequences used to generate certain characters and command functions
- Display current key mappings for these characters and functions

About the set keys Command

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.

Related Information

None

Syntax: Configuration

Here is the form of the set keys command used to change the key sequences that generate certain characters and command functions.

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

Syntax: Display

Here is the form of the set keys command used to display current key mappings.

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

Fields

function
is one of the following characters or control functions:

Note: ^ means press and hold the Ctrl key.

backchar
is the back character. The default is ^b.

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

erase
is the erase command. The default is ^h.

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

intr
is the interrupt command. The default is ^c.

kill
is the kill character. The default is ^u.

lnext
is 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
is the XON character. The default is ^q.

xoff
is the XOFF character. The default is ^s.

xona
is the auxiliary XON character. The default is ^q.

xoffa
is the auxiliary XOFF character. The default is ^s.

range
is 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.

Example: Displaying 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
```

Example: Changing 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

Use the set line command to configure and display options associated with a serial line.

Required Privileges

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

Related Information

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

- set ports on page 91
- set flow on page 57

Syntax: Configuration

```
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}]
```

Syntax: Display

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

Fields

baud

is 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

ignore
means that the Telnet break signal is ignored

send
means send the Telnet break signal on the serial line when the device server receives a break signal

escape
means send the escape sequence on the serial line when the device server receives a break signal

The default is ignore.

csize

is 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
means the device server ignores errors

null
means device server changes the error character to a null character

parmrk
means the device server “marks” the error with FF (16450 error byte)

dos
means that the device server marks the error with an error character

The default is ignore.

inpck

on
means input parity checking is turned on

off
means input error checking is turned off

The default is off.

istrip

on
means the high-order bit is stripped from each byte

off
means the high order bit is **not** stripped from each byte

The default is off.

onlcr

on
means that new line characters are mapped to carriage return/line feed characters

off
means that no mapping of new line characters occurs

The default is off.

otab

on
means that output tabs are converted to eight spaces

off
means that output tabs are **not** converted

The default is off.

parity

o
means odd parity is selected

e
means even parity is selected

n
means no parity is selected

m
means mark parity is selected

s
means space parity is selected

The default is n (no parity).

range
is the port or range of ports to which this command applies

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

The default is 1 stop bit.

Example: Displaying Serial Line Options

```
set line
```

Example: Configuring Baud, Parity and Stop Bits

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

set logins

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.

Related Information

None

Syntax: Configuration

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

Syntax: Display

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

Fields

cmdprompt

is 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

on
means that a user must log into the port

off
means that 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 91 for more information.

logprompt

is the login prompt displayed. The maximum length is 10 characters. Enclose this string in quotation marks if it includes spaces.

The default is login:.

passprompt

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

The default is password:dbps

passwd

on
means that users are required to supply a password to access the ports specified by the range field

off
means that 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 91).

range
is 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 (PortServer 8/16 only)
is 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

on
means that the device server displays connection status messages to users before the login prompt

off
means that the device server does **not** display connection status messages to users before the login prompt

The default is off.

write

on
means that configuration changes made by regular users can be saved and used for subsequent sessions by that user

off
means that configuration changes made by regular users are **not** saved

Example: Displaying Login Information on All Ports

```
set logins
```

Example: Displaying Login Information on a Range of Ports

```
set logins range=1
```

Example: Configuring 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
```

Example: Configuring 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

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.

Related Information

See set user on page 134 (the menu and defaultaccess fields) for information on setting up a user to use a menu.

Syntax: Creating Menus

Use this form of the set menu command to create a menu:

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

Syntax: Displaying Table Entries

Use this form of the set menu command to display the contents of the menu table:

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

Syntax: Displaying Lines of a Menus

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

Syntax: Removing Lines

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

Fields

c#=*command*

c
means that this is a command that is executed when a user selects this menu line

#
is a line number. Lines appear in numeric order on the menu.

command
is any command. Enclose commands containing spaces in quotation marks.

name
specifies a name for the menu. If this parameter is not used, menus are named menu*X*, 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
is a port or range of ports

rmentry
removes the specified line from the menu

m#=*string*

m
means that this is a text or informational line

#
is a line number for the menu. Lines appear in numeric order on the menu.

string
is a text string. Enclose strings with spaces in quotation marks.

show=on
displays menu entries identified on the range field

t#=*string*

t
means that this is a title line

#
is a line number for the menu. Each menu can have two title lines (t1 and t2).

string
is a text string. Enclose strings with spaces in quotation marks.

Example: Creating 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”
```

Example: Displaying the Menu Table

```
set menu
```

Example: Displaying the Contents of a Menu

```
set menu ra=1 show=on
```

set modem

Use the set modem command to

- Assign modem test and initialization scripts to ports
- 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.

Related Information

See set script on page 104 for more information on creating modem scripts.

Syntax: Configuration

Use this form of the set modem command to configure an association between a port and modem test and initialization scripts:

```
set modem [init={no | script | index-num}][range=range]
[test={no | script | index-num}]
```

Syntax: Display

Use this form of the set modem command to display modem table entries:

```
set modem [range=range]
```

Syntax: Clear

Use this form of the set modem command to clear an association between a port and modem test and initialization scripts:

```
set modem [init=no] [test=no]
```

Fields

init

is 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
- no, which clears an association between a port and an initialization script

range

is the range of ports to which this command applies

test

is 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
- no, which clears an association between a port and a test script

Example: Displaying the Current Port’s Scripts

In this example, the set modem command displays the script table.

```
set modem
```

Example: Displaying a Range of Ports’ Scripts

In this example, the set modem command displays the names of scripts associated with a range of ports.

```
set modem range=1-16
```

Example: Configuring a Port for Scripts

In this example, the set modem command configures an association between a port and test and initialization scripts.

```
set modem test=test1 range=1 init=init1
```

Example: Clearing a Port of Scripts

In this example, the set modem command clears an association between a port and test and initialization scripts.

```
set modem range=1 test=no init=no
```

set netlogins

Use the set netlogins command to:

- Configure the sequence of events that occur when a user logs into a server over the network.
- Display current netlogin settings.

Device Support

This command is supported on the PortServer TS 8/16 only.

Required Privileges

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

Related Information

See set logins command.

Syntax

```
set netlogins [rootprompt=string] [cmdprompt=string]
[logprompt=string] [passprompt=string]
```

Fields

cmdprompt

is 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

on
means that a user must log into the port

off
means that 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 91 for more information.

logprompt

is the login prompt displayed. The maximum length is 10 characters. Enclose this string in quotation marks if it includes spaces.

The default is login:.

passprompt

is 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

on
means that users are required to supply a password to access the ports

specified by the range field

off
means that 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 91).

range
is 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
is 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

on
means that the device server displays connection status messages to users before the login prompt

off
means that the device server does **not** display connection status messages to users before the login prompt

The default is off.

write

on
means that configuration changes made by regular users can be saved and used for subsequent sessions by that user

off
means that configuration changes made by regular users are **not** saved

Example: Displaying Netlogins Information on All Ports

```
set netlogins
```

Example: Displaying Netlogins Information on a Range of Ports

```
set netlogins range=1-2
```

Example: Configuring 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
```

Example: Configuring 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
```

set ports

Use the set ports command to

- Configure the port’s operating parameters
- Display the port’s operating parameters

Required Privileges

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

Related Information

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

- set line on page 78
- set flow on page 57
- set keys on page 76
- set logins on page 81
- set powerunit on page 97

Syntax: Configuration

Here is the form of the set ports command to configure the operating parameters of a port:

```
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}]
```

Syntax: Display

Here is the form of the set ports command to display operating parameters for a port:

```
set ports [range=range] [show={script | id | autoconnect}]
```

Fields

auto={on | off}

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.

- on means that they will be automatically connected to a destination.
- off means that they will **not** be automatically connected to a destination.

The default is off.

autoservice={default | raw | rlogin| telnet}

specifies the autoconnection service for this port, which is only used if auto=on. Choose one of the following:

- default, which normally means the Digi device will use Telnet. The exception is if the dport field is 0 or 513. In that case, rlogin is used.
- raw
- rlogin
- telnet

bin={on | off}
determines whether Telnet users of the port are provided with Telnet binary connections:

- on means that Telnet users are provided with Telnet binary connections.
- off means that Telnet users are provided with normal (ASCII) connections.

The default is off.

dest={*ip-addr* | none}
is the IP address of the destination system to which port users will be routed if auto=on. Specify none to disable the field.

dev
is the device type, which defines the device connected to the port. Typically, you can use the following to define the devices listed:

- Power units use dev=power
- Most printers can use dev=prn.
- Most dumb terminals can use dev=term.
- Most incoming modem connections can use dev=min.
- Most outgoing modem connections can use dev=mout.
- Most bidirectional modem connections can use dev=mio.
- Most Realport connections can use dev=rp.
- Most reverse Telnet connections can use dev=prn.
- Modem emulation uses 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	• The device generates a login when carrier is detected (DCD high) and data is received. • The device closes the port at carrier loss (DCD low). • DTR and RTS are low when the connection is idle. • This type does **not** support reverse Telnet or RealPort. • This type requires 10-pin cables with DCD and DTR cross-connected or an altpin cable.

Device Type	Attributes
hio	• The device generates a login when carrier is detected (DCD high) and data is received. • The device closes the port at carrier loss (DCD low). • DTR and RTS are low when the connection is idle. • This type requires 10-pin cables with DCD and DTR cross-connected or an altpin cable.
host	• The device does not generate a login. • The device opens the port at DCD high and closes the port at carrier loss (DCD low). • DTR and RTS are low when the connection is idle. • This type supports reverse Telnet and RealPort. • This type requires a cable that supports carrier detect (DCD).
ia	• The device never generates a login. • 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. • Specifying dev=ia enables port support for industrial automation. See "set ia" on page 65.
min	• The device server generates a login when carrier is detected (DCD high). • The device server closes the port at carrier loss (DCD low). • DTR and RTS are high when the connection is idle. • This type requires a 10-pin straight-through cable or an altpin cable. • Do not use dev=min for RealPort and reverse Telnet connections.
mio	• The device generates a login when carrier is detected (DCD high). • The device closes the port at carrier loss (DCD low). • DTR and RTS are high when the connection is idle. • This type requires a 10-pin straight-through cable or an altpin cable.
mout	• The device never generates a login. • The device closes the port at carrier loss (DCD low). • DTR and RTS are low when the connection is idle. • This type requires a 10-pin straight-through cable or an altpin cable. • dev=mout supports RealPort and reverse Telnet.
pm	• The device never generates a login. • This device’s characteristics are specific to modem emulation settings for a given port. • DTR and RTS are low when the connection is idle. • Use dev=pm when initiating communication with the device.

Device Type	Attributes
power (PortServer TS 8/16 only)	• The device never generates a login. • This device's characteristics are specific to power management settings for a given port. • DTR and RTS are low when the connection is idle. • Use dev=power when initiating communication with the power device. • Change from dev=power to other device name to stop communication with power unit.
prn	• The device never generates a login. • device server ignores carrier. • DTR and RTS are low when the connection is idle. • 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. • Use dev=prn for reverse Telnet connections.
rp	• The device never generates a login. • The device ignores carrier. • DTR and RTS are low when the connection is idle. • 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. • Use dev=rp for RealPort connections.
term	• The device generates a login when it receives data. • The device ignores loss of carrier (DCD low). • DTR and RTS are high when the connection is idle. • 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. • Do **not** use dev=term for RealPort and reverse Telnet connections.

The default is term.

Note: 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=*port*

is 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

Note: If you specify 0, Rlogin is used.

- None, which disables the field

The default is 0.

flushstchar={default | on | off}
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={none | *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=*id*
specifies a character string for the port, which can be used in console management applications to identify the device connected to the port. Enclose this string in quotation marks if there are spaces in the string.

keepalive={on | off}
determines whether the keepalive function is implemented with autoconnections. The default is off.

p[1-9]=*script-param*
are 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=*ports*
is the port or range of ports to which this command applies

scriptname=*name*
is 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=*sessions*
is the maximum number of sessions any user can run through this port

The range is 1-9, and the default is 4.

show={autoconnect | *id* | *script*}
displays autoconnect and script configuration information for the port specified and information on who is using the port.

termtype
is 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
is 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.

Example: Displaying Attributes of the Current Port

In this example, the set ports command displays attributes for the port to which the user is connected.

```
set ports
```

Example: Displaying Attributes for a Range of Ports

In this example, the set ports command displays attributes for a range of ports.

```
set ports range=1
```

Example: Configuring 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
```

set powerunit

Use the set powerunit command to:

- Configure power management
- Display power management configuration
- Clear power management configuration

Device Support

Only PortServer TS 8/16 devices use this command.

Required Privileges

Root privileges are required to use this command.

Related Information

See power on page 26 for information on managing power management devices.

Syntax: Configuration

Here is the form of the set powerunit command to configure the device for 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#]
```

Syntax: Display

Here is the form of the set powerunit command to display power management settings:

```
set powerunit [range=port][range=port group=group]
[range=port id=id][range=port outlet=outlet]
```

Syntax: Clear

Here is the form of the set powerunit command to clear power management settings:

```
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

is 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

is 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

specifies a particular outlet or range of outlets on the power control unit

range=*port*

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: Individual port	range=2
Example: List of ports	range=1,3,5
Example: Range of ports	range=1-5

size

is 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.

Example: Displaying the Entire Power Management Configuration

In this example, the entire power management configuration is displayed.

```
set powerunit
```

Example: Displaying the Power Management Configuration for a Port

In this example, port 7 power management configuration is displayed.

```
set powerunit range=7
```

Example: Displaying Configuration for an Outlet

In this example, user permissions for outlet 6 are displayed.

```
set powerunit range=7 outlet=3
```

Example: Configuring Remote Power Control Device (Basic)

This example produces a simple power management configuration .

```
set powerunit range=8 type=baytech size=10
```

Example: Configuring an Current Threshold

In this example, the current threshold is configured for 15 Amps.

```
set powerunit  range=8 alarm1=15
```

Example: Configuring a Temperature Threshold

In this example, the temperature threshold is configured for 32 degrees C.

```
set powerunit  range=8 temp1threshold=32
```

Example: Configuring 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
```

Example: Configuring a Group

```
set powerunit range=8 outlet=1-4 group=3
```

set radius

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

About RADIUS

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.

Related Information

None

Syntax: Configuration

Here is the form of the set radius command used to configure device server to use RADIUS servers to authenticate dial-in users.

```
set radius [accountingsocket=tcp-port] [authsocket=tcp-port]
[primary=ip-adr] [run={on|off}] [secondary=ip-adr]
[secret=password] [tolerant={on|off}]
```

Syntax: Display

Here is the form of the set radius command used to display RADIUS configuration status.

```
set radius
```

Fields

accountingsocket

is 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. If they are different, however, 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

is 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. If they are different, however, 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

is the IP address of the primary RADIUS server. This is the server that device server queries first. If this server is down or busy, the device server queries the secondary server (if there is one).

run

on
enables RADIUS authentication

off
disables RADIUS authentication

The default is off.

secondary
is the IP address of a secondary RADIUS server

secret
is 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
on means ignore unrecognized RADIUS attributes. Off means that the connection is denied if unrecognized RADIUS attributes are present.

Example: Displaying RADIUS Configuration Status

In this example, the set radius command displays the status of the current RADIUS configuration.

```
set radius
```

Example: Configuring a Primary RADIUS Server

In this example the set radius command configures device server to use a primary RADIUS server.

```
set radius run=on primary=199.150.150.10 secret=xyyzzz
```

Example: Configuring 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

Use the set route command to

- Manually configure IP routes
- Remove routes from the routing table
- Display the contents of the route table

About 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.

Related Information

See set forwarding on page 60 for information on configuring device server to use dynamic IP routes maintained by RIP.

Syntax: Configuration

Here is the form of the set route command used to manually configure and remove IP routes:

```
set route gateway=ip-adr wanname=name mask=mask metric=hops
net=net-adr range=range
```

Syntax: Display

Here is the form of the set route command used to display the route table:

```
set route
```

Fields

gateway
is 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.

mask
is the subnet mask used by the destination network

metric
is the number of routers through which a datagram must pass before reaching the destination network defined on the net field

net
is the IP network address of the destination network

wanname
is the interface to use for this route, which is one of the following

- For routes over a PPP link, it is the name of a set user command that defines a PPP user
- For routes over the Ethernet interface it is ether

Example: Displaying the Route Table

In this example, the set route command displays the entire route table.

```
set route
```

Example: Displaying a Range of Route Table Entries

In this example, the set route command displays a range of entries in the route table.

```
set route range=3-5
```

Example: Removing an Entry in the Route Table

In this example, the set route command removes an entry from the route table.

```
set route rmroute=on range=2
```

Example: Configuring a Route over a WAN Connection

In this example, the set route command configures a route that uses a WAN connection through a serial port.

```
set route net=199.150.144.8 mask=255.255.255.0 metric=3
wanname=user998 gateway=199.150.100.2
```

set script

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.

Related Information

See the following commands:

- set user on page 134 for information on assigning a login script to a user
- set chat on page 42 for information on telephone number string translation

Syntax: Configuration

Here is the form of the set script command used to configure or edit a modem or login script:

```
set script [name=name] [newname=new-name] s{1-24}=”stanza-content”
```

Note: The *stanza_content* value is enclosed in quotation marks.

Syntax: Display Entries

Here is the form of the set script command used to display entries in the script table:

```
set script range=range
```

Syntax: Display Stanzas

Here is the form of the set script command used to display all the stanzas of a script:

```
set script name=name show=on
```

Syntax: Delete a Script

Here is the form of the set script command used to delete a script from a script table:

```
set script {rmscript=on name=name | rmscript=name}
```

Fields

name
: is the name of the script

newname
: is 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 script specified

s {1-24}=*stanza-content*
is the number of a script stanza (1 through 24) and the contents of the stanza.

Note: The content 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
A*np*	Sets • Character size to *n*, which can be either 7 or 8 bits. • Parity to *p*, which can be one of the following values: 0=no parity, 1=odd 2=even 3=mark **Example:** s1=”A70”
B*n*	Transmits a break signal *n* milliseconds long. If *n* is not specified, the length is 250 milliseconds. **Example:** s7=”B100”
C*n*	Sets carrier loss detection. If *n*= • 0, carrier loss is not detected • 1, the modem hangs up if the port loses DCD **Example:** S2=”C1”
D+*m*	Raises a modem signal. If *m* is • 1, DTR is raised • 2, RTS is raised
D-*m*	Lowers a modem signal. If *m* is • 1, DTR is dropped • 2, RTS is dropped
E{*string*}	Writes the string either to • A user terminal (if running interactively) • To a trace buffer (if running in the background) This string can include any of the escape commands listed in “Script Escape Commands”, which follows this discussion. **Example:** S10=”E{Please Log In}”
F*n*	Pauses for *n* seconds and flushes input data. The default is 0. **Example:** s1=”F10”
G*s*	Immediately does one of the following, depending on the value of *s.* If *s* is • The number of a stanza, control is passed to that stanza • + (plus), the script is exited with a success message from E string • - (minus) the script is exited with a failure message from E string **Example:** s2=”G7”

Command	Description
H*s*	Sets the carrier lost (hang-up) recovery to stanza *s,* which is the number identifying another stanza or one of the following: • + (plus), which means Exit, indicating success • - (minus), which means Exit, indicating a general failure • * (star), which means indicate that the remote system is busy • = (equal), which means indicate that the remote system is down **Example:** s2=”H+”
M{*string*}	Writes *string* to a modem **Example:** s2=”M{at&f\c}” This string can include any of the escape commands listed in “Script Escape Commands”, which follows this discussion.
N*b*	Changes the baud rate. The range is 50 to 115,200. Rates under 110 bps should be used only on expansion ports. **Example:** s4=”N19200”
P*n*	Pauses for *n* seconds. If you do not specify a value for *n*, the default is 1 second. **Example:** s5=”P2”
Q*n*	Sets software flow control. If *n* is • 0, flow control is disabled • 1, flow control is enabled **Example:** s5=”Q0”
S*n*	Defines the time to wait (timeout), in seconds, for a modem signal or input data **Example:** s2=”S5”
T*s*	Defines the timeout recovery state. If the timeout is exceeded, control is passed to this stanza. **Example:** s2=”T8”
U*n*	Immediately executes the text of stanza *n*, as if it were inserted to replace this command. You can nest this command, up to a maximum of 10. **Example:** s2=”U4”
W+*m*	Waits for a modem signal to go high. If *m* is • 1, wait for DCD to go high • 2, wait for CTS to go high **Example:** s6=”W+1”
W-*m*	Waits for a modem signal to go low. If *m* is • 1, wait for DCD to go low • 2, wait for CTS to go low **Example:** s6=”W-1”
[*string*]*s*	Defines the *string* and the stanza to jump to when the *string* is received on a communications line. This string can include any of the escape commands listed in “Script Escape Commands”, which follows this discussion. **Example:** 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
^c	This is the character transmitted by an ASCII keyboard when the CTRL key is held down and the c key is pressed.
\b	Backspace
\f	Form feed
\t	Tab
\n	New line
\r	Return
\\	Backslash
\nnn	Octal byte value *nnn*
\xhh	Hexadecimal byte value *hh*
%n	Is a variable, where n is • A telephone number whose value comes from the n*n* field on the set user command • one of the following special characters: `*` (star), which generates a tone equivalent to dialing * on a touch-tone phone # (pound), which generates a tone equivalent to dialing # on a touch-tone phone =, which causes a pause of 2 seconds `w,` which causes a wait for a secondary dial tone `-` (minus), which is completely ignored and not passed to the modem.
%p	Is a variable, where *p* is an integer from 1 to 9. For login scripts, the value of *p* comes from the p*n* field on the set user command. For dialer scripts, options come from the p*n* field of the set device command.

Example: Displaying the Entire Script Table

```
set script
```

Example: Displaying an Entry in the Script Table

```
set script range=4
```

Example: Displaying 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
```

Example: Configuring a Login Script

In this example, set script commands define a login script. The script 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.

Script

```
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+”
```

Script Interpretation

Use the information that follows for help in interpreting the script.

- Here is an interpretation of what stanza S1 does:
  - — 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.
- Here is an interpretation of what stanza S2 does:
  - — 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.
- Here is an interpretation of what stanza S3 does:
  - — 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.
  - — Here is an interpretation of what stanza S4 does. This stanza 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.
  - — Here is an interpretation of what stanza S5 does. This stanza 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.

Example: Configuring a Dialer Script

In this example, the a telephone number is passed to the modem.

```
set script name=dialer1 s1=”M{atdt9524452624\r}”
```

set secureaccess

Use this command to disable Digi device services for users of inbound connections.

Required Privileges

Root privileges are required to use this command.

Related Information

None.

Syntax: Configuration

```
set secureaccess level={secure | high | normal} service={on | off}
```

Syntax: Display

```
set secureaccess
```

Fields

set secureaccess
displays secureaccess settings

level={secure | high | normal}
determines which group of services are on (available) for inbound users. Specify one of the following:

- secure, which means that SSH is the only service available to inbound users
- high, which means that SSH, HTTP, HTTPS, SNMP, RealPort, Secure RealPort, and SSL services are available to inbound users
- normal, which means all services are available

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

service={on | off}
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

If you specify ...	This service is turned on or off ...
ssh	SSH
telnet	Telnet

Example: Disabling Inbound Telnet Connections

```
set secureaccess telnet=off
```

Example: Disabling All Services Except SSH

```
set secureaccess level=secure
```

Example: Displaying Secure Access Settings

```
set secureaccess
```

set service

Use the set service command to

- Configure (associate) names with TCP and UDP service ports for use in filters
- Display entries in the service table

About 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.

Related Information

See set filter on page 53 for information on configuring filters.

Syntax: Configuration

Use this form of the set service command to associate names with TCP service ports:

```
set service name=name port={udp:port|tcp:port}
```

Syntax: Display

Use this form of the set service command to display entries in the service table:

```
set service [range=range]
```

Fields

name
  is the name to assign the service

port
  is the TCP or UDP port number for the service

range
is a range of entries in the service table, which is used to identify entries to display or delete

{rmservice=*name* | rmservice=on}

name
is the name of a service to be removed from the service table

on
means remove the service (or services) from the service table identified on the range field

Example: Displaying the Service Table

In this example, the set service command displays the entire service table.

```
set service
```

Example: Displaying an Entry 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
```

Example: Configuring 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
```

set snmp

Use the set snmp command to configure, enable, and disable device server's SNMP (Simple Network Management Protocol) agent.

Required Privileges

Normal user may display information. Root privileges are required to change settings.

Related Information

None

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={on|off}

determines whether an SNMP trap is sent when an authentication error occurs

on

means the agent sends an authentication trap to the SNMP manager when an authentication error occurs

off

means the agent silently ignores SNMP requests that fail authentication

The default is off.

cold_start_trap={on|off}

determines whether an SNMP trap is sent to the SNMP manager when a reboot occurs

on

means the agent sends a trap when a reboot occurs

off

means that a trap is not sent when a reboot occurs

The default is off.

contact

is a text string that identifies a contact person (usually an administrator). The entry must be surrounded by quotation marks if there are spaces in the text.

curr_thresh_exc_trap={on|off}
determines whether an SNMP trap is sent to the SNMP manager when the electrical current threshold on a power control device is exceeded

on
means the agent sends a trap when the threshold is exceeded

off
means that a trap is not sent when the threshold is exceeded

The default is off.

get_request=*community*
is 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
means the agent sends a trap when the link comes up

off
means that a trap is not sent when the link comes up

The default is off.

location
is a text string that describes device server’s location. The entry must be surrounded by quotation marks if there are spaces in the text.

name
is a text string that identifies device server. The entry must be surrounded by quotation marks if there are spaces in the text.

login_trap={on | off}
determines whether the device server sends a trap each time someone attempts to log into the system

on
means send a trap at each attempt to log in

off
means do not send a trap each time someone attempts to log in

The default is off.

run

on
starts the SNMP daemon

off
means the SNMP daemon will not start

The default is off.

set_request
displays a prompt of a password required to write to device server SNMP

managed objects. The default is private.

trap_dest
is the IP address of the system to which the agent should send traps

temp_thresh_exc_trap={on|off}
determines whether an SNMP trap is sent to the SNMP manager when the temperature threshold on a power control device is exceeded

on
means the agent sends a trap when the threshold is exceeded

off
means that a trap is not sent when the threshold is exceeded

The default is off.

Example: Displaying SNMP Configuration

In this example, the snmp command displays the SNMP configuration.

```
set snmp
```

Example: Configuring All Trap Options

In this example, all SNMP trap options are configured.

```
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

Use this command to configure the serial port socket ID feature.

PortServer TS 8/16 devices do not support this command.

About Serial Port Socket IDs

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.

Required Privileges

Root privileges are required to use this command.

Related Information

None.

Syntax: Configuration

Here is how you use the set socketid command to configure the serial port socketid feature:

```
set socketid range=range [state={on | off}
[string=”character-string”]
```

Syntax: Display

Here is how you use the set socketid command to display serial port socketid configuration settings:

```
set socketid [range=range] [verbose]
```

Fields

range=*range*
: is the port or ports configured with this command

state={on | off}
: turns the feature on or off for the port specified. The default is off.

string=*”character-string”*
: is an identification string 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 in the manner described in the following table:

To embed this character ...	Use this escape sequence ...
Backspace	\b
Form feed	\f
Tab	\t
New line	\n
Return	\r

To embed this character ...	Use this escape sequence ...
Backslash	\\
Hexadecimal byte value *hh*	\xhh

verbose

is used to displays the entire identification string when the string exceeds twenty characters. The verbose option is not necessary for strings under twenty characters.

Example: Displaying the Configuration for All Ports

In this example, the set socketid configuration settings for all ports are displayed:

```
set socketid
```

Example: Displaying the Configuration for a Specific Port

In this example, the set socketid configuration for port 2 is displayed:

```
set socketid range=1
```

Example: Configuring an Identification String

```
set socketid range=1 state=on string=”\fDevice 54”
```

Example: Configuring a Hexadecimal Identification String

```
set socketid range=1 state=on string=”\xae”
```

set tcpip

Use the set tcpip command to set operating characteristics of the device server TCP component. Configurable options include:

- The TCP port used by RealPort
- The interval TCP waits before retransmitting an unacknowledged segment
- How TCP handles idle connections
- Socket service values for reverse Telnet connections

Required Privileges

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

Related Information

None.

Syntax: Configuration

Here is the form of the set tcpip command to change TCP options:

```
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]
```

Syntax: Display

Here is the form of the set tcpip command to display TCP settings:

```
set tcpip
```

Fields

keepalive_active

on enables the keep-alive function, and off disables it. The default is off, but can be turned on by an application regardless of this setting. When you change this setting, you must reboot the device server.

keepalive_byte

on means that the device server sends a “garbage” byte of data to force the device at the other end of the connection to respond to the keep-alive packet. The default is off. When you change this setting, you must reboot the device server.

ip_ttl

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.

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

is 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

is 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

sets 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

is 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

Example: Configuring Keepalive Options

In this example, the device server TCP component is configured to do the following:

- Begin sending keepalive 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
```

Example: Configuring 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

Use the set telnetip command to

- Create configuration profiles for Telnet communication with particular devices. That is, the set telnetip command links an IP address to particular Telnet operating parameters.
- Display Telnet IP address table entries

Required Privileges

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

Related Information

None.

Syntax: Display

Use this form of the set telnetip command to display the current Telnet values for the device server:

```
set telnetip
```

Syntax: Add

Use this form of the set telnetip command to add an entry to the Telnet table, which can hold up to 30 entries:

```
set telnetip ip=ip-addr [mask=mask]
[mode={none|crbin|telprnt|striplf}] range=port
```

Fields

ip

is the IP address to add to the Telnet table

mask

is value of the mask to use for the IP address entered

The default is 255.255.255.255

mode

is the Telnet mode

none
means that no special Telnet mode is set

crbin
sets a Telnet binary connection where carriage returns are added with line feeds

telprnt
is used for a Telnet print connection

The default is none.

range

is the range of index entries to remove

Note: Before removing Telnet table entries it may be helpful to use set telnet without any options to display the existing Telnet table entries and their corresponding index numbers.

Example: Displaying Telnet Table Entries

In this example, the set telnet command displays current Telnet table entries.

```
set telnet
```

Example: Adding a Telnet Table Entry

In this example, the set telnet command adds a Telnet table entry.

```
set telnet ip=199.86.5.56 mask=255.255.255.0 mode=none
```

set terms

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

About the set terms Command

Here is some information on the set terms command:

- The set terms command configures device server to handle terminals that are **not** connected over a network.
- If users are to use the Ctrl key in a key sequence, use a carat character (^) in place of the Ctrl key when you configure the sequence.

Required Privileges

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

Related Information

None

Syntax: Configuration

Here is the form of the set terms command used to configure terminals:

```
set terms [clrseq=escape-seq] [npages=pages]
[swtseq=SessNumSequence] termtype=type
```

Syntax: Display

Here is the form of the set terms command used to display entries in the term table:

```
set terms [range=range]
```

Fields

clrseq

is the escape sequence that clears the terminal’s current screen. This should be the sequence specified by your terminal’s manufacturer.

npages

is the number of sessions available to this terminal type. This should be the same as the number of pages of screen memory available on the terminal.

The range is 1-9.

swtseq=*SessNumSequence*

is a number that identifies the session and the escape sequence used to access that session. This should be the sequence specified by your terminal’s manufacturer.

Note: There are no spaces between the number identifying the session and the key sequence used to access that session.

range

is the range of term table entries to display or remove

termtype

is a name for the terminal type. This name must match the name

- Specified on the termtype field of the set ports command
- 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.

Example: Displaying the Entire Term Table

In this example, the set terms command displays the entire term table.

```
set terms
```

Example: Displaying a Range of Entries in the Term Table

In this example, the set terms command displays a range of entries in the term table.

```
set terms range=4-6
```

Example: Configuring a Terminal Type

In this example, the set terms command configures a terminal type.

```
set terms termtype=Jet npages=4 clrseq=^! swtseq=1^]
swtseq=2^[swtseq=3^} swtseq=4^{
```

set time

Use the set time command to set and display the time and date PortServer TS 8/16 devices keep.

Required Privileges

Root privileges are required to use this command.

Related Information

None

Syntax

Here is how to use the set time command to set or display the time and date.

```
set time [{AM|PM}] [date=mn.day.yr] [dayofweek=day]
[hrmode={12|24}] [time=hr.mn.sec]
```

Fields

{AM|PM}
specifies the period of the day when hrmode=12

date
is the month (expressed numerically), day, and year (use only two digits for the year), separated by periods

dayofweek
is the day of the week (sun, mon, tue, wed, thu, fri, sat)

hrmode
is either 12 or 24

time
is the hour (24-hour clock), minute, and second, separated by periods

Example: Displaying the Time

In this example, the set time command displays the current time and date.

```
set time
```

Example: Setting the Time

In this example, the set time command sets the time and date.

```
set time time=17.05 date=12.25.97
```

set trace

Use the set trace command to do the following:

- Configure device server for tracing
- Display tracing information

Required Privileges

Root privileges are required to use this command.

Related Information

None

Syntax: Configuration

Use this form of the set trace command to configure tracing:

```
set trace [loghost=ip-addr][mask=type:severity]
[mode={historical | concurrent]} [state={on|off|dump}]
[syslog={on|off}]
```

Syntax: Display

Use this form of the set trace command to display the status of tracing information:

```
set trace
```

Fields

loghost
is the IP address of a host to which trace messages should be sent. This host must be running the syslog daemon.

mask=*type:severity*
is the type and nature of event that should be traced

type
is 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)

Type	Trace events associated with ...
ia	IA (industrial automation) 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)
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

is one of the severity levels listed in Table:

Severity	Meaning
+ (plus sign)	This is 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 examples that follow for clarification.
- (minus sign)	This is used to subtract severity levels from the trace. See the examples that follow.
critical (the default)	This means that tracing is done on only the most severe events. This level produces the least amount of trace data. Critical can be abbreviated with a “c”.
warning	This means tracing is done on critical events and on less severe events as well. This level produces more trace data than critical, but less than info. Warning can be abbreviated with a “w”.
info	This means tracing is done on many events. It produces more trace data than previous levels. Info can be abbreviated with an “i”.
debug	This is the level to use for debugging. Do not use this level for anything but debugging. Debug can be abbreviated with a “d”.

mode

historical
means that all trace messages stored in the buffer may be displayed by issuing the following command: `set trace state=dump`

concurrent
means that all trace messages are printed to the administrative terminal when state=on

state

on
means that all messages in the trace buffer are displayed. Once they are displayed, the state remains on.

off
means that tracing is off

dump
means that all messages in the trace buffer are displayed. Once they are displayed, the state returns to off.

The default is off.

syslog

on
means that trace messages are sent to the host identified on the loghost field

off
means that trace messages are not sent to a host

The default is off.

Example: Displaying Trace Settings

In this example, the set trace command displays current trace settings.

```
set trace
```

Example: Dumping a Trace

In this example, the set trace command dumps a previously recorded trace of ARP events.

```
set trace mask=arp:warning mode=historical state=dump
```

Example: Configuring Trace Levels

In this example, the set trace command configures tracing for future critical events.

```
set trace mask=arp:critical mode=concurrent state=on
```

Example: Using the + Sign to Extend the Trace

In this example, the set trace command configures tracing for info, warning, and debug trace levels.

```
set trace mask=arp:i+w+d
```

Example: Using the - Sign to Subtract a Severity Level

In this example, the warning severity level is subtracted from the trace settings specified in the previous example.

```
set trace mask=arp:-w
```

set udpdest

Use this command to configure destinations for serial over UDP communication.

About the UDP Destination Table

The UDP destination table can hold up to 64 entries per port.

Required Privileges

Anyone can display the UDP destination table. Root privileges are required to add entries.

Related Information

See set udpserial on page 132.

Syntax: Configuration

```
set udpdest [description=”string”] [ipaddress=dest-ip]
[ipport=port] port=serial-port range=index
```

Syntax: Remove

```
set udpdest rmudp=on range=index port=serial-port
```

Syntax: Display

```
set udpdest [port=serial-port range=index]
```

Fields

description=*string*
: is 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=*dest-ip*
: is the destination’s IP address

ipport=*port*
: is the UDP port number that will be used for communication with the destination

port=*serial-port*
: is 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

range=*index*
: is 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

Display Entries in the UDP Destination Table

In this example, entries from the UDP destination table are displayed.

```
set udpdest port=1-2 range=1,2-4,6
```

Example: Remove Entries from the UDP Destination Table

In this example, entries from the UDP destination table are displayed.

```
set udpdest rmudp=on port=1-2 range=1,2-4,6
```

Example: 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
```

Example: 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
```

set udpserial

Use this command to configure operating parameters for serial over UDP communication.

Required Privileges

This command requires root privileges.

Related Information

See set udpdest on page 130.

Syntax

```
set udpserial [delimiters=string]
[overflowpolicy={forward | flush}] range=ports [rmax=max]
[rtime=time] [stripdelimiters={on | off}]
```

Fields

delimiters=*string*

is 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.). Here are some rules and tips for specifying this string:

- 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, \x*hh*, 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={forward | flush}

determines how the Digi device responds when the buffer that holds the serial data overflows. Choose one of the following:

- forward, if you want the buffer’s contents sent to the destination
- flush, if you want the buffer’s content discarded

The default is to forward the data.

range=*ports*

is 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

is the maximum number of bytes the buffer can accumulate before the Digi device forwards the contents to the destination. The range is 1 to

65535 bytes, and the default is 1024 bytes.

rtime
: is the period to wait for the buffer to fill before forwarding it to its destination. The range is 1 to 60000 milliseconds, and the default is 100 milliseconds.

stripdelimiter={on | off}
: determines whether the Digi device strips the delimiter string from the message before sending the message to the destination

Example: 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
```

Example: 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
```

set user

Use the set user command to

- Display configuration attributes stored in the user table, such as whether a user must supply a password
- Configure 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: SSH2 is only supported on the server version and not on the client version.

About the User Table

- 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 134.
- 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: Configuration

Here is the form of the set user command used to configure user attributes:

```
set user [accesstime=time][addrcompress={on|off}][asyncmap=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]
```

Syntax: Display

Here is the form of the set user command used to display entries from the user table:

```
{set user {[name=name]|[range=range]} | set user name=name
network}
```

Syntax: Remove Entry

Here is the form of the set user command used to remove an entry from the user table.

```
set user [range=range] [rmuser={on|name}]
```

Fields

accesstime (PortServer TS 8/16 devices only)

is the period in which the user can access device server. Use the accesstime field to restrict the user's access to the time specified.

Use the keywords listed in the following table to specify day (or days) and hours:

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. Here are some examples:

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

on
means device server attempts to negotiate address compression on PPP connections

off
means device server will **not** attempt to negotiate address compression

The default is on.

asyncmap

is 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 most likely masks that you will want to use:

- FFFFFFFF, which means transpose all control characters
- 00000000, which means transpose none
- 000A0000, which means transpose Ctrl-Q and Ctrl-S

autoconnect

on
means that 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 yes, specify the autohost and autoport or autoservice fields.

off
means the user will **not** be automatically connected to another system

The default is off.

autohost
is 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=yes.

autoport
is the TCP port to use for the automatic connection. Use this field only if you specify autoconnect=yes.

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
is an alternate way to specify a TCP port for an autoconnect user (see the autoport field). Use this field only if you specify autoconnect=yes. Specify one of the following services:

- telnet
- rlogin
- raw (which means that data will be passed between the serial port and the TCP stream without modification)
- default, which normally means the Digi device will use 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
is the name of a filter (defined on the set filter command) that 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
is 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
is 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

on
means that a Telnet, Rlogin, PPP user can access the device server command line to issue commands

off
means that the user can **not** access the command line and can **not** issue commands

The default is on.

compression

vj
means that Van Jacobsen Header compression is used on PPP connections

none
means that header compression is not used on PPP connections

The default is vj, that is, Van Jacobsen Header compression is on.

connectesc
is 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

commandline
means that the device server command line is displayed to the user

menu
means that a menu is displayed to the user. If you specify this option, you must also specify a menu number on the menu field

autoconnect
means that device server automatically connects the user to the destination specified on the autohost field

netservice
starts PPP services. For inbound PPP users, defaultaccess=netservice is required. Do <u>not</u> use netservice for outbound PPP users.

outgoing
means that this user is limited to outgoing connections.

The default is commandline.

device

is the name of a device or a device pool (defined with the set device command) used for outbound PPP connections

dialout

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.

downdly

is the number of seconds the dialer script should delay before attempting to establish a PPP connection with a previously inaccessible host

The default is 0, which means do not delay in making the attempt to reconnect. The range is unlimited.

flushstchar={on | off | default}

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

is 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

is 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, which means that 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

is 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={on | off}

determines whether the keepalive function is implemented with autoconnections. The default is off.

keepup

is 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.

killescchar

is the kill character, which is used to close sessions. The default is ^u.

loadkey=*host:key*

applies to the devices listed in the following table:

Device	Required Hardware	Required Firmware
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	

- *host* is 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* is 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

is 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

is 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 can not be the IP address of the Ethernet interface.

loginscript
is 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
is 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
is the maximum number of ports that a Telnet or Rlogin user can be logged into at the same time

0 means that the user can be simultaneously logged into all ports specified on the ports field

menu

index-num
is the menu, identified by an index number in the menu table, that will be presented to this user

`off` and `0` (zero)
means that no menu is presented to the user

The default is off.

mtu
is the maximum transmission unit (frame size in bytes) to use for this PPPconnection. 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*...*
are 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
is the name that identifies this user

netrouting
specifies how RIP routing updates are handled on connections to this PPP user. Use this field only if the user is an IP router.

off
means that this user is not included in RIP updates

send
means propagate RIP updates to this user, but do not accept RIP updates from this user

receive
means accept RIP updates from this user, but do not send RIP updates to this user

both
means RIP updates will be sent to and received from this user

The default is off.

netservice

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
is a new name for a previously defined user

outgoing

on
means that the user can initiate outgoing serial connections. For outbound users, outgoing=on is required.

off
means that the user can **not** initiate outgoing connections

p1, p2 ...
are 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

is 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

is 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

on

means that device server waits for the remote system to begin PPP negotiations

off

means that device server may initiate PPP negotiations

The default is off.

Note: Do not set both sides of a PPP connection to passive=on.

passpacket

is the name of a filter designed to allow packets meeting filter criteria to pass through device server serial ports on PPP connections

password

on

means a device server password is required of this user

off

means a password is not required of this user

The default is on.

ports

is 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

means the remote user does not require PPP authentication

chap

means CHAP authentication is required

pap

means PAP authentication is required

both

means both CHAP and PAP authentication is required

The default is none.

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

protocompress

on
means device server attempts to negotiate protocol compression on PPP connections

off
means 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
is a different escape character than the ~ (tilde) character. This character is used for disconnecting from the remote host.

rmkey={on | off}
on enables the SSH2 public key defined on the loadkey field, and off disables this feature. The default is on.

rmtbusydly
is 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
is 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
is the Telnet escape character for this user. The default is ^] (Ctrl and right bracket)

vjslots
is the number of slots used for Van Jacobson 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.

Example: Displaying the Entire User Table

In this example, the set user command displays a list of users.

```
set user
```

Example: Displaying a Range of Entries in the User Table

In this example, the set user command displays a range of entries in the user table.

```
set user range=2-7
```

Example: Displaying a Single User

In this example, the set user command displays information on a single entry in the user table.

```
set user ra=1
```

Example: Configuring an Autoconnect User

In this example, the set user command configures an autoconnect user.

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

Example: Configuring an Inbound PPP User

In this example an inbound PPP user is configured.

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

```
set user name=pppin ippaddr=ip-pool localipaddr=143.191.3.4
```

Example: Configuring an Outbound PPP User

In this example, an outbound PPP user is configured.

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

```
set user name=pppout device=genmdm localipaddr=0.0.0.0 outgoing=on
n1=4452624
```

set wlan

This command is only available for the Digi One TS Wireless, PortServer TS 2 MEI Wireless, and PortServer TS 4 MEI Wireless. Use the set wlan command to configure or display entries in the wireless LAN configuration table.

Required Privileges

Root privileges are required to use this command.

Related Information

None

Syntax: Configuration

```
set wlan
[diversity={primary|secondary|tx_pri_rx_div}][rts_threshold=thresh
old][fragmentation_threshold=threshold]
[country_code={United_States|other_country_code_string}][authentic
ation={open_system|shared_key}]
[density={low|medium|high}][auto_ssid={on|off}][ssid=id-string]
[encryption_mode={none|64_bit|128_bit}][encryption_key=key]
```

Syntax: Display

```
show wlan
```

Fields (show and set)

authentication

open_system
means that the wlan device will use open system authentication

shared_key
means that the wlan device will use 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

on
means the wlan device automatically detects available SSIDs in its neighborhood and arbitrarily selects an SSID. If the arbitrarily chosen SSID is using encryption that doesn’t match our current encryption mode and key, the device will be unable to associate with an access point.

off
means the wlan device will use the configured SSID. The user will not be allowed to set auto_ssid to off if SSID is not set to some value other than “”.

Default is on

country_code
specifies the country code for the radio. 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

low
means that 1 wireless access point is in the vicinity

medium
means that 2 wireless access points are in the vicinity

high
means that 3 wireless access points are in the vicinity

The default is low.

diversity
specifies the antenna choice for transmit and receive

primary
means use the primary antenna for transmit and receive

secondary
means use the secondary antenna for transmit and receive

tx_pri_rx_div
means use the primary antenna for transmit and both antennae for receive

The default is tx_pri_rx_div.

encryption_key
specifies a zero, ten, or 26 digit (depending on encryption mode) hexadecimal encryption key. Ignored if encryption_mode=none.

The user must enter either zero digits (““), 10 digits, or 26 digits. No other lengths will accepted.

If the key does not have the right number of digits for the current encryption mode, the user will be warned.

If encryption key length is changed to zero and authentication is shared_key, the user is warned.

Note: Authentication is not affected by the setting for encryption_mode. Encryption key is a read-only field, it cannot be displayed.

encryption_mode

none
the device will not encrypt data packets

64_bit
the device will use WEP 64 encryption. This option requires a 5 byte (10 digit) encryption key

128_bit
the device will use 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 will be warned.

fragmentation_threshold

specifies the number of bytes used for the fragmentation boundary for directed messages. Ranges from 256 to 2346 (even numbers only), default of 2346.

rts_threshold

specifies the number of bytes used for the RTS/CTS handshake boundary. Ranges from 0 to 3000, default is 1600.

show wlan

In addition to displaying the current settings for all of the configuration fields except encryption_key (which cannot be read), the show command will also display current_link_status, current_channel, current_ssid, radio firmware version and hardware ID, receive signal strength, current transmit power, current transmit speed, and 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 on the left of the information

ssid

specifies the desired Set Service Identifier (SSID) for the wlan device. It 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.

Default is “digi”.

Fields (show only)

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 wlan 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 wlan device. This may be different than the SSID requested in the set ssid command

current_transmit_speed

indicates the current transmit speed for the radio. Can be 1, 2, 5.5 or 11 MB

radio_firmware_version

indicates 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
indicates the hardware revision of the radio. It is displayed in the form n, where n is a digit indicating the revision

receive_signal_strength
indicates the current receive signal strength as reported by the radio. Ranges are from 0 – 100.

Very Low - 0-25

Low - 26-49

Strong - 50-74

Excellent - 75-100

Example

```
set wlan ssid=”homeBase” encryption_mode=128
encryption_key=ab1F793f01578ebf567afeb567
```

```
set wlan ssid=”homeBase” em=128 ek=ab1F793f01578ebf567afeb567
```

show

Use the show command to display the following information on Digi One and PortServer TS 2/4 devices:

- Configuration settings
- Current versions of the Boot, POST, and OS components

Required Privileges

Anyone can use this command.

Related Information

None

General Syntax

```
show option [range=range]
```

Fields

option
is 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

Option	Displays events associated with ...	Works with Range Field
ippool	set ippool settings	no
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 not 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

range
is a configuration table entry or range of entries

Example: Displaying Current Versions of POST, Boot and EOS

In this example, the current versions of the POST, Boot and EOS are displayed.

```
show version
```

Example: Displaying User Setting

In this example, the settings for a user, identified by an index number in the user table, are displayed.

```
show user range=3
```

status

Use the status command to display information about your current Telnet or connect session.

Required Privileges

Anyone can use this command.

Related Information

See close on page 10. Typically you use the status command to determine which Telnet sessions to close.

Syntax

Here is how you issue the status command.

```
status
```

Example

In this example, the status command provides information on the user's current Telnet session.

```
status
```

telnet

Use the telnet command to establish a Telnet session with a remote system.

Required Privileges

Anyone can use this command.

Related Information

None

Syntax

Here is how you issue the telnet command.

```
telnet {hostname | host-ip-addr} [tcp-port]
```

Field Descriptions

hostname
is 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-add*r
is the IP address of the host to which you want a Telnet session

tcp-port
is the TCP port assigned the Telnet application on the remote system. The default is 23, the port typically used for Telnet.

Example: Telnetting 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
```

Example: Telnetting 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
```

Example: Telnetting 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

Use the traceroute command to display a list of routers through which an IP packet passes on its way to a particular destination.

Required Privileges

Anyone can use this command.

Related Information

None

Syntax

Here is the syntax for issuing the traceroute command.

```
traceroute ip-addr|name
```

Field

ip-addr **|** *name*
is either the IP address or the DNS name of the host to which you want a route traced

Example: Tracing a Route Using an IP Address

In this example, the traceroute command traces a route to a host using the specified IP address.

```
traceroute 199.150.150.74
```

Example: Tracing a Route Using a Name

In this example, the traceroute command traces a route to a host using a host name.

```
traceroute poe
```

uptime

Use the uptime command to display the amount of elapsed time since the last reboot.

Required Privileges

Anyone can use this command.

Syntax

Here is how to issue the uptime command:

```
uptime
```

Example

```
uptime
```

wan

Use the wan command to

- Initiate and control PPP connections
- Display the status of current connections

Required Privileges

Anybody can display the status of WAN connections. Root privileges are required to initiate or control WAN connections.

Related Information

See the following commands:

- set modem on page 86
- set filter on page 53

Syntax: Initiate and Control

Use this form of the wan command to initiate and control WAN connections:

```
wan [close=user-name] [initmodem=range] [start=user-name]
[testmodem=range] [verify={all|user-name}]
```

Syntax: Display

Use this form of the wan command to display the status of current 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

range
is 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 86 for information on test scripts.

verify

all
verifies that all connections are associated with real users, that is, users that are defined in the configuration

wanname

verifies that the user has been defined in the configuration

Note: Only incorrectly configured WAN interfaces produce a message in response to this command. If WAN interfaces are configured correctly, no message is returned.

Example: Closing a WAN Interface

In this example, a WAN connection is closed.

```
wan close=user-ppp01
```

Example: Starting a WAN Interface

In this example, the wan command initiates a WAN connection.

```
wan start=user-ppp01
```

Example: Displaying WAN Status Information

In this example, the wan command displays the status of the connection on port 2.

```
wan range=2
```

who

Use the who command to display a list of current device server users.

Required Privileges

Anyone can use this command.

Related Information

None

Syntax

Here is how you issue the who command.

```
who [range=tty-tty]
```

Field

range
  is either a tty connection or a range of connections identified by tty connection number

Example: Display List of all Users

In this example, a list of all current users is displayed.

```
who
```

Example: Display a Range of Users

In this example, a range of user connections is displayed.

```
who range=5-10
```

Index