Digi TransPort® Routers

for model LR54

User Guide

Revision history—90001461

Revision	Date	Description
A	August 2016	Initial release.
B	October 2016	Added features for TransPort firmware 1.2.0.
C	January 2017	Added support and usability features: traceroute, show dhcp, show tech-support, and traffic and data packet capture/traffic analyzer features.
D	April 2017	Added port forwarding and updated firewall topics. Added support for SIM PIN and unlocking a SIM card using a SIM PUK code. Updated Firewall section to include information on system firewall rules and to show enabling SSH and HTTPS access via the **wan** command. Added information on performing file management and viewing the event log from the web interface. Updated Configure a user and user command to include restrictions on characters in usernames.
E	June 2017	Added IP filtering; updated firewall topics; removed on-demand parameter value from interface state options; updated regulatory information for compliance with European Union (EU) Radio Equipment Directive (RE-D); miscellaneous editorial corrections and enhancements.
F	August 2017	Added documentation for TransPort firmware 3.0 features and enhancements: ▪ Certificate management for OpenVPN ▪ Dynamic Mobile Network Routing (DMNR) ▪ IPv6 addressing ▪ OpenVPN New commands: dmnr/show dmnr firewall6/show firewall6 openvpn-client/show openvpn-client openvpn-route openvpn-server/show openvpn-server openvpn-user pki Modified commands: ip-filter/show ip-filter lan/show lan ping wan/show wan

Revision	Date	Description
G	October 2017	Added documentation for TransPort version 3.1 features and enhancements: ■ Generic Routing Encapsulation (GRE) ■ About Python support ■ Quality of Service (QoS) ■ Remote Authentication Dial-In User Service (RADIUS) ■ Virtual Router Redundancy Protocol (VRRP) New commands: gre/show gre python/python-autostart/show python qos-filter/qos-queue radius vrrp/show vrrp
H	December 2017	Added documentation for TransPort version 3.2 features and enhancements: ■ Added support for dynamic DNS and web filtering. See Dynamic DNS and Web filtering (OpenDNS). ■ Added support for Digi Remote Manager device health reporting. See Enable health reporting. ■ Added Python autostart page to the webui. See Python autostart page. Added Device preference page to the webui. See Device preferences page. ■ Miscellaneous editorial enhancements and corrections to the user interface and the help system.

Trademarks and copyright

Disclaimers

Warranty

To view product warranty information, go to the following website:

www.digi.com/howtobuy/terms

Send comments

Documentation feedback: To provide feedback on this document, send your comments to techcomm@digi.com.

Customer support

Digi Technical Support: Digi offers multiple technical support plans and service packages to help our customers get the most out of their Digi product. For information on Technical Support plans and pricing, contact us at +1 952.912.3444 or visit us at www.digi.com/support.

Contents

Configuration and management

File system

Diagnostics and troubleshooting

Web reference

Command reference

Advanced topics

Configuration and management

Using the web interface

The first time you power on a TransPort device, the **Getting Started Wizard** steps you through the process of initial configuration. After the wizard completes, the next time you access the device, a login prompt appears. See Log in to the web interface for login instructions.

After you log in, the TransPort **Dashboard** appears. The **Dashboard** provides a snapshot of current activity for the device. See The dashboard for details.

In this help system, task topics show how to perform tasks:

Web

Shows how to perform a task using the web interface.

Command line

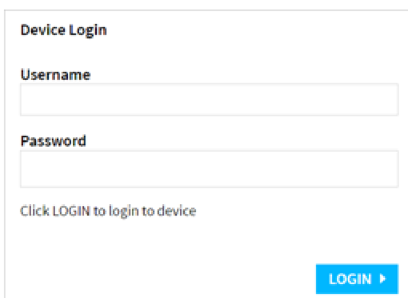
Shows how to perform a task using the command line interface.

Log in to the web interface

The first time you access a TransPort device, the **Getting Started Wizard** runs. This wizard steps you through the process getting your device initially configured and connected. After you run the Getting Started Wizard, the next time you access the device, a login prompt for the web interface appears.

Web

1. On the local network for your device, the default address is **http://192.168.1.1.** Enter this address in a web browser. The Device Login prompt displays:

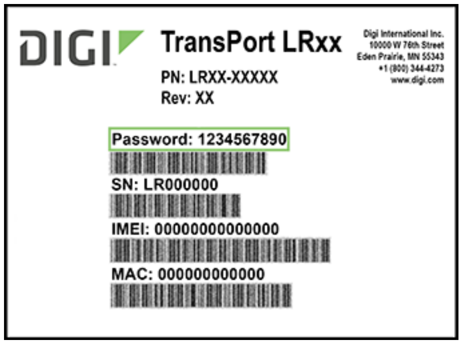


2. Enter your username and password to log into the device. Click **Login**.

   Use the unique password printed on the label on the bottom of the device if the password was not changed during initial setup.

   Username: **admin**

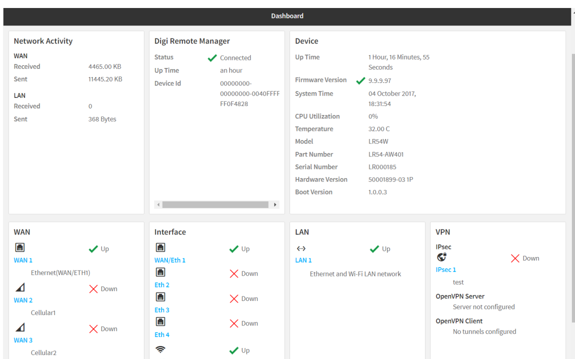
Password: See the label on bottom of device.



If the login is successful, the Dashboard for your TransPort device appears. See The dashboard for more information about this view.

The dashboard

The dashboard shows the current state of the device.



Dashboard display areas

Dashboard area	Description
Network activity	Summarizes network statistics: the total number of bytes sent and received over all Wide Area Networks (WANs) and Local Area Networks (LANs), including all WANs/LANs configured and active, disabled, and/or disabled.
Digi Remote Manager	Displays the device connection status for Digi Remote Manager, the amount of time the connection has been up, and the Digi Remote Manager device ID. See Remote Manager.
Device	Displays device status, statistics, and identifying information. See the show system command for details. For **Firmware Version**, a green checkmark ✔ indicates the firmware is up to date and a red X indicates a firmware update is available. See Update system firmware for instructions.

Dashboard area	Description
WAN	Displays all configured Wide Area Networks (WANs), the physical interface assigned to the WAN, and the current state of the WAN. Click a WAN to display detailed configuration and status information. See Wide Area Networks (WANs) for details.
Interface	Displays all configured and available physical interfaces for the device and their current states. See Interfaces for details.
LAN	Displays all configured Local Area Networks (LANs), the physical interface(s) assigned to the LAN, and the current state of the LAN. Click a LAN to display detailed configuration and status information. See Local Area Networks (LANs) for details.
VPN	Displays all configured Virtual Private Network (VPN) tunnels. See Virtual Private Networks (VPN) for details.

Log out of the web interface

Web

- Click the **Logout** button in the upper right corner of the web interface.

Using the command line

TransPort provides a command-line interface you can use to configure the device, display status and statistics, as well as update firmware and manage device files. See Command reference for details on all available commands.

In this help system, task topics show how to perform tasks:

From the web

Shows how to perform a task using the web interface.

From the command line

Shows how to perform a task using the command line interface.

Interfaces

TransPort devices have several physical communications interfaces. The available interfaces vary by device model. These interfaces can be bridged in a Local Area Network (LAN) or assigned to a Wide Area Network (WAN). This section covers configuring and managing these physical communication interfaces.

Ethernet interfaces

Ethernet interfaces can be used in LAN or WAN. There is no IP configuration set on the individual Ethernet interfaces. Instead, the IP configuration is set as part of configuring the LAN or WAN.

For more information on WANs, see Wide Area Networks (WANs).

For more information on LANs and their configuration, see Local Area Networks (LANs).

Configure Ethernet interfaces

To configure an Ethernet interface, you must configure the following items:

Required configuration settings

- Enable the Ethernet interface. The Ethernet interfaces are all enabled by default. You can set the Ethernet interface to **enabled or disabled**.
- Once configured, the Ethernet interface must be assigned to a LAN or a WAN. For more information, see Local Area Networks (LANs) and Configure a LAN or Wide Area Networks (WANs) and Configure a Wide Area Network (WAN).

Additional configuration settings

The following additional configuration settings are not typically configured to get an Ethernet interface working, but can be configured as needed:

- A description of the Ethernet interface.
- The duplex mode of the Ethernet interface. This defines how the Ethernet interface communicates with the device to which it is connected. The duplex mode defaults to **auto**, which means the TransPort device negotiates with the connected device on how to communicate.
- The speed of the Ethernet interface. This defines the speed at which the Ethernet interface communicates with the device to which it is connected. The Ethernet speed defaults to **auto**, which means it negotiates with the connected device as to what speed should be used.

Web

1. On the menu, click **Network > Interfaces > Ethernet**.
2. Select the Ethernet interface to configure.

3. In the **Edit Selected** box, enter the configuration settings:
   - **State**: Enable or disable the Ethernet interface. By default, all of the Ethernet interfaces are enabled.
   - **Description**: Optional: Enter a description for the Ethernet interface.
   - **Speed**: Optional: Select the speed for the Ethernet interface.
   - **Duplex**: Optional: Select the duplex mode for the Ethernet interface.
4. Click **Apply**.

Command line

1. Enable the Ethernet interface. By default, all of the Ethernet interfaces are enabled.

```
digi.router> eth 1 state on
```

2. Optional: Set the description for the Ethernet interface. For example:

```
digi.router> eth 1 description “Connected to Ethernet WAN router”
```

3. Optional: Set the duplex mode.

```
digi.router> eth 1 duplex {auto | full | half}
```

4. Optional: Set the speed.

```
digi.router> eth 1 speed {auto | 1000 | 100 | 10}
```

5. Save the configuration.

```
digi.router> save config
```

Show Ethernet status and statistics

From the web interface

A limited set of Ethernet status and statistics are available for the WAN to which the Ethernet interface belongs. For more complete Ethernet interface status and statistics, use the show eth command, described below.

You can view Ethernet status from the **Dashboard**.

Web

- On the menu, click **Dashboard**. The Interface section of the dashboard shows the status of all interfaces.

Command line

To show the status and statistics for the Ethernet interface, use the show eth command. For example:

```
digi.router> show eth


Eth Status and Statistics Port 1
```

```
-------------------------------------
 Description     : Factory default configuration for Ethernet 1
 Admin Status    : Up
 Oper Status     : Up
 Up Time         : 1 Day, 13 Hours, 30 Minutes, 23 Seconds

 MAC Address     : 00:50:18:21:E2:82
 DHCP            : off
 IP Address      : 10.52.19.242
 Netmask         : 255.255.255.0
 DNS Server(s)   :
 Link            : 1000Base-T Full-Duplex

 Received                             Sent
 --------                             ----
 Rx Unicast Packet    : 6198          Tx Unicast Packet    : 651
 Rx Broadcast Packet  : 316403        Tx Broadcast Packet  : 2
 Rx Multicast Packet  : 442690        Tx Multicast Packet  : 6
 Rx CRC Error         : 0             Tx CRC Error         : 0
 Rx Drop Packet       : 0             Tx Drop Packet       : 0
 Rx Pause Packet      : 0             Tx Pause Packet      : 0
 Rx Filtering Packet  : 1             Tx Collision Event   : 0
 Rx Alignment Error   : 0
 Rx Undersize Error   : 0
 Rx Fragment Error    : 0
 Rx Oversize Error    : 0
 Rx Jabber Error      : 0

Eth Status and Statistics Port 2
-------------------------------------
 Description     :
 Admin Status    : Up
 Oper Status     : Up
 Up Time         : 1 Day, 13 Hours, 30 Minutes, 23 Seconds

 MAC Address     : 00:50:18:21:E2:83
 DHCP            : off
 IP Address      : 10.2.4.20
 Netmask         : 255.255.255.0
 DNS Server(s)   :
 Link            : 100Base-T Full-Duplex

 Received                                Sent
 --------                                ----
 Rx Unicast Packet    : 5531          Tx Unicast Packet    : 2
 Rx Broadcast Packet  : 316403        Tx Broadcast Packet  : 2
 Rx Multicast Packet  : 442694        Tx Multicast Packet  : 2
 Rx CRC Error         : 0             Tx CRC Error         : 0
 Rx Drop Packet       : 0             Tx Drop Packet       : 0
 Rx Pause Packet      : 0             Tx Pause Packet      : 0
 Rx Filtering Packet  : 0             Tx Collision Event   : 0
 Rx Alignment Error   : 0
 Rx Undersize Error   : 0
 Rx Fragment Error    : 0
 Rx Oversize Error    : 0
 Rx Jabber Error      : 0

Eth Status and Statistics Port 3
-------------------------------------
```

```
 Description     :
 Admin Status    : Up
 Oper Status     : Up
 Up Time         : 1 Day, 13 Hours, 30 Minutes, 23 Seconds

 MAC Address     : 00:50:18:21:E2:84
 DHCP            : on
 IP Address      : 82.68.87.20
 Netmask         : 255.255.255.0
 DNS Server(s)   :
 Link            : 100Base-T Full-Duplex

 Received                                 Sent
 --------                                 ----
 Rx Unicast Packet    : 5530          Tx Unicast Packet    : 2
 Rx Broadcast Packet  : 316405        Tx Broadcast Packet  : 2
 Rx Multicast Packet  : 442699        Tx Multicast Packet  : 4
 Rx CRC Error         : 0             Tx CRC Error         : 0
 Rx Drop Packet       : 0             Tx Drop Packet       : 0
 Rx Pause Packet      : 0             Tx Pause Packet      : 0
 Rx Filtering Packet  : 0             Tx Collision Event   : 0
 Rx Alignment Error   : 0
 Rx Undersize Error   : 0
 Rx Fragment Error    : 0
 Rx Oversize Error    : 0
 Rx Jabber Error      : 0

Eth Status and Statistics Port 4
-------------------------------------
 Description     :
 Admin Status    : Up
 Oper Status     : Down
 Up Time         : 0 Seconds

 MAC Address     : 00:50:18:21:E2:85
 DHCP            : on
 IP Address      : Not Assigned
 Netmask         : Not Assigned
 DNS Server(s)   :
 Link            : No connection


 Received                                 Sent
 --------                                 ----
 Rx Unicast Packet    : 0             Tx Unicast Packet    : 0
 Rx Broadcast Packet  : 0             Tx Broadcast Packet  : 0
 Rx Multicast Packet  : 0             Tx Multicast Packet  : 0
 Rx CRC Error         : 0             Tx CRC Error         : 0
 Rx Drop Packet       : 0             Tx Drop Packet       : 0
 Rx Pause Packet      : 0             Tx Pause Packet      : 0
 Rx Filtering Packet  : 0             Tx Collision Event   : 0
 Rx Alignment Error   : 0
 Rx Undersize Error   : 0
 Rx Fragment Error    : 0
 Rx Oversize Error    : 0
 Rx Jabber Error      : 0

digi.router>
```

Cellular interfaces

The TransPort device has two cellular interfaces, named **cellular1** and **cellular2**. These cellular interfaces correspond to the physical SIM card slots **SIM1** and **SIM2**.

Only one cellular interface can be up at the same time. If both cellular interfaces are enabled to **on**, then the **cellular1** interface takes precedence.

A typical use case would be to have **cellular1** (**SIM1**) configured as the primary cellular interface and **cellular2** (**SIM2**) as a backup cellular interface. If the TransPort device cannot connect to the cellular network using **SIM1**, it will automatically failover to try to connect using **SIM2**.

To configure a default route for the cellular interface when it is up and to include the cellular interface in TransPort failover, the cellular interface must be assigned to a WAN.

For more information on WANs and their configuration, see Wide Area Networks (WANs).

Configure cellular interfaces

To configure a cellular interface, you need to configure the following:

Required configuration items

- Enable the cellular interface. The cellular interfaces are disabled by default. You can set the cellular interface to **enabled** or **disabled**.
- The Access Point Name (APN). The APN is specific to your cellular service.
- Depending on your cellular service, you may need to configure an APN username and password. This information is provided by your cellular provider.
- Once configured, if the interface is not already assigned to a WAN interface, assign it to a WAN interface. For more information, see Wide Area Networks (WANs) and Configure a Wide Area Network (WAN).

Additional configuration options

Additional configuration settings are not typically configured, but you can set them as needed:

- Preferred mode. The preferred mode locks the cellular interface to use a particular technology, for example, 4G or 3G. Depending on your cellular service and location, the cellular interface can automatically switch between the different technologies. You may want to lock the cellular interface to a particular technology to minimize disruptions.
- A description of the cellular interface.
- Connection attempts. This is the number of attempts the cellular module will attempt to connect to the cellular network before indicating a failure. It defaults to **20**, but you may want to configure this so that the WAN failover can switch to another interface more quickly.
- Some mobile accounts require a particular PIN code to access a particular SIM card. When the correct PIN code is supplied, the SIM card is accessible. If the PIN code is incorrect, no access is allowed to the SIM card. If several incorrect PIN codes are entered too often, then the SIM will be locked and a PIN Unlock Key (PUK) will be required. See Unlock a SIM card.

Web

1. Click **Network > Interfaces > Cellular**. The **Cellular** page appears.
2. Select an interface.

3. In the **Edit Selected** box, enter the settings:
   - **Description**: Optional: Provide a description of the cellular interface.
   - **Enabled:** Enable or disable the interface.
   - **APN**: Enter a descriptive name for the access point.
   - **APN Username**: Enter the user name for logging on to the access point.
   - **APN Password**: Enter the password for logging on to the access point.
   - **SIM PIN**: For SIMs that require a PIN, enter the PIN to activate the SIM.
   - **Preferred Mode**: Optional: Select the cellular technology on which the interface operates. You can select a particular technology or select **Auto** to have the device automatically select the technology.
   - **Connection Attempts:** Optional: Select the number of attempts to establish a cellular connection, after which the cellular module is power-cycled and another attempt to establish a cellular connection is made.
4. Click **Apply**.

Command line

1. Enable the cellular interface.

```
digi.router> cellular 1 state on
```

2. Configure an APN.

```
digi.router> cellular 1 apn your-apn
```

3. Optional: Set a preferred mode.

```
digi.router> cellular 1 preferred-mode 3g
```

4. Optional: Set a description for the cellular interface.

```
digi.router> cellular 1 description "AT&T Connection"
```

5. Optional: Configure the number of connection attempts. For example, to set the number of attempts to **10**, enter:

```
digi.router> cellular 1 connection-attempts 10
```

6. If necessary, enter the PIN for the SIM.

```
digi.router> cellular 1 pin your-sim-pin
```

7. If necessary, configure the APN username and password.

```
digi.router> cellular 1 apn-username your-apn-username
digi.router> cellular 1 apn-password your-apn-password
```

8. Save the configuration.

```
digi.router> save config
```

Show cellular status and statistics

Web

- On the menu, click **Dashboard**. The Interface section of the dashboard shows the status of all interfaces.

Command line

To show the status and statistics for a cellular interface, use the show cellular command. For a description of the output fields, see the show cellular command.

```
digi.router> show cellular

 Cellular Status and Statistics
 ------------------------------
 Admin status          : Up
 Oper status           : Up
 Module                : Sierra Wireless, Incorporated MC7455
 Firmware version      : SWI9X30C_02.08.02.00
 Hardware version      : 1.0
 IMEI                  : 359072060053523
 Temperature           : 35C

 SIM1 PIN              : PIN is OK
 SIM2 PIN              : PIN is invalid, 2 retries left
 SIM status            : Using SIM1 (SIM is ready)
 ICCID                 : 89014103278253188695

 Signal strength       : Excellent (69dBm)
 Signal quality        : Excellent (10dB)


 Registration status   : Registered
 Attachment status     : Attached

 Network provider      : AT&T, USA
 Connection type       : 3G
 Radio Band            : WCDMA 850
 Channel               : 4382

 APN in use            : Context 1: 12655.mcs


 IP address            : 172.20.1.7
 Mask                  : 255.255.255.240
 Gateway               : 255.255.255.0
 DNS servers           : 10.10.8.62, 10.10.8.64
```

```
                Received    Sent
                 --------   ----
Packets               26      25
Bytes               3379    3193
```

Switch the cellular carrier

Command line

You can switch the cellular carrier from the command line only.

1. To display a list of available carriers for your device, enter the **update carrier** command without parameters. For example:

```
digi.router> update carrier

Carrier Name        Firmware Version    Unique ID
-----------------------------------------------
ATT                 02.08.02.00         002.009_000
GENERIC             02.08.02.00         002.007_000
VERIZON             02.05.07.00         002.008_002

The current firmware image is ATT.
```

2. To switch from one carrier to another, enter the **update carrier** command, specifying the carrier name. For example, to switch the carrier from **AT&T** to **Verizon**, enter:

```
digi.router> update carrier verizon
Switching carrier to verizon.
Module is rebooting.  This can take up to 3 minutes ...
digi.router>
```

3. Save the configuration.

```
digi.router> save config
```

Note If your desired carrier is not displayed in the **update carrier** output as shown in step 1, you must first update the cellular module firmware using the update command, specifying the **update module** command variant. For more information, see Update cellular module firmware.

Unlock a SIM card

A SIM card can be locked if a user tries to set an invalid PIN for the SIM card too many times. In addition, some cellular carriers require a SIM PIN to be added before the SIM card can be used. If the SIM card is locked, the TransPort device cannot make a cellular connection.

To unlock a SIM card:

1. Use the show cellular command to see the status of a SIM card. In the show cellular output, look for the fields **SIM1 PIN status**, **SIM2 PIN status**, and **SIM status**. For example:

```
digi.router> show cellular

 Cellular Status and Statistics
 ------------------------------

 Admin status              : Up
 Oper status               : Down
 Module                    : Sierra Wireless, Incorporated MC7455
 Firmware version          : SWI9X30C_02.08.02.00
 Hardware version          : 1.0
 IMEI                      : 359072060053937
 Temperature               : 33C

 SIM1 PIN status           : New PIN is untested
 SIM2 PIN status           : Never connected
 SIM status                : Using SIM1 (SIM is locked)
 ICCID                     :
 ⋮
```

2. Use the unlock command to set a new PIN for the SIM card using the following syntax:

```
unlock <sim1 | sim2> <puk code> <new sim pin>
```

   For example, to unlock a SIM card in SIM slot SIM **1** with PUK code **12345678**, and set the new SIM PIN to **1234**:

```
digi.router> unlock sim1 12345678 1234
```

3. Save the configuration.

```
digi.router> save config
```

Note If the SIM remains in a locked state after using the unlock command, contact your cellular carrier.

Signal strength for 3G and 2G cellular connections

For 3G and 2G cellular connections, the current **RSSI** value determines signal strength. To view this value, enter the show cellular command.

- **Excellent**: > **-70 dBm**
- **Good**: **-70 dBm** to **-85 dBm**
- **Fair**: **-86 dBm** to **-100 dBm**

- **Poor**: **< -100 dBm** to **-109 dBm**
- **No service**: **-110 dBm**

Signal strength for 4G cellular connections

For 4G connections, the **RSRP** value determines signal strength. To view this value, enter the show cellular command.

- **Excellent**: > **-90 dBm**
- **Good**: **-90 dBm** to **-105 dBm**
- **Fair**: **-106 dBm** to **-115 dBm**
- **Poor**: **-116 dBm** to **-120 dBm**:
- **No service**: **< -120 dBm**

Tips for improving cellular signal strength

If the signal strength LEDs or the signal quality for your device indicate **Poor** or **No service**, try the following things to improve signal strength:

- Move the TransPort device to another location.
- Try connecting a different set of antennas, if available.
- Purchase a Digi Antenna Extender Kit:
  - Antenna Extender Kit, 1m
  - Antenna Extender Kit, 3m

Wi-Fi interfaces

Wi-Fi-enabled TransPort devices support up to **4** Wi-Fi interfaces on each of the 2.4 GHz and 5 GHz frequency bands. You can configure each Wi-Fi interface as an independent Wi-Fi access point with its own security settings. You can either leave it up to the access point to select the channel or select a specific channel to use for Wi-Fi interfaces.

Configure a channel for Wi-Fi 2.4 GHz interfaces

The default behavior for Wi-Fi communications is to leave it up to the TransPort device to select the channel, known as **auto** channel selection. However, you can select a specific channel to use for 2.4 GHz Wi-Fi interfaces. This setting is one of the global Wi-Fi configuration settings.

For Wi-Fi 2.4 GHz, channels **1** to **11** only are allowed, and not **12**, **13**, or **14**.

Web

1. On the menu, click **Network > Interfaces > Wi-Fi**.
2. Select a Wi-Fi interface to configure.
3. Edit the configuration settings as needed.
4. Click **Apply**.

Command line

To select a channel for Wi-Fi 2.4 GHz communications, the command is wifi-global and the parameter is **wifi-channel**. For example, to set the channel for **Wi-Fi 2.4 GHz** interfaces to channel **1**, enter:

```
digi.router> wifi-global wifi-channel 1
digi.router> save config
```

Configure a channel for Wi-Fi 5 GHz interfaces

The default channel for Wi-Fi 5 GHz interfaces is **36**.

The default behavior for Wi-Fi communications is to leave it up to the TransPort device to select the channel, known as **auto** channel selection. However, you can select a specific channel to use for 5 GHz Wi-Fi interfaces. This setting is one of the global Wi-Fi configuration settings.

For Wi-Fi 5 GHz, the following channels are allowed: **36**, **40**, **44**, **48**, **52**, **56**, **60**, **64**, **100**, **104**, **108**, **112**, **116**, **132**, **136**, **140**.

All channels but **36**, **40**, **44**, **48** are Dynamic Frequency Selection (DFS) channels.

Note You can set the DFS channels **52**, **56**, **60**, **64**, **100**, **104**, **108**, **112**, **116**, **132**, **136**, **140**, but the device may need to use a different channel. For example, you can configure the Wi-Fi 5 GHz channel to **56**, but the device might need to use channel **108** instead.

Web

1. On the menu, click **Network > Interfaces > Wi-Fi**.
2. Select a Wi-Fi interface to configure.
3. Edit the configuration settings as needed.
4. Click **Apply**.

Command line

To select a channel for Wi-Fi 5 GHz communications, the command is wifi-global and the parameter is **wifi5g-channel**. For example, to set the channel for **Wi-Fi 5 GHz** interfaces to channel **36**, enter:

```
digi.router> wifi-global wifi5g-channel 36
digi.router> save config
```

Configure an access point

This section describes how to configure a Wi-Fi 2.4 GHz access point and a Wi-Fi 5 GHz access point.

Required configuration items

Configuring a Wi-Fi access point involves configuring the following items:

- Enabling the Wi-Fi access point.
- The Wi-Fi access point's Service Set Identifier (SSID).

  You can configure the SSID to use the device's serial number by including **%s** in the SSID. For example, an **ssid** parameter value of **LR54_%s** resolves to **LR54_LR123456**.
- The password for the Wi-Fi interface. The password only needs to be set if WPA2-Personal or WPA-WPA2-Personal security is being used.
- Once configured, the Wi-Fi access point must be assigned to a LAN interface. For more information, see Local Area Networks (LANs) and Configure a LAN.

Additional configuration options

The following additional configuration settings are not typically configured to get an Wi-Fi access point working, but can be configured as needed:

- The type of security used on the Wi-Fi interface. The default is **WPA2-Personal**. Options include the following:
  - **None**: No security is used on the Wi-Fi network.
  - **WPA2-Personal**: A method of securing a Wi-Fi network using WPA2 with the use of the optional Pre-Shared Key (PSK) authentication. This security method was designed for home users without an enterprise authentication server.
  - **WPA/WPA2-Personal**: This security method is a mixed mode, providing WPA with Temporal Key Integrity Protocol (TKIP) encryption or WPA2 with Advanced Encryption Standard (AES) encryption supported by the access point.
  - **WPA2-Enterprise**: This security method is designed for enterprise networks and requires a RADIUS authentication server. This security method requires a more complicated setup, but provides additional security. Various kinds of the Extensible Authentication Protocol (EAP) are used for authentication.
  - **WPA/WPA2-Enterprise**: This security method is designed for enterprise networks and requires a RADIUS authentication server. This is a mixed mode method, providing WPA with TKIP encryption or WPA2 with AES encryption supported by the access point.
- A description of the access point.
- Disabling the broadcast of the SSID in broadcast packets. The default is to broadcast the SSID, but you can disable that broadcast to prevent clients from easily detecting the presence of this access point.
- Disabling one or both isolation modes for the Wi-Fi access point. There are 2 isolation modes. By default, both isolation modes are enabled, but you can disable one or both as needed.
  - **Client Isolation**: Prevents clients on the same access point from communicating with each other.
  - **AP Isolation**: Prevents clients on an access point from communicating with clients on other APs.
- Selecting a channel for Wi-Fi 2.4 GHz or 5 GHz communications. For more details, see Configure a channel for Wi-Fi 2.4 GHz interfaces and Configure a channel for Wi-Fi 5 GHz interfaces.

Web

1. On the menu, click **Network > Interfaces > Wi-Fi**.
2. Select a Wi-Fi interface to configure.

3. In the **Edit Selected** box, enter the configuration settings for the access point:
   - **Mode**: Select Access Point.
   - **SSID**: Enter the Wi-Fi access point's Service Set Identifier (SSID).
   - **Security**: Select **None**, **WPA-2 Personal**, or **WPA/WPA2-Mixed-Mode-Personal**, depending on the security for this access point.
   - If you selected **WPA-2-Personal**, or **WPA/WPA2-Mixed-Mode-Personal** security, enter the password in the **Password** and **Verify Password** fields.
   - **Description**: Optional: Enter a description of the access point.
   - **State**: Enable or disable the Wi-Fi access point when configuration is complete.
   - **Broadcast SSID**: Optional: Enable or disable broadcasting the SSID in beacon packets.
   - **Isolation - Client**: Optional: Enable or disable Wi-Fi client isolation mode.
   - **Isolation - Access Point**: Optional: Enable or disable Wi-Fi access point isolation mode.
4. Click **Apply**.

Command line

To configure the global settings for Wi-Fi communications, including selecting the channel for Wi-Fi communications, the command is wifi-global.

To configure a Wi-Fi 2.4 GHz access point, the command is wifi.

To configure a Wi-Fi 5 GHz access point, the command is wifi5g.

The following steps show using the wifi command. When configuring a Wi-Fi 5 GHz access point, use the wifi5g command. The parameters are the same.

1. Enable the Wi-Fi access point.

```
digi.router> wifi 1 state on
```

2. Enter the SSID for the Wi-Fi access point.

```
digi.router> wifi 1 ssid LR54-AP1
```

3. Enter the password for the Wi-Fi access point.

```
digi.router> wifi 1 password your-password
```

4. Optional: Enter the security for the Wi-Fi access point.

```
digi.router> wifi 1 security wpa-wpa2-personal
```

5. Optional: Enter a description for the Wi-Fi access point.

```
digi.router> wifi 1 description “Office AP”
```

6. Optional: Disable broadcasting the SSID in beacon packets.

```
digi.router> wifi 1 broadcast-ssid off
```

7. Optional: Disable Wi-Fi client isolation mode.

```
digi.router> wifi 1 isolate-clients off
```

8. Optional: Disable Wi-Fi access point isolation mode.

```
digi.router> wifi 1 broadcast-ssid off
```

9. Save the configuration.

```
digi.router> save config
```

Configure an access point with enterprise security

The WPA2-Enterprise and WPA-WPA2-Enterprise security modes allow a Wi-Fi access point to authenticate connecting Wi-Fi clients using a RADIUS server.

When the Wi-Fi access point receives an connection request from a Wi-Fi client, it authenticates the client with the RADIUS server before allowing the client to connect.

Using enterprise security modes allows for each Wi-Fi client to have different username and password which are configured in the RADIUS server and not the TransPort device.

Configuring a Wi-Fi access point to use an enterprise security mode involves configuring the following items:

Required configuration items

Configuring a Wi-Fi access point to use an enterprise security mode involves configuring the following items:

- Enabling the Wi-Fi access point.
- The Wi-Fi access point’s Service Set Identifier (SSID).
  You can configure the SSID to use the device's serial number by including **%s** in the SSID. For example, an **ssid** parameter value of **LR54_%s** resolves to **LR54_LR123456**.
- Setting the security mode to either **WPA2-enterprise** or **WPA-WPA2-enterprise**.
- RADIUS server IP address.
- RADIUS password.

Additional configuration options

Additional configuration options include:

- RADIUS server port.
- A description of the Wi-Fi access point.
- Disabling the broadcast of the SSID in broadcast packets. The default is to broadcast the SSID, but you can disable that broadcast to prevent clients from easily detecting the presence of this access point.

- Disabling one or both isolation modes for the Wi-Fi access point. There are 2 isolation modes. By default, both isolation modes are enabled, but you can disable one or both as needed.
  - **Client Isolation**: Prevents clients on the same access point from communicating with each other.
  - **AP Isolation**: Prevents clients on an access point from communicating with clients on other APs.
- Selecting a channel for Wi-Fi 2.4 GHz or 5 GHz communications. For more details, see Configure a channel for Wi-Fi 2.4 GHz interfaces and Configure a channel for Wi-Fi 5 GHz interfaces.

Web

1. On the menu, click **Network > Interfaces > Wi-Fi**.
2. Select a Wi-Fi interface to configure.
3. In the **Edit Selected** box, enter the configuration settings for the access point:
   - **Mode**: Select Access Point.
   - **SSID**: Enter the SSID for the device.
   - **Security**: Select **WPA-2-Enterprise**, or **WPA/WPA2-Mixed-Mode-Enterprise**, depending on the security for this access point.
   - If you selected **WPA-2 Personal**, or **WPA/WPA2-Mixed-Mode-Personal** security, enter the password in the **Password** and **Verify Password** fields.
   - **Description**: Optional: Enter a description of the access point.
   - **State**: Enable or disable the Wi-Fi access point when configuration is complete.
   - **Broadcast SSID**: Optional: Enable or disable broadcasting the SSID in beacon packets.
   - **Isolation - Client**: Optional: Enable or disable Wi-Fi client isolation mode.
   - **Isolation - Access Point**: Optional: Enable or disable Wi-Fi access point isolation mode.
   - **Radius Server**: Enter the IP address of the RADIUS server.
   - **Radius Port**: Optional: Enter the RADIUS server port.
   - **Radius Secret**: Enter the RADIUS password.
4. Click **Apply**.

Command line

To configure a Wi-Fi 2.4 GHz access point, the command-line command is wifi.

To configure a Wi-Fi 5 GHz access point, the command-line command is wifi5g.

The following steps show using the wifi command. When configuring a Wi-Fi 5 GHz access point, use the wifi5g command. The parameters are the same.

1. Enable the Wi-Fi access point.

```
digi.router> wifi 1 state on
```

2. Enter the SSID for the Wi-Fi access point.

```
digi.router> wifi 1 ssid LR54-AP1
```

3. Enter the security for the Wi-Fi access point.

```
digi.router> wifi 1 security wpa2-enterprise
```

4. Enter the RADIUS server IP address.

```
digi.router> wifi 1 radius-server 192.168.1.200
```

5. Enter the RADIUS password.

```
digi.router> wifi 1 radius-password your-radius-password
```

6. Optional: Enter the RADIUS server port.

```
digi.router> wifi 1 radius-server-port 3001
```

7. Optional: Enter a description for the Wi-Fi access point.

```
digi.router> wifi 1 description "Office AP"
```

8. Optional: Disable broadcasting the SSID in beacon packets.

```
digi.router> wifi 1 broadcast-ssid off
```

9. Optional: Disable Wi-Fi client isolation mode.

```
digi.router> wifi 1 isolate-clients off
```

10. Optional: Disable Wi-Fi access point isolation mode.

```
digi.router> wifi 1 broadcast-ssid off
```

11. Save the configuration.

```
digi.router> save config
```

Show Wi-Fi status and statistics

You can show summary statistics for all Wi-Fi 2.4 GHz and 5 GHz interfaces, and detailed statistics for an individual interface.

Web

- On the menu, click **Dashboard**. The Interface section of the dashboard shows the status of all interfaces.

Command line

Show summary statistics for Wi-Fi interfaces

To show the status and statistics for Wi-Fi 2.4 GHz interfaces, use the show wifi command. For example, to show status of all Wi-Fi 2.4 GHz interfaces, enter:

```
digi.router> show wifi

 Interface  Status  SSID                              Security
 -------------------------------------------------------------
 wifi1      Up      LR54-2.4G-LR000181                WPA2-Personal
 wifi2      Down    LR54-2.4G-Public-LR000181         None
 wifi3      Down    LR54-Office                       WPA2-Enterprise
 wifi4      Down                                      WPA2-Personal

digi.router>
```

To show the status and statistics for a Wi-Fi 5 GHz interface, use the show wifi5g command. For example:

```
digi.router> show wifi5g

 Interface  Status  SSID                              Security
 -------------------------------------------------------------
 wifi5g1    Up      LR54-5G-LR000181                  WPA2-Personal
 wifi5g2    Down    LR54-5G-Public-LR000181           None
 wifi5g3    Down                                      WPA2-Personal
 wifi5g4    Down                                      WPA2-Personal

digi.router>
```

Show detailed status statistics for a Wi-Fi interface

To show the status and statistics for a particular Wi-Fi 2.4 GHz interface, enter **show wifi *n***, where ***n*** is the Wi-Fi 2.4 GHz interface number. For example:

```
digi.router> show wifi 1

 wifi 1 Status and Statistics
 ----------------------------
 Admin Status      : Up
 Oper Status       : Up
 SSID              : LR54-2.4G-LR000181
 Security          : WPA2-Personal

 Received                              Sent
 --------                              ----
 Rx Bytes                 : 7185       Tx Bytes                 : 1639
 Rx Packets               : 42         Tx Packets               : 13
 Rx Compressed            : 0          Tx Compressed            : 0
 Rx Multicasts            : 30         Tx Collisions            : 0
 Rx Errors                : 0          Tx Errors                : 0
 Rx Dropped               : 0          Tx Dropped               : 0
 Rx FIFO Errors           : 0          Tx FIFO Errors           : 0
 Rx CRC Errors            : 0          Tx Aborted Errors        : 0
 Rx Frame Errors          : 0          Tx Carrier Errors        : 0
 Rx Length Errors         : 0          Tx Heartbeat Errors      : 0
 Rx Missed Errors         : 0          Tx Window Errors         : 0
 Rx Over Errors           : 0

 Connected Clients
 -----------------
 MAC Address        Connection Time  RSSI           Rate
 -----------------------------------------------------------------
 58:94:6B:7A:B4:6C  0h 0m 10s        -31,-31,-72    130Mbps


digi.router>
```

To show the status and statistics for a particular Wi-Fi 5 GHz interface, enter **show wifi5g *n***, where ***n*** is the Wi-Fi 5g interface number. For example:

```
digi.router> show wifi5g 1

 wifi5g 1 Status and Statistics
 ------------------------------
 Admin Status      : Up
 Oper Status       : Up
 SSID              : LR54-5G-LR000181
 Security          : WPA2-Personal

 Received                              Sent
 --------                              ----
 Rx Bytes                 : 8718       Tx Bytes                 : 1686
 Rx Packets               : 55         Tx Packets               : 14
 Rx Compressed            : 0          Tx Compressed            : 0
```

```
Rx Multicasts                   : 41          Tx Collisions                   : 0
Rx Errors                       : 0           Tx Errors                       : 0
Rx Dropped                      : 0           Tx Dropped                      : 0
Rx FIFO Errors                  : 0           Tx FIFO Errors                  : 0
Rx CRC Errors                   : 0           Tx Aborted Errors               : 0
Rx Frame Errors                 : 0           Tx Carrier Errors               : 0
Rx Length Errors                : 0           Tx Heartbeat Errors             : 0
Rx Missed Errors                : 0           Tx Window Errors                : 0
Rx Over Errors                  : 0

Connected Clients
-----------------
MAC Address        Connection Time  RSSI          Rate
-----------------------------------------------------------------
58:94:6B:7A:B4:6C  0h 0m 17s        -47,-52,-55    270Mbps

digi.router>
```

Serial interface

TransPort devices have a single serial port that provides access to the command-line interface.

Configure the serial interface

By default, the serial interface is **enabled**. To change serial configuration settings, use the serial command.

- Disable the serial interface.

```
digi.router> serial state off
digi.router> save config
```

- Enter a description for the serial interface.

```
digi.router> serial description “Command line access”
digi.router> save config
```

- Set the baud rate. For example, to set the baud rate to **9600**, enter:

```
digi.router> serial baud 9600
digi.router> save config
```

- Set the data bits. For example, to set the data bits to **7**, enter:

```
digi.router> serial databits 7
digi.router> save config
```

- Set the stop bits. For example, to set the stop bits to **2**, enter:

```
digi.router> serial stopbits 2
digi.router> save config
```

- Set the parity. For example, to set the parity to **odd**, enter:

```
digi.router> serial parity odd
digi.router> save config
```

- Set the flow control. For example, to set the flow control to **hardware**, enter:

```
digi.router> serial flowcontrol hardware
digi.router> save config
```

Show serial status and statistics

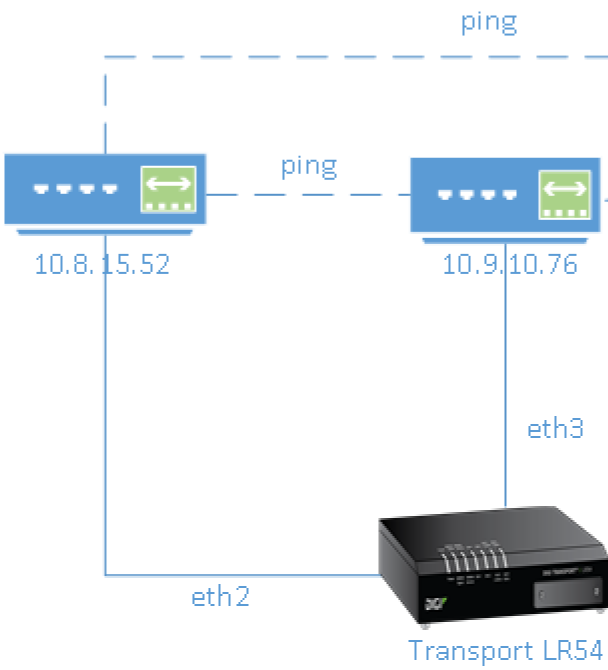
To show the status and statistics for the serial interface, use the show serial command. For example:

```
digi.router> show serial

 Serial 1 Status
 ---------------
 Description  :
 Admin Status : up
 Oper Status  : up
 Uptime       : 0:07:05
 Tx Bytes     : 4038
 Rx Bytes     : 81
 Overflows    : 0
 Overruns     : 0
 Line status  : RTS|CTS|DTR|DSR|CD0

digi.router>
```

Local Area Networks (LANs)

A Local Area Network (LAN) connects network interfaces together, such as Ethernet or Wi-Fi, in a logical Layer-2 network. You can configure up to **10** LANs.

The diagram shows a LAN connecting the **eth2**, **eth3**, and **eth4** interfaces for a TransPort LR54 unit. Once the LAN is configured and enabled, the devices connected to the network interfaces can communicate with each other, as demonstrated by the **ping** commands.



Configure a LAN

Configuring a Local Area Network (LAN) involves configuring the following items:

Required configuration items

- Identifying which interfaces are in the LAN.
- Enabling the LAN. LANs are disabled by default.
- Setting an IPv4 address and subnet mask for the LAN. While it is not strictly necessary for a LAN to have an IP address, if you want to send traffic from other networks to the LAN, you must configure an IP address.
- If you want to use IPv6 addressing for the LAN, you need to enable the LAN interface instance for IPv6 and configure several other settings. See Configure a LAN for IPv6.

Additional configuration options

- Setting a descriptive name for the LAN.
- Setting the Maximum Transmission Unit (MTU), or packet size, for packets sent over the LAN. For IPv6, the minimum MTU must be 1280.

Web

To create a new LAN:

1. On the menu, click **Network > Networks > LANs**. The LANs page appears.
2. Click **New Network**. See Local Networks page for field descriptions.
3. In the **IPv4** group, set the IP address and netmask:

   IP address: Enter the IPv4 address for the LAN.
   Netmask: Enter the subnet mask for the LAN.

4. In the **DHCP Server** group, configure the DHCP server. You can enable the DHCP server to assign IP addresses and other IP configurations to other hosts on the same local network. Addresses are assigned from a specified pool of IP addresses.

   Note For a LAN, the device uses the DHCP server that has the IP address pool in the same IP subnet as the LAN. If you set DHCP server values and find that they are not being served to your DHCP clients, review the LAN configuration in the **Local Networks** page to make sure that the specified **IP Start** and **IP End** values match the corresponding **IPv4** and **Netmask** settings for the interface.

5. In the **IPv6** group, configure **IPv6**. See Configure a LAN for IPv6.
6. In the **Advanced** group, enter the Maximum Transmission Unit (MTU), or packet size, for packets sent over the LAN.
7. Click **Apply**. The new LAN is added to the **LAN** page.

To modify an existing LAN:

1. On the menu, click **Network > Networks > LANs**. The LANs page appears.
2. Select a LAN and modify the settings as needed. See Local Networks page for field descriptions.
3. Click **Apply**.

Command line

1. Set the interfaces in the LAN. For example, to include **eth2**, **eth3**, and **eth4** interfaces in **lan1**, enter:

```
digi.router> lan 1 interfaces eth2,eth3,eth4
```

2. Enable the LAN. For example, to enable **lan1**:

```
digi.router> lan 1 state on
```

3. Optional: Set an IPv4 address for the LAN.

```
digi.router> lan 1 ip-address 192.10.8.8
```

4. Optional: Set a subnet mask for the LAN.

```
digi.router> lan 1 mask 255.255.255.0
```

5. Optional: Give a descriptive name to the LAN.

```
digi.router> lan 1 description ethlan
```

6. Optional: Set the MTU for the LAN.

```
digi.router> lan 1 mtu 1500
```

7. Save the configuration.

```
digi.router> save config
```

Show LAN status and statistics

Web

1. From the menu, click **Dashboard**. The **Network Activity** panel LAN section shows the total bytes received and sent over all LANs, and the **LAN** panel shows the configured LANs and their states.
2. Click a LAN to display or configure a LAN.

Command line

To show the status and statistics for a LAN, use the show lan command. For example, here is show lan output for a LAN on which IPv6 is enabled:

```
digi.router> show lan 1

 LAN 1 Status and Statistics
 ---------------------------
 Admin Status      : Up
 Oper Status       : Up

 Description       : Ethernet and Wi-Fi LAN network

 Interfaces        : eth3
 MTU               : 1500

 DHCP client       : Off
 IP Address        : 192.168.1.1
 Mask              : 255.255.255.0
 DNS Server(s)     : 8.8.8.8

 IPv6 Address(es)  : fe80::47/64 (Link local)
                     2001::1234:23:47:1/64 (Global)
```

```
                Received            Sent
                --------            ----
 Packets               0             137
 Bytes                 0           15026

digi.router>
```

If IPv6 were disabled on this LAN, the **show lan** output looks like this:

```
digi.router> show lan 1

 LAN 1 Status and Statistics
 ---------------------------
 Admin Status  : Up
 Oper Status   : Up

 Description   : Ethernet and Wi-Fi LAN network

 Interfaces    : eth3
 MTU           : 1500

 DHCP client   : Off
 IP Address    : 192.168.1.1
 Mask          : 255.255.255.0
 DNS Server(s) : 8.8.8.8

 IPv6 is disabled on this interface

                 Received            Sent
                 --------            ----
 Packets               0              209
 Bytes                 0            22946

digi.router>
```

Delete a LAN

Deleting a LAN involves removing the physical interface associations from the LAN, thereby disabling the LAN. The definition for the LAN still exists in the device configuration, but it has no active physical interface.

Web

1. On the menu, click **Network > Networks > LANs**. The LANs page appears.
2. On the **LANs** page, select the LAN to delete.
3. Click **Delete**.

Command line

Use the lan command and specify **!** for the **interfaces** parameter value to set it to **none**:

```
lan <lan-number> interfaces !
```

DHCP servers

You can enable DHCP in a TransPort device to assign IP addresses and to other hosts on the same local network. Addresses are assigned from a specified pool of IP addresses. For a local network, the device uses the DHCP server that has the IP address pool in the same IP subnet as the local network.

Note For a LAN, the device uses the DHCP server that has the IP address pool in the same IP subnet as the LAN. If you set DHCP server values and find that they are not being served to your DHCP clients, review the LAN configuration in the **Local Networks page** to make sure that the specified **IP Start** and **IP End** values match the corresponding **IPv4** and **Netmask** settings for the interface.

You can configure up to **10** DHCP servers.

When a host receives an IP configuration, the configuration is valid for a particular amount of time, known as the lease time. After this lease time expires, the configuration must be renewed. The host renews the lease time automatically.

Configure DHCP server settings

To configure a DHCP server, you need to configure the following:

Required configuration items

- Enable the DHCP server.
- The IP address pool: the range of IP addresses issued by the DHCP server to clients.
- The IP network mask given to clients.
- The IP gateway address given to clients.
- The IP addresses of the preferred and alternate Domain Name Server (DNS) given to clients.

Additional configuration options

- Lease time: The length, in minutes, of the leases issued by the DHCP server.

Web

In the web interface, the DHCP server is configured as part of configuring a LAN on the **Local Networks** page. See Configure a LAN.

Command line

1. Enable the DHCP server. By default, the DHCP server is disabled.

```
digi.router> dhcp-server 1 state on
```

2. Enter the starting address of the IP address pool:

```
digi.router> dhcp-server 1 ip-address-start 10.30.1.150
```

3. Enter the ending address of the IP address pool:

```
dhcp-server 1 ip-address-end 10.30.1.195
```

4. Enter the network mask:

```
digi.router> dhcp-server 1 mask 255.255.225.0
```

5. Enter the IP gateway address given to clients:

```
digi.router> dhcp-server 1 gateway 10.30.1.1
```

6. Enter the preferred DNS server address given to clients:

```
digi.router> dhcp-server 1 dns1 10.30.1.1
```

7. Enter the alternate DNS server address given to clients:

```
digi.router> dhcp-server 1 dns2 209.183.48.11
```

8. Enter the lease time:

```
digi.router> dhcp-server 1 lease-time 60
```

9. Save the configuration.

```
digi.router> save config
```

Show DHCP server settings

View DHCP status to monitor which devices have been given IP configuration by the TransPort device and to diagnose DHCP issues.

Web

1. On the menu, click **Network > Networks > LANs**. The LANs page appears.
2. Select a LAN.
3. In the **Configuration** settings, view the DHCP server settings for the LAN:
   - **DHCP Server**: Whether the DHCP server is enabled or disabled.
   - **IP Start**/**IP End**: These settings set the beginning and end of the IP address pool, or the range of IP addresses the DHCP server issues to clients.
   - **Lease Expires**: The length, in minutes, of the leases issued by the DHCP server.

Command line

To show the status of the DHCP server, use the show dhcp command. For example:

```
digi.router> show dhcp

DHCP Status
-----------
IP address        Hostname           MAC Address        Lease Expires At
--------------------------------------------------------------------------
192.168.123.123   IKY-CMS-JPINKN1    38:ea:a7:fd:de:cd  16:32:16, 14 Sep 2016
192.168.123.124   IKY-CMS-BOB        38:ea:a7:fd:a3:22  18:21:06, 14 Sep 2016

digi.router>
```

Wide Area Networks (WANs)

A Wide Area Network (WAN) provides connectivity to the internet or a remote network. A WAN configuration consists of the following:

- A physical interface, such as Ethernet or cellular
- Several networking parameters for the WAN, such as IP address, mask, and gateway
- Several parameters controlling failover

Using Ethernet interfaces in a WAN

Depending on model type, TransPort devices support several Ethernet interfaces. For example, a TransPort LR54 device has four Ethernet interfaces, named **eth1**, **eth2**, **eth3**, and **eth4**. Other models have fewer Ethernet interfaces, but the naming and numbering of interfaces is similar. You can use Ethernet interfaces as a WAN when connecting to the Internet, through a device such as a cable modem, as shown in the example.

By default, the **eth1** interface is configured as a WAN with both DHCP and NAT enabled. This means you should be able to connect to the Internet by connecting the **wan/eth1** interface to a device that already has an internet connection.

Conversely, the **eth2**, **eth3**, and **eth4** interfaces are by default configured as a Local Area Network (LAN). If necessary, you can assign these Ethernet interfaces to a WAN. For more information on Ethernet interfaces and their configuration, see Ethernet interfaces.

Using cellular interfaces in a WAN

TransPort devices support two cellular interfaces, named **cellular1** and **cellular2**.

To use a cellular interface as a WAN, the cellular interface must be configured to connect to the cellular network. For more information on cellular interfaces and their configuration, see Cellular interfaces.

WAN priority, default routes, and metrics

You can configure up to **10** WANs. **wan1** is the top priority, **wan2** is the second priority, and so on.

The TransPort device automatically adds a default IP route for the WAN when it comes up. The metric of the default route is based on the priority of the interface. For example, because **wan1** is the highest priority WAN, the default route for **wan1** has a metric of **1**, and the default route for **wan2** has a metric of **2**.

Handling WAN failures

If a WAN fails for any reason, the TransPort device automatically fails over from one WAN to the next available WAN.

For example, if you use an Ethernet interface as your primary WAN, and have a cellular interface configured as a backup interface, if the Ethernet interface fails (for example, if the Ethernet cable is broken), the TransPort device automatically starts to use the cellular interface until the Ethernet interface becomes active again.

For more information on WAN failover, see WAN failover.

Configure a Wide Area Network (WAN)

You can configure up to **10** Wide Area Network (WANs). Configuring a WAN consists of the following:

- Associating a physical interface, such as Ethernet or cellular with the WAN
- Optionally configuring networking parameters for the WAN, such as IP address, mask, and gateway
- Optionally configuring several parameters controlling failover
- Optionally configuring the WAN for IPv6 support

Assigning priority to WANs

You can assign priority to WANs based on the behavior you want to implement for primary and backup WAN interfaces. For example, if you want Ethernet to be your primary WAN with a cellular interface as backup, assign an Ethernet interface to **wan1** and assign a cellular interface to **wan2**.

WANs have priorities associated with them, which is based on a metric parameter set for each WAN. The TransPort device automatically adds a default IP route for the WAN when it comes up. The metric of the route is based on the priority of the interface. For example, as **wan1** is the highest priority, the default route for **wan1** has a metric of **1**, and the default route for **wan2** has a metric of **2**.

Configuring a WAN for IPv6

You can enable IPv6 on a per-WAN-interface basis. See Configure a WAN for IPv6.

Required configuration items

- Assign an interface to the WAN. By default, WANs are assigned the following physical interfaces:
  - **wan1**: **eth1**
  - **wan2**: **cellular1**
  - **wan3**: **cellular2**
- If you want to use IPv6 addressing for the WAN, enable the WAN for IPv6 and configure prefix delegation. See Configure a WAN for IPv6.

Additional configuration options

These additional configuration settings are not typically configured, but you can set them as needed.

For **Ethernet** interfaces:

- The IP configuration. WANs typically get their IP address configuration from the network to which they connect (for example, cellular). However, you can manually set the IP configuration as needed. The following manual configuration settings are available:

- IP address and mask.
- Gateway: required for Ethernet WANs if setting IP address manually, to create a default route over the WAN. If setting the IP address via DHCP, this setting is obtained automatically and does not need to be set.
- Preferred and alternate DNS server.

- Disable the DHCP client. Ethernet interfaces use DHCP client to get an IP address from a DHCP server (for example, from a cable modem). If you are manually configuring the IP address for the Ethernet interface, disable the DHCP client.
- Network Address Translation (NAT). NAT translates IP addresses from a private LAN to a public IP address. By default, NAT is enabled. Unless your LAN has a publicly-addressable IP address range, do not disable NAT.
- The IP probe settings. These settings control elements of the WAN failover feature, including sending of probe packets over the WAN interface to a specified device to determine whether the WAN is still up, timeouts, and switching between primary and backup interfaces. For more information on these settings, see the discussion of IP probing in Wide Area Networks (WANs).

Note A WAN configured for static IP takes precedence over a configuration derived via DHCP. This allows you to configure alternative DNS servers from those given to you by your network provider.

For **Cellular** interfaces:

- The IP probe settings. These settings control elements of the WAN failover feature, including sending of probe packets over the WAN interface to a specified device to determine whether the WAN is still up, timeouts, and switching between primary and backup interfaces. For more information on these settings, see the discussion of IP probing in Wide Area Networks (WANs).

Web

To create a new WAN

1. On the menu, click **Network > Networks > WANs**. The WANs page appears.
2. Click **New WAN Connection** and enter the following:

   Select WAN: Assign an index number to the WAN. This number sets the WAN priority for the WAN.

   Select interface: Select an interface to assign to the WAN.

   Enable: Enable or disable the new WAN.

3. In the **IPv4** group, configure IP address settings for IPv4 if you want to manually configure an IP address for the WAN.
4. In the **IPv6** group, enable and configure IPv6 if required for the WAN.
5. In the **Security** group, configure optional security settings for the WAN.
6. In the **Probing** group, configure optional probe host settings for the WAN.
7. Click **Apply**.

To modify an existing WAN

1. On the menu, click **Network > Networks > WANs**. The WANs page appears.
2. Select a WAN and modify settings as needed. See Wide Area Network (WAN) page for field descriptions.
3. Click **Apply**.

Command line

Configure basic WAN settings

1. Assign an interface to the WAN interface.

```
digi.router> wan 1 interface eth1
```

2. If using IPv6 addressing for the WAN, see Configure a WAN for IPv6.
3. Optional: Disable DHCP client mode.

```
digi.router> wan 1 dhcp off
```

4. Optional: Configure the IP address, mask, gateway, and DNS servers.

```
digi.router> wan 1 ip-address 10.1.2.2
digi.router> wan 1 mask 255.255.255.252
digi.router> wan 1 gateway 10.1.2.1
digi.router> wan 1 dns1 10.1.2.1
digi.router> wan 1 dns2 8.8.8.8
```

5. Optional: Set the speed.

```
digi.router> eth 1 speed {auto | 1000 | 100 | 10}
```

Configure IP probe settings

1. Optional: Configure the time, in seconds, to wait for this interface to connect and to receive a probe response before failing over to a lower priority interface.

```
digi.router> wan 1 timeout 60
```

2. Configure the IP host to probe.

```
digi.router> wan 1 probe-host 192.168.47.1
```

3. Optional: Configure the time, in seconds, to wait for a response to a probe. This value must be smaller than the probe-interval and timeout parameter values. If not, the configuration is considered invalid, and an error message is written to the system log.

```
digi.router> wan 1 probe-timeout 5
```

4. Optional: Configure the interval, in seconds, between sending probe packets. This value must be larger than the probe-timeout value. If not, the WAN failover configuration is considered invalid, and an error message is written to the system log.

```
digi.router> wan 1 probe-interval 20
```

5. Optional: Configure the size of the IP probe packet.

```
digi.router> wan 1 probe-size 120
```

6. Optional: Configure the time, in seconds, that the primary interface needs to be up before switching back to it as the active interface. If probing is active, no probes are permitted to be lost during this period. Otherwise, the timer is restarted. Accepted value is any integer from **0** to **3600**. The default value is **0**.

```
digi.router> wan 1 activate-after 30
```

7. Optional: Configure the time, in seconds, to wait before retrying this interface after failing over to a lower priority one. Use a large retry timeout when both interfaces are cellular interfaces. Accepted value is any integer from **10** to **3600**. The default value is **180**.

```
digi.router> wan 1 retry-after 1200
```

8. Save the configuration.

```
digi.router> save config
```

WAN failover

If a WAN fails for any reason, the TransPort device automatically fails over from one WAN to use another.

For example, if you use an Ethernet interface as your main WAN and cellular interface configured as a backup, if the Ethernet interface fails (for example, if the Ethernet cable is broken), the TransPort device automatically uses the cellular interface until the Ethernet interface becomes active again.

Conditions that cause failover

Conditions that can cause a WAN to go down and the TransPort to switch to another interface include:

- On an Ethernet interface, the cable for the Ethernet interface is broken or disconnected.
- On an Ethernet interface, the Ethernet cable modem is switched off.

Detecting when a WAN goes down: active and passive detection

There are two ways to detect when a WAN goes down: active detection and passive detection.

Active detection involves sending out IP probe packets (ICMP echo requests) to a particular host and waiting for a response. The WAN is considered to be down if there are no responses for a configured amount of time. The settings and behavior for active detection through IP probing are described in more detail below.

Passive detection involves detecting the WAN going down by monitoring its link status by some means other than sending IP probe packets; for example, if an Ethernet cable is disconnected or the state of a cellular interface changes from **on** to **off**.

IP probing

Problems can occur beyond the immediate WAN connection that prevent some IP traffic from reaching its destination. Normally this kind of problem does not cause the WAN to fail, as the connection continues to work while the core problem exists somewhere else in the network.

IP probing is a way to detect problems in an IP network. IP probing involves configuring the TransPort device to send out regular IP probe packets (ICMP echo requests) to a particular destination. If there are no responses to the probe packets, the TransPort device can bring down the WAN and switch to using another WAN until the IP network problem is resolved.

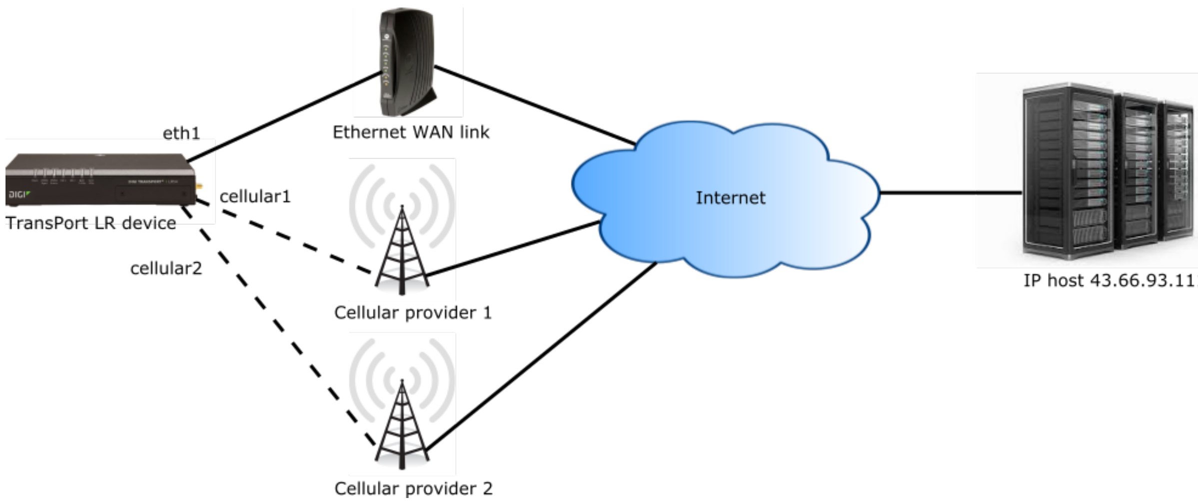
IP probing involves the following configuration settings:

- **timeout**: The time, in seconds, to wait for this interface to connect and to receive a probe response before failing over to a lower priority interface.
- **probe-host**: The IPv4 or fully qualified domain name (FQDN) of the address of the device itself. The WAN failover feature sends probe packets over the WAN to the IP address of this device.
- **probe-timeout**: The time, in seconds, to wait for a response to a probe. This value must be smaller than the probe-interval and timeout parameter values or the configuration is considered invalid, and an error message is written to the system log.
- **probe-interval**: The interval, in seconds, between sending probe packets. This value must be larger than the probe-timeout value. If not, the WAN failover configuration is considered invalid, and an error message is written to the system log.
- **probe-size**: The size of probe packets sent to detect WAN failures.
- **activate-after**: The time, in seconds, that the primary interface needs to be up before switching back to it as the active interface. If probing is active, no probes are permitted to be lost during this period. Otherwise, the timer is restarted.
- **retry-after**: The time, in seconds, to wait before retrying this interface after failing over to a lower priority one. Use a large retry timeout when both interfaces are cellular interfaces.

Most of the IP probing configuration parameters have default values, except for the IP address or name of the host to probe. Use of IP probes requires this IP address. For the rest of the parameters, the default values should be sufficient, but you can set them to different values as needed to suit your WAN failover requirements.

Example WAN failover: Ethernet to cellular

In this example WAN, the **eth1** interface associated with **wan1** serves as the primary WAN, while **cellular1** and **cellular2** are associated with **wan2** and **wan3**, respectively, and serve as backups.



To detect failover:

- The **eth1** interface uses IP probing to detect interface failure.
- The backup WANs, **wan2** and **wan3**, use passive techniques to detect interface failure.

Using the IP probing configured over the **eth1** interface, the TransPort device sends a probe packet of size **256** bytes to the IP host **43.66.93.111** every **10** seconds. If no responses are received for **60** seconds, the TransPort device brings the **eth1** interface down and starts using the **wan2** (**cellular1**) interface.

If the TransPort device cannot get a connection on the **wan2** (**cellular1**) interface, it attempts to use the **wan3** (**cellular2**) interface. It attempts to switch back to the **wan2** (**cellular1**) interface after **30** minutes (**1800** seconds).

The TransPort device continues to send probes out of the **eth1** interface. If it receives probe responses for **120** seconds, it reactivates the **wan1** interface and starts using it again as the primary WAN.

To achieve this WAN failover from the **eth1** to **cellular1** and **cellular2** interfaces, the WAN failover configuration commands are:

```
digi.router> cellular 1 state on
digi.router> cellular 2 state on
digi.router> wan 1 interface eth1
digi.router> wan 1 timeout 60
digi.router> wan 1 probe-host 43.66.93.111
digi.router> wan 1 probe-interval 10
digi.router> wan 1 probe-size 256
digi.router> wan 1 activate-after 120
digi.router> wan 2 interface cellular1
digi.router> wan 2 retry-after 1800
digi.router> wan 3 interface cellular2
```

Show WAN status and statistics

Web

1. On the menu, click **Network > Networks > WANs**. The WANs page appears.
2. Select a WAN.

The WAN page shows configuration parameters, as well as status and statistics for the interface assigned to the WAN.

Command line

Show WAN summary statistics

To show the status and statistics for a WAN, use the show wan command. For example:

```
digi.router> show wan

 # WAN Interface  Status  IP Address
 -----------------------------------
 1 eth1           Up      192.168.0.25
 2 cellular1      Up      172.20.1.7

digi.router>
```

Show status and statistics for the WAN physical interface

To view status and statistics for the physical interface for the WAN, enter the **show** command for that physical interface; for example, show eth or show cellular.

Show detailed WAN status

To show detailed status for a WAN, enter the show wan command, specifying the WAN instance number. For example, for a WAN on which IPv6 is enabled:

```
digi.router> show wan 1

 WAN 1 Status and Statistics

 ---------------------------
 WAN Interface      : eth1
 Admin Status       : Up
 Oper Status        : Up

 IP Address         : 47.0.0.101
 Mask               : 255.255.255.0
 Gateway            : 47.0.0.1
 DNS Server(s)      : 47.0.0.1, 8.8.8.8

 IPv6 Address(es)   : 2001:abcd:1234::1234:22:3/64 (Global)
                      fe80::20c:29ff:fef4:77fc/64 (Link local)
 IPv6 DNS Server(s) : 2001:abcd:1200:11:e4ff:fe09:3de3, 2001:4860:4860::8888

 Probes are not being used

               Received            Sent
               --------            ----
 Packets              4               4
 Bytes              836             796
```

When IP probing is enabled, the show wan output provides additional details, including how long it has been since the device received a probe response from the probe host:

```
digi.router> show wan 1

 WAN 1 Status and Statistics
 ---------------------------
 WAN Interface : eth1
```

```
 Admin Status  : Up
 Oper Status   : Up

 IP Address    : 10.52.18.120
 Mask          : 255.255.255.0
 Gateway       : 10.52.18.1
 DNS Server(s) : 8.8.8.8

 Probing                      : 10.52.18.1
 Last Probe Response received : 5 seconds ago

               Received            Sent
               --------            ----
 Packets           8356             640
 Bytes           673351           64841

digi.router>
```

If IP probing is disabled because the configuration is invalid, the output is similar to the following:

```
digi.router> show wan 1

 WAN 1 Status and Statistics
 ---------------------------
 WAN Interface : eth1
 Admin Status  : Up
 Oper Status   : Up

 IP Address    : 10.52.18.120
 Mask          : 255.255.255.0
 Gateway       : 10.52.18.1
 DNS Server(s) : 8.8.8.8

 Probes are not being used

            Received            Sent
            --------            ----
 Packets        8356             640
 Bytes        673351           64841

digi.router>
```

If IP probing is on, but the device has not yet received any replies, the output is similar to the following:

```
digi.router> show wan 1

 WAN 1 Status and Statistics
 ---------------------------
 WAN Interface : eth1
 Admin Status  : Up
 Oper Status   : Up

 IP Address    : 10.52.18.120
 Mask          : 255.255.255.0
 Gateway       : 10.52.18.1
 DNS Server(s) : 8.8.8.8

 Probing                      : 10.52.18.1
```

```
Waiting for first response

                Received            Sent
                --------            ----
Packets             8356             640
Bytes             673351           64841
```

Delete a WAN

Web

1. On the menu, click **Network > Networks > WANs**. The WANs page appears.
2. On the **WAN** page, select the WAN to delete.
3. Click **Delete**.

Command line

To delete a WAN, remove the physical interface associated with the WAN. Without a physical interface, the WAN is disabled. The WAN still exists in the device configuration, but it has no active physical interface.

For example, use the wan command to set the **interface** parameter value to **none**:

```
wan <wan-number> interface none
```

IPv6

IPv6 is an updated version of the Internet Protocol (IP). Until recently, the Internet has used a previous version, IPv4.

One of the reasons for IPv6 is the shortage of IPv4 addresses. Although Network Address Translation (NAT), which allows users to use one public IPv4 address for a whole private network, has mitigated this shortage to some extent, with more and more devices being connected to the internet, there are not many IPv4 addresses left.

IPv4 addresses are 32 bits long. Over 4 billion addresses are available through IPv4, though not all the addresses are usable. IPv6 addresses are 128 bits long. Taking into account the structure of the IPv6 address, there are 4.6×10^{18} globally routable addresses available. This equates to approximately 650 million IP addresses for each person in the world.

Since every device can have a globally routable IPv6 address, there is no NAT with IPv6. This means it is very important to properly configure IP filters and firewall rules to prevent direct attacks on hosts on the LAN networks. By default, a TransPort device blocks any incoming IPv6 traffic not associated with a connection established by a host on the LAN network.

IPv4 and IPv6 can co-exist on the same device. Each application can select the IP version to use. Some services, such as web server or Simple Network Management Protocol (SNMP) can accept connections on both IPv4 and IPv6.

TransPort devices support both IPv4 and IPv6 on WAN and LAN interfaces. Using IPv6 on WAN interfaces requires an ISP that supports IPv6.

Common IPv6 address types

There are several common IPv6 address types, distinguished by their beginning characters:

Address type	Beginning characters	Description
Global routable addresses	Either **2** or **3**	Each device using IPv6 on the Internet has a globally unique routable IPv6 address.
Link local addresses	**fe80**	Each device auto-generates a link-local address on every interface using IPv6. The interfaces use these addresses to communicate with other devices connected on the link.

Address type	Beginning characters	Description
Multicast addresses	**ff**	Addresses for sending packets to a group of devices. There are a number of well-known defined addresses, such as those for **All nodes** and **All routers**.
Unique local addresses (ULA)	**fc** or **fd**	Addresses for creating a site-specific network. While these addresses are globally unique, you cannot use them for routing on the Internet.

Auto address assignment

There are three modes in which a device can auto-configure itself with an IPv6 address and other network configuration. The mode the device uses is controlled by the Router Advertisement messages a router periodically sends out, or in response to a Router Solicitation message that a host sends.

Auto-configuration mode	Description
Stateless auto-configuration (SLAAC)	The device uses the prefix sent in the Router Advertisement message to generate a unique IPv6 usually by appending the interface's MAC address with EUI-64 encoding. The device can also learn gateway and DNS server information from the Router Advertisement message. The device uses Duplicate Address Detection (DAD) to ensure the auto-generated IPv6 address is unique.
DHCPv6	The device uses DHCPv6 to get an IPv6 address and other network configuration.
SLAAC + DHCPv6	The device uses a combination of SLAAC and DHCPv6. It uses SLAAC to auto-configures itself with an IPv6 address, and DHCPv6 to get other network configuration, such as DNS server information. This configuration mode is available because earlier versions of the Router Advertisement did not include any DNS server information. Therefore the device had to use DHCPv6 to get this information.

Prefix delegation

Prefix delegation is how a router asks for a prefix from the ISP that it can subnet and distribute through its LAN interfaces. Prefix delegation is an extension of the DHCPv6 protocol.

Normally, a router gets a **/64**-bit prefix using Router Advertisements, which cannot normally be subnetted. Therefore, a router uses prefix delegation to request a globally routable prefix it can distribute.

When the TransPort device receives a delegated prefix, it appends a subnet ID and assigns it to the LAN interfaces with IPv6 enabled. The subnet ID differs for each LAN. By default, the subnet ID is the LAN instance.

For example, if the delegated prefix is **2001:1234:5678:9ab0::/60**, the prefixes for LANs **1** to **4** are:

- LAN 1: **2001:1234:5678:9ab1/64**
- LAN 2: **2001:1234:5678:9ab2/64**
- LAN 3: **2001:1234:5678:9ab3/64**
- LAN 4: **2001:1234:5678:9ab4/64**

The router's LAN interfaces then advertise these prefixes using Router Advertisements and DHCPv6.

More information on IPv6

For more information, including key differences between IPv4 and IPv6, see this Digi white paper on IPv6.

Configure a LAN for IPv6

Currently, the only mode for auto-configuration of devices connected on the LAN is **DHCPv6**. Configuring a LAN for IPv6 involves Enable IPv6 on a LAN.

Enable IPv6 on a LAN

You can enable IPv6 on a per-LAN interface basis.

Enabling IPv6 on a LAN does not affect IPv4 operation. When IPv6 is enabled for a LAN, you can have IPv4 addresses on the LAN and hosts on the LAN can use IPv4 and IPv6 as required.

Web

1. On the menu, click **Network > Networks > LANs**. The LANs page appears.
2. Select the LAN on which you want to enable IPv6.
3. Open the **IPv6** group, and enable IPv6.

Command line

To enable IPv6 on a LAN, use the lan command **ipv6-state** parameter. For example:

```
digi.router> lan 1 ipv6-state on
digi.router> save config
```

Show LAN IPv6 status

Web

1. On the menu, click **Network > Networks > LANs**. All configured LANs appear.
2. Select a LAN. The LAN display expands to show the configuration parameters and the status and statistics for the interface assigned to the LAN. If IPv6 is enabled for the LAN and IPv6 addresses are assigned to it, the addresses display in the **IPv6 Address** field.

Command line

To show the IPv6 status on a LAN, use the show lan command. For example:

```
digi.router> show lan 1

 LAN 1 Status and Statistics
 ---------------------------
 Admin Status       : Up
 Oper Status        : Up

 Description        : Ethernet LAN network
 Interfaces         : eth2
 MTU                : 1500

 DHCP client        : Off
 IP Address         : 192.168.1.1
 Mask               : 255.255.255.0
 DNS Server(s)      : 8.8.8.8

IPv6 Address(es)    : fe80::8473:dff:fe69:ab41/64    (Link Local)
                      2600:1000:b03e:7ae9:1000::1/68 (Global)

                         Received          Sent
                        ---------          ----
 Packets                   167018         56253
 Bytes                   13487578       4608476
```

Configure a WAN for IPv6

Configuring a WAN for IPv6 involves these tasks:

- Enable IPv6 on a WAN
- Configure prefix delegation on a WAN

Enable IPv6 on a WAN

You can enable IPv6 on a per-WAN basis.

For IPv6 to work on a WAN interface, the ISP to which the WAN interface is connected must support IPv6.

Web

1. From the menu, click **Network > Networks > WANs**. The WANs page appears.
2. Select the WAN on which you want to enable IPv6.
3. Open the **IPv6** group, and enable IPv6.

Command line

To enable IPv6 on a WAN interface, use the wan command **ipv6-state** parameter. For example:

```
digi.router> wan 1 ipv6-state on
digi.router> save config
```

Configure prefix delegation on a WAN

When the WAN interface gets an IPv6 address, the TransPort device automatically sends a prefix delegation request to the ISP. By default, the TransPort device requests a **/60** prefix, which allows the device to support up to **15** LANs. The number of LANs that can be supported is equal to **2** raised to the power of ((64 - prefix-length) - 1). You can request a different prefix length from this default.

Note The TransPort is not guaranteed to receive a prefix of the requested length. For example, the TransPort device may request a **/60** prefix, but receive a **/62** prefix. This means you might have more LANs with IPv6 enabled than can be supported by the received prefix. In this case, the TransPort sets the prefix on the first LAN interfaces as defined by the number of available LANs.

Web

1. From the menu, click **Network > Networks > WANs**. The WANs page appears.
2. Select the WAN on which you want to configure prefix delegation.
3. Enter the length of the requested prefix in the **Requested Prefix Length** field.

Command line

To change the length of the requested prefix, use the wan command **ipv6-prefix-length** parameter. For example:

```
digi.router> wan 1 ipv6-prefix-length 56
digi.router> save config
```

Show WAN IPv6 status

Web

1. On the menu, click **Network > Networks > WANs**. All configured WANs appear.
2. Select a WAN. The WAN display expands to show the configuration parameters and the status and statistics for the interface assigned to the WAN. If IPv6 is enabled for the WAN and IPv6 addresses assigned to the WAN, the addresses display in the **IPv6 Address** field.

Command line

To show the IPv6 status on a WAN, use the show wan command. For example:

```
digi.router> show wan 2

 WAN 2 Status and Statistics
 ---------------------------
 WAN Interface       : cellular1
 Admin Status        : Up
 Oper Status         : Up

 IP Address          : 100.67.98.174
 Mask                : 255.255.255.252
 Gateway             :
 DNS Server(s)       : 198.224.186.135, 198.224.187.135
```

```
IPv6 Address(es)   : 2600:1000:b03e:7ae9:3038:63ff:fe47:4158/64 (Global)
                     fe80::3038:63ff:fe47:4158/64 (Link Local)
IPv6 DNS Server(s) : 2001:4888:12:ff00:106:d::, 2001:4888:13:ff00:123:d::

Probes are not being used

              Received            Sent
              --------            ----
Packets            503             939
Bytes           104697          130536
```

Security

TransPort devices have several device security features. This section covers configuring and managing these security features.

- Local users
- Firewall management with IP filters
- Remote Authentication Dial-In User Service (RADIUS)

Local users

To access a TransPort device (via the command-line interface or web interface), users must log in as a configured user of the device. This topic details the TransPort user model, as well as how to create, modify, and delete users.

Maximum number of users

TransPort allows you to configure up to **10** users for a device, **user 1** through **user 10**. Each user has a unique username, password, and access level.

Default user

As manufactured, each TransPort device comes with a default **user 1** configured as follows:

Username: **admin**

Password: The default password is displayed on the label on the bottom of the device. For example:

Access: **super**

Note The default password is a unique password for the device, and is the most critical security feature for the device. Anytime you reset the device to factory defaults, you should immediately change the password from the default to a custom password. Before deploying or mounting the TransPort device, take a photo of or otherwise record the default password, so you have the information available when you need it even if you cannot physically access the label on the bottom of the device.

You can change the default **user 1** configuration to match your site requirements.

User access levels

TransPort devices support three access levels: **super**, **read-write**, and **read-only**. These access levels determine the level of control users have over device features and settings.

Access level	Permissions allowed
super	The user can manage all features on TransPort devices. Devices can have multiple users with **super** access level. At least one user on each device must have a **super** access level to allow editing user access levels. If you or any other user deletes the only user with **super** access level, you must restore the default user configuration by resetting the device to factory defaults.
read-write	The user can manage all device features except security-related features, such as configuring user access, configuring firewalls, clearing logs, and so on.
read-only	The user can view device configuration and status, but cannot change the configuration or status.

Configure a user

To add, modify, or delete a user, you must be assigned the **super** access level. See User access levels for descriptions of user access levels.

To configure a user, you need to configure the following:

Required configuration items

- A username, up to **32** characters long.
- A password, from **1-128** characters long. For security reasons, passwords are stored in hash form. There is no way to get or display passwords in clear-text form.

Additional configuration options

- Setting user access level. The default access level for users is **super**. To restrict access for a user, assign either **read-write** or **read-only**. See User access levels for descriptions of user access levels.

Web

1. Click **Security > Authentication > Local Users**. The User Management page appears.
2. Click **New User**.

> **Note** When you add a new user using the web interface, TransPort creates a new user with the next available index number. When you create a new user using the command line, you cannot set or change the user index number assigned to a user.

3. Enter user account information:
   - **Username**: The username for the user. Usernames can be up to **32** characters long and are case-insensitive. They:
     - Must start with a letter (lowercase or uppercase) or underscore.
     - Can contain letters (lowercase and uppercase), digits, underscore (_), or hyphen (-).
     - Can end with a dollar sign (**$**).
     - No other characters are allowed.

     Examples of valid usernames: **_Username1234$** and **userName-1234**.

     Examples of invalid usernames: **-Username**, **user/name**, **userName$1234**
   - **Access**: The user access permission for the user: **super**, **read-write**, or **read-only**. For descriptions of these access permissions, see User access levels.
   - **Password/Confirm Password**: Password for the user.
4. Click **Apply**.

Command line

The user command configures users.

1. Configure the username. Usernames can be up to **32** characters long and are case-insensitive. They:
   - Must start with a letter (lowercase or uppercase) or underscore.
   - Can contain letters (lowercase and uppercase), digits, underscore (_), or hyphen (-).
   - Can end with a dollar sign (**$**).
   - No other characters are allowed.

   Examples of valid usernames: **_Username1234$** and **userName-1234**.

   Examples of invalid usernames: **-Username**, **user/name**, **userName$1234**

   For example:

   ```
   digi.router> user 1 name joeuser
   ```
2. Configure the password. For example:

   ```
   digi.router> user 1 password omnivers1031
   ```
3. Optional: Configure the access level. For example:

   ```
   digi.router> user 1 access read-write
   ```
4. Save the configuration.

   ```
   digi.router> save config
   ```

Delete a user

You can delete user definitions when they are no longer needed.

To add, modify, or delete a user, you must be assigned the **super** access level. See User access levels for descriptions of user access levels.

Web

1. Click **Security > Authentication > Local Users**. The User Management page appears.
2. Select the user to delete.
3. Click **Delete** and respond to the confirmation prompt.

Command line

Enter the following command:

```
digi.router> user n name !
```

For example, to delete the user **joeuser** that was previously assigned to **user 1**, enter:

```
digi.router> user 1 name !
digi.router> save config
```

Change a user's password

To add, modify, or delete a user, you must be assigned the **super** access level. See User access levels for descriptions of user access levels.

Web

1. Click **Security > Authentication > Local Users**. The User Management page appears.
2. Select the user.
3. Enter the new password.
4. Confirm the new password.
5. Click **Apply**.

Command line

Enter the user command, specifying the new password value:

```
user <user number> password <password-value>
```

For example:

```
user 6 password tester
```

Firewall management with IP filters

TransPort secures your network by controlling network traffic using a variety of mechanisms, such as Port forwarding (see Port forwarding) and **allow-https-access**/**allow-ssh-access** (see Wide Area Networks (WANs)).

IP filter rules allow you to further control network traffic by allowing and restricting access based on filter criteria.

For example, you can use an IP filter rule to:

- IP filter example: Allow additional traffic into the device
- IP filter example: Restrict access by rejecting traffic from a LAN to a WAN
- IP filter example: Restrict access to an open service
- IP filter example: Restrict access to a router service from LAN devices
- IP filter example: Restrict LAN-to-LAN for all but one service

IP filter source and destination options

Network traffic managed by IP filter rules can be categorized into three groups:

- **Incoming traffic:** Traffic destined to a service or application on the router.
- **Forwarded traffic:** Traffic flowing through the router from one network host to another.
- **Outgoing traffic:** Traffic originating from a service or application on the router.

If you want to create an IP filter rule that applies only to incoming traffic received using the source LAN or WAN, specify only the source option. In this case, incoming network traffic refers only to inbound traffic that is destined for a service on the router, not all traffic flowing through the router destined for another host.

If you want to create an IP filter rule that applies only to traffic flowing through the router received using a source LAN or WAN, specify both the source and destination options. The source and destination values must be different from each other or the rule is not applied.

Infrequently, you may need to create an IP filter rule that applies only to outgoing network traffic sent using the destination LAN or WAN. To do so, specify only the destination option. In this case, outgoing network traffic refers only to outbound traffic sent from a service on the router, not all traffic flowing through the router from another host.

Note Invalid IP filter rules are not applied. To be valid, a rule must include the **Source**, **Destination**, or both the **Source** and **Destination** options. The **Source** and **Destination** options must be different from each other.

Example: Incoming traffic rule

The following rule applies only to incoming traffic received from any configured WAN, regardless of other specified parameters.

Note The destination **None** value is the default and need not be specified.

```
ip-filter 1 src any-wan
ip-filter 1 dst none
```

IP filter criteria options

An IP filter rule applies only to network traffic (packets) matching the following set of filter criteria options:

- Protocol
- Source IP address
- Source IP port
- Destination IP address
- Destination IP port

After determining if the network traffic is incoming, outgoing, or forwarded traffic, the filter criteria are used to examine the network packet. If the packet matches the criteria, the rule action is applied and the packet is accepted, dropped, or rejected.

Example: SSH criteria

The following rule applies only to packets coming from a host with a 10.20.x.y IP address that are for the SSH server. SSH typically uses TCP protocol on port 22. The default values for source IP port and destination IP address are not used because they are not relevant for this filter criteria.

```
ip-filter 1 protocol tcp
ip-filter 1 src-ip-address 10.20.0.0/16
ip-filter 1 dst-ip-port 22
```

IP filter rule priority

IP filter rules are higher priority than port forward rules, the WAN command allowing HTTPS or SSH access, or rules that allow LAN access by default. Therefore, use IP filter rules to further filter traffic by port, IP address, or protocol.

IP filter rules are applied in order from 1 to the maximum number of rules. Use multiple rules to build a more secure environment where some services are allowed, while others are rejected. See IP filter examples.

Add an IP filter rule

Web

To add one or more IP filter rules:

1. On the menu, click **Security > Firewall**:
   - Select **Input IP Filters** to add an input IP filter.
   - Select **Routing IP Filters** to add a routing IP filter.
2. Within the set of rules you want to add, click ✚ (Add Rule) to create a new rule. See Firewall page for field descriptions.
3. When you have finished adding rules, click **Apply**.

Command line

To add an IP filter rule, use the ip-filter command.

For example, to create IP filter rule 3:

```
ip-filter 3 description Allow WAN SNMP only from 10.20 network
ip-filter 3 action accept
ip-filter 3 src any-wan
ip-filter 3 protocol tcp,udp
ip-filter 3 src-ip-address 10.20.0.0/16
```

```
ip-filter 3 dst-ip-port 161,162
ip-filter 3 state on
save config
```

Delete an IP filter rule

Web

To delete one or more IP filter rules:

1. On the menu, click **Security > Firewall**:
   - Select **Input IP Filters** to delete an input IP filter.
   - Select **Routing IP Filters** to delete a routing IP filter.
2. Select the rule you want to remove, and click 🗑.
3. Click **Apply**.

Command line

You cannot delete an IP filter rule using the command line, but you can disable a rule using the ip-filter command.

For example:

```
digi.router> ip-filter 4 state off
digi.router> save config
```

Edit an IP filter rule

Web

To edit an IP filter rule:

1. On the menu, click **Security > Firewall**:
   - Select **Input IP Filters** to edit an input IP filter.
   - Select **Routing IP Filters** to edit a routing IP filter.
2. Select the rule you want to edit and click **Edit Rule**.
3. When you have finished editing the rule, click **Apply**.

Command line

To edit an IP filter rule, use the ip-filter command.

For example, to edit the description for IP filter rule 3:

```
ip-filter 3 description Allow WAN SNMP only from 10.20 network
save config
```

Enable or disable an IP filter rule

Web

To enable or disable an IP filter rule:

1. On the menu, click **Security > Firewall**:
   - Select **Input IP Filters** to edit an input IP filter.
   - Select **Routing IP Filters** to edit a routing IP filter.
2. Select the rule you want to change, and enable or disable the rule.
3. When you have finished, click **Apply**.

Command line

To enable or disable an IP filter rule, use the ip-filter command **state** option.

For example, to enable IP filter 1:

```
digi.router> ip-filter 1 state on
digi.router> save config
```

To disable IP filter 1:

```
digi.router> ip-filter 1 state off
digi.router> save config
```

Show IP filter rules

Web

To show IP filter rules:

1. On the menu, click **Security > Firewall**. The **Firewall** page appears, displaying all configured IP filter rules.
2. Select **Input IP Filters** to view input IP filters and select **Routing IP Filters** to view routing IP filters.

Command line

To show IP filter rules, use the show ip-filter or ip-filter commands.

For example, to show a specific IP filter:

```
digi.router> show ip-filter 1

 IP Filter 1
 -----------
 Description               : Allow WAN SSH only from 10.20 network
 Action                    : Accept
 State                     : On

 Source                    : any-wan
 Destination               : none

 Filter Criteria
 ---------------
 Protocol                  : tcp udp
 Source IP Address         : 10.20.0.0/16
 Source IP Port            : 0
 Destination IP Address    :
 Destination IP Port       : 22
```

```
digi.router> ip-filter 1

  action                      accept
  description                 Allow WAN SSH only from 10.20 network
  dst                         none
  dst-ip-address
  dst-ip-port                 22
  protocol                    tcp,udp
  src                         any-wan
  src-ip-address              10.20.0.0/16
  src-ip-port                 0
  state                       on
```

To show all IP filters:

```
digi.router> show ip-filter

 #   State   Action    Source    Destination  Protocol    Description
 ---------------------------------------------------------------------------------
 1   On      Accept    any-wan   none         tcp udp     Allow WAN SSH only from 10.20 network
 2   On      Drop      any-lan   none         tcp udp     Restrict LAN from HTTP,HTTPS,SSH,SNMP
 3   On      Accept    any-wan   none         tcp udp     Allow WAN SNMP only from 10.20 network
 4   On      Reject    any-lan   any-wan      tcp udp     Restrict LAN to WAN for various email services
 5   On      Accept    lan1      any-lan      tcp         Allow LAN1 SSH to Other LANs
 6   On      Reject    lan1      any-lan      any         Restrict LAN1 from Accessing Other LANs
```

IP filter examples

The following examples show typical ways to use IP filters to control network traffic:

- IP filter example: Allow additional traffic into the device
- IP filter example: Restrict access by rejecting traffic from a LAN to a WAN
- IP filter example: Restrict access to an open service
- IP filter example: Restrict access to a router service from LAN devices
- IP filter example: Restrict LAN-to-LAN for all but one service

IP filter example: Allow additional traffic into the device

The following example shows how to allow SNMP access from a particular subnet on the WAN. Note that by default WAN access does not allow SNMP access.

WARNING! The commands in the following example open up SNMP access to your device. SNMP can be used to configure your device. Before allowing SNMP access, make sure you first secure your SNMP configuration using the snmp, snmp-user and snmp-community commands.

The example demonstrates that IP filter rules can override the default behavior for the firewall. By default, WAN traffic into the TransPort router is dropped if no other configuration or rules explicitly allow traffic in. That is, the default policy for the input chain in the firewall is to **DROP** traffic.

- Adds an IP filter **Accept** rule (the default) to allow incoming traffic on any WAN network additional access.
- Restricts the accepted network traffic so that only traffic from hosts on the 10.20 network to SNMP (ports 161 and 162) is allowed.
- Allows access to multiple protocols (the default). It allows both TCP and UDP access for the SNMP service.

```
digi.router> ip-filter 3 description Allow WAN SNMP only from 10.20 network
digi.router> ip-filter 3 action accept
digi.router> ip-filter 3 src any-wan
digi.router> ip-filter 3 protocol tcp,udp
digi.router> ip-filter 3 src-ip-address 10.20.0.0/16
digi.router> ip-filter 3 dst-ip-port 161,162
digi.router> ip-filter 3 state on
digi.router> save config
```

IP filter example: Restrict access by rejecting traffic from a LAN to a WAN

The following example shows how to restrict LAN devices from accessing services on the WAN (possibly the internet).

WARNING! The commands in the following example could remove your access to the Internet. If you or your users are connected through the LAN to the WAN, using email, the example rule prevents access.

The example demonstrates blocking access from a LAN device to a WAN network. By default, LAN devices are allowed access via the WAN and traffic is forwarded through the router. The example blocks direct mail access to servers on the WAN from LAN devices. Examples like this might be used to prevent access to common services that use a lot of bandwidth or are security risks to the LAN:

- Adds an IP filter **Reject** rule to reject traffic forwarded from any LAN host to any WAN host. The reject rule immediately fails the connection.
- Restricts the rejected traffic to a set of commonly used mail ports.
- Rejects access using multiple protocols (the default). It rejects both TCP and UDP access.

```
digi.router> ip-filter 4 description Restrict LAN to WAN for various email
services
digi.router> ip-filter 4 action reject
digi.router> ip-filter 4 src any-lan
digi.router> ip-filter 4 dst any-wan
digi.router> ip-filter 4 protocol tcp,udp
digi.router> ip-filter 4 dst-ip-port 25,2525,265,587,110,995,143,993
digi.router> ip-filter 4 state on
digi.router> save config
```

IP filter example: Restrict access to an open service

The following example shows how to turn on SSH access for a WAN and restrict SSH access to only a particular subnet of authorized hosts.

WARNING! The commands in the following example could prevent access to your device if connected from the WAN. To safely modify and test ip filter rules, use a scheduled reboot strategy.

The example demonstrates the following:

- Uses the reboot command to schedule a reboot of the device in case of accidental lockout. A scheduled reboot discards any changes that have not been saved and restores access.
- Adds an ip filter **Accept** rule (the default) to allow incoming traffic on any WAN network additional access.

- Restricts the accepted network traffic so that only traffic from hosts on the 10.20 network to SSH (port 22) is allowed.
- Turns off the **allow-ssh-access** option for the two currently configured WAN networks. The **allow-ssh-access** allows SSH access unrestricted by host or network.

```
# Schedule a reboot in 10 minutes in case we lock ourselves out of the device
reboot in 10

# Add the ip filter rule. Be sure to include src-ip-address of at least your
current session (if connected with ssh)
ip-filter 1 description Allow WAN SSH only from 10.20 network
ip-filter 1 action accept
ip-filter 1 src any-wan
ip-filter 1 src-ip-address 10.20.0.0/16
ip-filter 1 dst-ip-port 22
ip-filter 1 state on

# Now turn off allow all ssh access on any WAN where it was turned on previously
wan 1 allow-ssh-access off
wan 2 allow-ssh-access off

# Test the configuration. If all is good, save the configuration and cancel the
reboot before 10 minutes
save config
reboot cancel
```

IP filter example: Restrict access to a router service from LAN devices

The following example shows how to remove HTTP, HTTPS, SSH, SNMP access from a LAN. Note that by default, LAN traffic is allowed.

WARNING! The commands in the following example could prevent access to your device if connected from the LAN. To safely modify and test ip filter rules, use a scheduled reboot strategy.

The example demonstrates the following:

- IP filter rules have a higher precedence (priority) than many system firewall rules. By default for LANs, traffic is allowed into the TransPort router by built-in system firewall rules. This example changes the default allowed access, restricting LAN devices from access.
- Uses the reboot command to schedule a reboot of the device in case of accidental lockout. A scheduled reboot discards any changes that have not been saved and restores access.
- Adds an IP filter **Drop** rule to drop incoming traffic on any LAN network, thereby restricting additional access. A drop rule silently drops traffic, giving no indication to the connecting host.
- Restricts access to multiple protocols (the default) and multiple services (ports) to simplify creation of rules. It blocks both TCP and UDP access for all services even though only the SNMP service (ports 161 or 162) uses UDP.

```
# Schedule a reboot in 10 minutes in case we lock ourselves out of the device
reboot in 10
```

```
# Add the ip filter rule. If you are connected from the LAN using SSH this will
remove your access.
ip-filter 2 description Restrict LAN from HTTP,HTTPS,SSH,SNMP
ip-filter 2 action drop
ip-filter 2 src any-lan
ip-filter 2 protocol tcp,udp
ip-filter 2 dst-ip-port 80,443,22,161,162
ip-filter 2 state on

# Test the configuration. If all is good, save the configuration and cancel the
reboot before 10 minutes
save config
reboot cancel
```

IP filter example: Restrict LAN-to-LAN for all but one service

The following example shows how to restrict devices on LAN 1 (perhaps a public LAN) from communicating with devices on any other LAN (perhaps internal LANs) except for certain services. By default, LAN devices can communicate with other LANs.

On a Wi-Fi LAN, you can also configure client and access point isolation. These rules might typically be used when partial isolation is desirable.

WARNING! The commands in the following example could remove access to services for LAN devices. If you or your users are connected through the LAN, this example may prevent access.

The example demonstrates that multiple IP filter rules have an order precedence. Use multiple IP filter rules to build more complex access control than a single rule could provide:

- Creates two IP filter rules, one at index 5, the other at index 6.
- Rule 5 is an **Accept** rule that allows LAN 1 to access any LAN for the SSH service (port 22). It is executed before rule 6.
- Rule 6 is a **Reject** rule that restricts LAN 1 from accessing any protocol and any port on other LANs. It is executed after rule 5.

```
digi.router> ip-filter 5 description Allow LAN1 SSH to Other LANs
digi.router> ip-filter 5 action accept
digi.router> ip-filter 5 src lan1
digi.router> ip-filter 5 dst any-lan
digi.router> ip-filter 5 protocol tcp
digi.router> ip-filter 5 dst-ip-port 22
digi.router> ip-filter 5 state on

digi.router> ip-filter 6 description Restrict LAN1 from Accessing Other LANs
digi.router> ip-filter 6 action Reject
digi.router> ip-filter 6 src lan1
digi.router> ip-filter 6 dst any-lan
digi.router> ip-filter 6 protocol any
digi.router> ip-filter 6 state on
digi.router> save config
```

Certificate and key management

This section covers concepts and tasks for managing certificates and private keys.

Create a private key file

Command line

To create a private key file, use the pki command. For example:

```
digi.router> pki privkey testpriv.key 204
```

You can optionally encrypt the file using either the aes128 or aes256 options. If you choose to encrypt the file, you must provide a password that must be at least four characters in length. For example:

```
digi.router> pki privkey testpriv.key 2048 aes128 hello
```

Create a Diffie Hellman key file

Command line

To create a Diffie Hellman key file, use the pki command. For example:

```
digi.router> pki dh-file openvpndh.pem 2048

Creating Diffie Hellman file openvpndh.pem, 2048 bits
```

Note Generating a Diffie Hellman file can take up to 40 minutes. Make sure the default for command line timeout allows enough time to generate the file or the command will terminate. See the system **timeout** parameter for details on changing the command line timeout default.

List private key files

Command line

To list private key files, use the pki command. For example:

```
digi.router> pki list

Private key files
------------------------
tespriv.key
anotherpriv.key
```

Upload a private key file

Command line

To upload an externally-generated private key file from the upload folder to the list of private key files, use the pki command. For example:

```
digi.router> pki addkey mykeyfile.key
```

Delete a private key file

Command line

To delete a private key file, use the pki command. For example:

```
digi.router> pki list


Private key files
------------------------
testpriv.key
anotherpriv.key

digi.router> del testpriv.key
```

Create a certificate signing request (CSR)

Command line

To create a private key file, use the pki command. For example:

Note To show all **pki csr** command option settings within the page margin, the example shows the settings on multiple lines. However, TransPort does not allow you to continue a command line—the example is for display only.

```
digi.router> pki csr country GB state "North Yorkshire" locality Richmond
organization Digi organizational-unit "Digi Engineering" common-name www.example.com
testpriv.key testpriv.csr sha256


Country Name (letter code): GB
State or Province Name: North Yorkshire
Locality Name: Richmond

Organization Name: Digi
Organization Unit Name: Digi Engineering
Common Name: www.example.com
Email address:


testpriv.csr has been created
```

Remote Authentication Dial-In User Service (RADIUS)

TransPort supports Remote Authentication Dial-In User Service (RADIUS), a networking protocol that provides centralized authentication and authorization management for users who connect to the device.

With RADIUS support, the TransPort acts as a RADIUS client, which sends user credentials and connection parameters to a RADIUS server over UDP. The RADIUS server then authenticates the RADIUS client requests and sends back a response message to the TransPort.

When you are using RADIUS authentication, you can have both local users and RADIUS users able to log in to the device.

Note All TransPort usernames—RADIUS usernames and local usernames—must be unique. If a RADIUS user has the same username as a local user, the RADIUS user cannot log in.

Set up a RADIUS server

To use RADIUS authentication, you must set up a RADIUS server accessible by the TransPort prior to configuration. The process of setting up a RADIUS server varies by the server environment. An example of a RADIUS server is freeRADIUS and a quick-start guide for setting up a freeRADIUS server is here: http://wiki.freeradius.org/guide/Getting%20Started.

Set up a RADIUS backup server

TransPort also supports the use of a backup RADIUS server to which authentication requests are automatically sent when the primary RADIUS server is unavailable.

If both the primary and backup RADIUS servers are unavailable, the **local-auth** configuration can be used to fall back to local TransPort authentication. If the RADIUS servers are unavailable and the TransPort falls back to local authentication, only local device users are able to log in. In other words, after a fall-back event, RADIUS users cannot log in until the RADIUS servers are brought back up.

Use the local-auth parameter

The **local-auth** parameter configures how the TransPort behaves when all configured RADIUS servers are unavailable. In most situations, Digi recommends you enable **local-auth.** In this way, when the RADIUS servers are unavailable for any reason, local users can log in to the TransPort and configure other available servers.

If the RADIUS servers become unavailable and **local-auth** is disabled, no users can log in to the TransPort. Also, even if **local-auth** is disabled, no RADIUS user may have the same username as a user defined locally. If a RADIUS user has the same username as a local user, the RADIUS user cannot log in.

The table below shows how the primary RADIUS server, the backup RADIUS server, and local authorization work together.

Primary server available	Backup server available	Local authorization	Who can log in?
Yes	No	N/A	RADIUS and local users can log in.
No	Yes	N/A	RADIUS and local users can log in.

Primary server available	Backup server available	Local authorization	Who can log in?
No	No	Enabled	Only local users can log in. RADIUS users cannot log in until the RADIUS servers are brought back up.
No	No	Disabled	No users can log in.

Configure a RADIUS server

This section describes how to configure a RADIUS server for authentication and authorization.

Required configuration items

- Enable the RADIUS server. It is disabled by default.
- Define the primary server IP address or domain name.
- Define the primary server port. It is configured to 1812 by default.
- Define the primary server shared secret.
- Determine whether local authentication is used if a RADIUS server is unavailable. It is enabled by default.

Additional configuration options

- The server NAS ID. If left blank, the default value of **sshd** is sent out.
- Time in seconds before the request to the server times out. The default is 3 seconds and the maximum possible value is 10 seconds.
- Enable debug logging. It is disabled by default.
- Add a backup server in case the primary RADIUS server is unavailable. Configuration items similar to the primary RADIUS server are also available for the backup RADIUS server.

Web

1. On the menu, click **Security > RADIUS**. The RADIUS page appears.
2. Under the **Settings** section, enable the RADIUS-based authentication feature and configure the basic settings:
    a. Click **Enable** to turn RADIUS based authentication on.
    b. In the **NAS ID** field, enter a NAS ID for the TransPort. This attribute contains a string identifying the NAS originating the request to the RADIUS server. If the field is left blank, the default value of **sshd** is sent out.
    c. Click **Local Auth Fallback** to enable authentication of local TransPort users when the primary and backup RADIUS servers are unavailable.
    d. Click **Debug** to log RADIUS debug messages to the TransPort log. This is optional.
3. Under the **Primary Server Settings** section, configure the primary RADIUS server. See RADIUS page for detailed information.

4. If using a backup server, under the **Backup Server Settings** section, configure the backup RADIUS server. Configuring a backup server is optional. See RADIUS page for detailed information.
5. Click **Apply** to save the changes.

Command line

1. Set the RADIUS server IP address or FQDN:

```
digi.router> radius server 192.168.10.1
```

2. Set the RADIUS server port:

```
digi.router> radius server-port 1812
```

3. Set the RADIUS server secret:

```
digi.router> radius server-secret thisisasecret
```

4. (Optional) Set the RADIUS server nas-id:

```
digi.router> radius nas-id 123
```

5. (Optional) Establish whether using the local authentication fallback feature is desired:

```
digi.router> radius local-auth on
```

6. (Optional) Set the RADIUS server timeout:

```
digi.router> radius server-timeout 10
```

7. (Optional) Turn on debug logging:

```
digi.router> radius debug on
```

8. (Optional) Set a backup server IP address or domain name:

```
digi.router> radius backup-server radius.ny.domain
```

9. (Optional) Set a backup server port:

```
digi.router> radius backup-server-port 1813
```

10. (Optional) Set a backup server secret:

```
digi.router> radius backup-server-secret thisisthebackupsecret
```

11. (Optional) Set a backup server timeout:

```
digi.router> radius backup-server-timeout 10
```

12. Turn on the RADIUS server authentication:

```
digi.router> radius state on
```

13. Save the configuration:

```
digi.router> save config
```

Services and applications

These topics describe the network services and configurable aspects of running application programs on TransPort devices.

- Auto-run commands
- About Python support
- Port forwarding
- Using an SSH server

Auto-run commands

Auto-run commands are commands that are automatically run at boot-up. You can use auto-run commands for such tasks as:

- Starting a Python program
- Switching between configuration files
- Scheduling a reboot

The TransPort supports up to **10** auto-run commands. See autorun for details.

Required configuration items

Configure the command that is to be automatically run at boot up. See Use multiple configuration files to test configurations on remote devices for an example of using autorun commands to safely test configurations on a remote device.

Example: Update the configuration from file config.da0

```
autorun 1 command “update config config.da0”
```

Example: Run a timed reboot

```
autorun 2 command “reboot in 5”
```

About Python support

TransPort supports Python 3.6 and provides you with the ability to run Python applications on the device interactively or from a file. You can also specify Python programs to be run each time the TransPort starts up.

The following commands provide Python support:

- python
- python-autostart
- show python

Python version

Python 3.6

Uploading Python application files

To upload Python application files to your TransPort, use the File system page. See File system for details.

WARNING! If your Python application repeatedly writes to files or logs, it can cause excessive wear on the LR54 flash memory. Digi recommends keeping frequently-modified data in memory and writing to files only when required.

Run a Python application interactively

Command line

Use the python command to run a Python application interactively in the current CLI session. The Python application runs until it exits, displaying output and prompting for additional user input if needed. If you want to interrupt the application, enter **CTRL-C** or use the **python stop** command.

For example, the following command:

```
python health.py 120 ports storage
```

Runs the **health.py** application and passes three parameters to the application: **120**, **ports**, and **storage**.

Run an interactive Python session

Command line

Use the python command without specifying any parameters to start an interactive Python session. The Python session operates interactively using REPL (Read Evaluate Print Loop) to allow you to write Python code on the command line.

Configure Python application to autostart

Command line

Use the python-autostart command to specify a Python application to be run each time the TransPort starts up.

Here are some examples of the python-autostart command:

```
python-autostart 3 filepath "health.py"
python-autostart 3 args "120 ports storage"
python-autostart 3 on-exit "reboot"
python-autostart 3 state "on"

python-autostart 4 filepath "scripts/python/traffic.py"
python-autostart 4 args "300 --quiet"
python-autostart 4 on-exit "restart"
python-autostart 4 state "on"
```

Show running Python applications

Command line

Use the show python to list Python applications currently running on your TransPort.

For example:

```
digi.router> show python

 ID       File Name                            Arguments

 --------------------------------------------------------------------
 4990     health.py                            120 ports storage

 4993     scripts/python/traffic.py            300 --quiet

 6322     (interactive)
```

Stop a Python application

Command line

Use the python command **stop** parameter to stop a running Python application.

To stop an application:

1. Determine the Python application ID using the show python command.
2. Enter **python stop** command and provide the Python application ID.

For example:

```
digi.router > show python

ID             File Name                       Arguments
------------------------------------------------------------------------
4990           health.py                       120 ports storage
4993           scripts/python/traffic.py       300 --quiet


digi.router > python stop 4990
```

If you stop a Python application initiated by the python-autostart application, the application ends without executing the application **on-exit** action. That is, the application ends without causing a device reboot or application restart.

Get help for Python programming

You can use the following Digi tools to assist in Python programming for a TransPort:

- digidevice.cli module
- Help for executing CLI commands
- digidevice.datapoint module
- Help for uploading datapoints

digidevice.cli module

Command line

Use the **digidevice.cli** module to execute CLI commands and retrieve command output.

```
digi.router> python

Python 3.6.1
>>> from digidevice import cli
>>> print(cli.execute("show python"))

 ID       File Name                          Arguments

 -------------------------------------------------------------------------
 3141     scripts/python/traffic.py          300 --quiet

 4990     health.py                          120 ports storage

 5451     (interactive)
```

Help for executing CLI commands

Command line

Get help executing a CLI command by accessing help for **cli.execute**. For example:

```
digi.router> python

Python 3.6.1
>>> from digidevice import datapoint
>>> from digidevice import cli
>>> help(cli.execute)
Help on function execute in module digidevice.cli:
.
.
.
```

digidevice.datapoint module

Command line

Use the **digidevice.datapoint** module to upload data points to Digi Remote Manager. The Remote Manager connection must be enabled and connected. See Remote management and the cloud command for details.

```
digi.router> python

Python 3.6.1
>>> from digidevice import datapoint
>>> datapoint.upload('test/stream/one', 42)
>>>
```

Help for uploading datapoints

Command line

Get help for uploading datapoints to your TransPort by accessing help for **datapoint.upload**. For example:

```
digi.router> python

Python 3.6.1
>>> from digidevice import datapoint
>>> from digidevice import cli

>>> help(datapoint.upload)
Help on function upload in module digidevice.datapoint:
```

Port forwarding

Most computers connected to a router are protected by a firewall that prevents users on a public network from accessing servers on the private network. To allow a computer on the Internet to connect to a specific server on a private network, set up one or more port forwarding rules. Each port forwarding rule automatically maps and forwards an external request for a port on a WAN to an IP address and port on an internal LAN.

For a port forwarding rule to be applied, you must configure **From Port** and **To IP Address**, and set the rule to **Enabled**. Incomplete and incorrect port forwarding rules are not applied. You can configure a maximum of 30 port forwarding rules.

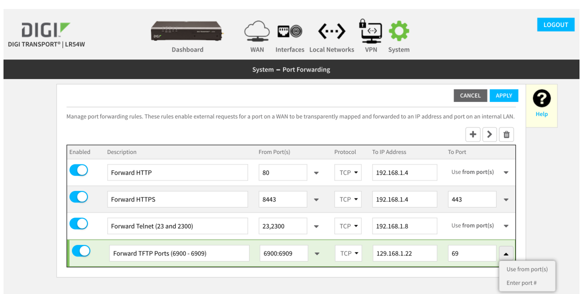
Add a port forwarding rule

Web

To add one or more port forwarding rules:

1. On the menu, click **Network > Services > Port Forwarding**. The **Port Forwarding** page appears.
2. Click **+** (Add Rule) to create a new rule. See Port forwarding page for field descriptions.
   For a port forwarding rule to be applied, you must configure **From Port** and **To IP Address**, and set the rule to **Enabled**. Incomplete and incorrect port forwarding rules are not applied.
3. When you have finished adding rules, click **Apply**.

Here's a sample of port forwarding rules:



Command line

To add a port forwarding rule, use the port-forward command.

For a port forwarding rule to be applied, you must configure **port** and **to-ip-address**, and set the **state** of the rule to **on** (the default state). Incomplete and incorrect port forwarding rules are not applied.

For example:

```
digi.router> port-forward 4 port 80
digi.router> port-forward 4 to-ip-address 192.168.47.1
digi.router> port-forward 4 state on
digi.router> save config
```

Delete a port forwarding rule

Web

To delete one or more port forwarding rules:

1. On the menu, click **Network > Services > Port Forwarding**. The **Port Forwarding** page appears.
2. Select the rule you want to remove, and click 🗑.
3. Click **Apply**.

Command line

You cannot delete a port forwarding rule using the command line, but you can disable a port forwarding rule using the port-forward command.

For example:

```
digi.router> port-forward 4 state off
digi.router> save config
```

Enable or disable a port forwarding rule

Web

To enable or disable a port forwarding rule:

1. On the menu, click **Network > Services > Port Forwarding**. The **Port Forwarding** page appears.
2. For each rule, use the slider on the **Enabled** field to enable or disable the rule as needed.
3. Click **Apply**.

Command line

To enable or disable a port forwarding rule, use the port-forward **state** parameter.

For example, to enable port forwarding rule 4:

```
digi.router> port-forward 4 state on
digi.router> save config
```

To disable port forwarding rule 4:

```
digi.router> port-forward 4 state off
digi.router> save config
```

Show port forwarding rules

Web

To show port forwarding rules:

- On the menu, click **Network > Services > Port Forwarding**. The **Port Forwarding** page appears. See Port forwarding page for field descriptions.

Command line

To show port forwarding rules, use the show port-forward command.

For example:

```
digi.router> show port-forward
```

Using an SSH server

TransPort devices have a Secure Shell (SSH) server for managing the device through the command-line interface over a SSH connection. Only the SSHv2 protocol is supported; earlier versions of SSH protocol are no longer considered secure.

Configure a Secure Shell (SSH) server

Command line

1. Enable the SSH server.

```
digi.router> ssh state on
```

2. Optional: Configure the port number for the SSH server.

```
digi.router> ssh port 50684
```

3. Save the configuration.

```
digi.router> save config
```

Use SSH to connect to the TransPort command-line interface

You can make SSH connections using utilities such as PuTTY, TeraTerm, or the Linux **ssh** command.

Command line

The following example shows how to use the Linux **ssh** command to connect to IP address **192.168.1.1** for the first time using the **admin** user account.

```
$ ssh admin@192.168.1.1
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be established.
RSA key fingerprint is 2c:db:01:65:2f:bb:a3:4f:c0:5e:dd:2d:e7:9f:7d:01.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.1' (RSA) to the list of known hosts.
Password: **********

Welcome admin
Access Level: super
Timeout     : 180 seconds
digi.router>
```

Terminate an SSH connection

Command line

To terminate an SSH connection:

- Exit the command-line interface using the exit command.

Remote management

These topics cover using remote management facilities to manage TransPort devices.

- Remote Manager
- Using Simple Network Management Protocol (SNMP)

Remote Manager

Digi Remote Manager® is a hosted remote configuration and management system that allows you to remotely manage a large number of devices. Digi Remote Manager has a web-based interface from which you can perform device operations, such as viewing and changing device configurations and perform firmware updates.

The Digi Remote Manager servers also provide a data storage facility.

Using Digi Remote Manager requires setting up a Digi Remote Manager account. To set up a Digi Remote Manager account and learn more about Digi Remote Manager, go to www.digi.com/products/cloud/digi-remote-manager.

To learn more about Digi Remote Manager features and functions, see the Digi Remote Manager User Guide.

Configure Digi Remote Manager

Digi Remote Manager is enabled by default. Once the TransPort device has a WAN connection, it automatically connects to Digi Remote Manager.

Additional configuration options

These additional configuration settings are not typically configured, but you can set them as needed:

- You can disable the Digi Remote Manager connection if it is not required.
- You can change the reconnection timer. By default, the device attempts to connect to Digi Remote Manager every **30** seconds.
- The non-cellular keepalive timeout. By default, the device will send a keepalive message to Digi Remote Manager and expect a keepalive message every **60** seconds when using a non-cellular WAN interface. You can change the non-cellular keepalive timeout value depending on your WAN characteristics.
- The cellular keepalive timeout. By default, the device will send a keepalive message to Digi Remote Manager and expect a keepalive message every **290** seconds when using a cellular WAN interface. You can change the cellular keepalive timeout length depending on your cellular interface characteristics.
- The keepalive count before the Remote Manager connection is dropped. By default, the device disconnects and attempts to reconnect to Remote Manager after **3** missed keepalive messages.

Web

Register device in Digi Remote Manager

- **If you have already registered your device**:

  If you have registered your device with Digi Remote Manager when you went through the

Getting Started Wizard:

1. Enter your credentials to log in to your Remote Manager account and click **Log In**.
2. A message appears showing the group into which your device has been registered in the **Remote Manager Status** section of the Digi Remote Manager page.

- **If you have not already registered the device**:
  1. On the menu, click **System > Administration > Remote Manager**. The **Digi Remote Manager** page appears.
  2. Enter your credentials to log in to your Digi Remote Manager account and click **Log In**.
  3. Select a group for you device in your Digi Remote Manager account, then click **Register Device**.
  4. If the registration succeeds, a message appears indicating that your device has been registered in your Digi Remote Manager account; for example:

```
This device is registered in your Digi Remote Manager account
Group location: Group C
```

Optional: Modify Digi Remote Manager settings

1. On the menu, click **System > Administration > Remote Manager**.
2. Enter the settings.
   - Enable or disable the TransPort device connection to Digi Remote Manager.
   - **Ethernet Keepalive**: The interval between sending keepalives to Digi Remote Manager over Ethernet interfaces.
   - **Cellular Keepalive**: The interval between sending keepalives to Digi Remote Manager over cellular interfaces.
   - **Reconnect Delay**: The reconnection timer for reconnecting to Digi Remote Manager after a disconnect. By default, the device attempts to connect to Digi Remote Manager every **30** seconds.
3. Click **Apply**.

Command line

- Disable the Digi Remote Manager connection.

```
digi.router> cloud state off
digi.router> save config
```

- Set the reconnect timer. For example, to set it to **60** seconds:

```
digi.router> cloud reconnect 60
digi.router> save config
```

- Set the non-cellular keepalive time. For example , to set it to **180** seconds:

```
digi.router> cloud keepalive 180
digi.router> save config
```

- Set the cellular keepalive time. For example, to set it to **600** seconds:

```
digi.router> cloud keepalive-cellular 600
digi.router> save config
```

- Set the keepalive count. For example, to set it to **5**:

```
digi.router> cloud keepalive-count 5
digi.router> save config
```

Show Digi Remote Manager connection status

Web

- On the menu, click **System > Administration > Remote Manager**.

The **Digi Remote Manager** page shows whether your device is connected to Digi Remote Manager, as well as device connection statistics.

Command line

To show the status of the Digi Remote Manager connection, use the show cloud command.

In the show cloud command output, the device ID is the unique identifier for the device on the Digi Remote Manager.

For example:

```
digi.router> show cloud

 Device Cloud Status
 -------------------

 Status    : Connected
 Server    : my.devicecloud.com
 Device ID : 00000000-00000000-0040FFFF-FF0F4594

 Uptime    : 1 Minute, 9 Seconds

            Received                      Sent
            --------                      ----
 Packets          13                        14
 Bytes            37                       218

digi.router>
```

Enable health reporting

You can enable the gathering of health metrics information for your device. Before enabling health reporting, make sure you first register your device with Digi Remote Manager. For instructions, see Configure Digi Remote Manager.

Web

1. From the menu, click **System > Remote Manager**.
2. Click **Open Remote Manager**.
3. Go to **Configuration > Remote Manager** page.
4. For the **Enable or disable health reporting** option, select **On**.
5. Click **Save** to save the configuration.

Command line

- Turn on health reporting for Digi Remote Manager:

```
digi.router> cloud health on
digi.router> save config
```

Using Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) is a protocol for remotely managing and monitoring network devices. Network administrators can use the SNMP architecture to manage nodes, including servers, workstations, routers, switches, hubs, and other equipment on an IP network, manage network performance, find and solve network problems, and plan for network growth.

Supported SNMP versions

TransPort devices support the SNMP versions **SNMPv1**, **SNMPv2c**, and **SNMPv3**.

The device supports up to **10** SNMPv1/SNMPv2c communities. Each community can have read-only or read-write access.

The device supports up to **10** SNMPv3 users. You can configure each user's access level as read-only or read-write, and configure security settings on an individual-user basis.

Supported Management Information Bases (MIBs)

TransPort devices support the following SNMP MIBs for managing the entities in a communication network:

- Standard SNMP MIBs
- An enterprise-specific MIB for the LR54, named **transport-lr54.mib**. This MIB is available for download from Digi Support.

Note You cannot use SNMPv1 with the Enterprise MIB because of the **COUNTER64** types used in the Enterprise MIB.

Configure SNMPv1 and SNMPv2

Command line

1. All SNMP versions are disabled by default. To enable support for SNMPv1 or SNMPv2c, enter:

```
digi.router> snmp v1 on
```

OR

```
digi.router> snmp v2c on
```

2. If using SNMPv1/v2c communities, configure a name for each community. For example:

```
digi.router> snmp-community 1 community public
```

3. The community access level defaults to **read-only**. To set the access level to **read-write**, enter:

```
digi.router> snmp-community 1 access read-write
```

4. Save the configuration.

```
digi.router> save config
```

Configure SNMPv3

Command line

1. All SNMP versions are disabled by default. To enable support for SNMPv3, enter:

```
digi.router> snmp v3 on
```

2. For each SNMPv3 user, give the user a name of up to **32** characters:

```
digi.router> snmp-user 1 user joe
```

3. Set the authentication type for the SNMPv3 user (**none**, **md5**, or **sha1**). To use privacy (DES or AES), the authentication type be either **md5** or **sha1**.

```
digi.router> snmp-user 1 authentication sha1
```

4. Set the authentication password for the SNMPv3 user. The password length can be between **8** and **64** characters.

```
digi.router> snmp-user 1 authentication-password authpassword
```

5. Set the privacy type for the SNMPv3 user (**none**, **aes**, or **des**):

```
digi.router> snmp-user 1 privacy des
```

6. Set the privacy password for the SNMPv3 user. The password length can be between **8** and **64** characters.

```
digi.router> snmp-user 1 privacy-password privpassword
```

7. Configure the access level for the SNMPv3 user.

```
digi.router> snmp-user 1 access read-write
```

8. Save the configuration.

```
digi.router> save config
```

Routing

This topic area covers configuring and managing routes for TransPort devices.

- IP routing
- Dynamic Mobile Network Routing (DMNR)
- Quality of Service (QoS)

IP routing

The TransPort device uses IP routes to decide where to send a packet it receives for a remote network. The process for deciding on a route to send the packet is as follows:

1. The device examines the destination IP address in the IP packet, and looks through the IP routing table to find a match for it.
2. If it finds a route for the destination, it forwards the IP packet to the configured IP gateway or interface.
3. If it cannot find a route for the destination, it uses a default route.
4. If there are two or more routes to a destination, the device uses the route with the longest mask.
5. If there are two or more routes to a destination with the same mask, the device uses the route with the lowest metric.

Configure general IP settings

Configuring general IP settings is one of the building blocks of setting up IP routing.

Optional configuration settings

- The IP hostname. This hostname identifies the TLR device on IP networks. It is an unqualified hostname. The default setting for the device is **LR54-%s** which expands to **LR54-<serial number>**.
- The administrative distance settings for connected and static routes. Administrative distance settings rank the type of routes, from the most to least preferred. When there are two or more routes to the same destination and mask, the route with the lowest metric is used. By default, routes to connected networks are preferred, with static routes being next. The administrative distance for each route type is added to the route's metric when it is added to the routing table. Configuring the administrative distance of a particular route type can alter the order of use for the routes. The two administrative distance settings are:
  - Administrative distance for connected network routes. The default value is **0**.
  - Administrative distance for static routes. The default value is **1**.

Web

In the web interface, general IP settings are configured as part of configuring a LAN or WAN. See Configure a LAN and Configure a Wide Area Network (WAN).

Command line

1. Set the hostname.

```
digi.router> ip hostname LR54-NewYork
```

2. Set the administrative distance for connected routes.

```
digi.router> ip admin-conn 3
```

3. Set the administrative distance for static routes.

```
digi.router> ip admin-static 5
```

4. Save the configuration.

```
digi.router> save config
```

Configure a static route

A static route is a manually configured routing entry. Information about the route is manually entered rather than obtained from dynamic routing traffic. TransPort devices supports up to **32** static routes.

Required configuration settings

- Setting the destination network and mask.
- Setting the gateway IP address for routes using LAN and WAN Ethernet interfaces. The gateway IP address should be on the same subnet as the IP address of the LAN or WAN Ethernet interface in use.
- Setting the interface name for routes using cellular interfaces.

Optional configuration settings

- Setting the metric for the route. The metric defines the order in which routes should be used if there are two routes to the same destination. In such a case, the smaller metric is used.

Command line

Use the route command to configure IP routes.

Example 1

To configure a static route to the **192.168.47.0/24** network using the **lan1** interface, which has an IP address of **192.168.1.1** and a gateway at IP address of **192.168.1.254**:

1. Set the destination network and mask.

```
digi.router> route 1 destination 192.168.47.0
digi.router> route 1 mask 255.255.255.0
```

2. Set the gateway IP address.

```
digi.router> route 1 gateway 192.168.1.254
```

3. Save the configuration.

```
digi.router> save config
```

Example 2

To configure a static route to the **44.1.0.0/16** network using the **cellular1** interface:

1. Set the destination network and mask.

```
digi.router> route 4 destination 44.1.0.0
digi.router> route 4 mask 255.255.0.0
```

2. Set the interface.

```
digi.router> route 4 interface cellular1
```

3. Optional: Set the metric.

```
digi.router> route 4 metric 5
```

4. Save the configuration.

```
digi.router> save config
```

Once the static route is configured, it should appear in the IPv4 routing table, which you can display using the show route command.

Show the IPv4 routing table

Command line

To display the IPv4 routing table, use the show route command.

```
digi.router> show route

 Destination          Gateway          Metric    Protocol     Idx       Interface Status
 -----------------------------------------------------------------------------------------
 10.1.2.0/24          192.168.1.254    1         Static       1         lan1      UP
 192.168.1.0/24       0.0.0.0          0         Connected              lan1      UP
 default              0.0.0.0          1         Connected              eth1      UP
 default              0.0.0.0          2         Connected              cellular1 UP

digi.router>
```

Delete a static route

Command line

To remove a static route from the routing table, clear the destination network configuration.

To revert the settings for the route destination, enter the route command, specifying the interface number, the destination parameter, and the exclamation mark (**!**) character. For example:

```
digi.router> route 1 destination !
digi.router> save config
```

Dynamic DNS

The Domain Name System (DNS) uses name servers to provide a mapping between computer-readable IP addresses and human-readable hostnames. This allows users to access websites and personal networks with easy-to-remember URLs. Unfortunately, IP addresses change frequently, invalidating these mappings when they do. Dynamic DNS has become the standard method of addressing this problem, allowing devices to update name servers with their new IP addresses.

By providing the TransPort LR devices with the hostname, service, and credentials obtained from a dynamic DNS provider, the router can automatically update the remote nameserver whenever your WAN or public IP address changes.

The TransPort LR supports the following Dynamic DNS providers:

- DynDNS https://dyn.com/
- No-IP https://www.noip.com/
- DNS-O-Matic https://www.dnsomatic.com/
- ChangeIP https://www.changeip.com/

Configure dynamic DNS

This section describes how to cofigure dynamic DNS on a TransPort LR device. For details on dynamic DNS, see Dynamic DNS

Required configuration items

Enable Dynamic DNS

- Service: Provide the name of a Dynamic DNS provider (for example, dyndns, dnsomatic, noip, changeip).
- Username: Provide username to be used to authenticate with your Dynamic DNS provider.
- Password: Provide the password corresponding to the username provided above.
- Hostname: Provide the URL for your Dynamic DNS provider, which will be linked to your IP address.

Additional configuration items

- ip-monitoring: Use this option to determine which IP address to monitor for changes. If you select WAN, the TransPort monitors the IP address of WAN interfaces. If you select Public, the TransPort monitors the public-facing IP address, regardless of the IP address of the WAN interface.

Command line

1. Set the dynamic DNS service:

```
digi.router> dynamic-dns service dyndns
```

2. Set the username and password for the dynamic DNS service:

```
digi.router> dynamic-dns username yourusername
digi.router> dynamic-dns password yourpassword
```

3. Set the hostname to update when your IP address changes:

```
digi.router> dynamic-dns hostname your.dynamicdns.hostname
```

4. Optional: Set ip-monitoring type for dynamic DNS:

```
digi.router> dynamic-dns ip-monitoring public
```

5. Enable Dynamic DNS:

```
digi.router> dynamic-dns state on
```

6. Save the configuration.

```
digi.router> save config
```

Web filtering (OpenDNS)

Web filtering allows you to control access to services that can be accessed through the TransPort device.

It does this by forwarding all Domain Name System (DNS) traffic to a web filtering service. This allows the network security administrator to configure a set of policies with the web filtering service that are applied to all routers with web filtering enabled. For example, a policy may allow or deny access to a specific service or type of service such as social media, gaming, and so on.

TransPort supports Cisco Umbrella (formally known as OpenDNS). For more information, see https://umbrella.cisco.com.

Configure web filtering using Cisco Umbrella

This section describes how to configure the web filter on a TransPort device using the Cisco Umbrella service.

To use Cisco Umbrella with your device, you must obtain an API token. For instructions on how to do this, see Cisco-Umbrella-Network-Device-Integrations.

CAUTION! Due to recent changes in Cisco Umbrella, if you have a legacy token generated prior to December 7, 2017, you cannot use the token with a TransPort device. Regenerate a token from your Umbrella console.

Once you have completed your Cisco Umbrella configuration, you can verify that your setup is working by following the steps outlined in How-to-test-for-successful-OpenDNS-configuration.

Required configuration items

- Set web filter customer-specific token.
- Enable web filter.

Command line

1. Set the web filter token:

```
digi.router> web-filter token <your_client_token>
```

2. Enable the web filter:

```
digi.router> web-filter state on
```

3. Save the configuration.

```
digi.router> save config
```

Clear device ID

If the device ID on your TransPort appears to be invalid, you can clear the device ID by using the clear **web-filter-id** command.

Command line

Clear the web filter ID:

```
digi.router> clear web-filter-id
```

Dynamic Mobile Network Routing (DMNR)

The Verizon Dynamic Mobile Network Routing (DMNR), based on the Network Mobility (NEMO) protocol, provides dynamic routing support for mobile or stationary routers using IPv4 addressing.

- Configure Verizon DMNR
- Show DMNR status

Configure Verizon DMNR

Web

1. On the menu, click **Network > Services > DMNR**. The **DMNR** page appears.
2. Provide DMNR configuration options. See DMNR page for field descriptions.
3. Click **Apply**.

Command line

To configure DMNR, use the dmnr command. For example:

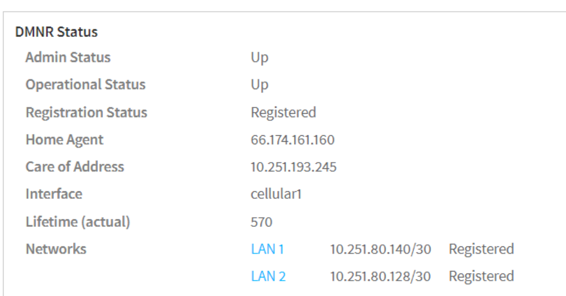
```
digi.router> dmnr home-agent 10.20.70.64
digi.router> dmnr local-networks lan2
digi.router> dmnr state on
digi.router> save config
digi.router>
```

Show DMNR status

Web

- On the menu, click **Network > Services > DMNR**. The **DMNR** page appears.

DMNR status appears in the right side of the display.



DMNR Status			
Admin Status	Up		
Operational Status	Up		
Registration Status	Registered		
Home Agent	66.174.161.160		
Care of Address	10.251.193.245		
Interface	cellular1		
Lifetime (actual)	570		
Networks	LAN 1	10.251.80.140/30	Registered
	LAN 2	10.251.80.128/30	Registered

Command line

To show DMNR status, use the show dmnr command. For example:

```
digi.router> show dmnr

DMNR Status
-----------

Admin Status          : Up
```

```
Operational Status   : Up
Registration Status  : Registered
Home Agent           : 66.174.161.160
Care of Address      : 10.251.193.245
Interface            : cellular1
Lifetime (actual)    : 570

       Local Network      Subnet              Status

       -------------      ------              -------

       lan1               10.251.80.140/30    Registered
       lan2               10.251.80.128/30    Registered


digi.router>
```

Quality of Service (QoS)

TransPort Quality of Service (QoS) queues and filters allow you to identify and prioritize traffic, as well as restrict bandwidth for a given queue.

You can categorize and prioritize traffic using QoS queues. Traffic associated with lower-numbered queues is given higher priority than traffic associated with higher-numbered queues, although there are exceptions depending on how you have configured bandwidth restrictions for the queues.

Each queue has one or more QoS filters used to identify traffic associated with the queue. As traffic flows through the router destined for a QoS-enabled WAN, it is associated with a queue based on QoS filter criteria. Once traffic is associated with a queue, it is prioritized and delivered according to the configured queue parameters.

This section describes how to enable QoS on one or more configured WANs and configure QoS queues and filters.

Configure QoS

Configuring QoS consists of the following:

- Enabling a configured WAN for QoS.
- Configuring from one to eight QoS queues using the eight tabs in the Queues panel. Queue 1 has the highest priority; queue 2 has second-highest priority, queue 3 has third-highest priority, and so on up to queue 8 which has the lowest priority.
- Configuring filters for each configured queue to force traffic to the queue. You can configure up to 32 filters.

Web

1. On the menu, click **Network > Services > QoS**. The **QoS** page appears.
2. Enable QoS on a configured WAN:
    a. In the WANs configuration panel, enable or disable one or more configured WANs. See Quality of Service (QoS) WANs page for field descriptions.
    b. Click **Apply**.

3. Create QoS queues:
    a. In the **Queues configuration** panel, configure from one to eight QoS queues. See Quality of Service (QoS) queues page for field descriptions.
    b. When you have finished configuring queues, click **Apply**.
4. Create filters for each configured queue:
    a. In the **Queues configuration** panel, scroll to the **Filters** section. See Quality of Service (QoS) queues page for field descriptions.
    b. Add one or more filters for each configured queue. You can configure a total of 32 filters for all queues.
    c. When you have finished configuring filters, click **Apply**.

Command line

- To enable QoS on a configured WAN, use the wan command. For example, to enable QoS on WAN 3 and set the bandwidth upstream to 8000 kbps:

```
digi.router> wan 3 qos on
digi.router> wan 3 bandwidth-upstream 8000
digi.router> save config
```

- To configure one or more QoS queues use the qos-queue command. For example:

```
digi.router> qos-queue 1 description myhighqosqueue
digi.router> qos-queue 1 borrow-upstream on
digi.router> qos-queue 1 dscp-class be
digi.router> qos-queue 1 state on
digi.router> save config
digi.router> qos-queue 2 description mymediumqosqueue
digi.router> qos-queue 2 borrow-upstream off
digi.router> qos-queue 2 state on
digi.router> save config
digi.router> qos-queue 3 description mylowqosqueue
digi.router> qos-queue 3 borrow-upstream off
digi.router> qos-queue 3 state on
digi.router> save config
```

- To configure filters for a configured QoS queue, use the qos-filter command. For example:

```
digi.router> qos-filter 1 queue 1
qos-queue 1:
digi.router> qos-queue

 qos-queue 1:
   bandwidth-upstream          2000
```

```
    borrow-upstream             on
    description                 VoIP Queue
    dscp-class                  do-not-set
    state                       on

  qos-queue 2:
    bandwidth-upstream          500
    borrow-upstream             on
    description                 Video Streaming
    dscp-class                  be
    state                       on

digi.router> qos-filter

  qos-filter 1:
    description                 VoIP traffic
    dscp                        ef
    dst-ip-address
    dst-ip-port                 0
    protocol                    any
    queue                       1
    src                         any-lan
    src-ip-address
    src-ip-port                 0
    state                       on

  qos-filter 2:
    description                 YouTube traffic
    dscp                        cs0
    dst-ip-address
    dst-ip-port                 0
    protocol                    any
    queue                       2
    src                         lan1
    src-ip-address
    src-ip-port                 0
    state                       on

  qos-filter 3:
    description                 Netflix traffic
    dscp                        cs0,cs1,cs2,cs3,cs4
```

```
dst-ip-address
dst-ip-port                 0
protocol                    tcp,udp
queue                       2
src                         lan2
src-ip-address              192.168.2.1
src-ip-port                 9000
state                       on
```

Show QoS configuration and status

Web

On the menu, click **Network > Services > QoS**. The **QoS** page appears.

Command line

To show the current QoS configuration use the qos-queue command and the qos-filter command with no parameters. For example:

```
digi.router> qos-queue

digi.router> qos-filter
```

Virtual Private Networks (VPN)

Virtual Private Networks (VPNs) are used to securely connect two private networks together so that devices can connect from one network to the other network using secure channels. These topics cover the various network protocols involved in VPNs, and configuring VPNs.

- IPsec
- OpenVPN
- Generic Routing Encapsulation (GRE)
- Virtual Router Redundancy Protocol (VRRP)

IPsec

IPsec is a suite of protocols for creating a secure communication link—an IPsec tunnel—between a host and a remote IP network or between two IP networks across a public network such as the Internet.

TransPort devices support to up **32** IPsec tunnels.

IPsec data protection

IPsec protects the data being sent across a public network by providing the following:

Data origin authentication
Authentication of data to validate the origin of data when it is received.

Data integrity
Authentication of data to ensure it has not been modified during transmission.

Data confidentiality
Encryption of data sent across the IPsec tunnel to ensure that an unauthorized device cannot read the data.

Anti-Replay
Authentication of data to ensure an unauthorized device has not injected it into the IPsec tunnel.

IPsec modes

IPsec can run in two different modes: **Tunnel** and **Transport**.

Currently, TransPort devices support tunnel mode only.

Tunnel
The entire IP packet is encrypted and/or authenticated and then encapsulated as the payload in a new IP packet.

Transport
Only the payload of the IP packet is encrypted and/or authenticated. The IP header is left untouched. This mode has limitations when using an authentication header, because the IP addresses in the IP header cannot be translated (for example, with Network Address Translation (NAT), as it would invalidate the authentication hash value.

Internet Key Exchange (IKE) settings

IKE is a key management protocol that allows IPsec to negotiate the security associations (SAs) that are used to create the secure IPsec tunnel.

SA negotiations are performed in two phases, known as **phase 1** and **phase 2**.

Phase 1

In phase 1, IKE creates a secure authenticated communication channel between the device and the peer (the remote device which is at the other end of the IPsec tunnel) using the configured pre-shared key and the Diffie-Hellman key exchange. This creates the IKE SAs that are used to encrypt further IKE communications.

There are two modes for the phase 1 negotiation: **Main mode** and **Aggressive mode**.

Main mode
Main mode is the default mode. It is slower than aggressive mode, but more secure, in that all sensitive information sent between the device and its peer is encrypted.

Aggressive mode
Aggressive mode is faster than main mode, but is not as secure as main mode, because the device and its peer exchange their IDs and hash information in clear text instead of being encrypted. Aggressive mode is usually used when one or both of the devices have a dynamic external IP address.

Phase 2

In phase 2, IKE negotiates the SAs for IPsec. This creates two unidirectional SAs, one for each direction. Once the phase 2 negotiation is complete, the IPsec tunnel should be fully functional.

There are two versions of IKE: **IKEv1** and **IKEv2**. Currently the LR54 only supports **IKEv1**.

IPsec and IKE renegotiation

To reduce the chances of an IPsec tunnel being compromised, the IPsec SAs and IKE SA are renegotiated at a regular interval. This results in different encryption keys being used in the IPsec tunnel.

Configure an IPsec tunnel

Configuring an IPsec tunnel with a remote device involves configuring the following items:

Required configuration items

IPsec tunnel configuration settings

- Enabling the IPsec tunnel. The IPsec tunnels are disabled by default. You can also set the IPsec tunnel state to **off** or **on**.
- The IP address or name of the remote device, also known as the **peer**, at the other end of the IPsec tunnel.
- The local and remote IDs at either end of the IPsec tunnel. The setting for the local ID must match the setting for the remote ID on the remote device, and the setting for the remote ID must match the setting for the local ID on the remote device.
- The local and remote IP networks at either end of the IPsec tunnel.
- The authentication protocol to use. This setting must match the authentication protocol configured on the remote device. The authentication options are:
  - **SHA1**
  - **SHA256**

  The default value is **SHA1**.

- The encryption protocol to use. This has to match the encryption protocol configured on the remote device. The encryption options are:
  - **AES – 128 bits**
  - **AES – 192 bits**
  - **AES – 256 bits**

  The default value is **AES – 128 bits**.
- The Encapsulating Security Payload (ESP) Diffie-Hellman group for the IPsec tunnel. This setting must match the Diffie-Hellman group configured on the remote device. The Diffie-Hellman group options are:
  - **None**
  - **Group 5** (1536 bits)
  - **Group 14** (2048 bits)
  - **Group 15** (3072 bits)
  - **Group 16** (4096 bits)

  The default value is **Group14**.

  The larger the number of bits, the more secure the IPsec tunnel. However, a larger bit length requires more computing power, which can slow down the tunnel negotiation and performance.
- The shared key the device and the remote device use to authenticate each other.

IKE configuration settings

- The IKE mode.
  - **Main**
  - **Aggressive**

  The default option is **Main**.
- The IKE authentication protocols to use for the IPsec tunnel negotiation. The authentication options are:
  - **SHA1**
  - **SHA256**

  The default is **SHA1**.

  You can select more than one authentication protocol. IKE negotiates with the remote device which to use. This setting does not need to match the IKE authentication protocols configured on the remote device, but at least one of the authentication protocols must be configured on the remote device.
- The IKE encryption protocols to use for the IPsec tunnel negotiation. The encryption options are:
  - **AES – 128 bits**
  - **AES – 192 bits**
  - **AES – 256 bits**

  The default is **AES – 128 bits**.

  You can select more than one encryption protocol. IKE negotiates with the remote device which encryption protocol to use. This setting does not need to match the IKE encryption protocols configured on the remote device, but at least one of the encryption protocols must be configured on the remote device.

- The IKE Diffie-Hellman groups to use for the IPsec tunnel negotiation. The Diffie-Hellman group options supported on TransPort devices are:
  - **Group 5** (1536 bits)
  - **Group 14** (2048 bits)
  - **Group 15** (3072 bits)
  - **Group 16** (4096 bits)

  The default value is **Group14**.

  You can select more than one Diffie-Hellman group. IKE negotiates with the remote device which group to use. This setting does not need to match the IKE Diffie-Hellman groups configured on the remote device, but at least of the Diffie-Hellman groups must be configured on the remote device.

Additional configuration items

The following additional configuration settings are not typically configured to get an IPsec tunnel working, but can be configured as needed:

Tunnel and key renegotiating

- The lifetime of the IPsec tunnel before it is renegotiated. This defaults to **1 hour** (**3600** seconds), and does not need to match the setting on the remote device.
- The number of bytes, also known as lifebytes, sent on the IPsec tunnel before it is renegotiated. By default, this setting is disabled, but can be configured up to **4 GB**. This setting does not need to match the setting on the remote device.
- The IKE lifetime before the keys are renegotiated. This defaults to **4800** seconds and does not need to match the IKE lifetime configured on the remote device.
- The amount of time before the IPsec lifetime expires, the renegotiation should start. This defaults to **540** seconds and does not need to match the setting on the remote device.
- The number of bytes before the IPsec lifebytes limit is reached before the key is renegotiated. By default, this is set to **0** and does not need to match the setting on the remote device.
- A randomizing factor for the number of seconds or bytes margin before the IPsec tunnel is renegotiated. This defaults to **100%** and does not need to match the setting on the remote device. This setting would be used if the device has a number of IPsec tunnels configured to ensure that the IPsec tunnels are not renegotiated at the same time which could put excessive load on the device.

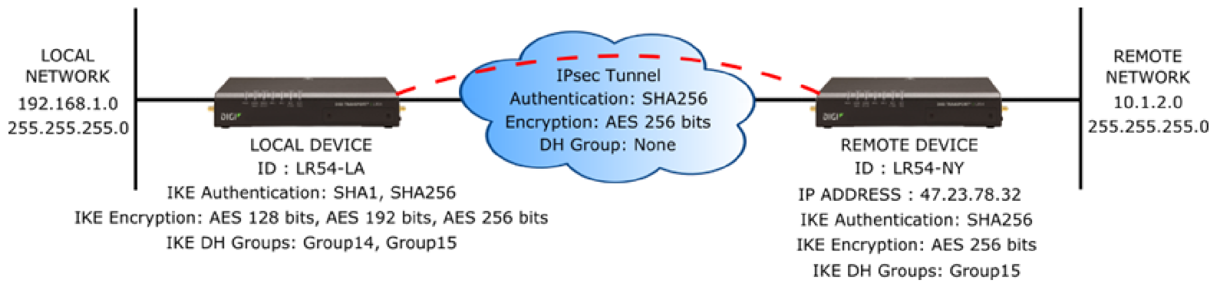
Other configuration items

- A description for the IPsec tunnel.
- The number of tries IKE will attempt to negotiate the IPsec tunnel with the remote device before giving up.

- The metric for the IPsec route. The metric defines the order in which the device uses routes if there are two routes to the same destination. In such a case, the device uses the route with the smaller metric. The default is 10 but you can configure the metric differently to increase or decrease the route's priority.

Example IPsec tunnel

Suppose you are configuring the following IPsec tunnel:



Web

Configure a new IPsec tunnel

1. **Prerequisite**: A configured LAN must be available for use in the IPsec tunnel. See Configure a LAN.
2. On the menu, click **Network > Networks > IPsec**. The **IPsec** page appears.
3. Click **New IPsec Tunnel**. The **IPsec** page displays the settings for a new IPsec tunnel. The settings are displayed in four groups: **Network**, **Encryption**, **Negotiation**, and **Lifetime**. Most of these settings groups have defaults which you can review and use or modify as needed. The Network settings involve settings you must supply.
4. In the **Select IPsec** setting, select a number to assign to the IPsec tunnel.
5. Enter the **Network** settings:
    - **State**: Enables or disables the IPsec tunnel when configuration is completed and the IPsec tunnel is available for use.
    - **IPSec Pre-Shared Key**: Enter the shared key the device and the remote device use to authenticate each other.
    - **Local IP Network**: The network used for the IPsec tunnel on the local side of the tunnel. Select a LAN from the list.
    - **Local Identifier**: Enter the local identifier for the IPsec tunnel. The value for the **Local Identifier** must match the value for the **Remote Identifier** on the remote device at the other end of the tunnel.
    - **Remote Peer IP Address or Name**: Enter the IP address or name of the remote device, also known as the **peer**, at the other end of the IPsec tunnel.
    - **Remote IP Network**: Enter the IP address of the network used for the IPsec tunnel on the remote side of the tunnel.

- **Remote IP Network Mask**: Enter the IP network mask of the network used for the IPsec tunnel on the remote side of the tunnel.
- **Remote Identifier**: Enter the remote identifier for the IPsec tunnel. The value for the Remote Identifier must match the value for the Local Identifier on the remote device at the other end of the tunnel.

6. Review the **Encryption** settings and modify as needed. These settings configure the encryption protocols to use for the IPsec tunnel negotiation.
7. Review the **Negotiation** settings and modify as needed. These settings configure detailed negotiation protocols and other options to use for the IPsec tunnel negotiation.
8. Review the **Lifetime** settings and modify as needed. These settings configure the duration of the IPsec tunnel before it is renegotiated, and the lifetime of the Internet Key Exchange (IKE) before the keys are renegotiated.
9. Click **Apply**.

Modify an existing IPsec tunnel

1. On the menu, click **Network > Networks > IPsec**. The IPsec page appears.
2. Select an IPsec tunnel and click **Edit**.
3. Modify the **Network**, **Encryption**, **Negotiation**, and **Lifetime** settings as needed.
4. Click **Apply**.

Command line

1. Enable the IPsec tunnel.

```
digi.router> ipsec 1 state on
```

2. Enter the IP address or name of the remote device.

```
digi.router> ipsec 1 peer 47.23.78.32
```

3. Enter the local and remote IDs.

```
digi.router> ipsec 1 local-id LR54-LA
digi.router> ipsec 1 remote-id LR54-NY
```

4. Enter the local and remote IP networks.

```
digi.router> ipsec 1 local-network 192.168.1.0
digi.router> ipsec 1 local-mask 255.255.255.0
digi.router> ipsec 1 remote-network 10.1.2.0
digi.router> ipsec 1 remote-mask 255.255.255.0
```

5. Enter the pre-shared key.

```
digi.router> ipsec 1 psk “secret-psk”
```

6. Enter the IPsec authentication, encryption, and Diffie-Hellman settings.

```
digi.router> ipsec 1 esp-authentication sha256
digi.router> ipsec 1 esp-encryption aes256
digi.router> ipsec 1 esp-diffie-hellman none
```

7. Enter the IKE authentication, encryption, and Diffie-Hellman settings.

```
digi.router> ipsec 1 ike-authentication sha1,sha256
digi.router> ipsec 1 ike-encryption aes128,aes192,aes256
digi.router> ipsec 1 ike-diffie-hellman group14,group15
```

8. Save the configuration.

```
digi.router> save config
```

Example: IPsec tunnel between a TransPort LR54 and TransPort WR44

The following figure shows a sample IPsec configuration between a TransPort LR54 and a TransPort WR44.

The configuration settings for both devices are as follows:

TransPort LR54 configuration

```
digi.router> lan 1

   state                          on
   description                    IPsec local net
   mtu                            1500
   interfaces                     eth2,eth3,eth4
   ip-address                     192.168.54.1
   mask                           255.255.255.0
   dns1
   dns2
   dhcp-client                    off

   digi.router> lan 2

   state                          on
   description                    Link to WR44
   mtu                            1500
   interfaces                     eth1
   ip-address                     10.0.0.54
```

```
   mask                           255.255.255.0
   dns1
   dns2
   dhcp-client                    off

digi.router> ipsec 1

   state                          on
   description                    Tunnel to WR44
   peer                           10.0.0.44
   local-network                  192.168.54.0
   local-mask                     255.255.255.0
   remote-network                 192.168.44.0
   remote-mask                    255.255.255.0
   esp-authentication             sha1
   esp-encryption                 aes128
   esp-diffie-hellman             none
   auth-by                        psk
   psk                            <configured>
   local-id                       10.0.0.54
   remote-id                      10.0.0.44
   lifetime                       3600
   lifebytes                      0
   margintime                     540
   marginbytes                    0
   random                         100
   ike                            1
   ike-mode                       aggressive
   ike-encryption                 aes128
   ike-authentication             sha1
   ike-diffie-hellman             group5
   ike-lifetime                   3600
   ike-tries                      3
   dpddelay                       30
   dpdtimeout                     150
   dpd                            off
```

TransPort WR44 configuration

```
# Link to TransPort LR54
eth 0 IPaddr "10.0.0.44"
eth 0 ipsec 1

# IPsec local network
eth 1 IPaddr "192.168.44.1"

# Route to remote network
route 0 IPaddr "192.168.54.0"
route 0 ll_ent "eth"

# IPsec tunnel configuration
eroute 0 peerip "10.0.0.54"
eroute 0 peerid "10.0.0.54"
eroute 0 ourid "10.0.0.44"
eroute 0 ouridtype 3
eroute 0 locip "192.168.44.0"
eroute 0 locmsk "255.255.255.0"
eroute 0 remip "192.168.54.0"
eroute 0 remmsk "255.255.255.0"
```

```
eroute 0 ESPauth "sha1"
eroute 0 ESPenc "aes"
eroute 0 authmeth "preshared"
eroute 0 autosa 2

# IKE configuration
ike 0 encalg "aes"
ike 0 keybits 128
ike 0 authalg "sha1"
ike 0 ltime 30000
ike 0 aggressive ON
ike 0 ikegroup 5

# Remote ID / Password
user 1 name "10.0.0.54"
user 1 epassword "MDp6Vko=
```

Debug an IPsec configuration

If you experience issues with an IPsec tunnel not being successfully negotiated with the remote end of the tunnel, you can enable IPsec debug messages to be written to a file. Once enabled, the debug messages are displayed in the file **ipsec.debug**.

To enable IPsec debugging, use the system command **ipsec-debug** parameter. This command creates a file named **ipsec.debug** to which low-level IPsec debugging messages are written.

```
digi.router> system ipsec-debug on
```

Show IPsec status and statistics

Web

- On the menu, click **Network > Networks > IPsec**. The **IPsec** page appears.

Command line

The show ipsec displays the status of the IPsec tunnels and statistics regarding their use.

Display summary status for IPsec tunnels

To display summary status and statistics of all configured IPsec tunnels, enter the show ipsec command without parameters.

```
digi.router> show ipsec

 #   Status  Peer             Local               Remote              Uptime
 ---------------------------------------------------------------------------
 1   Up      192.170.1.100    192.168.0.0/16      192.169.1.0/24      3 minutes

digi.router>
```

Display detailed status and statistics for an IPsec tunnel

To display detailed status and statistics of all configured IPsec tunnels, enter the show ipsec command, specifying the tunnel number.

```
digi.router> show ipsec 1

 IPsec 1 Status and Statistics
 -----------------------------
 Description      :
 Admin Status     : Up
 Oper Status      : Up
```

```
 Uptime            : 2 minutes

 Peer              : 192.170.1.100
 Local Network     : 192.168.0.0/16
 Remote Network    : 192.169.1.0/24

 IKE Information
 ---------------
 Key Negotiation   : IKEv1, aes128, sha1, modp2048
 SPIs              : 5078e20a02eb1e9c_i* 6b2cfcdf33b4125c_r

 Tunnel Information
 ------------------
 Rekeying In       : 68 minutes
 AH Cipher Suite   : Not Used
 ESP Cipher Suite  : aes128, sha1
 Renegotiating In  : 42 minutes
 Outbound ESP SAs  : d2fad10b, 9bcc91db
 Inbound ESP SAs   : 2af8bb94, 3be64703

 Dead Peer Detection is off

 Bytes In          : 0
 Bytes Out         : 0

digi.router>
```

OpenVPN

OpenVPN is an open-source Virtual Private Network (VPN) technology that creates secure point-to-point or site-to-site connections in routed or bridged configurations.

OpenVPN uses a custom security protocol that is Secure Socket Layer (SSL) / Transport Layer Security (TLS) for key exchange. It uses standard encryption and authentication algorithms for data privacy and authentication over TCP or UDP.

TransPort devices support **OpenVPN 2.4** in both client and server mode with the **net30**, **p2p**, and **subnet** OpenVPN topologies.

TransPort devices support **1** OpenVPN server and up to **10** OpenVPN clients.

The OpenVPN server supports the use of either an internal user list or an external RADIUS server for authentication using a username and password.

The OpenVPN server can push the network configuration, such as the topology and IP routes, to OpenVPN clients. This makes OpenVPN simpler to configure as it reduces the chances of a configuration mismatch between the client and server.

OpenVPN also supports cipher negotiation between the client and server. This means you can configure the OpenVPN server and clients with a range of different cipher options and the server will negotiate with the client on the cipher to use for the connection.

TransPort devices are compatible with OpenVPN running on Windows, Linux, and Mac OS X.

For more information on OpenVPN, see www.openvpn.net.

OpenVPN network interfaces

TransPort routers support several named interfaces for OpenVPN. The interface for OpenVPN server is named **ovpns**. For OpenVPN clients, there are multiple interfaces named **ovpn*x***, where ***x*** is the index number for a particular OpenVPN client.

Routing (TUN) mode

There are two modes for running OpenVPN: routing mode, also known as TUN, and bridging mode, also known as TAP.

In routing mode, each OpenVPN client is assigned a different IP subnet from the OpenVPN server and other OpenVPN clients. OpenVPN clients use Network Address Translation (NAT) to route traffic from devices connected on its LAN interfaces to the OpenVPN server.

The manner in which the IP subnets are defined depends on the OpenVPN topology in use:

OpenVPN Topology	Subnet definition method
net30	Each OpenVPN client is assigned a **/30** subnet within the IP subnet specified in the OpenVPN server configuration.
p2p	Each OpenVPN client uses a point to point link. This is not available for Windows clients.
subnet	Each OpenVPN client connected to the OpenVPN server is assigned an IP address within the IP subnet specified in the OpenVPN server configuration.

For more information on OpenVPN topologies, see this Wiki article on OpenVPN topology.

Bridging (TAP) mode

In bridging mode, a LAN interface on the OpenVPN server is assigned to OpenVPN. The LAN interfaces of the OpenVPN clients are on the same IP subnet as the OpenVPN server's LAN interface. This means that devices connected to the OpenVPN client's LAN interface are on the same IP subnet as devices.

Additional OpenVPN information

For more information on OpenVPN, see these resources:

Bridging vs. routing

OpenVPN/Routing

Configure an OpenVPN server for routing mode and certificate authentication

Required configuration settings

- Enable the OpenVPN server. The OpenVPN server is disabled by default.
- The IP network of the OpenVPN server (only needed when using routing mode).

- The server certificate and private key parameters should be loaded onto the TransPort device prior to using them. For more information on how to create private key files and certificates, see Certificate and key management. The process for loading this information onto the device varies by certificate and key type:
  - **Certificate authority (CA) certificate**: Copy the CA certificate and the CRL onto the TransPort device from the CA prior to using it.
  - **Private key and certificate**: There are two options to install a private key and certificate on the TransPort device:
    - Use the pki commands **pki privkey** and **pki csr** to generate the private key and certificate, copy the CRS to an external system to get it signed, then copy the signed certificate back onto the TransPort device.
    - Generate the private key and certificate, fully signed, on an external system and copy them onto the TransPort device. Use **pki addkey** command to import the private key into the private key store.
  - **If using a Diffie-Hellman (DH) file**: There are two options to install a DH file on the TransPort device:
    - Generate the DH file using the **pki dh-file** command on the TransPort device.
    - Generate a DH file on an external system and copy it onto the TransPort device.

Optional configuration settings

A description of the OpenVPN server.

- The OpenVPN topology. By default, **net30** is used.
- A subnet mask for the network when in routing mode.
- A primary and secondary DNS server.
- The ciphers and digest used by the OpenVPN server. For more information, see Configure ciphers and digests for use on the OpenVPN tunnel.
- The IP protocol (TCP or UDP) to use. By default, the TransPort device uses **UDP**. This must match the IP protocol configured on the OpenVPN client.
- The TCP/UDP Port to use. By default, the TransPort device uses port **1194**.
- You can enable compression con the OpenVPN tunnel. The compression options are **LZO** and **LZ4**.

Web

1. On the menu, click **Network > Networks > OpenVPN** and select **OpenVPN Server**. The **OpenVPN Server** page appears.
2. Click **Edit**. The **OpenVPN server** page displays the settings for the OpenVPN server.

3. Enter the **Connection** settings:
   - **Enable**: Enables or disables the OpenVPN server when configuration is completed.
   - **Logging Level**: The detail level of output that the OpenVPN server records in the system log. See Debug an OpenVPN tunnel for more information on logging levels.
4. Enter the **Network** settings:
   - **Network**: Enter the IP network to be used with the OpenVPN clients.
   - **Mask**: Enter the subnet mask for the IP subnet.
5. Review the **Encryption** settings and modify as needed. These settings configure the encryption protocols used with the OpenVPN tunnel.
   - **Digest**: Enter the digest to be used with the OpenVPN tunnel.
6. Enter the **Authentication** settings:
   - **Certificate authority (CA) certificate**: Enter the name of the Certificate Authority certificate to authenticate OpenVPN client certificates.
   - **Diffie-Hellman file**: Enter the name of the Diffie-Hellman file.
   - **Certificate**: Enter the name of the certificate to be used by the OpenVPN server.
   - **Private Key File**: Enter the private key file to be used by the OpenVPN server.
7. Review the **Lifetime** settings and modify as needed. These settings configure the OpenVPN tunnel keepalive and renegotiation.
8. Click **Apply**.

Command line

1. Enable the OpenVPN server.

```
digi.router> openvpn-server state on
```

2. Configure the IP network of the OpenVPN server.

```
digi.router> openvpn-server network 192.168.54.0
```

3. (Optional) Configure the IP subnet mask of the OpenVPN server.

```
digi.router> openvpn-server mask 255.255.255.128
```

4. (Optional) Configure a primary and secondary DNS server to be used with this OpenVPN tunnel. The DNS server configuration will be pushed to the OpenVPN client. The OpenVPN client can decide how to use these values. A TransPort OpenVPN client will ignore them.

```
digi.router> openvpn-server dns1 192.168.10.1
digi.router> openvpn-server dns2 192.168.10.2
```

5. Configure the CA certificate.

```
digi.router> openvpn-server ca cacert.pem
```

6. Configure the server certificate.

```
digi.router> openvpn-server cert ovpns.pem
```

7. Configure the server key.

```
digi.router> openvpn-server key ovpns.key
```

8. Configure the Diffie Hellman file.

```
digi.router> openvpn-server dh ovpns-dh.pem
```

9. (Optional) Configure the OpenVPN topology

```
digi.router> openvpn-server topology subnet
```

10. (Optional) Configure the IP protocol.

```
digi.router> openvpn-server protocol tcp
```

11. (Optional) Configure the TCP/UDP port.

```
digi.router> openvpn-server port 8894
```

12. (Optional) Enable compression.

```
digi.router> openvpn-server compression lzo
```

13. (Optional) Configure a description.

```
digi.router> openvpn-server description “LA OpenVPN server”
```

14. Save the configuration.

```
digi.router> save config
```

Configure an OpenVPN server to use username and password authentication

The OpenVPN server is able to authenticate clients using username and passwords. You can configure up to **10** usernames and passwords. If you need more than **10** usernames and passwords, use RADIUS authentication instead. See Configure an OpenVPN server to use RADIUS authentication for more information.

Web

1. On the menu, click **Network > Networks > OpenVPN** and select **OpenVPN Server**. The **OpenVPN Server** page appears.
2. Click **Edit**. The **OpenVPN server** page displays the settings for the OpenVPN Server.

3. Enter the **Authentication** settings:
   - **Certificate:** Enter the name of the certificate to be used by the OpenVPN server.
   - **Private Key File**: Enter the name of the private key file to be used by the OpenVPN server.
   - **Authenticate By**: Select **User name and password**.
4. Click **Apply**.
5. On the menu, click **VPN** and select **OpenVPN User Management**.
6. Click **New OpenVPN User**.
7. Enter user information:
   - **Username**: The name of the OpenVPN client.
     - Usernames can be up to **32** characters long and are case-sensitive.
     - Usernames cannot start with a number.
   - **Password/Confirm Password**: Password for the user.
8. Click **Apply**.

Command line

1. Configure the authentication mode to use username and password authentication.

```
digi.router> openvpn-server auth-by user-pass
```

2. Configure a user name and password. For example, to configure a username ny-office and password abcdefgh, the commands would be.

```
digi.router> openvpn-user 1 username ny-office
digi.router> openvpn-user 1 password abcdefgh
```

3. Save the configuration.

```
digi.router> save config
```

Configure an OpenVPN server to use RADIUS authentication

The OpenVPN server can authenticate clients using RADIUS instead of configuring usernames and passwords on the device.

To use RADIUS, set the OpenVPN authentication mode to username and password, and configure and enable the RADIUS server and secret.

Web

1. On the menu, click **Network > Networks > OpenVPN** and select **OpenVPN Server**. The **OpenVPN Server** page appears.
2. Click **Edit**. The **OpenVPN server** page displays the settings for the OpenVPN server.

3. Enter the **Authentication** settings:
   - **Auth-By**: Select **Username and password**.
   - **Radius Server State**: Enable the RADIUS server.
   - **Radius Server**: Configure the IP address or domain name of the RADIUS server.
   - **Radius Server Secret**: Configure the secret of the RADIUS server.
4. Click **Apply**.

Command line

1. Configure the authentication mode to use username and password authentication.

```
digi.router> openvpn-server auth-by user-pass
```

2. Configure OpenVPN to use RADIUS to authenticate users.

```
digi.router> openvpn-server radius-server-state on
```

3. Configure the RADIUS server address.

```
digi.router> openvpn-server radius-server 10.12.33.200
```

4. Configure the RADIUS server secret.

```
digi.router> openvpn-server radius-server-secret mysecret
```

5. (Optional) Configure the RADIUS server port. For example, to change the port to **8812**, the command is:

```
digi.router> openvpn-server radius-server-port 8812
```

6. Save the configuration.

```
digi.router> save config
```

Configure an OpenVPN client for routing mode and certificate authentication

As OpenVPN is designed to allow the OpenVPN server to push up a lot of the OpenVPN configuration to the OpenVPN client, it means that the client configuration is simplified.

Required configuration

- Enable the OpenVPN client. The OpenVPN client is disabled by default.
- The IP address or domain name of the OpenVPN server.

- The client certificate and private key parameters. For more information on how to create private key files and certificates, see Certificate and key management. The server certificate and private key parameters should be loaded onto the TransPort device prior to using them. For more information on how to create private key files and certificates, see Certificate and key management. The process for loading this information onto the device varies by certificate and key type:
  - **Certificate authority (CA) certificate**: Copy the CA certificate and the CRL onto the TransPort device from the CA prior to using it.
  - **Private key and certificate**: There are two options to install a private key and certificate on the TransPort device:
    - Use the pki commands **pki privkey** and **pki csr** to generate the private key and certificate, copy the CRS to an external system to get it signed, then copy the signed certificate back onto the TransPort device.
    - Generate the private key and certificate, fully signed, on an external system and copy them onto the TransPort device. Use **pki addkey** command to import the private key into the private key store.

Optional configuration

- A description of the OpenVPN client.
- The ciphers and digest used by the OpenVPN client. For more information, see Configuring ciphers and digests to be used on the OpenVPN tunnel.
- The IP protocol (TCP or UDP) to use. The default is to use **UDP**. This value must match the IP protocol configured on the OpenVPN server.
- The TCP/UDP Port to use. By default, port **1194** is used. This must match the TCP/UDP port configured on the OpenVPN server.
- The connection retry attempt period. By default, the OpenVPN client waits **5** seconds before retrying to connect to the OpenVPN server. After **5** unsuccessful attempts, the period doubles to a maximum of **300** seconds.

Web

1. On the menu, click **Network > Networks > OpenVPN** and select **OpenVPN Client**. The **OpenVPN Client** page appears.
2. Click **New OpenVPN Client**. The **OpenVPN client** page displays the settings for a new OpenVPN tunnel.
3. In the **Select OpenVPN Client** setting, select a number to assign to the OpenVPN client.
4. Enter **Connection** settings:
   - **State**: Enables or disables the OpenVPN client when configuration is completed.
5. Enter **Network** settings:
   - **Server**: Configure the IP address or domain name of the OpenVPN server.

6. Review **Encryption** settings and modify as needed. These settings configure the encryption protocols used with the OpenVPN tunnel.
   - **Digest**: Enter the digest to be used with the OpenVPN tunnel.
7. Enter **Authentication** settings:
   - **Certificate authority (CA) certificate**: Enter the name of the Certificate Authority certificate to authenticate OpenVPN server certificate.
   - **Certificate**: Enter the name of the certificate to be used by the OpenVPN client.
   - **Private Key File**: Enter the name of the private key file to be used by the OpenVPN client.
8. Click **Apply**.

Command line

1. Enable the OpenVPN client.

```
digi.router> openvpn-client 1 state on
```

2. Configure the IP address or the domain name of the OpenVPN server.

```
digi.router> openvpn-client 1 server 209.98.33.1
```

3. Configure the CA certificate.

```
digi.router> openvpn-client 1 ca cacert.pem
```

4. Configure the server certificate.

```
digi.router> openvpn-client 1 cert ovpnc1.pem
```

5. Configure the server key.

```
digi.router> openvpn-client 1 key ovpnc1.key
```

6. (Optional) Configure the IP protocol.

```
digi.router> openvpn-server protocol tcp
```

7. (Optional) Configure the TCP/UDP port.

```
digi.router> openvpn-client 1 port 8894
```

8. (Optional) Configure the connection retry interval.

```
digi.router> openvpn-client 1 connect-retry 10
```

9. (Optional) Configure a description.

```
digi.router> openvpn-server description “OpenVPN to LA office”
```

10. Save the configuration.

```
digi.router> save config
```

Configure an OpenVPN client to use username and password authentication

The configuration for an OpenVPN client to username and password is similar to that of the certificate authentication but instead of configuring a certificate and key, a username and password is configured.

Note that a CA certificate is still required to validate the OpenVPN server's certificate to prevent an attacker from replacing or spoofing the server.

Web

1. On the menu, click **Network > Networks > OpenVPN** and select **OpenVPN Client**. The **OpenVPN Client** page appears.
2. Click **New OpenVPN Client**. The **OpenVPN client** page displays the settings for a new OpenVPN tunnel.
3. In the **Select OpenVPN Client** setting, select a number to assign to the OpenVPN client.
4. Enter the **Connection** settings:
   - **State**: Enables or disables the OpenVPN client when configuration is completed.
5. Enter the **Network** settings:
   - **Server**: Configure the IP address or domain name of the OpenVPN server.
6. Review the **Encryption** settings and modify as needed. These settings configure the encryption protocols used with the OpenVPN tunnel.
   - **Digest**: Enter the digest to be used with the OpenVPN tunnel.
7. Enter the **Authentication** settings:
   - **Certificate authority (CA) certificate**: Enter the name of the Certificate Authority certificate to authenticate OpenVPN server certificate.
   - **Username**: Enter the username of the OpenVPN client. This must match the username configured on the OpenVPN server.
   - **Password**: Password of the OpenVPN client.
8. Click **Apply**.

Command line

- Configure the username and password. For example, to configure the username **ny-office** and password **abcdefgh**, the commands are:

```
digi.router> openvpn-client 1 username ny_office
digi.router> openvpn-client 1 password abcdefgh
```

Configure ciphers and digests for use on the OpenVPN tunnel

By default, the OpenVPN server negotiates with the OpenVPN client the cipher that will be used to encrypt data being sent over the OpenVPN tunnel. The ciphers that will be used for the negotiation can be configured as a list. In order for the negotiation to be successful, the OpenVPN client's cipher list must include the first cipher in the OpenVPN server's cipher list. OpenVPN clients that do not support cipher negotiation can use any cipher in the OpenVPN server's cipher list to connect.

To force the OpenVPN client or server to use a specific cipher, then only the desired cipher should be configured in the list.

By default, the OpenVPN client and server support the following ciphers for negotiation:

- AES 128 CBC
- AES 192 CBC
- AES 256 CBC
- AES 128 GCM
- AES 192 GCM
- AES 256 GCM

When using CBC encryption algorithms, the OpenVPN client and server will also use a digest to authenticate the data sent over the OpenVPN tunnel. The digest configured on the OpenVPN client must match the digest configured on the OpenVPN server.

By default, the OpenVPN client and server will use **SHA1** for authentication.

The digest is not used when a **GCM** encryption algorithm is in use, since GCM encryption includes built-in digest functionality.

Web

For OpenVPN Server

1. On the menu, click **Network > Networks > OpenVPN** and select **OpenVPN Server**. The **OpenVPN Server** page appears.
2. Click **Edit**. The **OpenVPN server** page displays the settings for the OpenVPN Server.
3. Enter the **Encryption** settings:
   - **Cipher**: Select the desired ciphers that the OpenVPN can use for an OpenVPN tunnel.

     Note The order of the ciphers is important for cipher negotiation. The first cipher in the list will be used if both the OpenVPN client and server support cipher negotiation.
4. Click **Apply**.

For OpenVPN Clients

1. On the menu, click **Network > Networks > OpenVPN** and select **OpenVPN Client**. The **OpenVPN Client** page appears.
2. Select the required OpenVPN client.
3. Click **Edit**. The **OpenVPN client** page displays the settings for the OpenVPN client.
4. Enter the **Encryption** settings:
   - **Cipher**: Select the desired ciphers that the OpenVPN can use for an OpenVPN tunnel.
5. Click **Apply**.

Command line

1. For the OpenVPN server, the command to configure the list of ciphers is **openvpn-server cipher**. For example, to configure the OpenVPN server to use either **AES 128 GCM** for cipher negotiation or allow **AES 256 GCM** cipher for OpenVPN clients that don't support cipher

negotiation, the command is:

```
digi.router> openvpn-server cipher aes-128-gcm,aes-256-gcm
```

2. For the OpenVPN server, the command to configure the digest is **openvpn-server digest**. For example, the command to configure the OpenVPN server to use **SHA256**, the command would be:

```
digi.router> openvpn-server digest sha256
```

3. For the OpenVPN client, the command to configure the list of ciphers is **openvpn-client *x* cipher**. For example, to configure the OpenVPN client 1 to use AES 256 GCM cipher only, the command would be:

```
digi.router> openvpn-client 1 cipher aes-256-gcm
```

4. For the OpenVPN client, the command to configure the digest is **openvpn-client *x* digest**. For example, the command to configure the OpenVPN client **1** to use **SHA256**, the command would be:

```
digi.router> openvpn-client 1 digest sha256
```

5. Save the configuration on the OpenVPN client and/or server.

```
digi.router> save config
```

Configure keepalives on the OpenVPN tunnels

You can configure keepalive message to be sent periodically to detect whether the OpenVPN tunnel is operational.

If there are no keepalive messages received for a configurable amount of time, the OpenVPN tunnel is be brought down and then renegotiated.

The keepalive interval and timeout is only configured on the OpenVPN server and is pushed up to the OpenVPN client during the tunnel negotiation. The OpenVPN server automatically doubles the configured keepalive timeout to ensure that the OpenVPN client times out first.

By default, a keepalive message will be sent by the OpenVPN client every **30** seconds and by the OpenVPN server every **60** seconds. The OpenVPN client will drop and renegotiate the tunnel if it does not receive a keepalive message for **150** seconds. The OpenVPN server will drop and renegotiate after **300** seconds.

Web

1. On the menu, click **Network > Networks > OpenVPN** and select **OpenVPN Server**. The **OpenVPN Server** page appears.
2. Click **Edit**. The **OpenVPN server** page displays the settings for the OpenVPN server.

3. Enter the **Lifetime** configuration:
   - **Keepalive Interval (Seconds)**: The interval at which keepalive messages are sent by the OpenVPN client. Keepalive messages are sent by the OpenVPN server at twice the interval.
   - **Keepalive Timeout (Seconds)**: The OpenVPN tunnel will be brought down and renegotiated if no messages have been received for the configured timeout.
4. Click **Apply**.

Command line

1. Configure the keepalive interval.

```
digi.router> openvpn-server keepalive-interval 10
```

2. Configure the keepalive timeout.

```
digi.router> openvpn-server keepalive-timeout 60
```

3. Save the configuration.

```
digi.router> save config
```

Configure renegotiation on the OpenVPN tunnels

The OpenVPN server to be configured to automatically renegotiate the OpenVPN tunnel after a specific amount of time or after a specific amount of data has been sent over the OpenVPN tunnel. The purpose of this renegotiation is to reduce the risk of the negotiated keys from becoming compromised from overuse.

Web

1. On the menu, click **Network > Networks > OpenVPN** and select **OpenVPN Server**. The **OpenVPN Server** page appears.
2. Click **Edit**. The **OpenVPN server** page displays the settings for the OpenVPN server.
3. Enter the **Lifetime** configuration:
   - **Time Until Tunnel Renegotiation (Seconds)**: OpenVPN tunnels are renegotiated after the tunnel has been up for the configured amount of time.
   - **Bytes Until Tunnel Renegotiation**: OpenVPN tunnels are renegotiated after the tunnel has had the configured amount of traffic sent over it.
4. Click **Apply**.

Command line

1. To configure the amount of data to be sent before renegotiating, the command is **openvpn-server reneg-bytes**. For example, the renegotiate the OpenVPN tunnel after **32 MB** of data has been sent, the command is:

```
digi.router> openvpn-server reneg-bytes 33554432
```

2. To configure the amount of time before renegotiating, the command is **openvpn-server reneg-sec**. For example, to renegotiate the OpenVPN tunnel after **2** hours have passed, the command is:

```
digi.router> openvpn-server reneg-sec 7200
```

3. Save the configuration.

```
digi.router> save config
```

Configure pushing routes to OpenVPN clients

The OpenVPN server can push route information to the OpenVPN client so that the client automatically learns routes to networks on the OpenVPN server LAN interfaces.

Configuring the routes on the OpenVPN server involves configuring the destination network and mask for each route.

Web

1. On the menu, click **Network > Networks > OpenVPN** and select **OpenVPN Route Management**. The **OpenVNP Route Management** page appears.
2. Click **+** (Add Rule) to create a new route.
3. Enter the route **Destination** and **Mask**.
4. Click **Apply**.

Command line

1. OpenVPN routes are configured using the **openvpn-route** command. For example to configure routes for **10.123.1.0/24** and **10.222.33.0/24** networks, the commands are:

```
digi.router> openvpn-route 1 destination 10.123.1.0
digi.router> openvpn-route 1 mask 255.255.255.0
digi.router> openvpn-route 2 destination 10.222.33.0
digi.router> openvpn-route 2 mask 255.255.255.0
```

2. Save the configuration.

```
digi.router> save config
```

Configure an OpenVPN client and server for bridge mode

The configuration for the bridge mode is the same as with routing mode except for the following differences:

- The OpenVPN server is not configured with an IP network or mask.
- A LAN interface is assigned to the OpenVPN server.
- A LAN interface is assigned to the OpenVPN client.

Web

For OpenVPN server

1. On the menu, click **Network > Networks > OpenVPN** and select **OpenVPN Server**. The **OpenVPN Server** page appears.
2. Click **Edit**. The **OpenVPN server** page displays the settings for the OpenVPN server.
3. Enter the **Network** settings:
   - **Bridge Mode**: Select the LAN interface to be bridged with the OpenVPN clients.
4. Click **Apply**.

For OpenVPN clients

1. On the menu, click **Network > Networks > OpenVPN** and select **OpenVPN Client**. The **OpenVPN Client** page appears.
2. Select the required OpenVPN client.
3. Click **Edit**. The **OpenVPN client** page displays the settings for the OpenVPN client.
4. Enter the **Network** settings:
   - **Bridge Mode**: Select the LAN interface to be bridged with the OpenVPN server.
5. Click **Apply**.

Command line

1. Configure the LAN interface to be assigned with the OpenVPN server.

```
digi.router> openvpn-server bridge-mode lan1
```

2. Configure the LAN interface to be assigned with the OpenVPN client.

```
digi.router> openvpn-client 1 bridge-mode lan1
```

3. Save the configuration on the OpenVPN client and/or server.

```
digi.router> save config
```

Show OpenVPN server status and statistics

Web

- On the menu, click **Network > Networks > OpenVPN** and select **OpenVPN Server**.

Command line

Enter the show openvpn-server command. For example:

```
digi.router> show openvpn-server

 OpenVPN Server Status
 ---------------------
 Description       : VPN server for remote employees
 Admin Status      : Up
 Oper Status       : Up
 Interface         : ovpns
 IP Address        : 10.8.0.1
 Mask              : 255.255.255.0
 MTU               : 1500

                                   Received                 Sent
                                   --------                 ----
 Interface Packets  :                     4                    4
 Interface Bytes    :                   288                  288
```

```
 Connected Client                    Real Address      Virtual Address          Bytes Received              Bytes
Sent   Connected Since
 --------------------------------------------------------------------------------------------------------------------
-----------------------------
 client                              203.0.113.3       10.8.0.2                           23550
4189   Thu Aug  3 17:12:21 2017

digi.router>
```

Show OpenVPN client status and statistics

Web

1. On the menu, click **Network > Networks > OpenVPN** and select **OpenVPN Client**.
2. Select the required OpenVPN client.

Command line

Display all enabled OpenVPN clients

The **show openvpn-client** command displays a summary of the OpenVPN clients configured on the device.

```
digi.router> show openvpn-client

 #  Status  Remote Server     IP Address        Mask              Description
 --------------------------------------------------------------------------------
----------------------
 1  Up      203.0.113.3       10.8.0.2          255.255.255.0     VPN connection
to main office

digi.router>
```

Display detailed status information for an OpenVPN client

Enter the show openvpn-client ***x*** command, where ***x*** is the index number of the client, from the first column of summary show openvpn-client command output. For example:

```
digi.router> show openvpn-client 1

 OpenVPN Client Status
 ---------------------
 Description       : VPN connection to main office
 Admin Status      : Up
 Oper Status       : Up
 Remote Server     : 203.0.113.3
 Interface         : ovpn1
 IP Address        : 10.8.0.2
 Mask              : 255.255.255.0
 MTU               : 1500

                                  Received                  Sent
                                  --------                  ----
 Interface Packets  :                   13                     9
 Interface Bytes    :                  940                   684
 Socket Bytes       :                 5201                  4908

digi.router>
```

Debug an OpenVPN tunnel

You can enable debugging on an OpenVPN server or on a specific OpenVPN client. When enabled, debugging messages display in the system log.

Enabling debugging is done by changing the logging level for messages on the OpenVPN server and the OpenVPN client. There are four logging levels, from **0** to **3**. Set this parameter to **0** to record only errors and warnings, and set it to **3** to record fairly complete log activity to help debug an OpenVPN tunnel.

Web

1. On the menu, click **Network > Networks > OpenVPN** and select **OpenVPN Server**. The **OpenVPN Server** page appears.
2. Set the **Logging Level** to **3**.
3. Click **Apply**.
4. On the menu, click **VPN** and select **OpenVPN Client**.
5. Select the OpenVPN client to configure.
6. Set the Logging Level to **3**.
7. Click **Apply**.

Command line

Enable display and logging of debugging messages on an OpenVPN server

To enable display and logging of debugging messages on an OpenVPN server, the command is **openvpn-server verb *n***, where ***n*** is the verbosity level for debugging messages. This value can range from **0**, which disables debugging messages, to **4**, the most detail. For example to set the verbosity level to 3:

```
openvpn-server verb 3
```

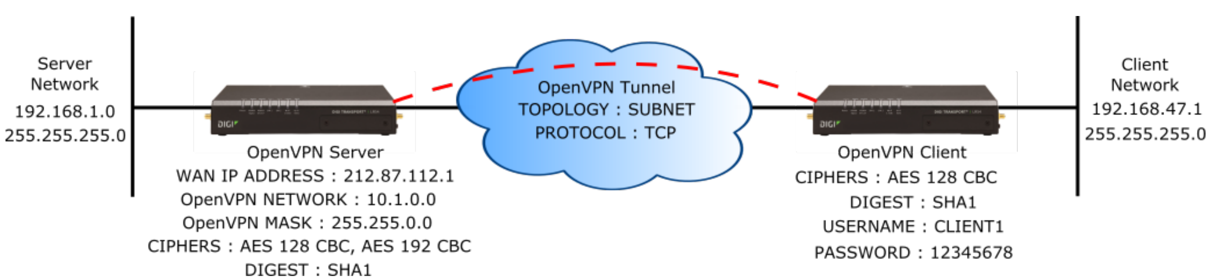
Enable display and logging of debugging messages on an OpenVPN client

To enable display and logging of debugging messages on an OpenVPN client, the command is **openvpn-client x verb *n***, where **n** is the verbosity level for debugging messages, again ranging from **0** to **4**. For example:

```
openvpn-client 1 verb 3
```

Example: OpenVPN tunnel in routing mode with username and password authentication

The following figure shows a sample OpenVPN tunnel in routing mode with username and password authentication:



The configuration settings for the OpenVPN client and server are as follows:

OpenVPN server configuration

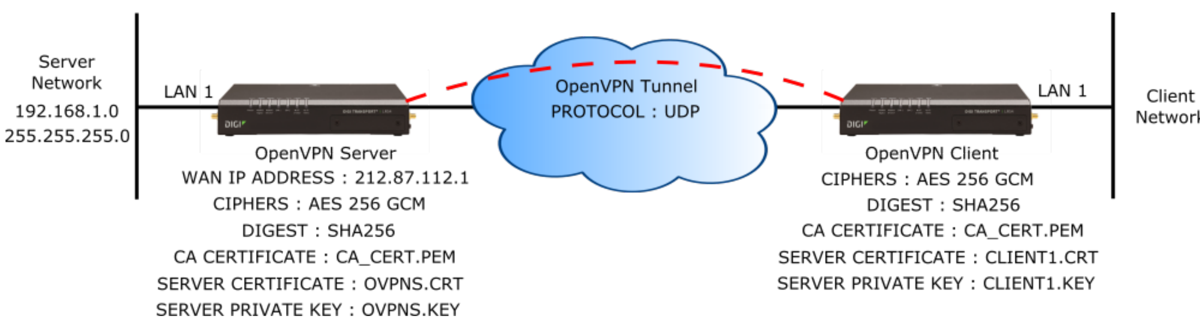
```
openvpn-server state on
openvpn-server topology subnet
openvpn-server protocol tcp
openvpn-server network 10.1.0.0
openvpn-server mask 255.255.0.0
openvpn-server cipher aes-128-cbc,aes-192-cbc
openvpn-server digest sha1
openvpn-server auth-by user-pass
openvpn-server cert ovpns.crt
openvpn-server key ovpns.key

# Client’s username and password
openvpn-user 1 username client1
openvpn-user 1 password 12345678

# Route to server’s LAN to be pushed to client
openvpn-route 1 destination 192.168.1.0
openvpn-route 1 mask 255.255.255.0
```

OpenVPN client configuration

```
openvpn-client 1 state on
openvpn-client 1 server 212.87.112.1
openvpn-client 1 protocol tcp
openvpn-client 1 cipher aes-128-cbc
openvpn-client 1 digest sha1
openvpn-client 1 ca ca.crt
openvpn-client 1 username client1
openvpn-client 1 password 12345678
```

Example: OpenVPN tunnel in bridging mode using certificate authentication

The following figure shows a sample OpenVPN tunnel in bridging mode using certificate authentication:



The configuration settings for the OpenVPN client and server are as follows:

OpenVPN server configuration

```
openvpn-server state on
openvpn-server bridge-mode lan1
openvpn-server protocol udp
```

```
openvpn-server cipher aes-256-gcm
openvpn-server auth-by certificate
openvpn-server ca ca_cert.pem
openvpn-server cert ovpns.crt
openvpn-server key ovpns.key
openvpn-server dh ovpns-dh.pem
```

OpenVPN client configuration

```
openvpn-client 1 state on
openvpn-client 1 server 212.87.112.1
openvpn-client 1 bridge-mode lan1
openvpn-client 1 protocol udp
openvpn-client 1 cipher aes-256-gcm
openvpn-client 1 ca ca.crt
openvpn-client 1 cert client1.crt
openvpn-client 1 key client1.key
```

Generic Routing Encapsulation (GRE)

Generic Routing Encapsulation (GRE) is an IP packet encapsulation protocol. You can use GRE to encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an IP network.

Create a GRE tunnel

Web

1. On the menu, click **Network > Services > GRE**. The **GRE** page appears.
2. Click **New GRE tunnel**.
3. Provide parameters for the new GRE tunnel. See New GRE tunnel page for field descriptions.
4. Click **Apply**.

Command line

To create a GRE tunnel, use the gre command. For example:

```
digi.router> gre 1 ip-address 172.16.1.1
digi.router> gre 1 mask 255.255.255.252
digi.router> gre 1 key 1
digi.router> gre 1 peer 172.16.0.2
digi.router> gre 1 state on
digi.router> save config
```

Delete a GRE tunnel

Web

1. On the menu, click **Network > Services > GRE**. The **GRE** page appears.
2. Select the tunnel you want to delete and click **Delete**.
3. Click **Apply**.

Command line

To delete a GRE tunnel, use the gre command to turn off the state for the tunnel and clear the peer. For example, to turn off GRE tunnel 1:

```
digi.router> gre 1 state off
digi.router> gre 1 peer !
digi.router> save config
```

Edit a GRE tunnel

Web

1. On the menu, click **Network > Services > GRE**. The **GRE** page appears.
2. Open the GRE tunnel you want to edit, and modify parameters as needed. See GRE page for field descriptions.
3. Click **Apply**.

Command line

To modify a GRE tunnel, use the gre command. For example, to change the key for GRE tunnel 2:

```
digi.router> gre 2 key 1234
digi.router> save config
```

Show GRE tunnels

Web

- On the menu, click **Network > Services > GRE**. The **GRE** page appears.

Command line

To show configured GRE tunnels, use the show gre command. For example:

```
digi.router> show gre
```

Example: GRE tunnel over an IPSec tunnel

This example show how to set up a GRE tunnel to run over an IPSec tunnel. This example configures the tunnels between two TransPorts. This setup can be configured using the command line interface (CLI) or the web interface.

1. Create a LAN on both TransPorts with no interfaces and assign each a private IP address with a mask of 255.255.255.255.

   TransPort 1

   ```
   digi.router> lan 10 ip-address 172.16.0.1
   digi.router> lan 10 mask 255.255.255.255
   digi.router> lan 10 interfaces !
   digi.router> lan 10 state on
   digi.router> save config
   ```

   TransPort 2

   ```
   digi.router> lan 10 ip-address 172.16.0.2
   digi.router> lan 10 mask 255.255.255.255
   digi.router> lan 10 interfaces !
   digi.router> lan 10 state on
   digi.router> save config
   ```

2. Create an IPSec tunnel between the LR54s using the LANs defined in step 1 as the local and remote networks.

   TransPort 1 (WAN IP address 1.1.1.1)

   ```
   digi.router> ipsec 1 local-network 172.16.0.1
   digi.router> ipsec 1 local-mask 255.255.255.255
   digi.router> ipsec 1 remote-network 172.16.0.2
   digi.router> ipsec 1 remote-mask 255.255.255.255
   digi.router> ipsec 1 peer 2.2.2.2
   digi.router> ipsec 1 psk key
   digi.router> ipsec 1 local-id tlr1
   digi.router> ipsec 1 remote-id tlr2
   digi.router> ipsec 1 state on
   digi.router> save config
   ```

   TransPort 2 (WAN IP address 2.2.2.2)

   ```
   digi.router> ipsec 1 local-network 172.16.0.2
   digi.router> ipsec 1 local-mask 255.255.255.255
   digi.router> ipsec 1 remote-network 172.16.0.1
   digi.router> ipsec 1 remote-mask 255.255.255.255
   ```

```
digi.router> ipsec 1 peer 1.1.1.1
digi.router> ipsec 1 psk key
digi.router> ipsec 1 local-id tlr2
digi.router> ipsec 1 remote-id tlr1
digi.router> ipsec 1 state on
digi.router> save config
```

3. Create a GRE tunnel between the two LANS you defined in step 1.

   TransPort 1

```
digi.router> gre 1 ip-address 172.16.1.1
digi.router> gre 1 mask 255.255.255.252
digi.router> gre 1 key 1
digi.router> gre 1 peer 172.16.0.2
digi.router> gre 1 state on
digi.router> save config
```

   TransPort 2

```
digi.router> gre 1 ip-address 172.16.1.2
digi.router> gre 1 mask 255.255.255.252
digi.router> gre 1 key 1
digi.router> gre 1 peer 172.16.0.1
digi.router> gre 1 state on
digi.router> save config
```

The GRE tunnel is created inside the IPsec tunnel defined in step 2.

Virtual Router Redundancy Protocol (VRRP)

TransPort devices support Virtual Router Redundancy Protocol (VRRP). VRRP is a standards-based protocol for managing a network redundancy problem, where a single default gateway on a network may result in a single point of failure. VRRP enables two or more routers to act as a single group called a Virtual Router, with one or more routers acting as backup routers in case the master router fails.

Using VRRP, a virtual IP address is shared among the routers in the same group and mapped to the master router. In the event the master router fails, the backup router with the highest priority takes over and the virtual IP address is mapped to it. The routers within a group use an election protocol to dynamically assign the virtual IP address to the router with the highest priority.

For further reading on VRRP, see https://en.wikipedia.org/wiki/Virtual_Router_Redundancy_Protocol.

Configure VRRP protocol

This section describes how to configure VRRP on a TransPort device.

Required configuration items

- Enable VRRP. It is disabled by default.
- Configure the interface that used by VRRP. It is configured to LAN1 by default.

- Configure the unique Router ID integer between 1 and 255 that identifies this router. It is configured to 1 by default.
- Configure the initial state for VRRP that this router will start with. It is configured to "backup" by default.
- Configure the virtual, shared IP address that clients on the LAN will use to connect to this router.
- Configure the VRRP Priority of this router. It is configured to 100 by default.
- Configure the interval in seconds between 1 and 60 at which this router will broadcast advertisement packets to other routers in the same group. It is set to 100 by default.

Additional configuration options

None.

Web

1. If you upgraded the TransPort from a pre-3.1 TransPort system, you need to update some of the DHCP server settings to allow VRRP to work properly. See Configure the default gateway and DNS server addresses for VRRP.
2. On the menu, click **Network > Services> VRRP**. The VRRP page appears.
3. Click the **State** toggle switch to "on" to turn on the VRRP instance.
4. From the **Interface** drop down, select the LAN interface on which VRRP should run.
5. In the **Router ID** field, enter the unique identifier for this router.
6. In the **Interval** field, enter the broadcast interval.
7. In the **Initial State** drop down, select the initial state at which the VRRP will start on this router.
8. In the **IP Address** field, enter the virtual IP address that is used by clients to connect to this router.
9. In the **Priority** field, enter the priority for this route in the group. Note that a router with higher priority gets preference when transitioning to the master router.
10. Click **Apply** to save the changes.

Command line

1. If you upgraded the TransPort from a pre-3.1 TransPort system, you need to update some of the DHCP server settings to allow VRRP to work properly. See for more information.
2. Set the VRRP interface:

```
digi.router> vrrp 1 interface lan2
```

3. Set this router's ID for VRRP:

```
digi.router> vrrp 1 router-id 157
```

4. Set the interval at which this router will send out broadcast packets:

```
digi.router> vrrp 1 interval 25
```

5. Set the initial state at which VRRP will start on this router:

```
digi.router> vrrp 1 initial-state master
```

6. Set the virtual IP address that clients on the LAN will use to connect to this router:

```
digi.router> vrrp 1 ip-address 172.16.32.101
```

7. Turn on VRRP:

```
digi.router> vrrp 1 state on
```

8. Save the configuration:

```
digi.router> save config
```

Configure the default gateway and DNS server addresses for VRRP

If you upgraded the TransPort from a pre-3.1 TransPort system, you need to update some of the DHCP server settings to allow VRRP to work properly. Specifically, the default gateway address and primary DNS server address must point to the VRRP virtual IP address. Set both addresses to **0.0.0.0**. The value 0.0.0.0 allows the LR54 to automatically use the VRRP virtual IP address when VRRP is enabled for that LAN or the IP address of the LR54 if VRRP is not enabled for that LAN.

You can use one of the following methods to reconfigure the DHCP server:

Web

Edit the settings for the LAN and click **Apply**. This updates the DHCP server settings to the correct default of **0.0.0.0**. If you are accessing the LR54 via this LAN interface, you need to reconnect to it using the new IP address. If desired, you may then change the IP address setting back to the original value.

Command line

Run the following commands, replacing **x** with the index of the LAN interface used for VRRP.

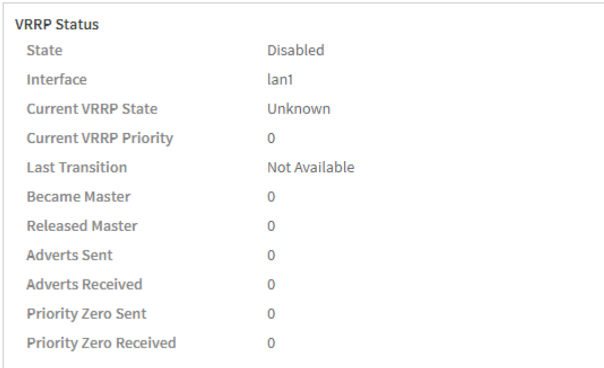
```
dhcp-server x gateway 0.0.0.0
dhcp-server x dns1 0.0.0.0
```

Show VRRP status and statistics

This section describes how to display VRRP status and statistics for a TransPort device.

Web

- On the menu, click **Network > Services> VRRP**. The VRRP page appears.



Command line

Enter the following command:

```
digi.router> show vrrp
```

```
VRRP Status and Statistics
--------------------------
State                  : Enabled
Interface              : lan1

Current State          : Master
Current Priority       : 144

Last Transition        : 01 Jan 00:34

Became Master          : 1
Released Master        : 0
Adverts Sent           : 414
Adverts Received       : 0
Priority Zero Sent     : 0
Priority Zero Received : 0
```

System settings

These topics cover administration and management tasks that need to be performed on TransPort devices periodically.

- Configure system settings
- Show system information settings
- Set system date and time
- Show system date and time
- Managing configuration files
- Reboot the device
- Reset the device to factory defaults

Configure system settings

The TransPort device has several system settings that control the general behavior of the device and information displayed about the device.

Web

On the menu, click **System > Administration**. System options include the following:

- **Remote Manager**: Configures the connection to Digi Remote Manager. See Remote Manager.
- **File System**: Displays the local file system for the TransPort device and allows you to perform file management operations. See File system.
- **Device Console**: Opens the Device Console, from which you can execute commands. See Execute a command from the web interface.
- **Logs**: Displays the event and system logs. See Logs.
- **Firmware Update**: Updates operating system firmware and other device firmware. See Firmware update.
- **Reboot**: Reboots the device. See Reboot the device.

Command line

Use the system command to configure the following system options:

- **System prompt for CLI:** The default system prompt is **digi.router>**. You can configure the system prompt to be any value of up to **16** characters. To use the device's serial number in the system prompt, include **%s** in the **prompt** parameter value. For example, a **prompt** parameter value of **LR54_%s** resolves to **LR54_LR123456**.
- **CLI timeout:** This is the time, in seconds, after which the command-line interface times out if there is no activity. The default is **180** seconds. You can specify any value between **60** and **3600** seconds.

- **Minimum event level to log:** The minimum event level that is logged in the event log. The default value is **info**, but you can also set the event level to the following levels: **emergency**, **alert**, **critical**, **error**, **warning**, **notice**, or **debug**. For more information on the event log, see Logs, Event log levels, and Configure options for event and system logs.
- **Name:** The name of this device.
- **Location:** The location of this device.
- **Contact:** Contact information for this device.
- **Default page size:** The page size for command-line interface output; that is, the number of lines of output displayed. The default value is **40**. You can set the page size to any value between **0** and **100**.
- **Device-specific passwords:** Encrypted passwords can be device-specific or not. When encrypted passwords are device-specific, they are more secure, but cannot be copied onto another device. By default, device-specific passwords are disabled, but you can enable them if required.
- **Description:** A description of this device.
- **TCP passthrough port:** By default, passthrough mode is disabled, but you can enable it by setting a TCP port of any value but **0**. A reboot is required for changes to this setting to take effect.
- **Getting Started Wizard:** By default, the Getting Started Wizard is enabled to start up at system startup, to perform initial device configuration. You can disable the wizard so it is skipped at system startup.
- **IPsec debugging messages:** These messages help diagnose issues with IPsec configuration and interoperability. The default setting for IPsec debugging messages is off, but you can enable them as needed. For more information on IPsec debugging, see Debug an IPsec configuration.

Command-line examples

- Change the system prompt.

```
digi.router> system prompt "LR54_%s"
digi.router> save config
```

- Set the command-line interface timeout. For example, to set the timeout to 60 seconds, enter:

```
digi.router> system timeout 60
digi.router> save config
```

- Configure the event log level. For example, to set the event log level to **warning**, enter:

```
digi.router> system log-level warning
digi.router> save config
```

- Set the page size for command-line interface output. For example, to set the output to **30** lines:

```
digi.router> system page 30
digi.router> save config
```

- Disable the Getting Started Wizard.

```
digi.router> system wizard off
digi.router> save config
```

Show system information settings

Web

1. On the menu, click **Dashboard**.
2. In the **Device** section of the dashboard, view the system information settings. For descriptions of these fields, see the show system command description.

Command line

To show system settings, use the show system command. For example:

```
digi.router> show system

 Model              : LR54W
 Part Number        : LR54-AW401
 Serial Number      : LR000130

 Hardware Version   : 50001899-03 A
 Using Bank         : 0
 Firmware Version   : 1.0.0.3-90c4383 06/19/16 20:31:29
 Bootloader Version: v1.0.0.2
 Using Config File  : config.da0

 Uptime             : 4 Hours, 59 Minutes, 4 Seconds
 System Time        : 20 June 2016, 13:01:04

 CPU                : 3% (min 1%, max 60%, avg 2%)
 Temperature        : 33C

 Description        :
 Location           :
 Contact            :

digi.router>
```

Set system date and time

Having an accurate date and time set on your device is important for a number of reasons, including validating certificates and having accurate timestamps on events in the event log.

There are two methods for setting system date and time:

- Using the Simple Network Time Protocol (SNTP). SNTP continually polls an external NTP time server on either a private company network or the Internet at a configured interval rate. SNTP usually provides an accuracy of less than a second.
- Setting the date and time manually.

Set the date and time using SNTP

Configuration options

- The SNTP server. By default, SNTP is configured to use the Digi SNTP server, **time.devicecloud.com**.
- The SNTP update interval. This is the interval at which TransPort checks the SNTP server for date and time. By default, SNTP is checked **once a day**. At bootup, the device attempts to send an update message to the configured SNTP server every **15** seconds until it receives a response. Once it receives a response, it reverts to the configured update interval.

Command line

To set the date and time using SNTP, use the sntp command.

1. Optional: Set the SNTP server. For example, to set the server to **time.digi.com**:

```
digi.router> sntp server time.digi.com
```

2. Optional: Set the SNTP update interval.

```
digi.router> sntp update-interval 10
```

3. Save the configuration.

```
digi.router> save config
```

Set the date and time manually

To set the date and time manually, use the date command. The date command specifies the time in **HH:MM:SS** format, where seconds are optional, followed by the date, in **DD:MM:YYYY** format.

For example, to manually set the time and date to **14:55:00** on **May 3, 2016**, enter:

```
digi.router> date 14:55:00 03:05:2016
```

Set the time zone and daylight saving time

When the date and time is set using SNTP, the system time is set to Universal Coordinated Time (UTC) and not to your local time. In addition, the date and time, whether it is set manually or using SNTP, does not automatically change to reflect Daylight Saving Time (DST). By setting the time zone, the device displays the local time for that time zone and automatically adjusts for daylight saving time.

You can set the time zone to any of the following values:

canada-atlantic, **canada-central**, **canada-eastern**, **canada-mountain**, **canada-newfoundland**, **canada-pacific**, **europe-central**, **europe-eastern**, **europe-western**, **none**, **uk-ireland**, **us-alaska**, **us-arizona**, **us-central**, **us-eastern**, **us-hawaii**, **us-indiana**, **us-mountain**, **us-pacific**. The default is **none**.

Optional: Set the time zone. For example, to set the time zone to US Eastern:

```
digi.router> system timezone us-eastern
```

Show system date and time

Web

1. On the menu, click **Dashboard**.
2. In the **Device** panel, view the **System Time** field.

Command line

To display the current system date and time, use the date command.

```
digi.router> date

system time: 14:55:06, 03 May 2016

digi.router>
```

Firmware update

Maintaining your TransPort device requires periodic updates to firmware for the main operating system and subsystems.

- Update system firmware
- Update cellular module firmware

Update system firmware

This topic shows how to update the TransPort operating system firmware.

System firmware files

The TransPort operating system firmware images consist of a single file with the following naming convention:

***<platform>-<version>*.bin**.

For example, **lr54-1.2.3.4.bin**.

Certificate management for firmware images

The system firmware files are signed to ensure that only Digi-approved firmware load onto the device. The TransPort device validates the system firmware image as part of the update process and only successfully updates if the system firmware image can be authenticated.

Multiple system firmware images

The TransPort device can store up to **2** system firmware images in its flash memory. The system firmware update operation overwrites the system firmware image not used with the new system firmware image. The TransPort device automatically switches to boot the new system firmware image when it is next rebooted. This means that the TransPort device should always have at least one good system firmware image. If a newly loaded firmware image is corrupted, the device automatically falls back to run the system firmware image it was running before the system firmware update.

Manage firmware updates using Digi Remote Manager

If you have a network of many devices, you can use Digi Remote Manager **Profiles** to manage firmware updates. Profiles ensures all your devices are running the correct firmware version and that all newly installed devices are updated to that same version. For more information, see the **Profiles** section of the Digi Remote Manager User Guide.

Web

Digi maintains a repository of available TransPort firmware versions. You can update system firmware to one of these versions, or upload a previously downloaded firmware file.

Update firmware from available versions in the Digi repository

1. On the menu, click **System > Administration > Firmware Update**.
2. Select a version from the **Available Versions** list. The system firmware file downloads.
3. Click **Update Firmware**.

Download and upload firmware

1. Download the TransPort operating system firmware from the Digi Support FTP site. Locations for the latest firmware are listed below.

Model	Latest firmware file location
TransPort LR54	http://ftp1.digi.com/support/firmware/transport/LR54/latest

2. Select **Upload firmware** from the **Available Versions** list.
3. Click **Choose File**.
4. Browse to the system firmware file location and select the file.
5. Click **Update Firmware**.

Command line

1. Download the TransPort operating system firmware from the Digi Support FTP site; locations for the latest firmware for each model are listed below.

Model	Latest firmware file location
TransPort LR54	http://ftp1.digi.com/support/firmware/transport/LR54/latest

2. Load the firmware image onto the device. To do so, use a Windows SFTP client, such as FileZilla, or use the Linux applications **scp** and **sftp**. For example, to use **scp**:

```
$ scp lr54-1.1.0.6.bin admin@192.168.1.1:lr54-1.1.0.6.bin
Password:
lr54-1.1.0.6.bin
                100%   22MB   1.0MB/s   00:22
$
```

3. Check that the firmware file has been successfully uploaded to the device.

```
digi.router> dir

  File                         Size   Last Modified
  ------------------------------------------------------
  ssh_host_rsa_key.pub          382   Fri May  6 11:05:02
  ssh_host_dsa_key.pub          590   Fri May  6 11:05:05
  config.da0                   1541   Mon May 23 12:32:22
  config.fac                   1760   Fri May  6 11:44:26
  lr54-1.1.0.6.bin         22935287   Mon Jul 23 12:36:31

  Remaining User Space: 79,015,936 bytes

digi.router>
```

4. Update the firmware by entering the update command, specifying the **firmware** keyword and the firmware file name.

```
digi.router> update firmware lr54-1.1.0.6.bin

Verifying lr54-1.1.0.6.bin, please wait ...
Verified lr54-1.1.0.6.bin
Updating firmware using lr54-1.1.0.6.bin, please wait ...
Firmware update complete. Please reboot to run new firmware.
digi.router>
```

5. Reboot the device to run the new firmware image using the reboot command.

```
digi.router> reboot
```

6. Once the device has rebooted, verify the running firmware version by entering the show system command.

```
digi.router> show system

Model              : LR54W
Part Number        : LR54-AW401
Serial Number      : LR000038

Hardware Version   : Not available
Using Bank         : 1
Firmware Version   : 1.1.0.6 06/17/16 13:37:58
Bootloader Version: 1003
Using Config File : config.da0

Uptime             : 14 Minutes, 29 Seconds
System Time        : 23 July 2016, 13:08:09

CPU                : 3% (min 1%, max 70%, avg 3%)
Temperature        : Not available

Description        :
Location           :
Contact            :

digi.router>
```

Update cellular module firmware

Digi provides the cellular module files for all certified cellular carriers for TransPort devices on the Digi repository of cellular module firmware files.

Enter the **update modem** command, specifying your carrier name: **att**, **verizon**, or **generic**. For example:

```
digi.router> update modem verizon

Start retrieving modem firmware files
verizon.nvu         100%[=====================>]  18.83K  --.-KB/s   in 0.08s
verizon.cwe         100%[=====================>]  61.22M   103KB/s   in 2m 59s
Done retrieving modem firmware files
Preparing modem for firmware download

Please wait for switching modem to download mode
Downloading
Firmwar
e.................................................................................
..
Flash Complete, Waiting for Modem to Reboot
```

```
...........................
Firmware Download Completed

PRI Upgrade successful
Firmware Upgrade successful
Firmware download completed
```

Managing configuration files

The TransPort configuration file contains all of the configuration for a device and the configuration is applied each time the device boots up.

Default configuration file

The default configuration file is named **config.da0**. If needed, you can change the default configuration file. See Switch configuration files for details.

Factory default configuration file

The configuration file named **config.fac** contains the factory default configuration. When you reset a device back to factory defaults, the **config.fac** is applied when the device boots up.

You can customize the **config.fac** file if you want to create a custom factory-default configuration.

Saving configuration changes

When you make a change to the TransPort configuration, the changes are not automatically saved to the configuration file. You must explicitly save configuration changes; otherwise, the configuration changes are discarded when the device next boots up. See Save configuration settings to a file for details.

Configuration file sections

There are several sections of note in the configuration file.

Timestamp section

The first section of the configuration file is a **timestamp** that identifies the date and time when the configuration file was saved and the user who updated the file.

```
digi.router> more config.da0

# Last updated by admin on Mon May 23 12:32:22 2016
```

Main configuration section

Next is the **main configuration section** of the configuration file. This section contains the commands and parameters required to configure features.

- Passwords in the file are stored in encrypted form. You cannot display passwords in clear-text form.
- Comment lines in the file begin with a pound sign **#** character.

```
lan 1 description "Ethernet and Wi-Fi LAN network"
lan 1 state "on"
lan 1 interfaces "eth2,eth3,eth4,wifi1,wifi5g"
lan 1 ip-address "192.168.1.1"
lan 2 description "Guest Wi-Fi network"
```

```
lan 2 interfaces "wifi2,wifi5g2"
lan 2 ip-address "192.168.2.1"
wifi 1 state on
wifi 1 ssid LR54-2.4G-%s
wifi 1 password "$00$U2FsdGVkX1++WEpeSUigEAS11pE+aU+uGGAqPgOF8iU="
wifi5g 1 state on
wifi5g 1 ssid LR54-2.4G-%s
wifi5g 1 password "$00$U2FsdGVkX1/aQwCR/VgIcG0r/Un/Px9a3XBRkPI9euQ="
user 1 name "admin"
user 1 password
"$6$n8bHC46Qo.TQfT/r$61hWHSyO71CYMrIOdUMUSB9vq7powrwcMftGAL912MLQutR9LHhW2k1LQrsZxETCz3sAw4DL4vZU20b1ZxxC."
⋮
```

Firewall configuration section

The next section is the **firewall configuration section**, containing rules for controlling which packets are allowed into and out of the device. For more information, see Using firewall and firewall6 commands.

```
[FIREWALL]
*nat
-A POSTROUTING -o eth1 -j MASQUERADE
COMMIT
[FIREWALL_END]

digi.router&gt;
```

Shared configuration files and device-specific passwords

TransPortpasswords are stored in the configuration file in an encrypted form and the passwords are not device-specific. Another TransPort can read the configuration file and decipher the encrypted form of the password. Because passwords are encrypted and cannot be displayed in clear text, you can safely share configuration files across multiple devices.

However, if you do not intend to share configuration files, you can enable the **device-specific passwords** option. When the **device-specific passwords** option is enabled, only the device on which the password was configured can decipher the password. See the system command **device-specific-passwords** parameter for details.

Save configuration settings to a file

Configuration changes are **not** automatically saved. This means that the device discards any unsaved changes when the device reboots.

Web

- On configuration pages, click **Apply** to save changes to the configuration file immediately.

Command line

Enter the **save config** command.

```
digi.router> save config
```

Switch configuration files

Command line

You can store multiple configuration files on a device, but the device uses only one configuration file when it reboots. The default configuration file is named **config.da0**.

To switch to another configuration file:

1. If needed, identify the current configuration file using the show system command.
2. Change the current configuration file using the update command.
3. If needed, create the configuration file you specified in the **update** command using the save command.

Step 1: Identify the current configuration file

To identify the current configuration file, use the show system command. For example:

```
digi.router> show system

Model             : LR54W
Part Number       : LR54-AW401
Serial Number     : LR000038

Hardware Version  : Not available
Using Bank        : 1
Firmware Version  : 1.1.0.6 06/17/16 13:37:58
Bootloader Version: 201602051801
Using Config File : config.da0

Uptime            : 14 Minutes, 29 Seconds
System Time       : 23 July 2016, 13:08:09

CPU               : 3% (min 1%, max 70%, avg 3%)
Temperature       : Not available

Description       :
Location          :
Contact           :

digi.router>
```

Step 2: Change the configuration file name

To change the name of the current configuration file, use the update command. For example:

```
digi.router> update config <filename>
```

The file you specified is used the next time the device reboots.

Step 3: Save the current configuration to the configuration file

If the configuration file name you specified on the update command does not exist, use the save command **config** parameter to create the new configuration file by saving the current configuration.

To save the current configuration, use the save command **config** parameter. For example:

```
digi.router> save config
```

Use multiple configuration files to test configurations on remote devices

You can use multiple configuration files and the autorun command to safely test a new configuration on a remote device that might result in the remote device going offline, in which case the device cannot be remotely accessed.

To test the configuration on a remote device, create a new configuration file with the configuration you want to test. In addition to the configuration, include two autorun commands:

- The first autorun command automatically reverts the device to use the original configuration file.
- The second autorun command schedules a reboot after a period of time.

Example: Test configuration file

For example, suppose you creates a test configuration file named **test.cfg**.

The **test.cfg** file changes the **cellular 1 apn** parameter and executes two autorun commands to automatically revert the device back to use the **config.da0** configuration file and to reboot in **5** minutes. It then saves the configuration to **test.cfg** and reboots the device.

```
update config test.cfg
cellular 1 apn new-apn-to-test
autorun 1 command “update config config.da0”
autorun 2 command “reboot in 5”
save config
reboot
```

If the TransPort device does not come back online, the device automatically reverts to the old (working) configuration file, **config.da0**, and reboots after **5** minutes.

If the device comes back online after being rebooted with the configuration—that is, the device connected with the new cellular Access Point Name (APN)— you can cancel the scheduled reboot using the **reboot cancel** command.

```
digi.router> reboot cancel
```

Using the copy and update commands, you can copy the configuration file to the final configuration file, and change the configuration file name.

```
digi.router> copy test.cfg config.da0
digi.router> update config config.da0
```

Reboot the device

You can reboot the TransPort device immediately, or schedule a reboot after a period of time or at a specific time.

You can cancel a scheduled reboot, if required.

Note Any unsaved configuration is lost during the reboot. You may want to save your configuration settings to a file before rebooting. See Save configuration settings to a file.

Web

- Click **System > Administration > Reboot**.

A message displays the maximum time expected for the reboot operation. When the reboot completes, the device reconnects and the **Device Login** page displays.

Command line

Reboot the device immediately

To reboot the device immediately, enter:

```
digi.router> reboot
```

Reboot the device after a period of time

To reboot the device after a period of time, enter the following command, where **MM** represents the number of minutes to wait before rebooting.

```
digi.router> reboot in MM
```

For example, to reboot in 5 minutes:

```
digi.router> reboot in 5
```

Reboot the device at a specific time

To reboot the device at a specific time, enter the following command, where **HH:MM** is the time at which to reboot. The time is in 24-hour format.

```
digi.router> reboot at HH:MM
```

For example, to reboot at 6:30 PM (18:30 hours):

```
digi.router> reboot at 18:30
```

Cancel a scheduled reboot

To cancel a scheduled reboot, enter:

```
digi.router> reboot cancel
```

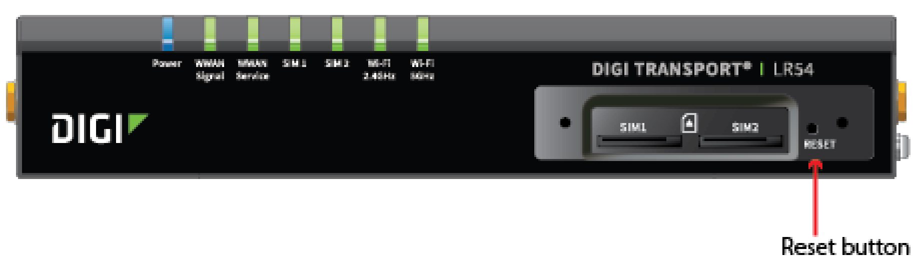
Reset the device to factory defaults

Resetting the device to factory defaults performs the following actions:

- Clears all configuration settings. When the device boots up again, it uses the configuration in file **config.fac**. If the **config.fac** file has been deleted, the device will regenerate it with the default Digi configuration.
- Deletes all user files including Python scripts.
- Regenerates SSH keys.
- Clears event and system log files.
- Creates a new event in the event log indicating a factory reset.

To reset the device to factory defaults:

1. Locate the reset button on your device. For the **TransPort LR54**, the **Reset** button is located beneath the SIM card slot cover on the front panel, to the right of SIM slot 2. Remove the SIM cover to access the **Reset** button.



2. Press and hold the **Reset** button for **15** seconds. The device reboots automatically.

   The device reset to factory defaults. Follow the instructions in the *TransPort Quick Start Guide* to reconfigure the device.

Diagnostics

These topics cover the diagnostics capabilities available for TransPort devices.

- Logs
- Analyze traffic
- Use the "ping" command to troubleshoot network connections
- Use the "traceroute" command to diagnose IP routing problems
- Use the "show tech-support" command

Logs

The **event log** contains events related to the functionality of the TransPort device. These events include information about configuration changes, interface state changes, user access, and so on.

The **system log** contains events related to the low-level system. While these events are typically not useful to end users, they are useful to Digi support and engineering when diagnosing device issues.

You can view logs from either the web interface or the command line.

Log entry format

Event and system log entries have the following format:

```
<timestamp> <level> <application> <event message>
```

For example, here is an event log entry showing a configuration change by the user **admin** to the **system timeout** parameter which has been logged by the command-line interface (CLI) application at the **info** log level:

```
2016-05-03 12:05:29.653107 user.info CLI[admin]: system timeout 3600
```

In the web interface Log viewer page, here is an event log entry showing the login to the command line interface by the user **admin**:

Date	Level	Source ▲	Message
− 2017-01-26 01:27:18.332389	user.notice	CLI[admin@web]:	Login by admin.

Configure options for event and system logs

You can configure options for event and system logs.

- For event logs, you can set the level of events you want to log, enable logging to a file, and enable logging to a syslog server.
- For system logs, you can enable logging to a file and enable logging to a syslog server.

Web

1. On the menu, click **System > Administration > Logs**.
2. Click **Log Configuration**.
3. Under **Event Log**:

   Log level: Select the log level. See Event log levels.

   Log to file: Enable or disable logging to a file.

Log to syslog: If you want to log to a syslog server, select a syslog server for the event log.

4. Under **System Log**:

   Log to file: Enable or disable logging to a file.

   Log to syslog: If you want to log to a syslog server, select a syslog server for the system log.

5. Click **Apply**.

Command line

Enter the system log-level command, specifying the event log level.

```
system log-level <level>
```

For example:

```
system log-level warning
```

Configure syslog servers

You can configure up to two syslog servers for storing event and system logs.

Web

1. On the menu, click **System > Administration > Logs**.
2. Click **Syslog Server Configuration**.
3. For each syslog you want to configure, provide the following:

   Server: Specify the IPv4 IP address for the server.

   Port: Specify the listening port for the server. The default is port **514**.

   Mode: Specify the mode for syslog traffic: UDP or TCP. The default is **UDP**.

4. Click **Apply**.

Command line

To configure syslog server 1:

```
syslog 1 server my_syslog1.company.com
syslog 1 server-port 516
syslog 1 mode udp
```

To configure syslog server 2:

```
syslog 2 server my_syslog2.company.com
syslog 2 server-port 517
syslog 2 mode udp
```

Display logs

Web

1. On the menu, click **System > Administration > Logs**.
2. Click **Log viewer**. See Log viewer page for details on all page fields.
3. To stream the event log, click ▶ under **Event Log.** To stream the system log, click ▶ under **System Log.** For more information on the controls in the Log Viewer, see Log viewer page.

Command line

To display the event log, use the show log command.

Note If the logs are stored in flash, the show log command displays the logs stored in flash.

For example:

```
digi.router> show log

2016-06-03 16:54:50.643501 user.notice CLI[admin]: Login by admin.
2016-06-03 16:54:47.245107 user.notice CLI[]: Login failure by .
2016-06-03 16:54:39.831107 user.info cellular_monitor[1245]: modem support =
HE910 4G support = 0
2016-06-03 16:54:39.653107 user.info cellular_monitor[1245]: Model = HE910
```

To display the system log, use the **show log system** command variant. For example:

```
digi.router> show log system

2017-01-26 00:22:36.157657 kern.warning kernel:ESW: Link Status Changed - Port2
Link Down
2017-01-26 00:22:36.157263 kern.info kernel:device wifi5g1 entered promiscuous
mode
2017-01-26 00:22:36.157263 kern.info kernel:device wifi1 entered promiscuous mode
2017-01-26 00:22:36.042680 kern.info kernel:lan1: port 3(eth4) entering
forwarding state
2017-01-26 00:22:36.042576 kern.info kernel:lan1: port 3(eth4) entering
forwarding state
2017-01-26 00:22:36.042255 kern.info kernel:device eth4 entered promiscuous mode
2017-01-26 00:22:33.312014 kern.info kernel:lan1: port 2(eth3) entering
forwarding state
2017-01-26 00:22:33.311843 kern.info kernel:lan1: port 2(eth3) entering
forwarding state
2017-01-26 00:22:33.297835 kern.info kernel:device eth3 entered promiscuous mode

digi.router>
```

Find and filter log file entries

You can find and filter log file entries based on search criteria entered in the Log Viewer Search bar. The find operation searches every field of a log file entry, including the date.

1. On the menu, click **System > Administration > Logs**.
2. Click **Log viewer**.
3. In the **Find** field, enter the text to search for in messages.
4. To clear the filter, delete the text in the **Find** field.

Save logs to a file

By default, the event and system logs are stored in RAM. This means the event and system logs are lost when the device is rebooted. You can configure the device to store the event and system logs in a file to help diagnose issues if the device is being rebooted. When enabled, the event log is stored in the file **event.log** and the system log is stored in the file **system.log**.

The maximum size of a log file is **2 MB**. When the event and system log files reach this size, they are backed up to **event.log.0** and **system.log.0** respectively, and the log file is cleared out.

WARNING! Saving event and system logs to files and keeping them resident for some time is not recommended for normal operations, as this practice can lead to additional wear to the LR54 flash memory.

Web

1. On the menu, click **System > Administration > Logs**.
2. Click **Log Configuration**.
3.
   - To write event log entries to a file: Under **Event Log** in the **Log to File** setting, click **On**.
   - To write system log entries to a file: Under **System Log**, in the **Log to File** setting, click **On**.
4. Click **Apply**.

Command line

To log events to the file **event.log** and **system.log**, use the system command, specifying the **log-to-file** parameter:

```
system log-to-file on
```

To log system events to the file **system.log**, use the system command, specifying the **log-system-to-file** parameter:

```
system log-system-to-file on
```

Download log files

The download operation downloads the entire event or system log, not just those entries currently displayed in the Log Viewer. For the event log, file **event.log** is downloaded. For the system log, file **system.log** is downloaded.

When your device is configured to save logs to a file, only the active log file can be downloaded through this procedure. If you need to download a backup log file (for example, **event.log.0**), you can download that backup log file using the **File System** download function. See Upload and download files.

1. On the menu, click **System > Administration > Logs**.
2. Click **Log viewer**. See Log viewer page for details on all page fields.
3. Under **Event Log** or **System Log**, click the button. The file download proceeds according to download procedures of the browser you are using, and stores the file in your browser's default download directory.

Clear logs

As needed, you can clear the event or system log. This results a single new entry in the event or system log after the previous events are cleared. This clear function is useful when you want to start all logs fresh from a certain point in time.

This operation is available from the command line only.

Command line

To clear the event log, use the **clear log** command. For example:

```
digi.router> clear log
```

To clear the system log, use the **clear log system** command. For example:

```
digi.router> clear log system
```

Event log levels

Events can be logged at various levels of severity. The log levels, from highest to lowest level of severity, are as follows:

Log level	Conditions indicated
Emergency	Device is unusable.
Alert	Events that should be resolved immediately.
Critical	A feature may not be working correctly.
Error	An error has occurred with a particular feature.
Warning	An error will occur if no action is taken.
Notification	Events that are unusual, but are not error conditions.
Informational	Normal operational messages that require no action.
Debugging	Useful information for Digi Technical Support and Engineering to use in debugging the device.

The default level at which events are logged is **info**, which means that any event of a level **info** or higher is logged. To change the event logging level, see Configure options for event and system logs.

Analyze traffic

The traffic analyzer captures data traffic on any of the WAN and LAN interfaces and decodes the captured data traffic for diagnosis.

You can capture data traffic on multiple interfaces at the same time, and define capture filters to reduce the amount of data traffic captured.

You can capture up to **10** MB of data traffic, in two **5** MB files.

To perform more detailed analysis, you can upload the captured data traffic from the device and view it using a third-party application, such as Wireshark (www.wireshark.org).

WARNING! Enabling data traffic capture significantly affects device performance.

Capture data traffic

You can capture up to **10** MB of data traffic, in **2** files of up to **5** MB each.

WARNING! Enabling data traffic capture significantly affects device performance.

To capture data traffic, use the analyzer command.

The analyzer command has the following parameters:

state
Enables or disables the capturing of data traffic. As this configuration can be saved, it means that the device can be configured to start capturing data as soon as it boots up.

interfaces
Defines the interfaces on which data is captured.

filter
Defines the capture filter to reduce the amount of data traffic being captured. The filters use the BPF syntax for defining filters, described at http://www.tcpdump.org/manpages/pcap-filter.7.html. See Example filters for capturing data traffic for examples of using the syntax to define filters.

Note Captured data traffic is captured into RAM and is lost when the device reboots, unless you save the traffic to a file. See Save captured data traffic to a file.

To capture data on the **eth1** and **cellular1** interfaces, the configuration commands are:

```
digi.router> analyzer state on
digi.router> analyzer interfaces eth1,cellular1
digi.router>
```

Example filters for capturing data traffic

To filter captured data, use the **analyzer** command filter parameter. For example:

```
digi.router> analyzer filter ip host 192.168.1.1
```

For more information on filtering, see http://www.tcpdump.org/manpages/pcap-filter.7.html.

The following are examples of filters on data traffic capturing for several types of network data.

Example IPv4 capture filters

Capture traffic to and from IP host **192.168.1.1**:

```
digi.router> analyzer filter ip host 192.168.1.1
```

Capture traffic from IP host **192.168.1.1**:

```
digi.router> analyzer filter ip src host 192.168.1.1
```

Capture traffic to IP host **192.168.1.1**:

```
digi.router> analyzer filter ip dst host 192.168.1.1
```

Capture traffic for a particular IP protocol:

```
digi.router> analyzer filter ip proto <protocol>
```

where **<protocol>** can be a number in the range of **1** to **255** or one of the following keywords: **\icmp**, **icmp6**, **igmp**, **pim**, **ah**, **esp**, **vrrp**, **\udp**, or **\tcp**.

Note **icmp**, **tcp**, and **udp** are also filter keywords and must be preceded with \ when used with **protocol**.

Capture traffic to and from a TCP port **80**:

```
digi.router> analyzer filter ip proto \tcp and port 80
```

Capture traffic to UDP port **53**:

```
digi.router> analyzer filter ip proto \udp and dst port 53
```

Capture traffic from UDP port **53**:

```
digi.router> analyzer filter ip proto \udp and src port 53
```

Capture to and from IP host **10.0.0.1** but filter out ports **22** and **80**:

```
digi.router> analyzer filter ip host 10.0.0.1 and not (port 22 or port 80)
```

Example Ethernet capture filters

Capture Ethernet packets to and from host **00:40:FF:0F:45:94**:

```
digi.router> analyzer filter ether host 00:40:FF:0F:45:94
```

Capture Ethernet packets from host **00:40:FF:0F:45:94**:

```
digi.router> analyzer filter ether src 00:40:FF:0F:45:94:
```

Capture Ethernet packets to host **00:40:FF:0F:45:94**:

```
digi.router> analyzer filter ether dst 00:40:FF:0F:45:94
```

Show captured data traffic

To view the captured data traffic, use the show analyzer command. The command output shows the following information for each packet:

- The packet number
- The timestamp for when the packet was captured
- The length of the packet and the amount of data captured
- Whether the packet was sent or received by the device
- The interface on which the packet was sent or received
- A hexadecimal dump of the packet of up to **256** bytes
- Decoded information of the packet

The output uses indents received packets as a visual cue for sent and received packets.

The output is paged. Press the spacebar to view the next page of data. Enter **Q** to navigate to the command prompt.

For example:

```
digi.router> show analyzer

Packet 1 : Nov-09-2016 09:26:06.256857, Length 74 bytes (Captured Length 74 bytes)

Sent on interface eth1

  00 04 2d f4 f8 aa 00 40  ff 0f 45 94 08 00 45 00   ..-....@ ..E...E.
  00 3c 19 73 00 00 7f 01  e2 da 2f 00 00 64 08 08   .<.s.... ../..d..
  08 08 08 00 08 e1 00 01  44 7a 61 62 63 64 65 66   ........ Dzabcdef
  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi

 Ethernet Header
   Destination MAC Addr : 00:04:2d:f4:f8:aa
   Source MAC Addr      : 00:40:ff:0f:45:94
   Ethernet Type        : IP (0x0800)
 IP Header
   IP Version           : 4
   Header Length        : 20 bytes
   ToS                  : 0x00
   Total Length         : 60 bytes
   ID                   : 6515 (0x1973)
   Flags                :
   Fragment Offset      : 0 (0x0000)
   TTL                  : 127 (0x7f)
   Protocol             : ICMP (1)
   Checksum             : 0xe2da
   Source IP Address    : 47.0.0.100
   Dest. IP Address     : 8.8.8.8
 ICMP Header
   Type                 : Echo Request (8)
   Code                 : 0
   Checksum             : 0x08e1
 ICMP Data
   61 62 63 64 65 66 67 68  69 6a 6b 6c 6d 6e 6f 70   abcdefgh ijklmnop
   71 72 73 74 75 76 77 61  62 63 64 65 66 67 68 69   qrstuvwa bcdefghi


 Packet 2 : Nov-09-2016 09:26:06.284248, Length 74 bytes (Captured Length 74 bytes)

 Received on interface eth1

           00 40 ff 0f 45 94 00 04  2d f4 f8 aa 08 00 45 00   .@..E... -.....E.
           00 3c e7 97 00 00 36 01  5d b6 08 08 08 08 2f 00   .<....6. ]...../.
           00 64 00 00 10 e1 00 01  44 7a 61 62 63 64 65 66   .d...... Dzabcdef
           67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
           77 61 62 63 64 65 66 67  68 69                     wabcdefg hi

         Ethernet Header
           Destination MAC Addr : 00:40:ff:0f:45:94
           Source MAC Addr      : 00:04:2d:f4:f8:aa
           Ethernet Type        : IP (0x0800)
         IP Header
           IP Version           : 4
           Header Length        : 20 bytes
           ToS                  : 0x00
           Total Length         : 60 bytes
           ID                   : 59287 (0xe797)
           Flags                :
           Fragment Offset      : 0 (0x0000)
           TTL                  : 54 (0x36)
           Protocol             : ICMP (1)
           Checksum             : 0x5db6
           Source IP Address    : 8.8.8.8
           Dest. IP Address     : 47.0.0.100
        ICMP Header
           Type                 : Echo Reply (0)
           Code                 : 0
           Checksum             : 0x10e1
        ICMP Data
           61 62 63 64 65 66 67 68  69 6a 6b 6c 6d 6e 6f 70   abcdefgh ijklmnop
           71 72 73 74 75 76 77 61  62 63 64 65 66 67 68 69   qrstuvwa bcdefghi

digi.router>
```

Clear captured data traffic

To clear the captured data traffic, use the clear command, specifying **clear analyzer**.

```
digi.router> clear analyzer
digi.router>
```

Save captured data traffic to a file

Data traffic is captured to RAM and not saved when the device reboots. To upload the file to a PC, you must first save the captured data to a file.

Command line

Use the **save** command. For example:

```
digi.router> save analyzer lan1.pcapng
digi.router>
```

Use the "ping" command to troubleshoot network connections

Use the ping command troubleshoot connectivity problems. See the ping command description for command syntax and examples.

Stop ping commands

To stop pings when the number of pings to send (the **count** parameter) has been set to a high value, enter **Ctrl+C**.

Ping to check internet connection

To check your internet connection, enter:

```
ping 8.8.8.8
```

Use the "traceroute" command to diagnose IP routing problems

Use the traceroute command to diagnose IP routing problems. This command traces the route to a remote IP host and displays results. The traceroute command differs from ping in that traceroute shows where the route fails, while ping simply returns a single error on failure.

See the traceroute command description for command syntax and examples. The traceroute command has several parameters, but they are generally not used or required:

- **hops**: The maximum number of hops to allow.
- **host**: The IP address of the destination host.
- **interface**: The interface for sending the route trace.
- **size**: The size, in bytes, of the message to send.
- **src-ip**: Use this source IP address for outgoing packets.
- **timeout**: The maximum number of seconds to wait for a response from a hop.

Example

This example shows using **traceroute** to verify that the TransPort device can route to host **8.8.8.8** (www.google.com) through the default gateway. The command output shows that **15** routing hops were required to reach the host:

```
digi.router> show route

Destination Gateway Metric Protocol Idx Interface Status
-------------------------------------------------------------------------------------
10.101.1.0/24 0.0.0.0 0 Connected lan1 UP
192.168.1.0/24 0.0.0.0 0 Connected lan3 UP
10.101.12.0/24 0.0.0.0 0 Connected lan4 UP
10.101.8.0/24 0.0.0.0 0 Connected lan2 UP
192.168.8.0/24 0.0.0.0 0 Connected eth1 UP
default 192.168.8.1 1 Static eth1 UP
digi.router>
digi.router> traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
1 192.168.8.1 (192.168.8.1) 0.613 ms 0.384 ms 0.452 ms
2 10.240.192.1 (10.240.192.1) 19.039 ms 19.070 ms 18.985 ms
3 96.34.84.22 (96.34.84.22) 19.279 ms 25.487 ms 27.848 ms
4 96.34.80.240 (96.34.80.240) 32.560 ms 96.34.80.238 (96.34.80.238) 32.593 ms 96.34.80.230 (96.34.80.230) 32.688
ms
5 96.34.2.12 (96.34.2.12) 32.494 ms 42.865 ms 96.34.81.23 (96.34.81.23) 32.418 ms
6 96.34.81.190 (96.34.81.190) 32.590 ms 31.993 ms 31.993 ms
7 96.34.2.12 (96.34.2.12) 42.367 ms 24.334 ms 29.216 ms
8 96.34.0.51 (96.34.0.51) 34.155 ms 33.648 ms 27.910 ms
9 96.34.148.2 (96.34.148.2) 34.194 ms 96.34.0.137 (96.34.0.137) 25.195 ms 37.465 ms
10 216.239.46.248 (216.239.46.248) 31.285 ms 31.068 ms 216.58.215.44 (216.58.215.44) 37.434 ms
11 96.34.148.2 (96.34.148.2) 40.958 ms 209.85.143.112 (209.85.143.112) 31.281 ms 96.34.148.2 (96.34.148.2) 40.600
ms
12 216.239.46.248 (216.239.46.248) 21.515 ms 209.85.250.70 (209.85.250.70) 63.989 ms 216.58.215.44 (216.58.215.44)
30.455 ms
13 209.85.251.163 (209.85.251.163) 26.121 ms 216.239.48.235 (216.239.48.235) 27.429 ms 209.85.251.161
(209.85.251.161) 26.867 ms
14 216.239.48.160 (216.239.48.160) 33.652 ms 64.233.174.11 (64.233.174.11) 45.731 ms 209.85.250.70 (209.85.250.70)
29.792 ms
15 216.239.48.235 (216.239.48.235) 30.280 ms 72.14.234.55 (72.14.234.55) 34.517 ms 209.85.251.243 (209.85.251.243)
38.733 ms
16 * 8.8.8.8 (8.8.8.8) 40.967 ms 44.762 ms
digi.router>
```

By entering a **whois** command on another Unix device, the output shows that the route is as follows:

1. **192/8**: The local network of the TransPort device.
2. 1**92.168.8.1**: The local network gateway to the Internet.
3. **96/8**: Charter Communications, the network provider.
4. **216/8**: Google Inc.

Stop the traceroute process

To stop the traceroute process, enter **Ctrl-C**.

Use the "show tech-support" command

The show tech-support command displays information useful for Digi Technical Support when handling issues with your device.

You can execute this command from the command-line interface or from the Device Console in the web interface.

The syntax for show tech-support is as follows:

```
show tech-support [filename]
```

The **filename** parameter is optional. If specified, the information is saved to the given filename.

The **show tech-support** command executes the following commands:

- **show system**
- **show config more**
- **config.da0** (or whichever configuration file is in use)

- **show route**
- **show lan**
- **show lan x**, for whichever LAN interface's **admin** status is **up**
- **show dhcp**
- **show wan**
- **show wan x**, for whichever WAN interface's **admin** status is **up**
- **show cellular**
- **show ipsec**
- **show ipsec x**, for whichever IPsec tunnel is configured (**state**=**on**)
- **show log**
- **show log system**
- **show firewall**
- **show firewall6**
- **show tech-support**

In the output, each executed command output is prefixed with the command name; for example:

```
show system
===========
```

File system

File system

The TransPort local file system has approximately **100 MB** of space available for storing files, such as Python programs, alternative configuration files and firmware versions, and release files, such as cellular module images.

See Managing configuration files for information on managing configuration files.

Create a directory

Web

1. On the menu, click **System > Administration > File System**. The **File System** page appears.
2. Navigate to the file system location where you want to create a directory and click ⊞. The **New Directory** dialog appears.
3. Enter a name for the directory and click **Create**.

   To create a nested directory, navigate to the subdirectory by double-clicking the parent directory. Click ⊞ for the New Directory dialog. Alternately, you can create a nested directory by including the parent directory with the slash delimiter **/** in the directory name field.

Command line

To make a new directory, use the mkdir command, specifying the name of the directory.

For example:

```
digi.router> mkdir test
digi.router> dir

 File                            Size   Last Modified
 -------------------------------------------------------
 test                                   Directory
 config.da0                       763   Sun Mar  5 12:36:20
 config.fac                       186   Mon Feb 21 03:00:17

 Remaining User Space: 102,457,344 bytes

digi.router>
```

Display directory contents

Web

1. On the menu, click **System > Administration > File System**. The **File System** page appears.
2. Double-click the directory row to navigate to a sub-directory and display contents.

Command line

To display directory contents, use the dir command. For example:

```
digi.router> dir

 File                            Size   Last Modified
 ---------------------------------------------------------
```

```
 test                              Directory
 config.da0                   763  Sun Mar  5 12:36:20
 config.fac                   186  Mon Feb 21 03:00:17

 Remaining User Space: 102,457,344 bytes


digi.router>
```

Change the current directory

Web

1. On the menu, click **System > Administration > File System**. The **File System** page appears.
2. Navigate to the desired directory or subdirectory.
3. To return to the home directory, click .

Command line

To change the current directory, use the cd command, specifying the directory name.

For example:

```
digi.router> dir

 File                        Size   Last Modified
 ---------------------------------------------------------
 test                               Directory
 config.da0                   763   Sun Mar  5 12:36:20
 config.fac                   186   Mon Feb 21 03:00:17

Remaining User Space: 102,457,344 bytes
digi.router>
digi.router> cd test

digi.router> dir

 File                        Size   Last Modified
---------------------------------------------------------

Remaining User Space: 102,457,344 bytes


digi.router>
```

Delete a directory

Web

1. On the menu, click **System > Administration > File System**. The **File System** page appears.
2. Select the directory to delete.
3. Click . A warning dialog displays.
4. Click **OK**.

Note This operation deletes any files in the directory along with the directory.

Command line

1. Make sure the directory is empty.
2. Use the rmdir command, specifying the name of the directory to remove. For example:

```
digi.router> dir

 File                          Size   Last Modified
 ---------------------------------------------------------
 test                                 Directory
 config.da0                     763   Sun Mar  5 12:36:20
 config.fac                     186   Mon Feb 21 03:00:17

Remaining User Space: 102,457,344 bytes
digi.router>
digi.router> rmdir test
Directory test is not empty
ERROR
digi.router>
digi.router> dir test

 File                          Size   Last Modified
 ---------------------------------------------------------
 config.tst                     186   Wed Apr  5 07:10:41

Remaining User Space: 102,457,344 bytes

digi.router>
digi.router> del test/config.tst
digi.router>
digi.router> rmdir test
digi.router>
digi.router> dir

 File                          Size   Last Modified
 ---------------------------------------------------------
 config.da0                     763   Sun Mar  5 12:36:20
 config.fac                     186   Mon Feb 21 03:00:17

Remaining User Space: 102,457,344 bytes

digi.router>
```

Display file contents

Web

There is no direct way to display file contents from the **System - File Management** page. Instead you must download the file and then view the downloaded file from a file editor.

1. On the menu, click **System > Administration > File System**. The **File System** page appears.
2. Select the file.
3. Click .
4. When the file is downloaded, open it with an editor.

Command line

To display the contents of a file, use the more command, specifying the name of the file. For example:

```
digi.router> more config.da0

# Last updated by username on Thu Nov 19 14:26:02 2015

eth 1 ip-address "192.168.1.1"
cellular 1 apn "mobile.o2.co.uk"
cellular 1 state "on"
user 1 name "username"
user 1 password "$1$4WdqUHrv$K.aB78KILuxVpesZtyveG/"

digi.router>
```

Copy a file

To copy a file, use the copy command, specifying the existing file name, followed by the name of the new copy.

For example, to copy file **config.da0** to a file in the main directory named **backup.da0**, and then to a file named **test.cfg** in the **test** directory, enter the following:

```
> digi.router> dir

 File                        Size   Last Modified
----------------------------------------------------------
 test                               Directory
 config.da0                   763   Sun Mar  5 12:36:20
 config.fac                   186   Mon Feb 21 03:00:17

Remaining User Space: 102,457,344 bytes
digi.router>
digi.router>
digi.router> copy config.da0 backup.da0
digi.router>
digi.router> dir

 File                        Size   Last Modified
----------------------------------------------------------
 test                               Directory
 config.da0                   763   Sun Mar  5 12:36:20
 config.fac                   186   Mon Feb 21 03:00:17
 backup.da0                   763   Wed Apr  5 07:22:29

Remaining User Space: 102,457,344 bytes
digi.router>
digi.router> copy config.da0 test/test.cfg

digi.router>
digi.router> dir test

 File                        Size   Last Modified
 ---------------------------------------------------------
 test.cfg                     763   Wed Apr  5 07:24:45

Remaining User Space: 102,457,344 bytes


digi.router>
```

Rename a file

Web

1. On the menu, click **System > Administration > File System**. The **File System** page appears.
2. Select the file to rename. Navigate to the file's directory location, if necessary.

3. Click ✎. Enter the new file name.
4. Click **OK**.

Command line

To rename a file, use the rename command, specifying the existing name and the new name.

For example:

```
digi.router> dir

 File                          Size   Last Modified
---------------------------------------------------------
 test                                 Directory
 config.da0                     763   Sun Mar  5 12:36:20
 config.fac                     186   Mon Feb 21 03:00:17
 backup.da0                     763   Wed Apr  5 07:22:29

Remaining User Space: 102,457,344 bytes
digi.router>
digi.router> rename backup.da0 test.da0
digi.router>
digi.router> dir

 File                          Size   Last Modified
---------------------------------------------------------
 test                                 Directory
 test.da0                       763   Wed Apr  5 07:22:29
 config.da0                     763   Sun Mar  5 12:36:20
 config.fac                     186   Mon Feb 21 03:00:17

Remaining User Space: 102,453,248 bytes

digi.router>
```

Delete a file

Web

1. On the menu, click **System > Administration > File System**. The **File System** page appears.
2. Select or navigate to the file to delete.
3. Click 🗑. A confirm delete dialog displays.
4. Click **OK**.

Note To delete all files in a directory, see Delete a directory.

Command line

To delete a file, use the del command, specifying the filename to delete.

For example, to delete a file named **test.cfg** in the **test** directory, enter the following:

```
digi.router>
digi.router> dir

 File                          Size   Last Modified
```

```
 ---------------------------------------------------------
 test                               Directory
 test.da0                      763  Wed Apr  5 07:22:29
 config.da0                    763  Sun Mar  5 12:36:20
 config.fac                    186  Mon Feb 21 03:00:17

 Remaining User Space: 102,453,248 bytes

digi.router>
digi.router> del test.da0
digi.router>
digi.router> dir test

 File                         Size   Last Modified
 ---------------------------------------------------------
 test.cfg                      763   Wed Apr  5 07:24:45

 Remaining User Space: 102,453,248 bytes


digi.router>
digi.router> del test/test.cfg
digi.router> dir test

 File                         Size   Last Modified
 ---------------------------------------------------------
 Remaining User Space: 102,449,152 bytes

digi.router>
```

Upload and download files

From the web interface

Web

Upload files

1. On the menu, click **System > Administration > File System**. The **File System** page appears.
2. Click .
3. Use the local file system to browse to the location of the file to upload. Select the file and click **Open** to start the upload.
4. A progress dialog appears. When the upload operation is complete, the file is displayed in the file list.

Download files

1. On the menu, click **System > Administration > File System**. The **File System** page appears.
2. Navigate to the file you want to download and click the file to select it.
   To download the event log, select file **event.log**. To download the system log, select file **system.log**.
3. Click . The file downloads to your system using your browser's download settings.

Command line

You can download and upload files using utilities such as Secure Copy (SCP), SSH File Transfer Protocol (SFTP), or an SFTP application, such as FileZilla.

Upload files using SCP

To upload a file to a device using SCP, use this syntax:

```
scp filename username@ip_address:filename
```

For example, to upload a file named **script.py** to a device at IP address **192.168.1.1**:

```
$ scp script.py john@192.168.1.1:script.py
Password:
script.py
    100%  3728    0.3KB/s   00:00
```

Download files using SCP

To download a file from a device using SCP, use this syntax:

```
scp username@ip_address:filename filename
```

For example, to download a file named **config.da0** to the local directory from a device at IP address **192.168.1.1** using the username **john**:

```
$ scp john@192.168.1.1:config.da0 config.da0
Password:
config.da0
    100%  254     0.3KB/s   00:00
```

Upload files using SFTP

This example uploads a file named **lr54-1.0.2.10.bin** to TLR device **192.168.1.1** using the username **john**:

```
$ sftp john@192.168.1.1
Password:
Connected to 192.168.1.1
sftp> put lr54-1.0.2.10.bin
Uploading lr54-1.0.2.10.bin to lr54-1.0.2.10.bin
lr54-1.0.2.10.bin
     100%  24M  830.4KB/s   00:00
sftp> exit
$
```

Download files using SFTP

This example downloads a file named **config.da0** from TransPort device **192.168.1.1** using the username **john** to the local directory:

```
$ sftp john@192.168.1.1
Password:
Connected to 192.168.1.1
sftp> get config.da0
Fetching config.da0 to config.da0
config.da0
     100%  254    0.3KB/s   00:00
sftp> exit
$
```

Diagnostics and troubleshooting

Troubleshooting tools and resources

There are several tools and resources available within your TransPort device and on the Digi website for dealing with configuration or other device issues.

- Logs
- Analyze traffic
- Use the "ping" command to troubleshoot network connections
- Use the "traceroute" command to diagnose IP routing problems
- Use the "show tech-support" command
- Reboot the device
- Digi support site
- Digi knowledge base

Digi support site

For support for your TransPort device, go to www.digi.com/support.

Digi knowledge base

To access the Digi knowledge base, go to knowledge.digi.com/.

Troubleshooting Ethernet interfaces

Ethernet LED does not illuminate

Device cannot communicate on WAN/ETH1 port

Device cannot communicate on ETH2, ETH3, or ETH4 ports

Ethernet LED does not illuminate

Problem

Ethernet LED does not illuminate on the **WAN/ETH1**, **ETH2**, **ETH3**, or **ETH4** ports.

Probable Cause

The most likely cause is a bad connection or a bad Ethernet cable.

Solution

1. Replace the Ethernet cable and verify that both ends are plugged in. if the Ethernet LED is now illuminated on the Ethernet port, skip the rest of these steps .

2. Open the command line interface. Enter the command **eth n**, where **n** is replaced with the Ethernet port number. In the **eth** command output, verify that the state of the Ethernet port is set to **on**. For example, if you are diagnosing port **WAN/ETH1**, enter:

```
digi.router> eth 1
   description
   duplex                       auto
   mtu                          1500
   speed                        auto
   state                        on

digi.router>
```

3. If the state is set to **off**, enter another eth command to change the state to be **on** and see if that fixes the problem. For example, to change the state of port **WAN/ETH1**, enter:

```
digi.router> eth 1 on
```

4. Enter **show eth n** (where n is replaced with the Ethernet port number) from the TransPort device. Verify that the **Operational Status** is **Up** and that the **Link** status does not say **No connection**. For example, on Ethernet port **WAN/ETH1**, enter:

```
digi.router> show eth 1
 Eth Status and Statistics Port 1
 --------------------------------
 Description      :
 Admin Status     : Up
 Oper Status      : Down
 Up Time          : 48 Minutes, 23 Seconds

 MAC Address      : 00:40:FF:0F:48:1C
 Link             : No connection

 Received                             Sent
 --------                             ----
 Rx Unicast Packet     : 21512        Tx Unicast Packet    : 16147
 Rx Broadcast Packet   : 917          Tx Broadcast Packet  : 8
 Rx Multicast Packet   : 5638         Tx Multicast Packet  : 7
 Rx CRC Error          : 0            Tx CRC Error         : 0
 Rx Drop Packet        : 0            Tx Drop Packet       : 0
 Rx Pause Packet       : 0            Tx Pause Packet      : 0
 Rx Filtering Packet   : 13631488     Tx Collision Event   : 0
 Rx Alignment Error    : 0
 Rx Undersize Error    : 0
 Rx Fragment Error     : 0
 Rx Oversize Error     : 0
 Rx Jabber Error       : 0
```

5. If the **Link** status shows there is **No connection**, try plugging the Ethernet cable into a different Ethernet port.
6. If the new Ethernet port shows the same **No connection** status, either the cable is bad, or there is a problem at the other end. If the new port shows a valid connection, something may be wrong with the TransPort hardware. Contact Digi Technical Support.

Device cannot communicate on WAN/ETH1 port

Problem

The TransPort device cannot communicate on its **WAN/ETH1** port.

Probable Cause

The most likely cause is that the WAN port is not correctly configured.

Solution

The following steps assume you are using **WAN/ETH1** as a WAN port, which is the default configuration. If you are using **WAN/ETH1** as a LAN port, see the steps in Device cannot communicate on ETH2, ETH3, or ETH4 ports.

1. Check the Ethernet LED for the **WAN/ETH1** port. If the LED is not lit, verify the physical connection following the steps in Ethernet LED does not illuminate.
2. Open the command line interface. Enter **show wan n**, where n is the number of the WAN. In the command output, verify that the IP Address, mask, and gateway are set. For example, if **WAN/ETH1** is configured for **WAN1**, which is the default configuration, enter:

```
digi.router> show wan 1

 WAN 1 Status and Statistics
 ---------------------------
 WAN Interface : eth1
 Admin Status  : Up
 Oper Status   : Down

 IP Address    :
 Mask          :
 Gateway       :
 DNS Server(s) :

Probes are not being used

              Received            Sent
              --------            ----
Packets          28225           16256
Bytes         19551951         3199259
```

3. If the IP configuration is not set, as shown above, the most likely problem is that the port has not been configured correctly. To view the current configuration, enter the command **wan n**, where **n** is the number of the WAN. In the command output, verify that the interface for the WAN is set to the Ethernet port. Set the correct interface if necessary. For example:

```
digi.router> wan 1

   activate-after            0
   allow-https-access        off
   allow-ssh-access          off
   dhcp                      on
   dns1
   dns2
   gateway
   interface                 eth1
   ip-address
   mask                      255.255.255.0
   nat                       on
   probe-host
   probe-interval            60
   probe-size                64
   probe-timeout             5
   retry-after               300
   timeout                   300
```

4. If the interface is correct, but the port still does not get an IP configuration, enter another **wan n** command for that port to verify that the DHCP setting is correct. If the network to which the WAN is connected uses DHCP to assign IP addresses, make sure DHCP is on for the WAN port.

```
digi.router> wan 1

   activate-after             0
   allow-https-access         off
   allow-ssh-access           off
   dhcp                       on
   dns1
   dns2
   gateway
   interface                  eth1
   ip-address
   mask                       255.255.255.0
   nat                        on
   probe-host
   probe-interval             60
   probe-size                 64
   probe-timeout              5
   retry-after                300
   timeout                    300
```

5. If the network does not use DHCP to assign IP addresses, you need to disable DHCP on the WAN port, and configure a static IP address. For example, if your network uses static IP addresses and the TransPort device has been assigned the address **10.10.10.10** with subnet mask **255.255.255.0** and a gateway of **10.10.10.1**, you would enter the following commands:

```
digi.router> wan 1 dhcp off
digi.router> wan 1 ip-address 10.10.10.10
digi.router> wan 1 mask 255.255.255.0
digi.router> wan 1 gateway 10.10.10.1
```

6. If these steps do not resolve your problem, contact Digi Technical Support.

Device cannot communicate on ETH2, ETH3, or ETH4 ports

Problem

The TransPort device is not able to communicate on its **ETH2**, **ETH3**, or **ETH4** port.

Probable Cause

Ports **ETH2**, **ETH3**, and **ETH4** are usually bridged together to form a LAN. The most likely problem is that the LAN is not correctly configured.

Solution

1. Check the Ethernet LED for the Ethernet port. If the LED is not lit, verify the physical connection, following the steps in Ethernet LED does not illuminate.
2. Open the command line interface. Enter the command **lan n**, where **n** is the number of the LAN with which the Ethernet port is associated. In the command output, verify that the Ethernet port really is assigned to the LAN. For example, if the port is supposed to be associated with **LAN 1**, enter:

```
digi.router> lan 1

  description                 Ethernet and Wi-Fi LAN network
  dhcp-client                 off
  dns1
  dns2
  interfaces                  eth2,eth3,eth4,wifi1,wifi5g1
  ip-address                  192.168.1.1
  mask                        255.255.255.0
  mtu                         1500
  state                       on
```

3. If the Ethernet port is not listed as one of the LAN's interfaces, add it using the command **lan n interfaces**, where **n** is the Ethernet port number.
4. Verify that the LAN is enabled. If needed, enter the command **lan n state on** to enable the LAN.

```
digi.router> lan 1

  description                 Ethernet and Wi-Fi LAN network
  dhcp-client                 off
  dns1
  dns2
  interfaces                  eth2,eth3,eth4,wifi1,wifi5g1
  ip-address                  192.168.1.1
  mask                        255.255.255.0
  mtu                         1500
  state                       on
```

5. Verify that the LAN is configured with an IP address. Use the **lan n ip-address**command to set the IP address if necessary.

```
digi.router> lan 1

  description                  Ethernet and Wi-Fi LAN network
  dhcp-client                  off
  dns1
  dns2
  interfaces                   eth2,eth3,eth4,wifi1,wifi5g1
  ip-address                   192.168.1.1
  mask                         255.255.255.0
  mtu                          1500
  state                        on
```

6. Use the **dhcp-server** command to verify the LAN's DHCP server is set up correctly. The gateway field should be set to the LAN's IP address, and the ip-address-start and ip-address-end fields should be within the subnet configured for the LAN port. For example, suppose the LAN is configured with the IP address **192.168.1.1** and subnet **255.255.255.0**. If DHCP server **1** was used to service the LAN, its configuration should look something like this:

```
digi.router> dhcp-server 1

  dns1                         192.168.1.1
  dns2
  gateway                      192.168.1.1
  ip-address-end               192.168.1.199
  ip-address-start             192.168.1.100
  lease-time                   1440
  mask                         255.255.255.0
  state                        on
```

7. Verify that the PC or device plugged into that port has been configured to use DHCP to get an IP address.
8. If the PC still cannot communicate with the Ethernet port, try plugging a different PC into the port and see if that can communicate over the port. If it can, the problem is with the first PC or device.

9. Enter the **show dhcp** command to verify that there are some available DHCP leases left. For example, the DHCP server configuration creates a range of **100** DHCP leases, and the DHCP status below shows that only one is in use. If your status showed that all available DHCP leases were in use, you would have to either update the DHCP server configuration to add more leases, or remove some devices from the LAN.

```
digi.router> show dhcp

DHCP Status
 -----------
 IP address      Hostname            MAC Address        Lease Expires At
 -----------------------------------------------------------------------
 192.168.1.100   WAL-CMS-PJACO1      6c:19:8f:b1:68:99  17:23:05, 04 Apr
2017

digi.router>
```

10. If you still have communications issues with the LAN port, contact Digi Technical Support.

Troubleshooting cellular interfaces

Verify cellular connectivity

Test SIM slot 1

1. With the router powered off, insert a SIM card into the **SIM 1** slot of the TransPort device.
2. Access the TransPort command line interface. See Command line interface access options.

3. Issue the following command to confirm that the device acknowledges the SIM card:

```
digi.router> cellular 1 state on
digi.router> show cellular
```

The cellular status and statistics should be displayed. Look for the SIM status and whether the **ICCID** can be read:

```
Cellular Status and Statistics
------------------------------
…
SIM status                : Using SIM1
ICCID                     : 89333603603003003000
```

If the **ICCID** does not appear in the cellular status and statistics, repeat this procedure with a different SIM card. If the **ICCID** still does not display, request an RMA with the reason **SIM SLOT 1 DETECTION FAIL**.

Test cellular connectivity with SIM 1

Note Make sure that both antennas are connected and the router is located in an area with good signal strength.

1. With the router powered off, insert a SIM card into the **SIM 1** slot of the TransPort device.
2. Open the command line interface. See Command line interface access options.
3. Configure an APN for SIM 1. Issue the following commands:

```
digi.router> cellular 1 apn my_apn
digi.router> cellular 1 state on
digi.router> show cellular
```

If the APN requires a username and password, add the following:

```
digi.router> cellular 1 apn-password my_apn_password
digi.router> cellular 1 apn-username my_apn_username
Warning: Wait for up to 5 minutes and check for a valid IP address
```

The cellular status and statistics table should appear. Look for the IP address:

```
Cellular Status and Statistics
------------------------------
…
IP address                : 10.123.456.90
Mask                      : 255.255.255.248
```

```
Gateway                  : 255.255.255.0
DNS servers              : 192.168.1.1, 192.168.1.2
```

If a valid IP address is not found, issue the show tech-support command from the device and email the command output to Digi Technical Support for assistance. To extract the show tech-support output from the device, see the following application note: http://ftp1.digi.com/support/documentation/TLR_QN04_show_tech_support.PDF

Test SIM slot 2

1. With the router powered off, insert a SIM card into the SIM 2 slot of the TransPort device.
2. Open the command line interface. See Command line interface access options.
3. Issue the following commands to confirm that the device acknowledges that the SIM card is installed in SIM slot 2:

```
digi.router> cellular 1 state off
digi.router> cellular 2 state on
digi.router> show cellular
```

The cellular status and statistics table should appear. Look for the **SIM status** and if the **ICCID** can be read.

```
Cellular Status and Statistics
------------------------------
…
SIM status               : Using SIM2
ICCID                    : 89333603603003003000
```

If the **ICCID** does not appear, try with a different SIM card. If the **ICCID** still does not appear, contact Digi Technical Support, with the following subject line and problem description: **SIM slot 2 detection fail**.

Test cellular connectivity with SIM 2

1. Make sure that both antennas are connected and the router is located in an area with good signal strength.
2. With the router powered off, insert a SIM card into the SIM 2 slot of the LR54.
3. Open the command line interface. See Command line interface access options.
4. Configure an APN for SIM 2. Issue the following commands:

```
digi.router> cellular 1 state off
digi.router> cellular 2 apn my_apn
digi.router> cellular 2 state on
digi.router> show cellular
```

If the APN requires a username and password, add the following:

```
digi.router> cellular 2 apn-password my_apn_password
digi.router> cellular 2 apn-username my_apn_username
```

```
Cellular Status and Statistics
------------------------------
…
IP address             : 10.123.456.90
Mask                   : 255.255.255.248
Gateway                : 255.255.255.0
DNS servers            : 192.168.1.1, 192.168.1.2
```

If a valid IP address is NOT found, enter the show tech-support command from the device and email the command output to Digi Technical Support for assistance. For instructions on extracting show tech-support output from the device, see the following application note:

http://ftp1.digi.com/support/documentation/TLR_QN04_show_tech_support.PDF

Check cellular signal strength

1. While the internet link is still connected from following steps in Verify cellular connectivity, access the command line interface. See Command line interface access options.
2. Enter the show cellular command. In the output, view the values displayed for the **Signal strength** and **Signal quality** fields:

```
digi.router> show cellular

 Cellular Status and Statistics
 ------------------------------
 ⋮
 Signal strength       : Excellent (69dBm)
 Signal quality        : Excellent (10dB)
 ⋮
```

3. Check that the signal strength is roughly what you normally get with the same antenna in the test location, which should be **+/- 10 dBm**. If the signal strength is much worse than normal, try these things:
   - Swap the antennas with another set.
   - Insert a SIM card from a different carrier.
4. Ideally, repeat the test on a known working TransPort device that contains the same type of radio module in the same location. Make sure this known working TransPort device is connected using the same antenna and the same provider. If it does, and the signal strength is much better (**+ 10 dBm**) than the suspected bad router, contact Digi Technical Support, with the following subject line and problem description: **Cellular signal strength low**.

Troubleshooting the serial interface

Verify serial connectivity

Problem

When using the command line interface, command output displays unusual or garbled characters.

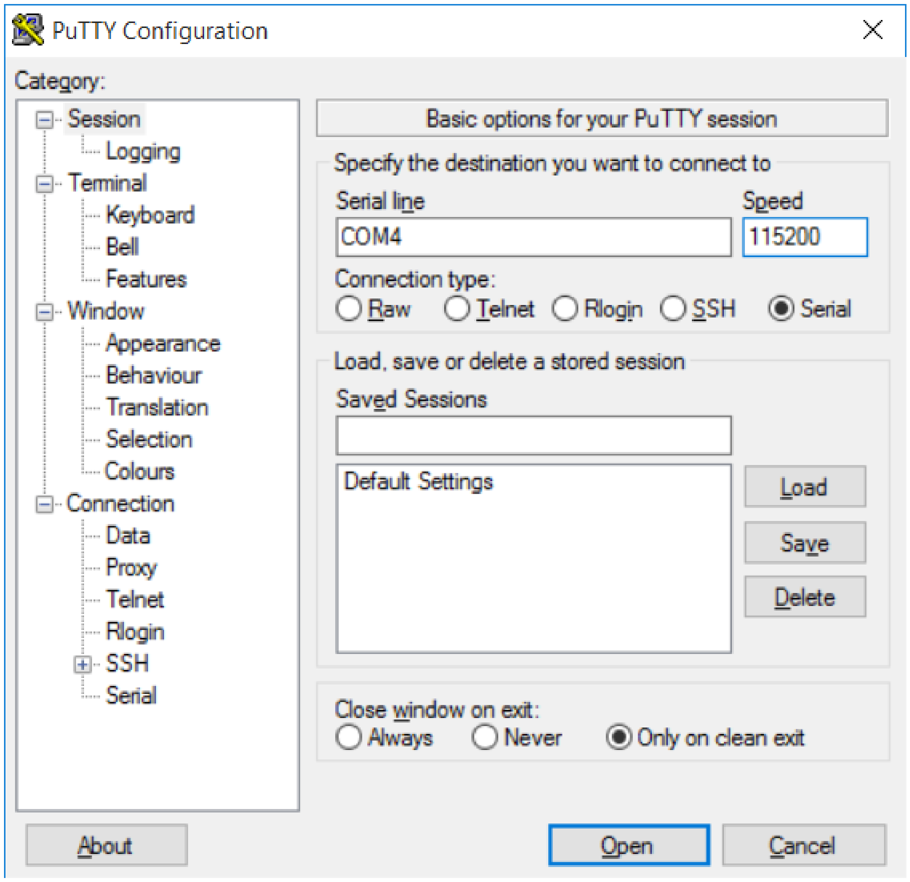
Probable causes

- Serial cable is bad.
- Wrong type of serial cable is being used for the serial connection.
- Wrong pinout being used for the serial connection.
- The baud rate setting for serial communication is set to different rates on either end of the connection.

Solution

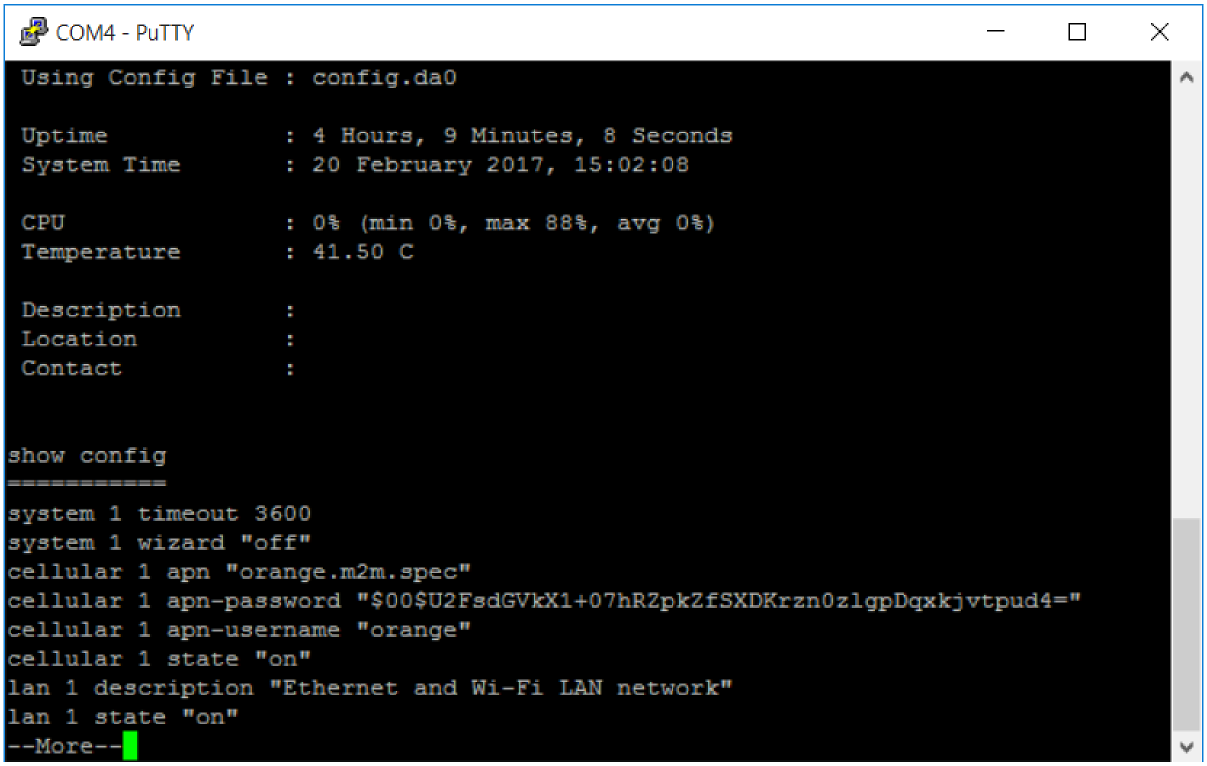
Test the serial connection.

1. Using a straight-through serial cable, connect a PC serial port to the TransPort device. For pinout details, see the hardware reference guide for your model.
2. Open a terminal application such as PuTTy, with the following serial port configuration:
    - Serial Port: **COM X**, where **X** is the serial port number of the computer, usually **1**.
    - Speed: **115200**
    - Connection type: depending on the application, make sure **Serial** is selected for the connection type.



3. Click **Open**. A terminal window appears.
4. When prompted, enter your current username and password.

5. Check that you can send and receive command line interface commands, for example, enter show tech-support:



6. If the command output does not contain any garbled or unusual output, the serial connection is up and working appropriately.
   If the command output has garbled output or unusual characters, continue to the next step.
7. Connect to the TransPort device web interface over the network. See Log in to the web interface if you need help accessing the web interface.
8. On the web interface, click **System** and select **Device Console**. The Device Console displays.

9. In the Device Console, enter the command **serial 1**. The serial settings display.

10. Verify that the serial port is configured for **115200** baud, **8** databits, **1** stopbit, **no** flow control, and **no** parity. Verify that the **state** setting of the serial interface is **on**. For example:

```
digi router > serial 1

baud 115200
databits 8
description
flowcontrol none
parity none
state on
stopbits 1
```

11. If the serial configuration is incorrect, follow the instructions in Configure the serial interface to set the correct configuration.
12. If you have verified that the serial ports on both the PC and the TransPort device are correctly configured, and you still cannot access the command-line interface over the console, try replacing the serial cable.
13. If serial issues persist after following these steps, contact Digi Technical Support, with the subject line **Serial connectivity issues**.

TransPort LR54 model-specific troubleshooting

The following topics apply to TransPort LR54 models only.

Check TransPort54 LEDs

Recover a TransPort54 device

Check TransPort54 LEDs

To check that all LEDs are working properly, set the device into recovery mode. See Recover a TransPort54 device. This forces all LEDs to flash. Make sure to turn off and turn back on the unit once this test has been completed to retrieve full functionality.

If any of the LEDs do not light up properly during the bootup or device recovery process, contact Digi Technical Support. In the email subject line and problem description, specify **x LED failure**, where **x** is any of the following LED names:

- **Power**
- **WWAN Signal**
- **WWAN Service**
- **SIM 1**
- **SIM 2**
- **Wi-Fi 2.4GHz**
- **Wi-Fi 5GHz**
- **WAN/ETH1***

- **ETH2***
- **ETH3***
- **ETH4***

*On these ports, the upper Ethernet LED illuminates if a working network cable is attached only.

Recover a TransPort54 device

If other troubleshooting steps do not resolve issues you are experiencing with your TransPort54 device, you may need to perform a device recovery procedure.

Condition

When applying the power, the only LED that illuminates is the **Power** LED.

Probable cause

Corrupted firmware image on the device.

Solution

Follow the steps below to recover the device. The device recovery operation loads new firmware onto a TransPort LR54 device.

Note This process does not update or erase any previous configuration in the device. If you want to erase the current configuration, perform a factory reset instead; see Reset the device to factory defaults.

Assemble required equipment

Recovering a TransPort device requires the following:

- A PC running a Microsoft Windows-based operating system or any other operating system that allows web browsing and file upload with an Ethernet port.
- An Ethernet cable to connect the TransPort device and the PC.
- An Internet connection to download the latest firmware image from our support web site. You can perform this download operation on a separate computer.

The diagram shows how the equipment is connected during the device recovery process.

CAUTION! The computer must be connected to the **ETH2** port of the TransPort device for the recovery process to work.

Download the latest system firmware image

Download the latest system firmware image file. Go to the firmware download link listed in the topic Update system firmware. Download the **lr54-*.bin** file.

Configure a static IP address on the PC

Configure the following static IP address on the Ethernet interface on the PC:

- IP address: **192.168.1.2**
- Mask: **255.255.255.0**

The TransPort LR54 device will use an IP address of **192.168.1.1**.

Set the device to recovery mode

1. Disconnect the device from power.
2. Locate the **Reset** button on the device.

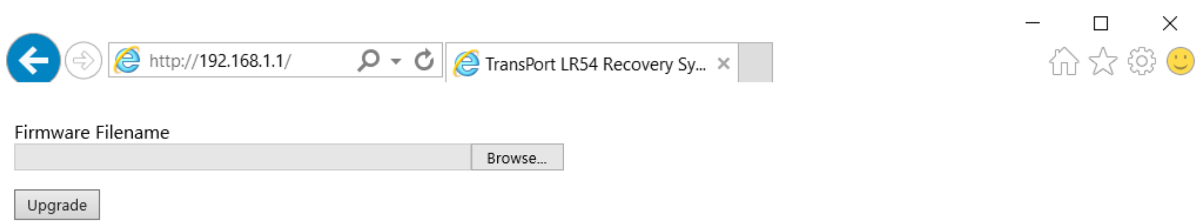
   TransPort LR54: The **Reset** button is located beneath the SIM card slot cover on the front panel, to the right of SIM slot 2. Remove the SIM cover to access the **Reset** button.

3. Press and hold the **Reset** button while connecting the power, and keep holding down the **Reset** button while the unit powers up.
4. Watch for all the LEDs on the device to blink.

5. Wait for all the LEDs to turn off and the **Power** LED to be blink rapidly. The device is now in recovery mode.
6. Now you can release the **Reset** button.

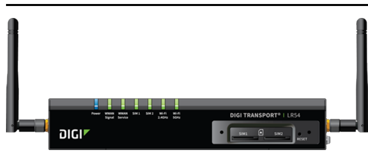
Upload new firmware

1. Open a web browser and navigate to **http://192.168.1.1**. The TransPort LR54 Recovery System navigation window appears.



2. Click the **Browse** button. Select or navigate to the previously downloaded firmware file.
3. Click **Upgrade**.
4. The **Power** LED blinks slowly during the upgrade process. This process takes approximately **30** seconds. When the process completes, all LEDs will be blinking.

WARNING! Do not remove the power from the unit during this process.

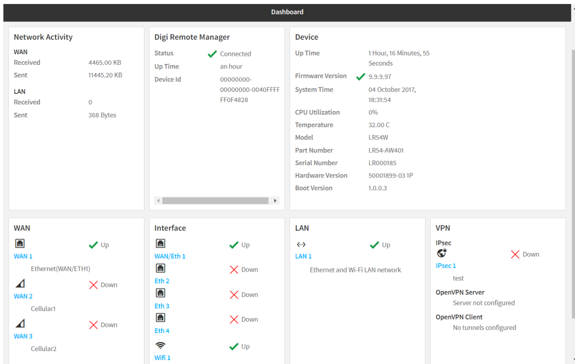


5. Disconnect the power and reconnect it. The firmware has been successfully loaded on to TransPort LR54 device and is ready to use.

Web reference

The dashboard

The dashboard shows the current state of the device.



Dashboard display areas

Dashboard area	Description
Network activity	Summarizes network statistics: the total number of bytes sent and received over all Wide Area Networks (WANs) and Local Area Networks (LANs), including all WANs/LANs configured and active, disabled, and/or disabled.
Digi Remote Manager	Displays the device connection status for Digi Remote Manager, the amount of time the connection has been up, and the Digi Remote Manager device ID. See Remote Manager.
Device	Displays device status, statistics, and identifying information. See the show system command for details. For **Firmware Version**, a green checkmark ✔ indicates the firmware is up to date and a red X indicates a firmware update is available. See Update system firmware for instructions.
WAN	Displays all configured Wide Area Networks (WANs), the physical interface assigned to the WAN, and the current state of the WAN. Click a WAN to display detailed configuration and status information. See Wide Area Networks (WANs) for details.
Interface	Displays all configured and available physical interfaces for the device and their current states. See Interfaces for details.
LAN	Displays all configured Local Area Networks (LANs), the physical interface(s) assigned to the LAN, and the current state of the LAN. Click a LAN to display detailed configuration and status information. See Local Area Networks (LANs) for details.
VPN	Displays all configured Virtual Private Network (VPN) tunnels. See Virtual Private Networks (VPN) for details.

DMNR page

Use the DMNR page to configure and view Verizon Dynamic Mobile Network Routing (DMNR).

Configuration options

Option	Description
Enable	Enables or disables DMNR. Specifies the current state of DMNR. The default is **disabled**.
Home agent	Specifies the IPv4 address for home agent.
Networks to route	Specifies the IPv4 addresses for the LANs to advertise. Select one or more available configured LANs or **None**. The default is **None**.
Advanced	
Authorization key	Specifies the character string for accessing the mobile network. The default is **VzWNeMo**.
SPI	Specifies the security parameter index. Enter an integer from 0 to 4294967295. The default is **256**.
Home network (tunnel)	Specifies an IP address for the mobile network; that is, the tunnel address that represents the mobile network. The default is **1.2.3.4**.
Lifetime	Specifies the number of seconds until the authorization key expires. Enter an integer from 120 to 65535. The default is **600**.
MTU	Specifies the maximum transmission unit in bytes for the tunnel. Enter an integer from 68 to 1476. The default value is **1476**.

Status display

Option	Description
Admin status	Shows the current administrative status: **Up** or **Down**.
Operational status	Shows the current operational status: **Up** or **Down**.
Registration status	Shows the current registration status: **Registered** or **Unregistered**.
Home agent	Shows the IP address for the Verizon home agent.
Care of address	Shows the current point of attachment IP address for DMNR.
Interface	Shows the interface for DMNR.
Lifetime (actual)	Shows the actual lifetime in seconds for the current DMNR authorization.
Networks	Shows the networks currently being advertised by DMNR.

File system page

Use the **File system** page to display and manage the files and directories in the local file system of your TransPort device.

Navigation options

Field/Button	Description
	Navigates to the home or **/** directory of the file system. As you navigate through the file system, the path is displayed in breadcrumbs to the right of ; for example: > app > dist To return to the home directory, click .
	Uploads directory or file to the TransPort file system.
	Creates a directory. You can create nested directories by specifying the path, separated by **/**.
	Displayed when a file is selected. Downloads the selected file from the TransPort file system. The file is downloaded to the default download directory for your browser.
	Displayed when a directory or file is selected. Renames the selected directory or file.
	Displayed when a directory or file is selected. Deletes the selected directory or file.
File list	The rest of the page lists the directories and files in the file system. Initially, all directories and files listed alphabetically, starting with directories first. All columns are sortable.
Name	The directory or file name.
Size	File size.
Last modified	Date the directory or file was last modified.

Firewall page

Use the **Firewall** page to create and manage IP filter rules.

- **Input IP filter:** Manage your input filters in this section of the Firewall page.
- **Routing IP filter:** Manage your routing and output filters in this section of the Firewall page.

Depending on the address you provide for a filter, TransPort creates rules for either IPv4 or IPv6.

Note Because output filters are rarely needed, all output filter rules you create display with a warning to notify you that you may not need to use an output filter rule.

See IP filter source and destination options and IP filter criteria options for information on configuring IP filter rules.

Input IP filter options

Option	Description
Enabled	Enables or disables the IP filter rule. The default is **enabled**.
Description	Description for the rule. Specify a string value up to **255** characters long.
Action	Specifies what to do with received packets: **Accept**, **Drop**, or **Reject** packets. The default is **Accept**.
Src	Specifies the interface for the incoming packets: **ANY-LAN**, **ANY-WAN**, or a specific LAN or WAN. The default is **NONE**.
Address	Specifies the source IP address for incoming packets. If you do not specify an address, the filter is applied to all addresses. Specify the address in IPv4 or IPv6 format. The format for the source IP address and the destination IP address must match. To force either IPv4 or IPv6 version, enter a default address: ■ For IPv4 0.0.0.0/0 ■ For IPv6 ::/0
Port	Specifies the destination port on the router for incoming packets. You can enter a port number, a range of ports, or a list of ports. If you do not specify a port, the filter is applied to all ports.
Protocol	Specifies the protocol for incoming packets: **tcp**, **udp**, and **icmp**. If you do not specify a protocol, the filter is applied to all protocols.

Routing IP filter options

Option	Description
Enabled	Enables or disables the IP filter rule. The default is **enabled**.

Option	Description
Description	Description for the rule. Specify a string value up to **255** characters long.
Action	Specifies what to do with received packets: **Accept**, **Drop**, or **Reject** packets. The default is **Accept**.
Src	Specifies the interface for the incoming packets: **ANY-LAN**, **ANY-WAN**, or a specific LAN or WAN. The default is **NONE**.
Address	Specifies the source IP address for incoming packets. If you do not specify an address, the filter is applied to all addresses. Specify the IP address in IPv4 or IPv6 format. The format for the source IP address and the destination IP address must match. To force either IPv4 or IPv6 version, enter a default address: ■ For IPv4 0.0.0.0/0 ■ For IPv6 ::/0
Port	Specifies the source port number. You can enter a port number, a range of ports, or a list of ports. If you do not specify a port, the filter is applied to all ports.
Dest	Specifies the destination interface for forwarded packets: **ANY-LAN**, **ANY-WAN**, or a specific LAN or WAN.
Address	Specifies the destination IP address for incoming packets. If you do not specify an address, the filter is applied to all addresses. Specify the address in IPv4 or IPv6 format. The format for the source IP address and the destination IP address must match. To force either IPv4 or IPv6 version, enter a default address: ■ For IPv4 0.0.0.0/0 ■ For IPv6 ::/0
Port	Specifies the destination port number. You can enter a port number, a range of ports, or a list of ports. If you do not specify a port, the filter is applied to all ports.
Protocol	Specifies the protocol for incoming packets: **tcp**, **udp**, and **icmp**. If you do not specify a protocol, the filter is applied to all protocols.

GRE page

Use the GRE tunnel page to create or modify a GRE tunnel. You can configure up to 10 GRE tunnels.

Configuration options

Option	Description
Enable	Enables or disables the GRE tunnel. The default is **disabled**.
Description	Description for the GRE tunnel. Specify a string value up to 255 characters long.
IP Address	Specifies the IPv4 address for the GRE tunnel.
Subnet Mask	Specifies the subnet mask for the GRE IP address in IPv4 format.
Peer	Specifies the remote peer address for the GRE tunnel in IPv4 format.
Key	Specifies the key to use for the GRE tunnel, a 4-byte unsigned integer. Specify an integer from 0 to 4294967295. The default is no key.

Status display

Option	Description
Admin Status	Shows the current administrative status: **Up** or **Down**.
Oper Status	Shows the current operational status: **Up** or **Down**.
IP Address	Shows the IP address for the GRE tunnel.
Subnet Mask	Shows the subnet mask for the GRE IP address.
Peer	Shows the IP address for the GRE peer.
Key	Shows the key for the GRE tunnel.
Packets	Shows the number of received and sent packets for the GRE tunnel.
Bytes	Shows the number of received and sent bytes for the GRE tunnel.

Cellular locked pin page

A SIM card can be locked if any user tries to set an invalid PIN for the SIM card too many times. In addition, some cellular carriers require a SIM PIN to be added before the SIM card can be used. If the SIM card is locked, the TransPort device cannot make a cellular connection.

The show cellular command indicates whether a SIM card is set to a locked state. In the show cellular output, look for the fields **SIM1 PIN status**, **SIM2 PIN status**, and **SIM status**. For example:

```
digi.router> show cellular

 Cellular Status and Statistics
 ------------------------------

 Admin status              : Up
 Oper status               : Down
 Module                    : Sierra Wireless, Incorporated MC7455
 Firmware version          : SWI9X30C_02.08.02.00
 Hardware version          : 1.0
 IMEI                      : 359072060053937
 Temperature               : 33C

 SIM1 PIN status           : New PIN is untested
 SIM2 PIN status           : Never connected
 SIM status                : Using SIM1 (SIM is locked)
 ICCID                     :
 ⋮
```

Command line

Unlocking a SIM card can be performed from the command line interface only.

1. To unlock the SIM card, use the unlock command to set a new PIN for the SIM card using the following command syntax:

   ```
   unlock <sim1 | sim2> <puk code> <new sim pin>
   ```

   Where:

   <sim1 | sim2> indicates whether the SIM card to unlock is in the SIM1 or SIM2 SIM card slot.

   <puk code> is the code to unlock the SIM card. The PUK code can be between 8 and 10 digits long.

   <new sim pin> is the new PIN for the SIM card. This PIN can be between 4 and 8 digits long. Using this parameter changes the PIN for the SIM card to a new value.

   For example:

   To unlock a SIM card in SIM slot SIM **1** with PUK code **12345678**, and set the new SIM PIN to **1234**:

   ```
   digi.router> unlock sim1 12345678 1234
   ```

   When the command operations are complete, the unlock command displays one of the following messages to indicate the state of the SIM:

```
SIM x is permanently locked and must be replaced.
```

```
The PUK code is invalid. You have x retries left before the SIM is
permanently locked.
```

```
The new PIN has been set.
Please use the "save config" command to save the new PIN to the
configuration.
```

2. If the SIM remains in a locked state after using the unlock command, contact your cellular carrier.
3. Save the configuration.

```
digi.router> save config
```

Device preferences page

Use the Device preferences page to configure system settings.

Configuration options

Option	Description
Name	The name of this device. Accepted value is any string up to 255 characters.
Description	A description of this device. Accepted value is any string up to 255 characters.
Contact	Contact information for this device. Accepted value is any string up to 255 characters.
Location	The location of this device. Accepted value is any string up to 255 characters.
Timezone	Sets the system timezone. By setting the time zone, the device displays the local time for that time zone and automatically adjusts for daylight saving time.
Session timeout	The time, in seconds, after which a web or command-line interface session times out if there is no activity. Accepted value is any integer from 60 to 3600. The default value is **300**.

Status display

Option	Description
Up time	Displays the amount of time the device has been up without interruption.
Firmware version	Shows the firmware version running on the device.

Option	Description
System time	Shows the system time and date.
CPU utilization	Shows the current percentage of CPU utilization.
Temperature	Shows the current device temperature in celsius.
Model	Shows the device model.
Part number	Shows the device part number.
Serial number	Shows the device serial number.
Hardware version	Shows the device hardware version.
Boot version	Shows the device boot version.

Interfaces—cellular page

Use the Cellular interface page to create and manage cellular interfaces.

Option	Description
Enable	Enables or disables the interface. The default is **enabled**.
Description	Description for the interface. Specify a string value up to **255** characters long.
APN	Specifies the Access Point Name (APN) for the cellular interface. Enter a string up to 63 characters long.
APN username	Specifies the username for the APN. Enter a string up to 63 characters long.
APN password	Specifies the password for the APN. Enter a string up to 128 characters long.
SIM pin	Specifies PIN to activate the SIM. The PIN is a number between 4 to 8 digits long. If no value is specified for this parameter, no PIN is needed to activate the SIM. Enter a string up to 64 characters long.
Preferred mode	Specifies the preferred mode for the cellular interface: Auto, 4G, 3G, or 2G. The default is **Auto**.
Connection attempts	Specifies the number of attempts to establish a cellular connection. After this number of attempts, the cellular module is power cycled, and the device attempts to make a cellular connection again. Enter an integer from 10 to 500. The default is **20**.

Interfaces—Ethernet page

Use the Ethernet interface page to manage Ethernet interfaces.

Option	Description
Enable	Enables or disables the interface. The default is **enabled**.
Description	Description for the interface. Specify a string up to **255** characters long.
Speed	Specifies the speed in Mbps for the Ethernet interface: Automatic, 10Mbps, 100Mbps, or 1000Mbps. The default is **Automatic**.
Duplex	Specifies the duplex mode for the Ethernet interface: Automatic, Full, or Half. The default is **Automatic**.

Interfaces—Wi-Fi page

Use the WiFi interface page to manage Wi-Fi interfaces.

Option	Description
Mode	Shows the mode for the Wi-Fi interface: **Access Point**.
SSID	Specifies the Service Set Identifier (SSID) for the Wi-Fi interface. You can configure the SSID to use the device's serial number by including the percent (%s) symbol in the SSID. For example, if you specify an SSID value **LR54_%s** resolves to **LR54_LR123456**. Enter a string up to 32 characters long.
Security	Specifies the security type for the Wi-Fi interface: none, wpa2-personal, wpa-wpa2-personal, wpa2-enterprise, or wpa-wpa2-enterprise. The default is **wpa2-personal**.
Password	Specifies the password for the Wi-Fi interface. The password must be 8-63 ASCII or 64 hexadecimal characters. Enter a string up to 64 characters long.
Verify password	Re-enter the password for the WiFi interface. The text you enter must match the text you entered for **Password**.
Description	Description for the interface. Specify a string value up to **255** characters long.
Enable	Enables or disables the interface. The default is **enabled**.
Broadcase SSID	Enables or disables broadcasting the SSID in beacon packets. Disabling the SSID prevents clients from easily detecting the presence of this access point. The default value is **Enabled**.
Isolation client	Enables or disables Wi-Fi client isolation, which prevents clients connected to the Wi-Fi access point from communicating with each other. The default value is **Enabled**.
Isolation access point	Enables or disables clients on a Wi-Fi access point from communicating with clients on other Access Points. The default value is **Enabled**.

IPsec page

Use the IPsec page to configure IPsec tunnels. You can configure up to 32 tunnels.

Network options

Option	Description
Description	Description for the IPsec tunnel. Specify a string value up to **255** characters long.
Enable	Enables or disables the IPsec tunnel. The default is **enabled**.
IPsec pre-shared key	Specifies the preshared key for the IPsec tunnel. Enter a string up to 128 characters long.
Local IP network	Specifies the local network IP address for this IPsec tunnel. Enter an IPv4 address.
Local identifier	Specifies the local ID used for this IPsec tunnel. Enter a string up to 31 characters long.
Remote peer IP address or name	Specifies the remote peer for this IPsec tunnel. Enter a fully qualified domain name.
Remote IP network	Specifies the remote network IP address for this IPsec tunnel. Enter an IPv4 address.
Remote IP network mask	Specifies the remote network mask for this IPsec tunnel. Enter an IPv4 address.
Remote identifier	Specifies the remote ID used for this IPsec tunnel. Enter a string up to 31 characters long.

Encryption options

Option	Description
ESP encryption	Selects the ESP encryption type for IPsec tunnel. Select multiple values of aes128, aes192 and aes256. The default is **aes128**.
ESP authentication	Selects the Encapsulating Security Payload (ESP) authentication type used for the IPsec tunnel. Select multiple values of sha1 and sha256. The default value **sha1**.
ESP Diffie Hellman group	Selects the Encapsulating Security Payload (ESP) Diffie-Hellman group used for the IPsec tunnel. Select multiple values of none, group5, group14, group15 and group16. The default is **group14**.

Negotiation options

Option	Description
Internet Key Exchange (IKE)	Selects the Internet Key Exchange (IKE) version to use for this IPsec tunnel. The default is **1**.
IKE negotiation mode	Selects the IKEv1 mode to use for this IPsec tunnel: main or aggressive. The default is **main**.
IKE encryption	Selects the IKE encryption type for this IPsec tunnel. Select multiple values of aes128, aes192 and aes256. The default is **aes128**.
IKE authentication	Selects the IKE authentication type for this IPsec tunnel: sha1 or sha256. The default is **sha1**.
IKE Diffie Hellman group	Selects the IKE Diffie-Hellman group for this IPsec tunnel. Diffie-Hellman is a public-key cryptography protocol for establishing a shared secret over an insecure communications channel. Diffie-Hellman is used with Internet Key Exchange (IKE) to establish the session keys that create a secure channel. Select multiple values of group5, group14, group15 and group16. The default is **group14**.

Lifetime options

Option	Description
IPsec tunnel lifetime before renegotiation	
Time threshold max (seconds)	Specifies the timeout, in seconds, for dead peer detection. Enter an integer from 1 to 3600. The default value is **3600**.
Data threshold max (bytes)	Specifies the dead peer detection transmit delay. Enter an integer from 1 to 3600. The default value is **0**.
IKE Lifetime before key renegotiation	
Time threshold max (seconds)	Specifies the lifetime for the IKE key, in seconds. Enter an integer from 180 to 4294967295. The default is **4800**.

Local Networks page

Use the Local Networks page to configure and manage local networks. For each local network, you can configure the following options.

Configuration options

Option	Description
Enable	Enables or disables the network. The default is **disabled**.
Interfaces	Specifies one or more physical interfaces for the LAN. The default is **none**.
Description	Specifies a description for the network. Enter a string up to 63 characters long.
IPv4	
IP address	Specifies the IPv4 address for the network.
Netmask	Specifies the netmask for IP address in IPv4 format. The default value is **255.255.255.0**.
DHCP server	
DHCP server	Enables or disables a DHCP server. The default is **disabled**.
IP start	Specifies the start IP address for the range of IP addresses the DHCP server issues to clients.
IP end	Specifies the end IP address for the range of IP addresses the DHCP server issues to clients.
Lease expires	Specifies the lease length, in minutes, issued by the DHCP server.
IPv6	
Enable IPv6	Enables or disables IPv6 addressing. The default is **disabled**.
Advanced	
MTU	Specifies the maximum Transmission Unit (MTU), or packet size, for packets sent over the LAN. Enter an integer from 128 to 1500. The default value is **1500**. For IPv6 addresses, the minimum MTU value must be **1280**.

Status display

Option	Description
Interfaces	Shows the interfaces for the LAN.
Admin status	Shows the administrative status for the LAN: Up or Down.

Option	Description
Oper status	Shows the operational status for the LAN: Up or Down.
IPv4 address	Shows the IPv4 address for the LAN.
Netmask	Shows the IPv4 netmask for the LAN.
DHCP client	Shows the status of the DHCP client: On or Off.
IPv6	Shows whether IPv6 is enabled or disabled.
Packets	Shows packets received and sent on the LAN.
Bytes	Shows bytes received and sent on the LAN.

Log configuration page

Use the **Log configuration** page to configure options for event and system logs.

Event log options

Option	Description
Log level	Specifies the level for logs. The default is **Informational**. For a list of log levels, see Event log levels.
Log to file	Enable or disable saving the event log to a file on the device. The default is Disabled. Digi recommends that you do not download logs to your device unless instructed to do so by support services.
Log to Syslog	Specifies a syslog server on which to store event logs. By default, the event log is not saved on a syslog server.

System log options

Option	Description
Log to file	Enable or disable saving the system log to a file on the device. The default is Disabled. Digi recommends that you do not download logs to your device unless instructed to do so by support services.
Log to Syslog	Specifies a syslog server on which to store system logs. By default, the system log is not saved on a syslog server.

WARNING! Digi recommends that you do not download log files to your device. Keeping log files on your device during normal operations can cause unnecessary wear on the device flash memory.

Log viewer page

Use the **Log viewer** page to stream and download event and system logs.

Log viewer controls

Field/Button	Description
	Stream entries from the event log, system log, or both.
	Pause the stream of incoming log messages.
	Download the event or system log files.
>>	Expand the event and system logs control panel to configure the number of recent messages to show. The default is 10 messages.
<<	Collapse the expanded log viewer controls panel.

Message display

Field/Button	Description
	Indicates the message is from the event log.
	Indicates the message is from the system log.
Date	Timestamp for the log message.
Level	Log level for the message.
Source	Source device application that generated the message.
Message	Message text.
Find	Search or filter log messages. All fields in the message display are included in the search, such as the **Date**, **Level**, and so on. See Find and filter log file entries.

New GRE tunnel page

Use the **New GRE tunnel** page to configure a new GRE tunnel.

Configuration options

Option	Description
Select Tunnel	Specifies the number for the tunnel, an integer from 1 to 10. By default, tunnel numbers are assigned from 1 to 10 and the next available tunnel number is used.
Enable	Enables or disables the GRE tunnel. The default is **enabled**.
Description	Description for the GRE tunnel. Specify a string value up to 255 characters long.
IP Address	Specifies the IPv4 address for the GRE tunnel.
Subnet Mask	Specifies the subnet mask for the GRE IP address in IPv4 format.
Peer	Specifies the remote peer address for the GRE tunnel in IPv4 format.
Key	Specifies the key to use for the GRE tunnel, a 4-byte unsigned integer. Specify an integer from 0 to 4294967295. The default is no key.

Status display

Option	Description
Admin Status	Shows the current administrative status: **Up** or **Down**.
Oper Status	Shows the current operational status: **Up** or **Down**.
IP Address	Shows the IP address for the GRE tunnel.
Subnet Mask	Shows the subnet mask for the GRE IP address.
Peer	Shows the IP address for the GRE peer.
Key	Shows the key for the GRE tunnel.
Packets	Shows the number of received and sent packets for the GRE tunnel.
Bytes	Shows the number of received and sent bytes for the GRE tunnel.

New Wide Area Network (WAN) page

Use the New Wide Area Networks (WAN) page to configure a new WAN.

New WAN connection

Option	Description
Select WAN	Select an available index number for the new WAN.
Select interface	Select an available interface for the WAN.
Enable	Enable or disable the network. The default is **Enabled**.

Configuration options—cellular

Option	Description
Select WAN	Select an available index number for the new WAN.
Select interface	Select an available interface for the WAN.
Enable	Enable or disable the network. The default is **Enabled**.
IPv6	
Enable IPv6	Enable or disable IPv6 addressing. The default is **disabled**.
Requested prefix length	Specifies the length, in bits, of the IPv6 address prefix to request from the upstream router for this WAN. The size of the prefix determines how many LANs can support IPv6. Request a prefix length of 60 bits or less to support up to 16 LANs. Enter an integer from 48 to 64. The default value is **60**.
Security	
Allow HTTPS	Enable or disable HTTPS access for the WAN. The default is **Disabled**.
All SSH	Enable or disable SSH access for the WAN. The default is **Disabled.**
Probing	
Probe host	Specifies the IPv4 or fully qualified domain name (FQDN) of the address of the device itself. The WAN failover feature sends probe packets over the WAN to the IP address of this device. Value should be a fully qualified domain name.
Probe interval	Specifies the interval, in seconds, between sending probe packets. The value for must be larger than the Probe timeout value. If not, the WAN failover configuration is considered invalid, and an error message is written to the system log. Accepted value is any integer from 2 to 3600. The default value is **60**.

Option	Description
Probe size	Specifies the size of probe packets sent to detect WAN failures. Accepted value is any integer from 64 to 1500. The default value is **64**.
Probe timeout	Specifies the timeout, in seconds, to wait for a response to a probe. The value for this parameter must be smaller than the Probe interval and timeout parameter values or the configuration is considered invalid, and an error message is written to the system log. Accepted value is any integer from 1 to 60. The default value is **5**.
Activate after	Specifies the time, in seconds, that the primary interface needs to be up before switching back to it as the active interface. If probing is active, no probes are permitted to be lost during this period. Otherwise, the timer is restarted. Accepted value is any integer from 0 to 3600. The default value is **0**.
Retry after	Specifies the time, in seconds, to wait before retrying this interface after failing over to a lower priority one. Use a large retry timeout when both interfaces are cellular interfaces. Accepted value is any integer from 10 to 3600. The default value is **180**.
Timeout	Specifies the time, in seconds, to wait for the physical interface to connect and to receive a probe response before failing over to a lower priority interface. Accepted value is any integer from 10 to 3600. The default value is **180**.

Configuration options—Ethernet

Option	Description
Enable	Enable or disable the network. The default is **Enabled**.
IPv4	
Configure using	Specifies configuration method: Manually or DHCP. The default is **DHCP**.
IP address	For manually configured WAN only. Specifies the IPv4 address for the WAN.
Netmask	For manually configured WAN only. Specifies the IPv4 netmask for the WAN.
Gateway	For manually configured WAN only. Specifies the IPv4 gateway address for the WAN.
DNS1	For manually configured WAN only. Specifies the IPv4 address for the primary DNS server.
DNS2	For manually configured WAN only. Specifies the IPv4 address for the secondary DNS server.
IPv6	
Enable IPv6	Enable or disable IPv6 addressing. The default is **disabled**.
Requested prefix length	Specifies the length, in bits, of the IPv6 address prefix to request from the upstream router for this WAN. The size of the prefix determines how many LANs can support IPv6. Request a prefix length of 60 bits or less to support up to 16 LANs. Enter an integer from 48 to 64. The default value is **60**.

Option	Description
Security	
Allow HTTPS	Enable or disable HTTPS access for the WAN. The default is **Disabled**.
Allow SSH	Enable or disable SSH access for the WAN. The default is **Disabled.**
Probing	
Probe host	Specifies the IPv4 or fully qualified domain name (FQDN) of the address of the device itself. The WAN failover feature sends probe packets over the WAN to the IP address of this device. Value should be a fully qualified domain name.
Probe interval	Specifies the interval, in seconds, between sending probe packets. The value for must be larger than the Probe timeout value. If not, the WAN failover configuration is considered invalid, and an error message is written to the system log. Accepted value is any integer from 2 to 3600. The default value is **60**.
Probe size	Specifies the size of probe packets sent to detect WAN failures. Accepted value is any integer from 64 to 1500. The default value is **64**.
Probe timeout	Specifies the timeout, in seconds, to wait for a response to a probe. The value for this parameter must be smaller than the Probe interval and timeout parameter values or the configuration is considered invalid, and an error message is written to the system log. Accepted value is any integer from 1 to 60. The default value is **5**.
Activate after	Specifies the time, in seconds, that the primary interface needs to be up before switching back to it as the active interface. If probing is active, no probes are permitted to be lost during this period. Otherwise, the timer is restarted. Accepted value is any integer from 0 to 3600. The default value is **0**.
Retry after	Specifies the time, in seconds, to wait before retrying this interface after failing over to a lower priority one. Use a large retry timeout when both interfaces are cellular interfaces. Accepted value is any integer from 10 to 3600. The default value is **180**.
Timeout	Specifies the time, in seconds, to wait for the physical interface to connect and to receive a probe response before failing over to a lower priority interface. Accepted value is any integer from 10 to 3600. The default value is **180**.

Status display

Option	Description
Interface	Shows the interface for the WAN.
Admin status	Shows the administrative status for the WAN: Up or Down.
Oper status	Shows the operational status for the WAN: Up or Down.
IP address	Shows the IP address for the WAN.
Netmask	Shows the Netmask for the WAN.
Gateway	Shows the Gateway for the WAN.

Option	Description
DNS servers	Shows the DNS servers for the WAN.
IPv6	Shows whether IPv6 is enabled or disabled for the WAN.
Packets	Shows the number of received and sent packets for the WAN.
Bytes	Shows the number of received and sent bytes for the WAN.

OpenVPN client page

Use the OpenVPN client page to set up OpenVPN clients.

Connection options

Option	Description
Enable	Enables or disables the OpenVPN client connection. The default is **disabled**.
Description	Description for the OpenVPN client. Specify a string value up to **255** characters long.
Port	Port number to which this OpenVPN client attempts to connect. Enter an integer from **1** to **65535**. The default is **1194**.
Protocol	Protocol that this OpenVPN client uses to connect: **UDP** or **TCP**. The default is **UDP**.
Logging Level	Specifies the level of output this OpenVPN client records in the system log. Specify an integer from 0 to 4. The default is **0**.

Network options

Option	Description
Server	IP address or fully-qualified domain name of the OpenVPN server to which this OpenVPN client attempts to connect. This option is required.
Pull Routes	Enables or disables the OpenVPN client to accept routes that are pushed from the OpenVPN server. The default is **enabled**.
NAT	Enables or disables Network Address Translation (NAT) for outgoing packets on the OpenVPN client network interface. Note that the OpenVPN client uses NAT only if the Bridge mode is disabled. The default is **enabled**.
Bridge Mode	Specify a LAN as an Ethernet bridge (TAP) for this OpenVPN client or disable Bridge mode. **Note** Although using Bridge mode eliminates the need for routing between networks (required by TUN mode), Bridge mode can cause scalability issues since all broadcast traffic flows over the OpenVPN tunnel. The default is **Off**.

Encryption options

Option	Description
Cipher	Encryption algorithm or list of algorithms the OpenVPN client can use to encrypt and decrypt data channel packets. The OpenVPN client accepts the cipher pushed by the server if it is in this list. If the OpenVPN server supports cipher negotiation, the OpenVPN client can accept additional ciphers that are not in this list. Select one or more ciphers: **aes-128-cbc**, **aes-192-cbc**, **aes-256-cbc**, **aes-128-gcm**, **aes-192-gcm**, and **aes-256-gcm**. The default is **aes-256-gcm,aes-256-cbc,aes-192-gcm,aes-192-cbc,aes-128-gcm,aes-128-cbc**.
Digest	Digest algorithm the OpenVPN client uses to sign and authenticate data channel packets. Select one of the following: **sha1**, **sha224**, **sha256**, **sha384**, or **sha512**. The default is **sha1**.

Authentication options

Option	Description
Certificate Authority (CA) certificate	CA certificate file this OpenVPN client uses to validate the certificate presented by the server. See Certificate and key management.
Certificate Revocation List (CRL) file	CRL file this OpenVPN client uses to prevent connection to a server that presents a revoked certificate.
CA/CRL directory path (capath)	CA and CRL directory path for this OpenVPN client. You provide multiple CA and CRL files. Use the c_rehash tool to create CA certificates with a **.0** filename extension and CRLs with a **.r0** filename extension.
Certificate	Public certificate file for this OpenVPN client. The file is in PEM format.
Private Key File	Private key file for this OpenVPN client. The file is in PEM format.
Username	Username the OpenVPN client uses to authenticate with the OpenVPN server. A username is a string up to **32** characters long.
Password	Password the OpenVPN client uses to authenticate with the OpenVPN server. A password is a string up to **128** characters long.
Confirm Password	A string of up to 128 characters long that should exactly match the value used for the **password** parameter.

Lifetime options

Option	Description
Connect Retry	Number of seconds to wait between connection attempts. After five **5** unsuccessful attempts, the wait time is doubled for each subsequent connection attempt, up to a maximum wait time of **300** seconds. Accepted value is any integer from **1** to **60**. The default value is **5**.

OpenVPN route management page

User the OpenVPN route management page to manage routes for OpenVPN servers.

Route options

Option	Description
Description	Description for the OpenVPN route. Users cannot modify this description. It will always be **Route1**, **Route2**, etc.
Destination	IP address in IPv4 format for the destination.
Mask	Mask for the destination address in IPv4 format. The default is **255.255.255.0**.

OpenVPN server page

Use the OpenVPN server page to configure and display an OpenVPN server.

Connection options

Option	Description
Enable	Enables or disables the OpenVPN server. The default is **disabled**.
Description	Description for the OpenVPN server. Specify a string value up to **255** characters long.
Port	Port number to which this OpenVPN server attempts to connect. Enter an integer from **1** to **65535**. The default is **1194**.
Protocol	Protocol that this OpenVPN server uses to connect: **UDP** or **TCP**. T lhe default is **UDP**.
Compression	Compression algorithm this OpenVPN server uses to compress data channel packets: off, lzo, or lz4. The default is **off**.
Logging level	Specifies the level of output this OpenVPN server records in the system log. Specify an integer from 0 to 4. The default is **0**.

Network options

Option	Description
Network	If Bridge mode is disabled, specifies the IP address in IPv4 format of the local network for this OpenVPN tunnel. The value typically ends with **.0** to match the subnet mask.
Mask	If Bridge mode is disabled, specifies the local subnet for this OpenVPN tunnel in IPv4 format. The default is **255.255.255.0**.
Bridge Mode	Specify a LAN as an Ethernet bridge (TAP) for this OpenVPN server or disable bridge mode. **Note** Although using bridge mode eliminates the need for routing between networks (required by TUN mode), bridge mode can cause scalability issues since all broadcast traffic flows over the OpenVPN tunnel. The default is **Off**.
Topology	Network topology this OpenVPN server uses to assign IP addresses to OpenVPN clients. This value is used only if Bridge mode is disabled. Select one of the following values: **net30**, **p2p**, or **subnet**. The default is **net30**.
Primary DNS	IP address in IPv4 format of the primary DNS server. This value is pushed to OpenVPN clients if Bridge mode is disabled.
Secondary DNS	IP address in IPv4 format of the secondary DNS server. This value is pushed to OpenVPN clients if Bridge mode is off.

Encryption options

Option	Description
Cipher	Encryption algorithm or list of algorithms the OpenVPN server can use to encrypt and decrypt data channel packets. The OpenVPN server pushes the first cipher in the list to OpenVPN clients that support cipher negotiation. OpenVPN clients that do not support cipher negotiation can connect using any cipher in this list. Select one or more ciphers: **aes-128-cbc**, **aes-192-cbc**, **aes-256-cbc**, **aes-128-gcm**, **aes-192-gcm**, and **aes-256-gcm**. The default is **aes-256-gcm,aes-256-cbc,aes-192-gcm,aes-192-cbc,aes-128-gcm,aes-128-cbc**.
Digest	Digest algorithm the OpenVPN server uses to sign and authenticate data channel packets. Select one of the following: **sha1**, **sha224**, **sha256**, **sha384**, or **sha512**. The default is **sha1**.

Authentication options

Option	Description
Certificate Authority (CA) certificate	Certificate file this OpenVPN server uses to validate the certificate presented by the clients. See Certificate and key management.
Certificate Revocation List (CRL) file	CRL file this OpenVPN server uses to prevent connection to a client that presents a revoked certificate.
CA/CRL directory path (capath)	CA and CRL directory path for this OpenVPN server. You can provide multiple CA and CRL files. Use the c_rehash tool to create CA certificates with a **.0** filename extension and CRLs with a **.r0** filename extension. See rehash for details.
Diffie-Hellman file	Diffie-Hellman parameters this OpenVPN server uses for shared secret generation. This file is in PEM format.
Certificate	Public certificate file for this OpenVPN server. The file is in PEM format.
Private Key File	Private key file for this OpenVPN server. The file is in PEM format.
Authenticate By	Configures authentication to use **username and password**, **certificates**, or **both**. The default is **certificates**.
Radius Server State	Enables or disables the Radius server. The default is **disabled**.
Radius Server	IP address in IPv4 format for the RADIUS server for OpenVPN.
Radius Server Port	Port for the RADIUS server. Specify an integer from **1** to **65535**. The default is **1812**.
Radius Server Secret	Secret for the RADIUS server. Specify a string up to **64** characters long.

Lifetime options

Option	Description
OpenVPN Keepalive	
Keepalive Interval (Seconds)	Specifies the interval at which to send a ping message if no other traffic is sent in either direction between the OpenVPN client and server. This value is also pushed to the client. To disable the ping-based keepalive mechanism, set this parameter to **0**. The default is **30**.
Keepalive Timeout (Seconds)	Specifies the amount of time at which to restart the OpenVPN tunnel if no traffic is detected. This value should be five to six times as large as the **Keepalive interval**. This value is doubled before it is set on the server. This value is also pushed to the client. To disable the ping-based keepalive mechanism, set this parameter to **0**. Specify an integer from **0** to **3600**. The default is **150**.
OpenVPN Renegotiation	
Time Until Tunnel Renegotiation (seconds)	Number of seconds before the data channel encryption key is renegotiated. Specify an integer from **60** to **86400**. The default is **3600**.
Bytes Until Tunnel Renegotiation	Number of bytes sent/received before the data channel encryption key is renegotiated. To disable data channel encryption key renegotiation, set this parameter to **0**. Specify an integer from **0** to **4000000000**. The default is **0**.

OpenVPN user management page

Use the OpenVPN user management page to add, edit, and delete VPN users.

Configuration options

Option	Description
Username	Username for OpenVPN user. Specify a string up to **32** characters long.
Password	Password for OpenVPN user. Specify a string up to **128** characters long.
Confirm password	Re-enter the password for the OpenVPN user.

Port forwarding page

Use the Port forwarding page to configure and view port forwarding rules. Each port forwarding rule automatically maps and forwards an external request for a port on a WAN to an IP address and port on an internal LAN. In this way, users can access servers on a private network when they are not directly connected to the private network.

For a port forwarding rule to be applied, you must configure **From Port** and **To IP Address**, and set the rule to **Enabled**. You can configure a maximum of 30 port forwarding rules.

Configuration options

Each port forwarding rule shows the following fields:

Option	Description
Enabled	Enables or disables the port forwarding rule. The default is **enabled**. **Note** Invalid rules are not applied.
Description	Description for the rule. Specify a string value up to **255** characters long.
From Port	Port or ports to forward packets from. A port is an integer value from **0** to **65535**. The default is **0**. Specify a single port, a list of ports, or a range of ports: ■ To specify a list of ports, use a comma (**,**) to separate the ports in the list. For example: **443,22,31**. ■ To specify a range of ports, use a colon (**:**) to separate the low and high ports in the range. For example: **22:31**.
Source	Source WAN or LAN of incoming traffic to be forwarded. Select Any, Any-LAN, Any-WAN, or an available LAN or WAN. The default is **Any**.
Protocol	Protocol to which the rule applies: **UDP**, **TCP**, or **UDP and TCP**. The default is **TCP**.
To IP address	IP address in IPv4 format that packets are forwarded to.
To Port	Port to forward packets to. A port is an integer value from **0** to **65535**. Enter a port number or the **Use from port(s)** option to map the ports specified by **From Port** as the **To Port**. The default is **Use from port(s)**.

Python autostart page

Use the Python autostart page to set up Python files to be executed when the device reboots.

Option	Description
Enable	Enables or disables Python file for autostart.The default is **disabled**.
Filepath	Specifies the Python file to run when the device reboots. Files are run in the order listed.

Option	Description
Args	Specifies arguments to pass to the Python script.
On exit	Specifies the action to take when the script completes. Select None, Restart, or Reboot. the default is **None**.

Quality of Service (QoS) queues page

Use the Quality of Services (QoS) queues page to manage QoS queues.

Configuration options

Configure from one to eight QoS queues using the eight tabs in the Queues panel. Queue 1 has the highest priority; queue 2 has second-highest priority, queue 3 has third-highest priority, and so on up to queue 8 which has the lowest priority.

Field/Button	Description
Enabled	Enables or disables the QoS queue. The default is **disabled**.
Description	Specifies a description for the QoS queue that displays as the tab label for the queue. Specify a string value up to **255** characters long.
Bandwidth upstream	Specifies the amount of bandwidth this queue can use in Kbps or Mbps. For Kbps, enter an integer from 0 to 1000000; for Mbps, enter an integer from 1 to 1000. The default is **0**.
Borrow upstream	Enables (allows) or disables (prohibits) additional bandwidth for this queue if any unused bandwidth is available. The default is **enabled**.
Tag packet (DSCP)	Tags packets with a specified Differentiated Services Code Point (DSCP). Select a value from the drop-down list. The default is **do not set**; that is, do not tag packets.

QoS filters

Field/Button	Description
Enabled	Enables or disables the QoS filter. For a new filter, the default is **enabled**.
Description	Specifies a description for the QoS filter. Specify a string value up to **255** characters long.
Queue	Specifies the queue number to associate with the QoS filter. Specify an integer from 1 to 8, corresponding to queue 1, queue 2, queue 3, and so on. The default is **0** or the current queue being edited.
Protocol	Specifies the protocols for incoming packets. Select one or more specific protocols from the drop-down or select **any** to include all protocols. The default is **any**.
Src	Specifies the source LAN or LANs of incoming packets. Select a specific LAN from the drop-down list or specify **any** to include all LANs. The default is **any**.
Src IP	Specifies the IPv4 or IPv6 source address of incoming packets. Use a simple IPv4 or IPv6 address or use CIDR notation. For example, 192.168.100.0/24, fe80::/10.

Field/Button	Description
Src port	Specifies the port or ports for incoming packets. A port is an integer value from **0** to **65535**. Specify a single port, a list of ports, or a range of ports: ■ To specify a list of ports, use a comma (**,**) to separate the ports in the list. For example: **443,22,31**. ■ To specify a range of ports, use a colon (**:**) to separate the low and high ports in the range. For example: **22:31**. The default is **0**.
Dst IP	Specifies the IPv4 or IPv6 destination address of outgoing packets. Use a simple IPv4 or IPv6 address or use CIDR notation. For example, 192.168.100.0/24, fe80::/10.
Dst port	Specifies the port or ports for outgoing packets. A port is an integer value from **0** to **65535**. Specify a single port, a list of ports, or a range of ports: ■ To specify a list of ports, use a comma (**,**) to separate the ports in the list. For example: **443,22,31**. ■ To specify a range of ports, use a colon (**:**) to separate the low and high ports in the range. For example: **22:31**. The default is **0**.
DSCP	Specifies one or more DSCP tags to filter incoming packets. Select one or more DSCP categories or any. The default is **any**.

Quality of Service (QoS) WANs page

Use the Quality of Services (QoS) WANs page to enable QoS for a configured WAN.

Configuration options

Field/Button	Description
Interface	Displays the interface for the configured WAN.
Enable QoS	Enables or disables Quality of Service (QoS) on this WAN interface. The default is **disabled**.
Bandwidth upstream	Sets the upstream bandwidth of the WAN interface in Kbps or Mbps. For Kbps, enter an integer from 1 to 1000000; for Mbps, enter an integer from 1 to 1000. The default is **1000 Mbps**.

RADIUS page

Use the RADIUS server page to create or modify RADIUS servers.

Settings options

Option	Description
Enable	Enable or disable RADIUS authentication for system administrators. The value is either **on** or **off**. The default is **off**.
NAS ID	A unique identifier for this network access server (NAS). You can use the fully-qualified domain name of the NAS or any arbitrary string. The accepted value is any string up to **64** characters. If left blank, the default value of **sshd** is sent out.
Local Auth Fallback	Determines whether to use local authentication if the RADIUS server does not respond before the timeout expires. The value is either **on** or **off**. The default value is **on**.
Debug	Enable or disable additional debug messages from the RADIUS client. These messages are added to the system log. The value is either **on** or **off**. The default value is **off**.

Primary Server Settings

Option	Description
Primary Server	The IP address or fully-qualified domain name of the RADIUS server to use to authenticate system administrators. The value should be a fully qualified domain name.

Option	Description
Primary Server Port	The UDP port number for the RADIUS server. The accepted value is any integer from **1** to **65535**. The default value is **1812**.
Primary Server Secret	The shared secret for the RADIUS server. The secret cannot contain spaces. The accepted value is any string up to **64** characters.
Primary Server Timeout	The amount of time in seconds to wait for the RADIUS server to respond. The accepted value is any integer from **1** to **10**. The default value is **3**.

Backup Server Settings

Option	Description
Backup Server	The IP address or fully-qualified domain name of the backup RADIUS server to use to authenticate system administrators when the main RADIUS server is not available. The value should be a fully qualified domain name.
Backup Server Port	The UDP port number for the backup RADIUS server. The accepted value is any integer from **1** to **65535**. The default value is **1812**.
Backup Server Secret	The shared secret for the backup RADIUS server. The secret cannot contain spaces. The accepted value is any string up to **64** characters.
Backup Server Timeout	The amount of time in seconds to wait for the backup RADIUS server to respond. The accepted value is any integer from **1** to **10**. The default value is **3**.

Digi Remote Manager page

Use the Digi Remote Manager page to configure the TransPort device connection to Digi Remote Manager. For information on Digi Remote Manager, see Digi Remote Manager.

Administration options

Option	Description
Enable	Enables or disables connection to Digi Remote Manager for this device. The default is **disabled**.
Ethernet keepalive	Specifies the Ethernet keepalive timeout in seconds. Enter an integer from 10 to 7200. The default is **60**.
Cellular keepalive	Specifies the cellular keepalive timeout in seconds. Enter an integer from 10 to 7200. The default is **290**.
Keepalive count	Specifies the number of times a keepalive message is missed before the Remote Manager connection is dropped. Enter an integer from 2 to 10. The default is **3**.
Reconnect delay	Specifies the the time, in seconds, between the device's attempts to connect to Digi Remote Manager. Enter an integer from 10 to 3600. The default is **30**.

Register device

Option	Description
Username	Specifies the Digi Remote Manager username.
Password	Specifies the password for the Digi Remote Manager user.

Status display

Option	Description
Status	Shows the current Digi Remote Manager status: Connected or Disconnected.
Up time	Shows the amount of time the device has been connected to Digi Remote Manager.
Device ID	Shows the Digi Remote Manager ID for the device.

Syslog server configuration page

Use the **Syslog server configuration** page to configure syslogs for storing event and system logs. You can configure up to two syslog servers.

Configuration options

Option	Description
Server	Specify the IP address for the server.
Port	Specify the listening port for the server. The default is port **514**.
Mode	Specify the mode for syslog traffic: UDP or TCP. The default is **UDP**.

User Management page

Use the User management page to create and edit TransPort users.

Note You cannot edit the current active user.

Option	Description
Username	Specifies the username for the user. Usernames are case-insensitive strings that must start with a letter or underscore (_), but can contain letters, digits, underscores (_), and hyphens (-). In addition, a username can end with a dollar sign ($). No other characters are allowed. Enter a string up to 32 characters long.
Access	Specifies the user access control for the user: Read-only, Read-write, or Super. The default is **Super**.
Password	Specifies the password for the user. A password can be any string up to 128 characters long.
Confirm password	Re-enter the password for the user. The value you enter for **Confirm password** must match the **Password** value.

VRRP page

Use the VRRP page to create or modify the VRRP protocol.

Configuration parameters

Option	Description
State	Enable or disable Virtual Router Redundancy Protocol (VRRP). The value is either **on** or **off**. The default value is **off**.
Interface	The LAN interface on which to run VRRP. The accepted values can be one of the following: **LAN1**, **LAN2**, **LAN3**, **LAN4**, **LAN5**, **LAN6**, **LAN7**, **LAN8**, **LAN9**, or **LAN10**. The default value is **LAN1**.
Router ID	The ID of the VRRP virtual router. The accepted value is any integer from **1** to **255**. The default value is **1**.
Interval	The time in seconds between VRRP advertisement packets. All of the routers in the VRRP group should use the same interval. The accepted value is any integer from **1** to **60**. The default value is **1**.
Initial State	The initial VRRP state of this router when it is enabled. The accepted value is either **backup** or **master**. The default value is **backup**.

Option	Description
IP Address	The virtual IP address assigned to the VRRP virtual router. Each client on the LAN should use this address as the default gateway. Typically, the DHCP server distributes this address to each client. The value should be an IPv4 address.
Priority	The VRRP priority of this router. The accepted value is any integer from **1** to **255**. The default value is **100**.

Status

Option	Description
State	Specifies whether the VRRP daemon is configured to be running.
Interface	Displays the current interface being used by the VRRP daemon.
Current VRRP State	The state of the VRRP daemon on this router.
Current VRRP Priority	The current VRRP priority of this router.
Last Transition	The most recent date this router transitioned between VRRP states.
Became Master	The total number of times this router has transitioned into the VRRP master state.
Released Master	The total number of times this router has transitioned out of the VRRP master state.
Adverts Sent	The total number of VRRP advertisements sent by this router.
Adverts Received	The total number of VRRP advertisements received by this router.
Priority Zero Sent	The total number of VRRP packets with a priority of '0' sent by this router.
Priority Zero Received	The total number of VRRP packets with a priority of '0' received by this router.

Wide Area Network (WAN) page—Cellular

Use the Wide Area Networks (WAN) page to configure and manage WANs.

Configuration options—cellular

Option	Description
Enable	Enables or disables the network. The default is **Enabled**.
IPv6	
Enable IPv6	Enables or disables IPv6 addressing. The default is **disabled**.
Requested prefix length	Specifies the length, in bits, of the IPv6 address prefix to request from the upstream router for this WAN. The size of the prefix determines how many LANs can support IPv6. Request a prefix length of 60 bits or less to support up to 16 LANs. Enter an integer from 48 to 64. The default value is **60**.
Security	
Allow HTTPS	Enables or disables HTTPS access for the WAN. The default is **Disabled**.
All SSH	Enables or disables SSH access for the WAN. The default is **Disabled.**
Probing	
Probe host	Specifies the IPv4 or fully qualified domain name (FQDN) of the address of the device itself. The WAN failover feature sends probe packets over the WAN to the IP address of this device. Value should be a fully qualified domain name.
Probe interval	Specifies the interval, in seconds, between sending probe packets. The value for must be larger than the Probe timeout value. If not, the WAN failover configuration is considered invalid, and an error message is written to the system log. Accepted value is any integer from 2 to 3600. The default value is **60**.
Probe size	Specifies the size of probe packets sent to detect WAN failures. Accepted value is any integer from 64 to 1500. The default value is **64**.
Probe timeout	Specifies the timeout, in seconds, to wait for a response to a probe. The value for this parameter must be smaller than the Probe interval and timeout parameter values or the configuration is considered invalid, and an error message is written to the system log. Accepted value is any integer from 1 to 60. The default value is **5**.
Activate after	Specifies the time, in seconds, that the primary interface needs to be up before switching back to it as the active interface. If probing is active, no probes are permitted to be lost during this period. Otherwise, the timer is restarted. Accepted value is any integer from 0 to 3600. The default value is **0**.
Retry after	Specifies the time, in seconds, to wait before retrying this interface after failing over to a lower priority one. Use a large retry timeout when both interfaces are cellular interfaces. Accepted value is any integer from 10 to 3600. The default value is **180**.

Option	Description
Timeout	Specifies the time, in seconds, to wait for the physical interface to connect and to receive a probe response before failing over to a lower priority interface. Accepted value is any integer from 10 to 3600. The default value is **180**.

Status display

Option	Description
Interface	Shows the interface for the WAN.
Admin status	Shows the administrative status for the WAN: Up or Down.
Oper status	Shows the operational status for the WAN: Up or Down.
IP address	Shows the IP address for the WAN.
Netmask	Shows the Netmask for the WAN.
Gateway	Shows the Gateway for the WAN.
DNS servers	Shows the DNS servers for the WAN.
IPv6	Shows whether IPv6 is enabled or disabled for the WAN.
Packets	Shows the number of received and sent packets for the WAN.
Bytes	Shows the number of received and sent bytes for the WAN.

Wide Area Network (WAN) page—Ethernet

Use the Wide Area Networks (WAN) page to configure and manage WANs.

Configuration options—Ethernet

Option	Description
Enable	Enables or disables the network. The default is **Enabled**.
IPv4	
Configure using	Specifies configuration method: Manually or DHCP. The default is **DHCP**.
IP address	For manually configured WAN only. Specifies the IPv4 address for the WAN.
Netmask	For manually configured WAN only. Specifies the IPv4 netmask for the WAN.
Gateway	For manually configured WAN only. Specifies the IPv4 gateway address for the WAN.
DNS1	For manually configured WAN only. Specifies the IPv4 address for the primary DNS server.
DNS2	For manually configured WAN only. Specifies the IPv4 address for the secondary DNS server.
IPv6	
Enable IPv6	Enables or disables IPv6 addressing. The default is **disabled**.
Requested prefix length	Specifies the length, in bits, of the IPv6 address prefix to request from the upstream router for this WAN. The size of the prefix determines how many LANs can support IPv6. Request a prefix length of 60 bits or less to support up to 16 LANs. Enter an integer from 48 to 64. The default value is **60**.
Security	
Allow HTTPS	Enables or disables HTTPS access for the WAN. The default is **Disabled**.
Allow SSH	Enables or disables SSH access for the WAN. The default is **Disabled.**
Probing	
Probe host	Specifies the IPv4 or fully qualified domain name (FQDN) of the address of the device itself. The WAN failover feature sends probe packets over the WAN to the IP address of this device. Value should be a fully qualified domain name.
Probe interval	Specifies the interval, in seconds, between sending probe packets. The value for must be larger than the Probe timeout value. If not, the WAN failover configuration is considered invalid, and an error message is written to the system log. Accepted value is any integer from 2 to 3600. The default value is **60**.

Option	Description
Probe size	Specifies the size of probe packets sent to detect WAN failures. Accepted value is any integer from 64 to 1500. The default value is **64**.
Probe timeout	Specifies the timeout, in seconds, to wait for a response to a probe. The value for this parameter must be smaller than the Probe interval and timeout parameter values or the configuration is considered invalid, and an error message is written to the system log. Accepted value is any integer from 1 to 60. The default value is **5**.
Activate after	Specifies the time, in seconds, that the primary interface needs to be up before switching back to it as the active interface. If probing is active, no probes are permitted to be lost during this period. Otherwise, the timer is restarted. Accepted value is any integer from 0 to 3600. The default value is **0**.
Retry after	Specifies the time, in seconds, to wait before retrying this interface after failing over to a lower priority one. Use a large retry timeout when both interfaces are cellular interfaces. Accepted value is any integer from 10 to 3600. The default value is **180**.
Timeout	Specifies the time, in seconds, to wait for the physical interface to connect and to receive a probe response before failing over to a lower priority interface. Accepted value is any integer from 10 to 3600. The default value is **180**.

Status display

Option	Description
Interface	Shows the interface for the WAN.
Admin status	Shows the administrative status for the WAN: Up or Down.
Oper status	Shows the operational status for the WAN: Up or Down.
IP address	Shows the IP address for the WAN.
Netmask	Shows the Netmask for the WAN.
Gateway	Shows the Gateway for the WAN.
DNS servers	Shows the DNS servers for the WAN.
IPv6	Shows whether IPv6 is enabled or disabled for the WAN.
Packets	Shows the number of received and sent packets for the WAN.
Bytes	Shows the number of received and sent bytes for the WAN.

Wide Area Network (WAN) page

Use the Wide Area Networks (WAN) page to configure and manage WANs.

Configuration options—cellular

Option	Description
Enable	Enables or disables the network. The default is **Enabled**.
IPv6	
Enable IPv6	Enables or disables IPv6 addressing. The default is **disabled**.
Requested prefix length	Specifies the length, in bits, of the IPv6 address prefix to request from the upstream router for this WAN. The size of the prefix determines how many LANs can support IPv6. Request a prefix length of 60 bits or less to support up to 16 LANs. Enter an integer from 48 to 64. The default value is **60**.
Security	
Allow HTTPS	Enables or disables HTTPS access for the WAN. The default is **Disabled**.
All SSH	Enables or disables SSH access for the WAN. The default is **Disabled.**
Probing	
Probe host	Specifies the IPv4 or fully qualified domain name (FQDN) of the address of the device itself. The WAN failover feature sends probe packets over the WAN to the IP address of this device. Value should be a fully qualified domain name.
Probe interval	Specifies the interval, in seconds, between sending probe packets. The value for must be larger than the Probe timeout value. If not, the WAN failover configuration is considered invalid, and an error message is written to the system log. Accepted value is any integer from 2 to 3600. The default value is **60**.
Probe size	Specifies the size of probe packets sent to detect WAN failures. Accepted value is any integer from 64 to 1500. The default value is **64**.
Probe timeout	Specifies the timeout, in seconds, to wait for a response to a probe. The value for this parameter must be smaller than the Probe interval and timeout parameter values or the configuration is considered invalid, and an error message is written to the system log. Accepted value is any integer from 1 to 60. The default value is **5**.
Activate after	Specifies the time, in seconds, that the primary interface needs to be up before switching back to it as the active interface. If probing is active, no probes are permitted to be lost during this period. Otherwise, the timer is restarted. Accepted value is any integer from 0 to 3600. The default value is **0**.
Retry after	Specifies the time, in seconds, to wait before retrying this interface after failing over to a lower priority one. Use a large retry timeout when both interfaces are cellular interfaces. Accepted value is any integer from 10 to 3600. The default value is **180**.

Option	Description
Timeout	Specifies the time, in seconds, to wait for the physical interface to connect and to receive a probe response before failing over to a lower priority interface. Accepted value is any integer from 10 to 3600. The default value is **180**.

Configuration options—Ethernet

Option	Description
Enable	Enables or disables the network. The default is **Enabled**.
IPv4	
Configure using	Specifies configuration method: Manually or DHCP. The default is **DHCP**.
IP address	For manually configured WAN only. Specifies the IPv4 address for the WAN.
Netmask	For manually configured WAN only. Specifies the IPv4 netmask for the WAN.
Gateway	For manually configured WAN only. Specifies the IPv4 gateway address for the WAN.
DNS1	For manually configured WAN only. Specifies the IPv4 address for the primary DNS server.
DNS2	For manually configured WAN only. Specifies the IPv4 address for the secondary DNS server.
IPv6	
Enable IPv6	Enables or disables IPv6 addressing. The default is **disabled**.
Requested prefix length	Specifies the length, in bits, of the IPv6 address prefix to request from the upstream router for this WAN. The size of the prefix determines how many LANs can support IPv6. Request a prefix length of 60 bits or less to support up to 16 LANs. Enter an integer from 48 to 64. The default value is **60**.
Security	
Allow HTTPS	Enables or disables HTTPS access for the WAN. The default is **Disabled**.
Allow SSH	Enables or disables SSH access for the WAN. The default is **Disabled.**
Probing	
Probe host	Specifies the IPv4 or fully qualified domain name (FQDN) of the address of the device itself. The WAN failover feature sends probe packets over the WAN to the IP address of this device. Value should be a fully qualified domain name.
Probe interval	Specifies the interval, in seconds, between sending probe packets. The value for must be larger than the Probe timeout value. If not, the WAN failover configuration is considered invalid, and an error message is written to the system log. Accepted value is any integer from 2 to 3600. The default value is **60**.

Option	Description
Probe size	Specifies the size of probe packets sent to detect WAN failures. Accepted value is any integer from 64 to 1500. The default value is **64**.
Probe timeout	Specifies the timeout, in seconds, to wait for a response to a probe. The value for this parameter must be smaller than the Probe interval and timeout parameter values or the configuration is considered invalid, and an error message is written to the system log. Accepted value is any integer from 1 to 60. The default value is **5**.
Activate after	Specifies the time, in seconds, that the primary interface needs to be up before switching back to it as the active interface. If probing is active, no probes are permitted to be lost during this period. Otherwise, the timer is restarted. Accepted value is any integer from 0 to 3600. The default value is **0**.
Retry after	Specifies the time, in seconds, to wait before retrying this interface after failing over to a lower priority one. Use a large retry timeout when both interfaces are cellular interfaces. Accepted value is any integer from 10 to 3600. The default value is **180**.
Timeout	Specifies the time, in seconds, to wait for the physical interface to connect and to receive a probe response before failing over to a lower priority interface. Accepted value is any integer from 10 to 3600. The default value is **180**.

Status display

Option	Description
Interface	Shows the interface for the WAN.
Admin status	Shows the administrative status for the WAN: Up or Down.
Oper status	Shows the operational status for the WAN: Up or Down.
IP address	Shows the IP address for the WAN.
Netmask	Shows the Netmask for the WAN.
Gateway	Shows the Gateway for the WAN.
DNS servers	Shows the DNS servers for the WAN.
IPv6	Shows whether IPv6 is enabled or disabled for the WAN.
Packets	Shows the number of received and sent packets for the WAN.
Bytes	Shows the number of received and sent bytes for the WAN.

Command reference

Command-line interface basics

This section describes how to use the TransPort command line interface.

Command line interface access options

You can access the TransPort command line interface through the **serial1** interface or through a SSH connection.

You can use open-source terminal software, such as PuTTY and TeraTerm.

Alternatively, you can open the command line interface in the web interface, where it is called the Device Console.

Log in to the command line interface

1. Connect to the TransPort device via the Serial 1 interface or with a SSH connection.
    - For Serial connections, the baud rate is **115200**, **8** data bits, **no** parity, **1** stop bit, and **no** flow control.
    - For SSH connections, the default IP address of the device is **192.168.1.1**.
2. At the login prompt, enter the username and password. The default username is **admin**. The password for your device is printed on the device label; look for the value after **Default Password:**.


```
Username: admin
Password: **********
```

3. A welcome message appears, followed by the current access permission level for your username and the timeout for the command session, followed by the TLR command prompt.

```
Welcome admin
Access Level: super
Timeout     : 3600 seconds
digi.router>
```

Exit the command line interface

Enter the exit command.

Execute a command from the web interface

1. On the menu, click **System > Device console**. The device console appears.

```
digi.router>
```

2. To display the currently supported list of commands for the device, type the question mark (**?**) character after the system prompt:

```
digi.router> ?
```

3. To display help for a specific command, enter the command followed by the question mark (?) character.

   For example, to get help for the pki command, enter:

```
digi.router> pki ?
```

Display command and parameter help using the ? character

Entering **?** displays help text for all commands, individual commands, and command parameters. For example:

```
digi.router> eth ?

Configures an Ethernet interface

Syntax:
eth <1 - 4> <parameter> <value>

Available Parameters:
 Parameter     Description
----------------------------------------------------------------------------
description    Ethernet interface description
duplex         Ethernet interface duplex mode
mtu            Ethernet interface MTU
speed          Ethernet interface speed
state          Enables or disables Ethernet interface

digi.router> eth
```

To display help on parameters, enter the command, the interface number as needed, and parameter name, followed by the **?** character. For example, to display help on the **eth** command's **speed** parameter, enter:

```
digi.router> eth 1 speed ?

Syntax            : eth 1 speed <value>
Description       : Ethernet interface speed
Current Value     : auto
Valid Values      : auto, 10, 100, 1000
Default value     : auto

digi.router> eth 1 speed
```

To use the **?** character in a parameter value, enclose it within **"** characters. For example, to display the help text for the **system** command's **description** parameter:

```
system 1 description ?
```

To set the **system** command **description** parameter to **?**:

```
system 1 description "?"
```

Revert command settings using the ! character

To revert command settings to their defaults, use the **!** character.

To revert the default setting of the interfaces parameter on the **lan** command, enter:

```
digi.router> lan 1 interfaces !
```

To use the **!** character in a parameter value, enclose it within **"** characters. For example, to reset the Wi-Fi SSID to the default (blank):

```
wifi 1 ssid !
```

To set the Wi-Fi SSID to **!abc**:

```
wifi 1 ssid "!abc"
```

Auto-complete commands and parameters

When entering a command and parameter, pressing the **Tab** key causes the command-line interface to auto-complete as much of the command and parameter as possible.

Auto-complete applies to these command elements only :

- Command names. For example, entering **cell<Tab>** auto-completes the command as **cellular**
- Parameter names. For example:
  - **ping int<Tab>** auto-completes the parameter as **interface**
  - **system loc<Tab>**auto-completes the parameter as **location**.
- Parameter values, where the value is one of an enumeration or an on|off type; for example, **eth 1 duplex auto|full|half**

Auto-complete does not function for:

- Parameter values that are string types
- Integer values
- File names
- Select parameters passed to commands that perform an action

Enter configuration commands

Configuration commands configure settings for various device features. Configuration commands have the following format:

```
<command> <instance> <parameter> <value>
```

Where <instance> is the index number associated with the feature. For example, this command configures the **eth1** Ethernet interface:

```
digi.router> eth 1 ip-address 10.1.2.3
```

For commands with only one instance, you do not need to enter the instance. For example:

```
digi.router> system timeout 100
```

Entering strings in configuration commands

For string parameters, if the string value contains a space, the value must be enclosed in quotation marks; For example, to assign a descriptive name for the device using the **system** command, enter:

```
digi.router> system description "HQ router"
```

Save configuration settings to a file

Configuration changes are **not** automatically saved. This means that the device discards any unsaved changes when the device reboots.

Web

- On configuration pages, click **Apply** to save changes to the configuration file immediately.

Command line

Enter the **save config** command.

```
digi.router> save config
```

Switch configuration files

Command line

You can store multiple configuration files on a device, but the device uses only one configuration file when it reboots. The default configuration file is named **config.da0**.

To switch to another configuration file:

1. If needed, identify the current configuration file using the show system command.
2. Change the current configuration file using the update command.
3. If needed, create the configuration file you specified in the **update** command using the save command.

Step 1: Identify the current configuration file

To identify the current configuration file, use the show system command. For example:

```
digi.router> show system

Model             : LR54W
Part Number       : LR54-AW401
Serial Number     : LR000038

Hardware Version  : Not available
Using Bank        : 1
```

```
Firmware Version  : 1.1.0.6 06/17/16 13:37:58
Bootloader Version: 201602051801
Using Config File : config.da0

Uptime            : 14 Minutes, 29 Seconds
System Time       : 23 July 2016, 13:08:09

CPU               : 3% (min 1%, max 70%, avg 3%)
Temperature       : Not available

Description       :
Location          :
Contact           :

digi.router>
```

Step 2: Change the configuration file name

To change the name of the current configuration file, use the update command. For example:

```
digi.router> update config <filename>
```

The file you specified is used the next time the device reboots.

Step 3: Save the current configuration to the configuration file

If the configuration file name you specified on the update command does not exist, use the save command **config** parameter to create the new configuration file by saving the current configuration.

To save the current configuration, use the save command **config** parameter. For example:

```
digi.router> save config
```

Display status and statistics using "show" commands

show commands display status and statistics for various features. For example:

- show config displays all the current configuration settings for the device. This is a particularly useful during initial device startup after running the Getting Started Wizard, or when troubleshooting the device.
- show system displays system information and statistics for the device, including CPU usage.
- show eth displays status and statistics for specific or all Ethernet interfaces.
- show cellular displays status and statistics for specific or all cellular interfaces.

? (Display command help)

Displays help text for all commands, individual commands, and command parameters.

To display help on parameters, enter the command name, the interface number as needed, and parameter name, followed by the **?** character.

To use the **?** character in a parameter value, enclose it within **"** characters. For example, to display the help text for the **system** command's **description** parameter:

```
system 1 description ?
```

To set the **system** command **description** parameter to **?**:

```
system 1 description "?"
```

! (Revert command settings)

Reverts an individual command element to its default.

For example, to revert the default setting of interfaces on the **lan** command, enter:

```
digi.router> lan 1 interfaces !
```

To use the **!** character in a parameter value, enclose it within **"** characters. For example, to reset the Wi-Fi SSID to the default (blank):

```
wifi 1 ssid !
```

To set the Wi-Fi SSID to **!abc**:

```
wifi 1 ssid "!abc"
```

analyzer

Configures the network packet capture feature. Enabling data traffic capture significantly affects device performance.

Syntax

```
analyzer <parameter> <value>
```

Parameters

state

Enables or disables packet capture.

Accepted values can be one of off or on. The default value is off.

interfaces

The member interfaces for the packet capture operation. List the interfaces, separated by commas.

Accepted values can be multiple values of none, lan1, lan2, lan3, lan4, lan5, lan6, lan7, lan8, lan9, lan10, eth1, eth2, eth3, eth4, wifi1, wifi2, wifi3, wifi4, wifi5g1, wifi5g2, wifi5g3, wifi5g4, cellular1, cellular2 and lo. The default value is none.

filter

The filter for capturing data packets, in BPF format. If you do not specify a filter, the capture operation captures all incoming and outgoing packets.

Accepted value is any string up to 255 characters.

autorun

Configures commands to be automatically run at boot-up. You can use auto-run commands for tasks such as switching configuration files, or scheduling a reboot. You can configure up to 10 auto-run commands. Use the python-autostart command to schedule python programs.

This command is available to super users only.

Syntax

```
autorun <1 - 10> <parameter> <value>
```

Parameters

command

Command to run.

Accepted value is any string up to 100 characters.

Examples

- ```
  autorun 1 command "copy config.da0 config.backup"
  ```

  Automatically copy a file.
  ```

cd

Changes the current directory.

Syntax

```
cd [dir]
```

Parameters

dir

When a directory name is specified, 'cd' changes the current directory to it.

cellular

Configures a cellular interface.

Syntax

```
cellular <1 - 2> <parameter> <value>
```

Parameters

state

Enables or disables the cellular interface.

Accepted values can be one of off or on. The default value is off.

description

A description of the cellular interface.

Accepted value is any string up to 63 characters.

apn

The Access Point Name (APN) for the cellular interface.

Accepted value is any string up to 63 characters.

apn-username

The username for the APN.

Accepted value is any string up to 63 characters.

apn-password

The password for the APN.

Accepted value is any string up to 128 characters.

preferred-mode

The preferred cellular mode for the cellular interface.

Accepted values can be one of auto, 4g, 3g or 2g. The default value is auto.

connection-attempts

The number of attempts to establish a cellular connection. After this number of attempts, the cellular module is power cycled, and the device attempts to make a cellular connection again.

Accepted value is any integer from 10 to 500. The default value is 20.

pin

PIN to activate the SIM. The PIN is a number between 4 to 8 digits long. If no value is specified for this parameter, no PIN is needed to activate the SIM.

Accepted value is any string up to 64 characters.

Examples

- ```
  cellular 1 state on
  ```

  Enable the Cellular 1 interface.

- ```
  cellular 1 state off
  ```

  Disable the Cellular 1 interface.

- ```
  cellular 2 apn broadband
  ```

  Set the SIM slot 2 APN to 'broadband.'

- ```
  cellular 1 username my-username
  ```

  Set the SIM slot 1 username to 'my-username.'

- ```
  cellular 1 password my-password
  ```

  Set the SIM slot 1 password to 'my-password.'
  ```

clear

Clears system status and statistics, such as the event log, firewall counters, traffic analyzer log, etc.

This command is available to super users only.

Syntax

```
clear firewall
clear firewall6
clear log
clear log system
clear log all
clear analyzer
clear web-filter-id
```

Parameters

firewall

Clears firewall counters.

firewall6

Clears firewall IPv6 counters.

log

Clears event log.

analyzer

Clears the traffic analyzer log.

web-filter-id

Clears the device ID provided by the Cisco Umbrella service. The router automatically acquires a device ID whenever web filtering is enabled.

Examples

- ```
  clear firewall
  ```

  Clear the packet and byte counters in all firewall rules.

- ```
  clear firewall6
  ```

  Clear the packet and byte counters in all IPv6 firewall rules.

- ```
  clear log
  ```

  Clear the TLR event log and leaves an entry in the log after clearing.
  ```

- ```
  clear log system
  ```
  Clear the system/kernel event log and leaves an entry in the log after clearing.
- ```
  clear analyzer
  ```
  Clear the traffic analyzer log.
- ```
  clear web-filter-id
  ```
  Clear the Cisco Umbrella device ID.
  ```

cloud

Configures Digi Remote Manager settings.

Syntax

```
cloud <parameter> <value>
```

Parameters

state

Enable or disable Digi Remote Manager.

Value is either on or off. The default value is on.

server

The name of the Digi Remote Manager server.

Value should be a fully qualified domain name. The default value is my.devicecloud.com.

reconnect

The time, in seconds, between the device's attempts to connect to Digi Remote Manager.

Accepted value is any integer from 10 to 3600. The default value is 30.

keepalive

The interval, in seconds, used to contact the server to validate connectivity over a non-cellular interface.

Accepted value is any integer from 10 to 7200. The default value is 60.

keepalive-cellular

The interval, in seconds, used to contact the server to validate connectivity over a cellular interface.

Accepted value is any integer from 10 to 7200. The default value is 290.

keepalive-count

Number of keepalives missed before the device disconnects from Remote Manager.

Accepted value is any integer from 2 to 10. The default value is 3.

health

Enable or disable health metric reporting to Digi Remote Manager.

Value is either on or off. The default value is on.

copy

Copies a file.

This command is available to all users.

Syntax

```
copy source dest
```

Parameters

source

The source file to be copied to the location specified by 'dest.'

dest

The destination file, or file to which the source file is copied.

date

Manually sets and displays the system date and time.

Syntax

```
date [HH:MM:SS [DD:MM:YYYY]]
```

Parameters

time

System time, specified in the 24-hour format HH:MM:SS.

date

System date, specified in the format DD:MM:YYYY.

Examples

- ```
  date 14:55:00 03:05:2016
  ```

  Set the system date and time to 14:55:00 on May 3, 2016.
  ```

del

Deletes a file.

This command is available to all users.

Syntax

```
del file
```

Parameters

file

The file to be deleted.

dhcp-server

Configures Dynamic Host Configuration Protocol (DHCP) server settings.

Syntax

```
dhcp-server <1 - 10> <parameter> <value>
```

Parameters

state

Enables or disables this DHCP server.

Value is either on or off. The default value is off.

ip-address-start

The first IP address in the pool of addresses to assign.

Value should be an IPv4 address.

ip-address-end

The last IP address in the pool of addresses to assign.

Value should be an IPv4 address.

mask

The IP network mask given to clients.

Value should be an IPv4 address. The default value is 255.255.255.0.

gateway

Override the IP gateway address given to clients. By default, the gateway address given to clients is the IP address of the LAN with the same index as this DHCP server. If VRRP is enabled for this LAN, the VRRP virtual IP address is given to clients instead. However, if a gateway address is explicitly specified here, that address is given to clients instead of the LAN or VRRP IP address.

Value should be an IPv4 address.

dns1

Override the preferred DNS server address given to clients. By default, the DNS server address given to clients is the IP address of the LAN with the same index as this DHCP server. If VRRP is enabled for this LAN, the VRRP virtual IP address is given to clients instead. However, if a DNS server address is explicitly specified here, that address is given to clients instead of the LAN or VRRP IP address.

Value should be an IPv4 address.

dns2

Alternate DNS server address given to clients.

Value should be an IPv4 address.

lease-time

The length, in minutes, of the leases issued by this DHCP server.

Accepted value is any integer from 2 to 10080. The default value is 1440.

dir

Displays the contents of the current directory.

Syntax

```
dir [dir]
```

Parameters

dir

Lists information about the directory (by default, the current directory).

dmnr

Configures dynamic mobile network routing

Syntax

```
dmnr <parameter> <value>
```

Parameters

state

Enables or disables DMNR.

Value is either on or off. The default value is off.

home-agent

The IP address of the home agent.

Value should be an IPv4 address.

home-network

The IPv4 address of the home network. Use a simple IP address, or use CIDR notation (example: 192.168.100.0/24).

Accepted value is any string up to 18 characters. The default value is 1.2.3.4.

key

Authorization key for the home agent.

Accepted value is any string up to 255 characters. The default value is VzWNeMo.

spi

Security parameter index used to identify the security association.

Accepted value is any integer from 0 to 4294967295. The default value is 256.

lifetime

The lifetime of the registration to the home agent.

Accepted value is any integer from 120 to 65535. The default value is 600.

mtu

The maximum transmission unit (MTU) of the underlying tunnel.

Accepted value is any integer from 68 to 1476. The default value is 1476.

local-networks

Allows you to select the lans to advertise.

Accepted values can be multiple values of none, lan1, lan2, lan3, lan4, lan5, lan6, lan7, lan8, lan9 and lan10. The default value is none.

dsl

UNUSED

Syntax

```
dsl <parameter> <value>
```

Parameters

unused

UNUSED

Accepted value is any string up to 63 characters.

dynamic-dns

Configures the dynamic DNS client on this device. This client notifies a dynamic DNS service of the IP address of this device. This allows external users to access this device using a fixed domain name, even when the public IP address of the device changes due to WAN failover or DHCP lease expiration.

Syntax

```
dynamic-dns <parameter> <value>
```

Parameters

state

Enables or disables the dynamic DNS client.

Value is either on or off. The default value is off.

service

Specifies the dynamic DNS service to which this dynamic DNS client will push updates.

Accepted values can be one of dyndns, noip, changeip or dnsomatic. The default value is dyndns.

hostname

The domain name that refers to this device. This domain name is provided when registering with the dynamic DNS service.

Value should be a fully qualified domain name.

username

The username used to authenticate with the dynamic DNS service.

Accepted value is any string up to 255 characters.

password

The password used to authenticate with the dynamic DNS service.

Accepted value is any string up to 255 characters.

ip-monitoring

Specify wheather dynamic DNS client monitors the IP address of this device or monitors a web service that returns a public IP address.

Accepted values can be one of wan or public. The default value is public.

eth

Configures an Ethernet interface.

Syntax

```
eth <1 - 4> <parameter> <value>
```

Parameters

state

Enables or disables the Ethernet interface.

Accepted values can be one of off or on. The default value is on.

description

A description of the Ethernet interface.

Accepted value is any string up to 63 characters.

duplex

The duplex mode the device uses to communicate on the Ethernet network. The keyword 'auto' causes the device to sense the mode used on the network and adjust automatically.

Accepted values can be one of auto, full or half. The default value is auto.

speed

Transmission speed, in Mbps, the device uses on the Ethernet network. The keyword 'auto' causes the device to sense the Ethernet speed of the network and adjust automatically.

Accepted values can be one of auto, 10, 100 or 1000. The default value is auto.

mtu

The Maximum Transmission Unit (MTU) transmitted over the Ethernet interface.

Accepted value is any integer from 64 to 1500. The default value is 1500.

Examples

- ```
  eth 3 mask 255.255.255.0
  ```

  Set network mask of Ethernet interface 3 to 255.255.255.0.

- ```
  eth 3 state on
  ```

  Enable Ethernet interface 3.

- ```
  eth 3 state off
  ```

  Disable Ethernet interface 3.
  ```

exit

Exits the TransPort LR command-line interface.

Syntax

```
exit
```

firewall

Configures the firewall. The TransPort LR firewall is a full stateful firewall to control which packets are allowed into and out of the device. Firewalls can filter packets based on the IP address, protocol, TCP ports, and UDP ports. You can also use the firewall to do port forwarding. The TransPort LR firewall is based on the open-source firewall named iptables. It uses the same syntax as the iptables firewall, except that the rules start with firewall instead of iptables. The firewall syntax is case-sensitive. For more information on configuring the firewall, see the Firewall section of the TransPort LR User Guide and these external sources: http://www.netfilter.org/documentation and https://help.ubuntu.com/community/IptablesHowTo

This command is available to super users only.

Syntax

```
firewall rule
```

Parameters

rule

Firewall rule.

firewall6

Configures the IPv6 firewall. The TransPort LR firewall is a full stateful firewall to control which packets are allowed into and out of the device. Firewalls can filter packets based on the IP address, protocol, TCP ports, and UDP ports. You can also use the firewall to do port forwarding. The TransPort LR firewall is based on the open-source firewall named iptables. It uses the same syntax as the iptables firewall, except that the rules start with firewall instead of iptables. The firewall syntax is case-sensitive. For more information on configuring the firewall, see the Firewall section of the TransPort LR User Guide and these external sources: http://www.netfilter.org/documentation and https://help.ubuntu.com/community/IptablesHowTo

This command is available to super users only.

Syntax

```
firewall6 rule
```

Parameters

rule

Firewall rule.

gre

Configures a GRE tunnel.

Syntax

```
gre <1 - 10> <parameter> <value>
```

Parameters

state

Enables or disables this GRE tunnel.

Value is either on or off. The default value is off.

description

A description of this GRE tunnel.

Accepted value is any string up to 255 characters.

ip-address

IPv4 address for this GRE interface.

Value should be an IPv4 address.

mask

IPv4 subnet mask for this GRE interface.

Value should be an IPv4 address.

peer

Remote peer for this GRE interface.

Value should be an IPv4 address.

key

The key to use for this GRE tunnel.

Accepted value is any string up to 10 characters.

ip

Configures Internet Protocol (IP) settings.

Syntax

```
ip <parameter> <value>
```

Parameters

admin-conn

Administrative distance value for connected routes. Administrative distance values rank route types from most to least preferred. If there are two routes to the same destination that have the same mask, the device uses a route's 'metric' parameter value to determine which route to use. In such a case, the administrative distances for the routes determine the preferred type of route to use. The administrative distance is added to the route's metric to calculate the metric the routing engine uses. Usually, connected interfaces are most preferred, because the device is directly connected to the networks on such interfaces, followed by static routes.

Accepted value is any integer from 0 to 255. The default value is 0.

admin-static

Administrative distance value for static routes. See 'admin-conn' for how routers use administrative distance.

Accepted value is any integer from 0 to 255. The default value is 1.

hostname

IP hostname for this device.

Accepted value is any string up to 63 characters.

ip-filter

Configures IP filter rules.

Syntax

```
ip-filter <1 - 32> <parameter> <value>
```

Parameters

description

The description of this rule.

Accepted value is any string up to 255 characters.

state

Enables or disables an IP filter rule.

Value is either on or off. The default value is off.

action

Accepts, drops, or rejects IP packets.

Accepted values can be one of accept, drop or reject. The default value is accept.

src-ip-address

The IPv4 or IPv6 source address of the incoming packet. Use a simple IPv4 or IPv6 address, or use CIDR notation (example: 192.168.100.0/24, fe80::/10)

Accepted value is any string up to 43 characters.

src-ip-port

The source port(s) of the incoming packet. Use a simple port, a range (lowport:highport) or a list (port1,port2...,portn). Default '0' implies 'Any'. Source port is ignored when protocol does not explicitly include tcp or udp.

Accepted value is any string up to 255 characters. The default value is 0.

dst-ip-address

The IPv4 or IPv6 destination address of the incoming packet. Use a simple IPv4 or IPv6 address, or use CIDR notation (example: 192.168.100.0/24, fe80::/10)

Accepted value is any string up to 43 characters.

dst-ip-port

The destination port(s) of the incoming packet. Use a simple port, a range (lowport:highport) or a list (port1,port2...,portn). Default '0' implies 'Any'. Dest port is ignored when protocol does not explicitly include tcp or udp.

Accepted value is any string up to 255 characters. The default value is 0.

src

The WAN or LAN that is the source of incoming traffic. Required if 'dst' is not specified. Must be different than 'dst'.

Accepted values can be one of none, any-lan, lan1, lan2, lan3, lan4, lan5, lan6, lan7, lan8, lan9, lan10, any-wan, wan1, wan2, wan3, wan4, wan5, wan6, wan7, wan8, wan9, wan10, dmnr-tunnel, any-gre, gre1, gre2, gre3, gre4, gre5, gre6, gre7, gre8, gre9 or gre10. The default value is none.

dst

The WAN or LAN that is the destination of outgoing traffic. Required if 'src' is not specified. Must be different than 'src'.

Accepted values can be one of none, any-lan, lan1, lan2, lan3, lan4, lan5, lan6, lan7, lan8, lan9, lan10, any-wan, wan1, wan2, wan3, wan4, wan5, wan6, wan7, wan8, wan9, wan10, dmnr-tunnel, any-gre, gre1, gre2, gre3, gre4, gre5, gre6, gre7, gre8, gre9 or gre10. The default value is none.

protocol

The protocol of the incoming packet. Use a single protocol, a list (tcp,udp,icmp), or exclusive value (any). When set to 'any', src-ip-port and dst-ip-port values are ignored.

Accepted values can be multiple values of tcp, udp, icmp and any. The default value is tcp,udp.

ipsec

Configures an IPsec tunnel. Up to 32 IPsec tunnels can be configured.

Syntax

```
ipsec <1 - 32> <parameter> <value>
```

Parameters

state

Enables or disables the IPsec tunnel.

Accepted values can be one of off or on. The default value is off.

description

A description of this IPsec tunnel.

Accepted value is any string up to 255 characters.

peer

The remote peer for this IPsec tunnel.

Value should be a fully qualified domain name.

local-network

The local network IP address for this IPsec tunnel.

Value should be an IPv4 address.

local-mask

The local network mask for this IPsec tunnel.

Value should be an IPv4 address.

remote-network

The remote network IP address for this IPsec tunnel.

Value should be an IPv4 address.

remote-mask

The remote network mask for this IPsec tunnel.

Value should be an IPv4 address.

esp-authentication

The Encapsulating Security Payload (ESP) authentication type used for the IPsec tunnel.

Accepted values can be multiple values of sha1 and sha256. The default value is sha1.

esp-encryption

ESP encryption type for IPsec tunnel

Accepted values can be multiple values of aes128, aes192 and aes256. The default value is aes128.

esp-diffie-hellman

The Encapsulating Security Payload (ESP) Diffie-Hellman group used for the IPsec tunnel.

Accepted values can be multiple values of none, group5, group14, group15 and group16. The default value is group14.

auth-by

The authentication type for the IPsec tunnel.

Accepted values can be multiple values of psk. The default value is psk.

psk

The preshared key for the IPsec tunnel.

Accepted value is any string up to 128 characters.

local-id

The local ID used for this IPsec tunnel.

Accepted value is any string up to 31 characters.

remote-id

The remote ID used for this IPsec tunnel.

Accepted value is any string up to 31 characters.

lifetime

Number of seconds before this IPsec tunnel is renegotiated.

Accepted value is any integer from 60 to 86400. The default value is 3600.

lifebytes

Number of bytes sent before this IPsec tunnel is renegotiated. A value of 0 means the IPsec tunnel will not be renegotiated based on the amount of data sent.

Accepted value is any integer from 0 to 4000000000. The default value is 0.

margintime

The number of seconds before the 'lifetime' limit to attempt to renegotiate the security association (SA).

Accepted value is any integer from 1 to 3600. The default value is 540.

marginbytes

The number of bytes before the 'lifebytes' limit to attempt to renegotiate the security association (SA).

Accepted value is any integer from 0 to 1000000000. The default value is 0.

random

The percentage of the total renegotiation limits that should be randomized.

Accepted value is any integer from 0 to 200. The default value is 100.

ike

The Internet Key Exchange (IKE) version to use for this IPsec tunnel.

Accepted value is any integer from 1 to 1. The default value is 1.

ike-mode

The IKEv1 mode to use for this IPsec tunnel.

Accepted values can be one of main or aggressive. The default value is main.

ike-encryption

The IKE encryption type for this IPsec tunnel.

Accepted values can be multiple values of aes128, aes192 and aes256. The default value is aes128.

ike-authentication

The IKE authentication type for this IPsec tunnel.

Accepted values can be multiple values of sha1 and sha256. The default value is sha1.

ike-diffie-hellman

The IKE Diffie-Hellman group for this IPsec tunnel. Diffie-Hellman is a public-key cryptography protocol for establishing a shared secret over an insecure communications channel. Diffie-Hellman is used with Internet Key Exchange (IKE) to establish the session keys that create a secure channel.

Accepted values can be multiple values of group5, group14, group15 and group16. The default value is group14.

ike-lifetime

The lifetime for the IKE key, in seconds.

Accepted value is any integer from 180 to 4294967295. The default value is 4800.

ike-tries

The number of attempts to negotiate this IPsec tunnel before failing.

Accepted value is any integer from 0 to 100. The default value is 3.

dpddelay

Dead peer detection transmit delay.

Accepted value is any integer from 1 to 3600. The default value is 30.

dpdtimeout

Timeout, in seconds, for dead peer detection.

Accepted value is any integer from 1 to 3600. The default value is 150.

dpd

Enables or disables dead peer detection. Dead Peer Detection (DPD) is a method of detecting a dead Internet Key Exchange (IKE) peer. The method uses IPsec traffic patterns to minimize the number of messages required to confirm the availability of a peer.

Value is either on or off. The default value is off.

metric

The metric for the IPsec route. The metric defines the order in which the device uses routes if there are two routes to the same destination. In such a case, the device uses the IPsec route with the smaller metric.

Accepted value is any integer from 0 to 255. The default value is 10.

Examples

- ```
  ipsec 3 state on
  ```

  Enable IPsec tunnel 3.

- ```
  ipsec 3 state off
  ```

  Disable IPsec tunnel 3.

- ```
  ipsec 3 esp-authentication sha256
  ```

  Set ESP authentication for IPsec tunnel 3 to SHA256.

- ```
  ipsec 3 esp-encryption aes256
  ```

  Set ESP encryption for IPsec tunnel 3 to AES 256 bit keys.

- ```
  ipsec 3 esp-diffie-hellman group15
  ```

  Set IPsec tunnel 3 to use ESP Diffie-Hellman group 15 for negotiation.
  ```

lan

Configures a Local Area Network (LAN). A LAN is a group of Ethernet and Wi-Fi interfaces.

Syntax

```
lan <1 - 10> <parameter> <value>
```

Parameters

state

Enables or disables a LAN.

Value is either on or off. The default value is off.

description

A descriptive name for the LAN.

Accepted value is any string up to 63 characters.

mtu

Maximum Transmission Unit (MTU) for the LAN.

Accepted value is any integer from 128 to 1500. The default value is 1500.

interfaces

The physical interfaces for the LAN.

Accepted values can be multiple values of none, eth1, eth2, eth3, eth4, wifi1, wifi2, wifi3, wifi4, wifi5g1, wifi5g2, wifi5g3 and wifi5g4. The default value is none.

ip-address

IPv4 address for the LAN. While it is not strictly necessary for a LAN to have an IP address, an IP address must be configured to send traffic from and to the LAN.

Value should be an IPv4 address.

mask

IPv4 subnet mask for the LAN.

Value should be an IPv4 address. The default value is 255.255.255.0.

dns1

Preferred DNS server.

Value should be an IPv4 address.

dns2

Alternate DNS server.

Value should be an IPv4 address.

dhcp-client

Enables or disable the DHCP client for this LAN.

Value is either on or off. The default value is off.

ipv6-state

Enables or disables IPv6 support on this LAN.

Value is either on or off. The default value is off.

ipv6-mode

Selects configuration method to provision clients on this LAN. Currently only DHCPv6 is supported.

Accepted values can be one of dhcpv6. The default value is dhcpv6.

mkdir

Creates a directory.

This command is available to all users.

Syntax

```
mkdir dir
```

Parameters

dir

The directory to be created.

more

Displays the contents of a file.

Syntax

```
more [file]
```

Parameters

file

File to be displayed.

openvpn-client

Configures an OpenVPN client.

Syntax

```
openvpn-client <1 - 10> <parameter> <value>
```

Parameters

state

Enables or disables this OpenVPN client.

Value is either on or off. The default value is off.

description

A description of this OpenVPN client.

Accepted value is any string up to 255 characters.

server

The IP address or fully-qualified domain name of the OpenVPN server to which this OpenVPN client attempts to connect.

Value should be a fully qualified domain name.

port

The port number to which this OpenVPN client attempts to connect.

Accepted value is any integer from 1 to 65535. The default value is 1194.

protocol

The protocol (TCP or UDP) that this OpenVPN client uses to connect.

Accepted values can be one of udp or tcp. The default value is udp.

connect-retry

The number of seconds to wait between connection attempts. After 5 unsuccessful attempts, the wait time is doubled for each subsequent connection attempt, up to a maximum wait time of 300 seconds.

Accepted value is any integer from 1 to 60. The default value is 5.

bridge-mode

Enables Ethernet bridge (TAP) mode for this OpenVPN client. This eliminates the need for routing between networks as required by TUN mode, but may have scalability issues, since all broadcast traffic will flow over the OpenVPN tunnel.

Accepted values can be one of off, lan1, lan2, lan3, lan4, lan5, lan6, lan7, lan8, lan9 or lan10. The default value is off.

cipher

The encryption algorithm or list of algorithms the OpenVPN client can use to encrypt and decrypt data channel packets. The OpenVPN client will accept the cipher pushed by the server if it is in this list. If the OpenVPN server supports cipher negotiation, the OpenVPN client may accept additional ciphers that are not in this list.

Accepted values can be multiple values of aes-128-cbc, aes-192-cbc, aes-256-cbc, aes-128-gcm, aes-192-gcm and aes-256-gcm. The default value is aes-256-gcm,aes-256-cbc,aes-128-gcm,aes-128-cbc.

digest

The digest algorithm the OpenVPN client uses to sign and authenticate data channel packets.

Accepted values can be one of sha1, sha224, sha256, sha384 or sha512. The default value is sha1.

ca

The CA certificate this OpenVPN client uses to validate the certificate presented by the server. This file is in PEM format and is often named 'ca.crt' or similar.

Accepted value is any string up to 63 characters.

crl

The CRL this OpenVPN client uses to prevent connection to a server that presents a revoked certificate. This file is in PEM format and is often named 'crl.pem' or similar.

Accepted value is any string up to 63 characters.

capath

The CA and CRL directory path for this OpenVPN client. This allows you to provide multiple CA and CRL files. You should use the c_rehash tool to create CA certificates with a '.0' filename extension and CRLs with a '.r0' filename extension.

Accepted value is any string up to 63 characters.

cert

The public certificate for this OpenVPN client. This file is in PEM format and is often named 'client.crt' or similar.

Accepted value is any string up to 63 characters.

key

The private key for this OpenVPN client. This file is in PEM format and is often named 'client.key' or similar.

Accepted value is any string up to 63 characters.

username

The username the OpenVPN client uses to authenticate with the OpenVPN server.

Accepted value is any string up to 32 characters.

password

The password the OpenVPN client uses to authenticate with the OpenVPN server.

Accepted value is any string up to 128 characters.

pull-routes

Allows the OpenVPN client to accept or reject routes that are pushed from the OpenVPN server.

Value is either on or off. The default value is on.

verb

Adjusts the amount of output that this OpenVPN client records in the system log. Set this parameter to 0 to record only errors and warnings. Set this parameter to 3 to record a fairly complete activity log.

Accepted value is any integer from 0 to 4. The default value is 0.

nat

Enables Network Address Translation (NAT) for outgoing packets on the OpenVPN client network interface. NAT allows a computer on a local network to send a request to a computer behind the OpenVPN server without adding additional routes on the OpenVPN server. NAT changes the source IP address of the outgoing packet to the IP address of the OpenVPN client, hiding the local network from the OpenVPN server. Since the request appears to come from the OpenVPN client, the response packet is destined for the OpenVPN client, and the OpenVPN server properly routes it to the correct OpenVPN client. The OpenVPN client only uses NAT if the 'bridge-mode' parameter is set to 'off'.

Value is either on or off. The default value is on.

openvpn-route

Specifies the routes the OpenVPN server pushes to OpenVPN clients so they can access resources located behind the OpenVPN server. These resources would be otherwise unavailable since they are on different subnets than the OpenVPN tunnel itself. Typically, these routes would only be needed for non-bridged (TUN) configurations.

Syntax

```
openvpn-route <1 - 10> <parameter> <value>
```

Parameters

destination

Destination network for the route. This value typically ends with '.0' to match the subnet mask.

Value should be an IPv4 address.

mask

Subnet mask for the route.

Value should be an IPv4 address. The default value is 255.255.255.0.

openvpn-server

Configures an OpenVPN server.

Syntax

```
openvpn-server <parameter> <value>
```

Parameters

state

Enables or disables the OpenVPN server.

Value is either on or off. The default value is off.

description

A description of this OpenVPN server.

Accepted value is any string up to 255 characters.

network

The local network for this OpenVPN tunnel if 'bridge-mode' is set to off. This value typically ends with '.0' to match the subnet mask.

Value should be an IPv4 address.

mask

The local subnet for this OpenVPN tunnel if 'bridge-mode' is set to off.

Value should be an IPv4 address. The default value is 255.255.255.0.

dns1

The IPv4 address of the primary DNS server. This value is pushed to OpenVPN clients if 'bridge-mode' is set to off.

Value should be an IPv4 address.

dns2

The IPv4 address of the secondary DNS server. This value is pushed to OpenVPN clients if 'bridge-mode' is set to off.

Value should be an IPv4 address.

port

The port this OpenVPN server uses to listen for incoming connections from OpenVPN clients.

Accepted value is any integer from 1 to 65535. The default value is 1194.

topology

The network topology this OpenVPN server uses to assign IP addresses to OpenVPN clients. This value is only used if 'bridge-mode' is set to off.

Accepted values can be one of net30, p2p or subnet. The default value is net30.

protocol

The protocol (TCP or UDP) this OpenVPN server uses to listen for incoming connections from OpenVPN clients.

Accepted values can be one of udp or tcp. The default value is udp.

bridge-mode

Enables Ethernet bridge (TAP) mode for this OpenVPN server. This eliminates the need for routing between networks as required by TUN mode, but may have scalability issues, since all broadcast traffic will flow over the OpenVPN tunnel.

Accepted values can be one of off, lan1, lan2, lan3, lan4, lan5, lan6, lan7, lan8, lan9 or lan10. The default value is off.

cipher

The encryption algorithm or list of algorithms the OpenVPN server can use to encrypt and decrypt data channel packets. The OpenVPN server will always push the first cipher in the list to OpenVPN clients that support cipher negotiation. OpenVPN clients that do not support cipher negotiation can connect using any cipher in this list.

Accepted values can be multiple values of aes-128-cbc, aes-192-cbc, aes-256-cbc, aes-128-gcm, aes-192-gcm and aes-256-gcm. The default value is aes-256-gcm,aes-256-cbc,aes-128-gcm,aes-128-cbc.

digest

The digest algorithm the OpenVPN server uses to sign and authenticate data channel packets.

Accepted values can be one of sha1, sha224, sha256, sha384 or sha512. The default value is sha1.

auth-by

Configures authentication to use certs, username/password, or both.

Accepted values can be one of certs, user-pass or both. The default value is certs.

ca

The CA certificate this OpenVPN server uses to validate all certificates presented by clients. This file is in PEM format and is often named 'ca.crt' or similar.

Accepted value is any string up to 63 characters.

crl

The CRL this OpenVPN server uses to deny access to any client that presents a revoked certificate. This file is in PEM format and is often named 'crl.pem' or similar.

Accepted value is any string up to 63 characters.

capath

The CA and CRL directory path for this OpenVPN server. This allows you to provide multiple CA and CRL files. You should use the c_rehash tool to create CA certificates with a '.0' filename extension and CRLs with a '.r0' filename extension.

Accepted value is any string up to 63 characters.

dh

The Diffie-Hellman parameters this OpenVPN server uses for shared secret generation. This file is in PEM format and is often named 'dh2048.pem' or similar. Leave blank to use Elliptic Curve Diffie-Hellman key exchange.

Accepted value is any string up to 63 characters.

cert

The public certificate for this OpenVPN server. This file is in PEM format and is often named 'server.crt' or similar.

Accepted value is any string up to 63 characters.

key

The private key for this OpenVPN server. This file is in PEM format and is often named 'server.key' or similar.

Accepted value is any string up to 63 characters.

radius-server

The IP address for the RADIUS server for OpenVPN.

Value should be an IPv4 address.

radius-server-port

The port for the RADIUS server.

Accepted value is any integer from 1 to 65535. The default value is 1812.

radius-server-secret

The secret for the RADIUS server.

Accepted value is any string up to 64 characters.

radius-server-state

Enables or disables RADIUS authentication.

Value is either on or off. The default value is off.

compression

The compression algorithm this OpenVPN server uses to compress data channel packets.

Accepted values can be one of off, lzo or lz4. The default value is off.

verb

Adjusts the amount of output that this OpenVPN server records in the system log. Set this parameter to 0 to record only errors and warnings. Set this parameter to 3 to record a fairly complete activity log.

Accepted value is any integer from 0 to 4. The default value is 0.

keepalive-interval

Sends a ping message if no other traffic is sent in either direction between the OpenVPN client and server. This value is also pushed to the client. To disable the ping-based keepalive mechanism, set this parameter to 0.

Accepted value is any integer from 0 to 3600. The default value is 30.

keepalive-timeout

Restarts the OpenVPN tunnel if no traffic is detected for this many seconds. This value should typically be 5-6 times as large as the 'keepalive-interval' value. This value is doubled before it is set on the server. This value is also pushed to the client. To disable the ping-based keepalive mechanism, set this parameter to 0.

Accepted value is any integer from 0 to 3600. The default value is 150.

reneg-bytes

Number of bytes sent/received before data channel encryption key is renegotiated. To disable data channel encryption key renegotiation, set this parameter to 0.

Accepted value is any integer from 0 to 4000000000. The default value is 0.

reneg-sec

Number of seconds before the data channel encryption key is renegotiated.

Accepted value is any integer from 60 to 86400. The default value is 3600.

openvpn-user

Configures an OpenVPN server user.

Syntax

```
openvpn-user <1 - 10> <parameter> <value>
```

Parameters

username

Username for OpenVPN user.

Accepted value is any string up to 32 characters.

password

Password for OpenVPN user.

Accepted value is any string up to 128 characters.

ping

Sends ICMP echo (ping) packets to the specified destination address.

Syntax

```
ping [ipv6] [count n] [interface ifname] [size bytes] destination
```

Parameters

ipv6

Specifies whether the destination address to ping is an IPv6 address.

count

Number of pings to send.

interface

The interface from which pings are sent.

size

The number of data bytes to send.

destination

The name of the IP host to ping.

Examples

- ```
  ping ipv6 ipv6.google.com
  ```
  Ping the ipv6 host 'ipv6.google.com'
- ```
  ping 8.8.8.8
  ```
  Ping IP address 8.8.8.8 with packets of default size 56 bytes
- ```
  ping count 10 size 8 8.8.8.8
  ```
  Ping IP address 8.8.8.8 for 10 times
- ```
  ping interface eth2 count 5 8.8.8.8
  ```
  Ping IP address 8.8.8.8 for 5 times via Ethernet interface 2

pki

The public key infrastructure is used to manage private key and certificate files to secure network activities.

This command is available to super users only.

Syntax

```
pki privkey <privkeyfile> <size> [aes128|aes256 <passphrase>]
pki list
pki del <privkeyfile>
pki addkey <privkeyfile>
pki csr [country c] [state st] [locality l] [organization o] [organizational-unit
ou] [common-name cn] [email e] [passphrase pw] <privkeyfile> <csr-file> <digest>
pki dh-file <parameter-file> <size>
```

Parameters

csr

Create a Certificate Signing Request.

privkey

Generate a private key file.

list

Show the private key files.

del

Remove a private key file.

addkey

Add an externally-generated private key file to the list of private key files.

dh-file

Generate a Diffie Hellman parameter file using the PEM format.

Examples

- ```
  privkey mykeyfile.key 2048
  ```

  Generates an unencrypted mykeyfile.key with 2048 bits rsa

- ```
  privkey mykeyfile.key 4096 aes256 "my secret phrase"
  ```

  Generates an encrypted mykeyfile.key with 4096 bits rsa

- ```
  dh-file mydhfile.pem 1024
  ```
  Generates a Diffie Hellman 1024 bit parameter file
- ```
  list
  ```
  Lists the existing key files
- ```
  del mykeyfile.key
  ```
  Deletes mykeyfile.key from the list of key files
- ```
  addkey mykeyfile.key
  ```
  Moves the externally-generated file mykeyfile.key from the upload folder into the list of private key files
- ```
  csr common-name www.example.com mykeyfile.key my.csr sha256
  ```
  Create a Certificate Signing Request with a common name
  ```

port-forward

Configures port forwarding rules.

Syntax

```
port-forward <1 - 30> <parameter> <value>
```

Parameters

port

The TCP or UDP port or ports from which incoming packets are forwarded.

Accepted value is any string up to 255 characters.

to-port

The TCP or UDP port that packets are forwarded to after being received on the incoming port(s).

Accepted value is any integer from 0 to 65535. The default value is 0.

to-ip-address

The IPv4 address that packets are forwarded to after being received on the incoming interface.

Value should be an IPv4 address.

description

The description of this rule.

Accepted value is any string up to 255 characters.

state

Enables or disables a port forward rule. Invalid rules are not enabled.

Value is either on or off. The default value is off.

protocol

The protocol or protocols of the packets to forward.

Accepted values can be one of tcp, udp or tcp-and-udp. The default value is tcp-and-udp.

src

The WAN or LAN that is the source of incoming traffic to be forwarded.

Accepted values can be one of any, any-lan, lan1, lan2, lan3, lan4, lan5, lan6, lan7, lan8, lan9, lan10, any-wan, wan1, wan2, wan3, wan4, wan5, wan6, wan7, wan8, wan9 or wan10. The default value is any.

Examples

- ```
  port-forward 4 port 80
  ```

  Forward port 80 to the to-port and to-ip-address
  ```

- ```
  port-forward 4 port 1000:2000
  ```
  Forward all ports in the range 1000-2000
- ```
  port-forward 4 port 23,24,25
  ```
  Forward ports in the list 23,24,25
- ```
  port-forward 4 src any-wan
  ```
  Forwards traffic from WANs only
  ```

pwd

Displays the current directory name.

Syntax

```
pwd
```

Parameters

python

Start Python

This command is available to super users only.

Syntax

```
python
python <filepath> [args]
python stop <id>
```

Parameters

filepath

The path to the python file.

args

Arguments to send to the python file.

id

The id of the python file to be stopped.

python-autostart

Configure Python applications to be run at startup.

This command is available to super users only.

Syntax

```
python-autostart <1 - 4> <parameter> <value>
```

Parameters

filepath

Path to the file to be run

Accepted value is any string up to 255 characters.

on-exit

Action taken when the application exits

Accepted values can be one of none, restart or reboot. The default value is none.

args

Arguments sent to the application

Accepted value is any string up to 255 characters.

state

Enables or disable application startup

Accepted values can be one of on or off. The default value is on.

qos-filter

Configures QoS filters.

Syntax

```
qos-filter <1 - 32> <parameter> <value>
```

Parameters

description

The description of this filter.

Accepted value is any string up to 255 characters.

state

Enables or disables a QoS filter.

Value is either on or off. The default value is off.

queue

All traffic matching this filter is sent to this queue.

Accepted value is any integer from 0 to 8. The default value is 0.

src-ip-address

The IPv4 or IPv6 source address of the incoming packet. Use a simple IPv4 or IPv6 address, or use CIDR notation (example: 192.168.100.0/24, fe80::/10)

Accepted value is any string up to 43 characters.

src-ip-port

The source port(s) of the incoming packet. Use a simple port, a range (lowport:highport) or a list (port1,port2...,portn). Default '0' implies 'Any'. Source port is ignored when protocol does not explicitly include tcp or udp.

Accepted value is any string up to 255 characters. The default value is 0.

dst-ip-address

The IPv4 or IPv6 destination address of the incoming packet. Use a simple IPv4 or IPv6 address, or use CIDR notation (example: 192.168.100.0/24, fe80::/10)

Accepted value is any string up to 43 characters.

dst-ip-port

The destination port(s) of the incoming packet. Use a simple port, a range (lowport:highport) or a list (port1,port2...,portn). Default '0' implies 'Any'. Dest port is ignored when protocol does not explicitly include tcp or udp.

Accepted value is any string up to 255 characters. The default value is 0.

src

The interface that is the source of incoming traffic.

Accepted values can be one of any, any-lan, lan1, lan2, lan3, lan4, lan5, lan6, lan7, lan8, lan9 or lan10. The default value is any.

protocol

The protocol of the incoming packet. Use a single protocol, a list (tcp,udp,icmp), or exclusive value (any). When set to 'any', src-ip-port and dst-ip-port values are ignored.

Accepted values can be multiple values of tcp, udp, icmp and any. The default value is tcp,udp.

dscp

The Differentiated Services Field values to match. Use a single value, a list (ef,af11,af21), or exclusive value (any).

Accepted values can be multiple values of any, be, af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, ef, cs0, cs1, cs2, cs3, cs4, cs5, cs6 and cs7. The default value is any.

qos-queue

Configures a QoS queue

Syntax

```
qos-queue <1 - 8> <parameter> <value>
```

Parameters

state

Enables or disables this QoS queue.

Value is either on or off. The default value is off.

description

A description of this QoS queue.

Accepted value is any string up to 255 characters.

bandwidth-upstream

Amount of bandwidth that is guaranteed to this queue in kbps. The sum of the guaranteed bandwidth for all queues should not exceed the bandwidth of the slowest WAN with QoS enabled.

Accepted value is any integer from 0 to 1000000. The default value is 0.

borrow-upstream

Allow the queue to use additional bandwidth if there is any unused.

Value is either on or off. The default value is on.

dscp-class

Set the DSCP class of outbound packets using this queue.

Accepted values can be one of do-not-set, be, af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, ef, cs0, cs1, cs2, cs3, cs4, cs5, cs6 or cs7. The default value is do-not-set.

radius

Configures RADIUS authentication for system administrators, restricting access to the web and command line interfaces.

This command is available to super users only.

Syntax

```
radius <parameter> <value>
```

Parameters

state

Enable or disable RADIUS authentication for system administrators.

Value is either on or off. The default value is off.

server

The IP address or fully-qualified domain name of the RADIUS server to use to authenticate system administrators.

Value should be a fully qualified domain name.

server-port

The UDP port number for the RADIUS server.

Accepted value is any integer from 1 to 65535. The default value is 1812.

server-secret

The shared secret for the RADIUS server. Secret can not contain spaces, an open bracket ([), or a close bracket (]).

Accepted value is any string up to 64 characters.

nas-id

A unique identifier for this network access server (NAS). The fully-qualified domain name of the NAS is often used, but any arbitrary string may be used. String may not contain spaces, an open bracket ([), or close bracket (]).

Accepted value is any string up to 64 characters.

server-timeout

The amount of time in seconds to wait for the RADIUS server to respond.

Accepted value is any integer from 3 to 10. The default value is 3.

local-auth

Whether to use local authentication if the RADIUS server does not respond before the timeout expires.

Value is either on or off. The default value is on.

debug

Enable or disable additional debug messages from the RADIUS client. These messages are added to the system log.

Value is either on or off. The default value is off.

backup-server

The IP address or fully-qualified domain name of the backup RADIUS server to use to authenticate system administrators when the main RADIUS server is not available.

Value should be a fully qualified domain name.

backup-server-port

The UDP port number for the backup RADIUS server.

Accepted value is any integer from 1 to 65535. The default value is 1812.

backup-server-secret

The shared secret for the backup RADIUS server. Secret can not contain spaces, an open bracket ([), or a close bracket (]).

Accepted value is any string up to 64 characters.

backup-server-timeout

The amount of time in seconds to wait for the backup RADIUS server to respond.

Accepted value is any integer from 3 to 10. The default value is 3.

reboot

Reboots the device immediately or at a scheduled time. Performing a reboot will not automatically save any configuration changes since the configuration was last saved.

This command is available to all users.

Syntax

```
reboot [[in M][at HH:MM][cancel]]
```

Parameters

in

For a scheduled reboot, the minutes before the device is rebooted.

at

For a scheduled reboot, the time to reboot the device, specified in the format HH:MM.

cancel

Cancels a scheduled reboot.

rename

Renames a file.

This command is available to all users.

Syntax

```
rename oldName newName
```

Parameters

oldName

Old file name.

newName

New file name.

rmdir

Deletes a directory.

This command is available to all users.

Syntax

```
rmdir dir
```

Parameters

dir

The directory to be removed.

route

Configures a static route, a manually-configured entry in the routing table.

Syntax

```
route <1 - 32> <parameter> <value>
```

Parameters

destination

The destination IP network for the static route.

Value should be an IPv4 address.

mask

The destination IP netmask for the static route.

Value should be an IPv4 address.

gateway

The gateway to use for the static route.

Value should be an IPv4 address.

metric

The metric for the static route. The metric defines the order in which the device uses routes if there are two routes to the same destination. In such a case, the device uses the route with the smaller metric.

Accepted value is any integer from 0 to 255. The default value is 0.

interface

The name of the interface to which packets are routed.

Accepted values can be one of none, cellular1, cellular2, gre1, gre2, gre3, gre4, gre5, gre6, gre7, gre8, gre9 or gre10. The default value is none.

save

Saves the configuration to flash memory. Unless you issue this command, all configuration changes since the configuration was last saved are discarded after a reboot.

This command is available to all users.

Syntax

```
save config
save analyzer
```

Parameters

config

Saves all configuration to flash memory.

analyzer

Saves the current captured traffic to a file.

Examples

- ```
  save config
  ```

  Save the current configuration to flash memory.

- ```
  save analyzer packets.pcapng
  ```

  Saves the current captured traffic to packets.pcapng.

serial

Configures a serial interface.

Syntax

```
serial <1 - 4> <parameter> <value>
```

Parameters

state

Enables or disables the serial interface.

Value is either on or off. The default value is on.

description

A description of the serial interface.

Accepted value is any string up to 63 characters.

baud

The data rate in bits per second (baud) for serial transmission.

Accepted values can be one of 110, 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400, 460800 or 921600. The default value is 115200.

databits

Number of data bits in each transmitted character.

Accepted values can be one of 8 or 7. The default value is 8.

parity

Sets the parity bit. The parity bit is a method of detecting errors in transmission. It is an extra data bit sent with each data character, arranged so that the number of 1 bits in each character, including the parity bit, is always odd or always even.

Accepted values can be one of none, odd or even. The default value is none.

stopbits

The number of stop bits sent at the end of every character.

Accepted values can be one of 1 or 2. The default value is 1.

flowcontrol

The type of flow control signals to pause and resume data transmission. Available options are software flow control using XON/XOFF characters, hardware flow control using the RS232 RTS and CTS signals, or no flow control signals.

Accepted values can be one of none, software or hardware. The default value is none.

show analyzer

Displays the traffic analyzer log.

Parameters

description

Display the traffic analyzer log.

show cellular

Displays cellular interface status and statistics.

Parameters

description

A description of the cellular interface.

admin-status

Whether the Cellular interface is sufficiently configured to be brought up.

oper-status

Whether the Cellular interface is up or down.

module

Manufacturer's model number for the cellular module.

firmware-version

Manufacturer's version number for the software running on the cellular module.

hardware-version

Manufacturer's version number for the cellular module hardware.

imei

International Mobile Station Equipment Identity (IMEI) number for the cellular module, a unique number assigned to every mobile device.

sim-status

Which SIM slot is currently in use by the device.

signal-strength

A measure of the signal level of the cellular network, measured in dB.

signal-quality

An indicator of the quality of the received cellular signal, measured in dB.

registration-status

The status of the cellular module's connection to a cellular network.

network-provider

Network provider for the cellular network.

temperature

Current temperature of the cellular module, as read and reported by the temperature sensor on the cellular module.

connection-type

Cellular connection type.

radio-band

The radio band on which the cellular module is operating.

channel

The radio channel on which the cellular module is operating.

pdp-context

The current Packet Data Protocol (PDP) connection context. A PDP context contains routing information for packet transfer between a mobile station (MS) and a gateway GPRS support node (GGSN) to have access to an external packet-switching network. The PDP context identified by an exclusive MS PDP address (the mobile station's IP address). This means that the mobile station will have as many PDP addresses as activated PDP contexts.

ip-address

IP address for the cellular interface.

mask

Address mask for the cellular interface.

gateway

IP address of the remote end of the cellular connection.

dns-servers

IP addresses of the DNS servers in use for the cellular interface.

rx-packets

Number of packets received by the cellular module during the current data session.

tx-packets

Number of packets transmitted by the cellular module during the current data session.

rx-bytes

Number of bytes received by the cellular module during the current data session.

tx-bytes

Number of bytes transmitted by the cellular module during the current data session.

attachment-status

The status of the cellular module's attachment to a cellular network.

iccid

Integrated Circuit Card Identifier (ICCID). This identifier is unique to each SIM card.

sim1-pin-status

SIM1 PIN Status.

sim1-pin-retries

Number of retries PIN left on SIM1

sim2-pin-status

SIM2 PIN Status.

sim2-pin-retries

Number of PIN retries left on SIM2

show cloud

Displays Digi Remote Manager connection status and statistics.

Parameters

status

Status of the device connection to the Digi Remote Manager.

server

The URL of the connected Digi Remote Manager.

deviceid

Device ID for Digi Remote Manager connection.

uptime

Amount of time, in seconds, that the Digi Remote Manager connection has been established.

rx-bytes

Number of bytes received from Digi Remote Manager.

rx-packets

Number of packets received from Digi Remote Manager.

tx-bytes

Number of bytes transmitted to Digi Remote Manager.

tx-packets

Number of packets transmitted to Digi Remote Manager.

show config

Displays the current device configuration.

Parameters

config

The current configuration running on the device.

show dhcp

Displays information about DHCP connected clients.

Parameters

dhcp

Displays the DHCP status.

show dmnr

Displays local networks and their DMNR details.

Parameters

admin-status

Whether DMNR is sufficiently configured to be brought up.

oper-status

Whether the DMNR tunnel is up or down.

registration-status

Displays the DMNR registration state as it negotiates with the Home Agent.

home-agent

Displays the IP address of DMNR Home Agent.

care-of-address

Displays the IP address of DMNR Care of Address.

interface

Displays the interface used by the DMNR tunnel.

lifetime

Displays the actual lifetime status.

local-networks

Displays the local networks and their DMNR status.

show dsl

UNUSED

Parameters

unused

UNUSED

show eth

Displays Ethernet interfaces status and statistics.

Parameters

description

A description of the Ethernet interface.

admin-status

Whether the Ethernet interface is sufficiently configured to be brought up.

oper-status

Whether the Ethernet interface is up or down.

uptime

Amount of time the Ethernet interface has been up.

mac-address

The MAC address, or physical address, of the Ethernet interface.

link-status

The current speed and duplex mode of the Ethernet interface.

link-speed

The current speed of the Ethernet interface.

link-duplex

The current duplex mode of the Ethernet interface.

rx-unicast-packets

The number of unicast packets transmitted on the Ethernet interface.

tx-unicast-packets

The number of unicast packets transmitted on the Ethernet interface.

rx-broadcast-packets

The number of broadcast packets received on the Ethernet interface.

tx-broadcast-packets

The number of broadcast packets transmitted on the Ethernet interface.

rx-multicast-packets

The number of multicast packets received on the Ethernet interface.

tx-multicast-packets

The number of multicast packets transmitted on the Ethernet interface.

rx-crc-errors

The number of received packets that do not contain the proper cyclic redundancy check (CRC), or checksum value.

tx-crc-errors

The number of transmitted packets that do not contain the proper cyclic redundancy check (CRC), or checksum value.

rx-drop-packets

The number of received packets that have been dropped on the Ethernet interface.

tx-drop-packets

The number of transmitted packets that have been dropped on the Ethernet interface.

rx-pause-packets

The number of pause packets received on the Ethernet interface. An overwhelmed network node can send a packet, which halts the transmission of the sender for a specified period of time.

tx-pause-packets

The number of pause packets transmitted on the Ethernet interface.

rx-filtering-packets

The number of received packets that were blocked or dropped through packet filtering.

tx-collisions

The number of collision events detected in transmitted data. Collisions occur when two devices attempt to place a packet on the network at the same time. Collisions are detected when the signal on the cable is equal to or exceeds the signal produced by two or more transceivers that are transmitting simultaneously.

rx-alignment-error

The number of received packets that do not end on an 8-bit boundary, known as an alignment error.

rx-undersize-error

The number of received packets that do not end on an 8-bit boundary, known as an alignment error.

rx-fragment-error

The number of received packets that contain fewer than the required minimum of 64 bytes, and have a bad CRC. Fragments are generally caused by collisions.

rx-oversize-error

The number of received packets that are larger than the maximum 1518 bytes and have a good CRC.

rx-jabber-error

The number of packets that are greater than 1518 bytes and have a bad CRC. If a transceiver does not halt transmission after 1518 bytes, it is considered to be a jabbering transceiver.

rx-packets

The number of packets received on the Ethernet interface.

tx-packets

The number of packets transmitted on the Ethernet interface.

rx-bytes

The number of bytes received on the Ethernet interface.

tx-bytes

The number of bytes transmitted on the Ethernet interface.

rx-errors

The total number of received packets that are marked as errors.

tx-errors

The total number of transmitted packets that are marked as errors.

tx-carrier-error

The number of transmission failures due to improper signaling, as with a duplex mismatch.

rx-fifo-error

The number of events in which the Ethernet driver detects an inability to service the receive packet queue, as with processor congestion.

tx-fifo-error

The number of events in which the Ethernet driver detects an inability to service the transmit packet queue, as with processor or network congestion.

show firewall

Displays the firewall status and statistics. By default, all firewall tables are displayed. To display individual tables, specify the table name on the show firewall command. In the command output, the policy for each chain is also displayed in brackets after the chain name. The firewall keeps a counter for each rule which counts the number of packets and bytes that have been matched against the rule. This is a useful tool to determine if a rule is correctly detecting packets. To clear the counters, use the 'clear firewall' command.

Parameters

filter

The currently defined filter table for IPv4.

mangle

The currently defined mangle table for IPv4.

raw

The currently defined raw table for IPv4.

nat

The currently defined nat table for IPv4.

show firewall6

Displays the firewall status and statistics. By default, all firewall tables are displayed. To display individual tables, specify the table name on the show firewall6 command. In the command output, the policy for each chain is also displayed in brackets after the chain name. The firewall keeps a counter for each rule which counts the number of packets and bytes that have been matched against the rule. This is a useful tool to determine if a rule is correctly detecting packets. To clear the counters, use the 'clear firewall6' command.

Parameters

filter

The currently defined filter table for IPv6.

mangle

The currently defined mangle table for IPv6.

show gre

Displays Generic Routing Encapsulation (GRE) tunnel status and statistics.

Parameters

admin-status

Whether the GRE tunnel is sufficiently configured to be brought up.

oper-status

Whether the GRE tunnel is up or down.

description

Description of the GRE tunnel.

ip-address

IP address for the GRE tunnel.

mask

Subnet mask for the GRE tunnel.

peer

Remote peer for this GRE tunnel.

key

Key being used by this GRE tunnel.

rx-bytes

Number of bytes received by the GRE tunnel.

rx-packets

Number of packets received by the GRE tunnel.

tx-bytes

Number of bytes transmitted by the GRE tunnel.

tx-packets

Number of packets transmitted by the GRE tunnel.

show ip-filter

Displays IP filter rules status.

Parameters

description

The description of this rule.

state

Whether the IP filter rule is enabled or disabled.

action

The action taken when the rule matches.

src-ip-address

The IPv4 source address of the incoming packet. Use a simple IP address, or use CIDR notation (example: 192.168.100.0/24)

src-ip-port

The source port(s) of the incoming packet. Use a simple port, a range (lowport:highport) or a list (port1,port2...,portn). Default '0' implies 'Any'. Source port is ignored when protocol does not explicitly include tcp or udp.

dst-ip-address

The IPv4 destination address of the incoming packet. Use a simple IP address, or use CIDR notation (example: 192.168.100.0/24)

dst-ip-port

The destination port(s) of the incoming packet. Use a simple port, a range (lowport:highport) or a list (port1,port2...,portn). Default '0' implies 'Any'. Dest port is ignored when protocol does not explicitly include tcp or udp.

src

The WAN or LAN that is the source of incoming traffic.

dst

The WAN or LAN that is the destination of outgoing traffic.

protocol

The protocol of the incoming packet. Use a single protocol, a list (tcp,udp,icmp), or exclusive value (any). When set to 'any', src-ip-port and dst-ip-port values are ignored.

show ipsec

Displays IPsec tunnel status and statistics.

Parameters

description

A description for this IPsec tunnel.

admin-status

Whether this IPsec tunnel is sufficiently configured to be brought up.

oper-status

Whether this IPsec tunnel is up or down.

uptime

Amount of time, in seconds, this IPsec tunnel has been up.

peer-ip

Peer IP address for this IPsec tunnel.

local-network

Local network for this IPsec tunnel.

local-mask

Local network mask for this IPsec tunnel.

remote-network

Remote network for this IPsec tunnel.

remote-mask

Remote network mask for this IPsec tunnel.

key-negotiation

Key negotiation used for this IPsec tunnel.

rekeying-in

Amount of time before the keys are renegotiated.

ah-ciphers

Authentication Header (AH) Ciphers.

esp-ciphers

Encapsulating Security Payload (ESP) Ciphers.

renegotiating-in

Renegotiating in.

outbound-esp-sas

Outbound ESP Security Associations (SA).

inbound-esp-sas

Inbound ESP Security Associations (SA).

rx-bytes

Number of bytes received over the IPsec tunnel.

tx-bytes

Number of bytes transmitted over the IPsec tunnel.

ike-spis

IKE Security Parameter Indexes.

show ipstats

Displays system-level Internet Protocol (IP) status and statistics.

Parameters

rx-bytes

Number of bytes received.

rx-packets

Number of packets received.

rx-multicast-packets

Number of multicast packets received.

rx-multicast-bytes

Number of multicast bytes received.

rx-broadcast-packets

Number of broadcast packets received.

rx-forward-datagrams

Number of forwarded packets received.

rx-delivers

Number of received packets delivered.

rx-reasm-requireds

Number of received packets that required reassembly.

rx-reasm-oks

Number of received packets that were reassembled without errors.

rx-reasm-fails

Number of received packets for which reassembly failed.

rx-discards

Number of received IP packets that have been discarded.

rx-no-routes

Number of received packets that have no routing information associated with them.

rx-address-errors

Number of received packets containing IP address errors.

rx-unknown-protos

Number of received packets where the protocol is unknown.

rx-truncated-packets

Number of received packets where the data was truncated.

tx-bytes

Number of bytes transmitted.

tx-packets

Number of packets transmitted.

tx-multicast-packets

Number of multicast packets transmitted.

tx-multicast-bytes

Number of multicast bytes transmitted.

tx-broadcast-packets

Number of broadcast packets transmitted.

tx-forward-datagrams

Number of forwarded packets transmitted.

tx-frag-requireds

Total number of transmitted IP packets that required fragmenting.

tx-frag-oks

Number of transmitted IP packets that were fragmented without errors.

tx-frag-fails

Number of transmitted IP packets for which fragmentation failed.

tx-frag-creates

Number of IP fragments created.

tx-discards

Number of transmitted IP packets that were discarded.

tx-no-routes

Number of transmitted IP packets that had no routing information associated with them.

show lan

Displays Local Area Network (LAN) status and statistics.

Parameters

admin-status

Whether the LAN is sufficiently configured to be brought up.

oper-status

Whether the LAN is up or down.

description

Description of the LAN.

interfaces

The physical interfaces for the LAN.

mtu

Maximum Transmission Unit for the LAN.

ip-address

IP address for the LAN.

dhcp-client

Enables or disable the DHCP client for this LAN.

mask

Subnet mask for the LAN.

dns1

Preferred DNS server.

dns2

Alternate DNS server.

rx-bytes

Number of bytes received by the LAN.

rx-packets

Number of packets received by the LAN.

tx-bytes

Number of bytes transmitted by the LAN.

tx-packets

Number of packets transmitted by the LAN.

ipv6-address

The IPv6 address or addresses assigned to the LAN.

show log

Displays log(event or system/kernel).

Parameters

system

Display the system/kernel log.

show openvpn-client

Displays status and statistics about this OpenVPN client.

Parameters

description

A description of this OpenVPN client.

admin-status

Whether this OpenVPN client is configured to be running.

oper-status

Whether this OpenVPN client is actually running.

server

The IP address or fully-qualified domain name of the OpenVPN server to which this OpenVPN client attempts to connect.

interface

The name of the local virtual network interface (TUN/TAP adapter) that this OpenVPN client uses.

ip-address

The IP address assigned to the local virtual network interface (TUN/TAP adapter) that this OpenVPN client uses.

mask

The subnet mask assigned to the local virtual network interface (TUN/TAP adapter) that this OpenVPN client uses.

mtu

The Maximum Transmission Unit (MTU) size configured for the local virtual network interface (TUN/TAP adapter) that this OpenVPN client uses.

interface-rx-bytes

The number of bytes received on the local virtual network interface (TUN/TAP adapter) that this OpenVPN client uses.

interface-tx-bytes

The number of bytes transmitted on the local virtual network interface (TUN/TAP adapter) that this OpenVPN client uses.

interface-rx-packets

The number of packets received on the local virtual network interface (TUN/TAP adapter) that this OpenVPN client uses.

interface-tx-packets

The number of packets transmitted on the local virtual network interface (TUN/TAP adapter) that this OpenVPN client uses.

socket-rx-bytes

The number of bytes received on the local UDP/TCP socket that this OpenVPN client uses.

socket-tx-bytes

The number of bytes transmitted on the local UDP/TCP socket that this OpenVPN client uses.

show openvpn-server

Displays status and statistics about this OpenVPN server.

Parameters

description

A description of this OpenVPN server.

admin-status

Whether this OpenVPN server is configured to be running.

oper-status

Whether this OpenVPN server is actually running.

interface

The name of the local virtual network interface (TUN/TAP adapter) that this OpenVPN server uses.

ip-address

The IP address assigned to the local virtual network interface (TUN/TAP adapter) that this OpenVPN server uses.

mask

The subnet mask assigned to the local virtual network interface (TUN/TAP adapter) that this OpenVPN server uses.

mtu

The Maximum Transmission Unit (MTU) size configured for the local virtual network interface (TUN/TAP adapter) that this OpenVPN server uses.

interface-rx-bytes

The number of bytes received on the local virtual network interface (TUN/TAP adapter) that this OpenVPN server uses.

interface-tx-bytes

The number of bytes transmitted on the local virtual network interface (TUN/TAP adapter) that this OpenVPN server uses.

interface-rx-packets

The number of packets received on the local virtual network interface (TUN/TAP adapter) that this OpenVPN server uses.

interface-tx-packets

The number of packets transmitted on the local virtual network interface (TUN/TAP adapter) that this OpenVPN server uses.

show port-forward

Displays port forwarding rules.

Parameters

port

The TCP or UDP port or ports from which incoming packets are forwarded.

to-port

The TCP or UDP port that packets are forwarded to after being received on the incoming port(s).

to-ip-address

The IPv4 address that packets are forwarded to after being received on the incoming interface.

description

The description of this rule.

state

Enables or disables a port forward rule. Invalid rules are not enabled.

protocol

The protocol or protocols of the packets to forward.

src

The WAN or LAN that is the source of incoming traffic to be forwarded.

show python

Displays running Python applications

Parameters

applications

Displays running Python applications

show route

Displays all IP routes in the IPv4 routing table.

Parameters

destination

Destination of the route.

gateway

The gateway for the route.

metric

The metric assigned to the route.

protocol

The protocol for the route.

idx

The index number for the route.

interface

The interface for the route.

status

Status of the route.

show serial

Displays serial interface status and statistics.

Parameters

description

A description of the serial interface.

admin-status

Whether the serial interface is sufficiently configured to be brought up.

oper-status

Whether the serial interface is up or down.

uptime

Amount of time the serial interface has been up.

tx-bytes

Number of bytes transmitted over the serial interface.

rx-bytes

Number of bytes received over the serial interface.

overrun

Number of times the next data character arrived before the hardware could move the previous character.

overflow

Number of times the received buffer was full when additional data was received.

line-status

The current signal detected on the serial line.

show system

Displays system status and statistics.

Parameters

model

The model name for the device.

part-number

The part number for the device.

serial-number

The serial number for the device.

hardware-version

The hardware version for the device.

bank

The current firmware flash memory bank in use.

firmware-version

The current firmware version running on the device.

bootloader-version

The current bootloader version running on the device.

config-file

The current configuration file loaded on the device.

uptime

The time the device has been up.

system-time

The current time on the device.

cpu-usage

Current CPU usage.

cpu-min

Minimum CPU usage.

cpu-max

Maximum CPU usage.

cpu-avg

Average CPU usage.

description

Description for this device.

location

Location details for this device.

contact

Contact information for this device.

temperature

The current temperature of the device.

core-temperature

The current temperature of the CPU core.

show tech-support

Displays information needed by Digi Technical Support when diagnosing device issues.

Parameters

output-file

The name of the file to which the command output is written. Optional.

show vrrp

Displays VRRP tunnel status and statistics.

Parameters

state

Whether the VRRP daemon is configured to be running.

interface

Displays current interface being used by the VRRP daemon.

current-state

The state of the VRRP daemon on this router.

current-master

Displays IP address and priority of the router that is currently the VRRP master.

current-priority

The current VRRP priority of this router.

last-transition

The most recent date that this router transitioned between VRRP states.

became-master

The total number of times that this router has transitioned into the VRRP master state.

released-master

The total number of times that this router has transitioned out of the VRRP master state.

adverts-sent

The total number of VRRP advertisements sent by this router.

adverts-received

The total number of VRRP advertisements received by this router.

priority-sent

The total number of VRRP packets with a priority of '0' sent by this router.

priority-received

The total number of VRRP packets with a priority of '0' received by this router.

show wan

Displays Wide Area Network (WAN) status and statistics.

Parameters

admin-status

Whether the WAN is sufficiently configured to be brought up.

oper-status

Whether the WAN is up or down.

interface

The physical interface assigned to the WAN.

ip-address

IP address for the WAN.

dns1

Preferred DNS server.

dns2

Alternate DNS server.

gateway

The gateway to use for the static route.

mask

Subnet mask for the WAN.

rx-bytes

Number of bytes received by the WAN.

rx-packets

Number of packets received by the WAN.

tx-bytes

Number of bytes transmitted by the WAN.

tx-packets

Number of packets transmitted by the WAN.

probe-host

The IPv4 address or fully qualified domain name (FQDN) of the device to send probes to.

probe-resp-seconds

Number of seconds since the device received the last probe response. A value of -1 indicates that probes are disabled. A value of -2 indicates the device has not received any probe responses yet.

ipv6-address

The IPv6 address or addresses assigned to the WAN.

ipv6-dns1

Preferred IPv6 DNS server.

ipv6-dns2

Alternate IPv6 DNS server.

show web-filter

Displays status for the web filtering service used for all WAN traffic.

Parameters

state

Whether web filtering is enabled.

device-id

Device ID from the Cisco Umbrella Network Device Registration API.

show wifi

Displays status and statistics for a Wi-Fi 2.4 GHz interface.

Parameters

interface

The name of the Wi-Fi 2.4 GHz interface.

description

A descriptive name for the Wi-Fi 2.4 GHz interface.

admin-status

Whether the Wi-Fi 2.4 GHz interface is sufficiently configured to be brought up.

oper-status

Whether the Wi-Fi 2.4 GHz interface is up or down.

channel

The radio channel on which the Wi-Fi 2.4 GHz interface is operating.

ssid

Service Set Identifier (SSID) for the Wi-Fi 2.4 GHz interface.

security

Security for the Wi-Fi 2.4 GHz interface.

rx-bytes

The number of bytes received by the Wi-Fi 2.4 GHz interface.

tx-bytes

The number of bytes transmitted by the Wi-Fi 2.4 GHz interface.

rx-packets

The number of packets transmitted by the Wi-Fi 2.4 GHz interface.

tx-packets

The number of packets transmitted by the Wi-Fi 2.4 GHz interface.

rx-multicasts

The number of receive multicasts by the Wi-Fi 2.4 GHz interface.

tx-collisions

The number of transmit collisions by the Wi-Fi 2.4 GHz interface.

rx-errors

The number of receive errors by the Wi-Fi 2.4 GHz interface.

tx-errors

The number of transmit errors by the Wi-Fi 2.4 GHz interface.

rx-dropped

The number of receive packets dropped by the Wi-Fi 2.4 GHz interface.

tx-dropped

The number of transmit packets dropped by the Wi-Fi 2.4 GHz interface.

rx-fifo-errors

The number of receive FIFO errors by the Wi-Fi 2.4 GHz interface.

tx-fifo-errors

The number of transmit FIFO errors by the Wi-Fi 2.4 GHz interface.

rx-crc-errors

The number of received packets by the Wi-Fi 2.4 GHz interface that do not contain the proper cyclic redundancy check (CRC), or checksum value.

tx-aborted-errors

The number of transmit aborted errors by the Wi-Fi 2.4 GHz interface.

rx-frame-errors

The number of receive frame errors by the Wi-Fi 2.4 GHz interface.

tx-carrier-errors

The number of transmit carrier errors by the Wi-Fi 2.4 GHz interface.

rx-length-errors

The number of receive length errors by the Wi-Fi 2.4 GHz interface.

tx-heartbeat-errors

The number of transmit heartbeat errors by the Wi-Fi 2.4 GHz interface.

rx-missed-errors

The number of receive missed errors by the Wi-Fi 2.4 GHz interface.

tx-window-errors

The number of transmit window errors by the Wi-Fi 2.4 GHz interface.

rx-over-errors

The number of receive over errors by the Wi-Fi 2.4 GHz interface.

show wifi5g

Displays status and statistics for a Wi-Fi 5 GHz interface.

Parameters

interface

The name of the Wi-Fi 5 GHz interface.

description

A descriptive name for the Wi-Fi 5 GHz interface.

admin-status

Whether the Wi-Fi 5 GHz interface is sufficiently configured to be brought up.

oper-status

Whether the Wi-Fi 5 GHz interface is up or down.

channel

The radio channel on which the Wi-Fi 5 GHz interface is operating.

ssid

Service Set Identifier (SSID) for the Wi-Fi 5 GHz interface.

security

Security for the Wi-Fi 5 GHz interface.

rx-bytes

The number of bytes received by the Wi-Fi 5 GHz interface.

tx-bytes

The number of bytes transmitted by the Wi-Fi 5 GHz interface.

rx-packets

The number of packets transmitted by the Wi-Fi 5 GHz interface.

tx-packets

The number of packets transmitted by the Wi-Fi 5 GHz interface.

rx-multicasts

The number of receive multicasts by the Wi-Fi 5 GHz interface.

tx-collisions

The number of transmit collisions by the Wi-Fi 5 GHz interface.

rx-errors

The number of receive errors by the Wi-Fi 5 GHz interface.

tx-errors

The number of transmit errors by the Wi-Fi 5 GHz interface.

rx-dropped

The number of receive packets dropped by the Wi-Fi 5 GHz interface.

tx-dropped

The number of transmit packets dropped by the Wi-Fi 5 GHz interface.

rx-fifo-errors

The number of receive FIFO errors by the Wi-Fi 5 GHz interface.

tx-fifo-errors

The number of transmit FIFO errors by the Wi-Fi 5 GHz interface.

rx-crc-errors

The number of received packets by the Wi-Fi 5 GHz interface that do not contain the proper cyclic redundancy check (CRC), or checksum value.

tx-aborted-errors

The number of transmit aborted errors by the Wi-Fi 5 GHz interface.

rx-frame-errors

The number of receive frame errors by the Wi-Fi 5 GHz interface.

tx-carrier-errors

The number of transmit carrier errors by the Wi-Fi 5 GHz interface.

rx-length-errors

The number of receive length errors by the Wi-Fi 5 GHz interface.

tx-heartbeat-errors

The number of transmit heartbeat errors by the Wi-Fi 5 GHz interface.

rx-missed-errors

The number of receive missed errors by the Wi-Fi 5 GHz interface.

tx-window-errors

The number of transmit window errors by the Wi-Fi 5 GHz interface.

rx-over-errors

The number of receive over errors by the Wi-Fi 5 GHz interface.

snmp

Configures Simple Network Management Protocol (SNMP) management for this device.

Syntax

```
snmp <parameter> <value>
```

Parameters

v1

Enables or disables SNMPv1 support.

Value is either on or off. The default value is off.

v2c

Enables or disables SNMPv2c support.

Value is either on or off. The default value is off.

v3

Enables or disables SNMPv3 support.

Value is either on or off. The default value is off.

port

The port on which the device listens for SNMP packets.

Accepted value is any integer from 0 to 65535. The default value is 161.

authentication-traps

Enables or disables SNMP authentication traps.

Value is either on or off. The default value is off.

Examples

- ```
  snmp v1 on
  ```

  Enable SNMPv1 support.

- ```
  snmp v2c on
  ```

  Enable SNMPv2c support.

- ```
  snmp port 161
  ```

  Set the SNMP listening port to 161.
  ```

snmp-community

Configures SNMPv1 and SNMPv2c communities.

Syntax

```
snmp-community <1 - 10> <parameter> <value>
```

Parameters

community

SNMPv1 or SNMPv2c community name.

Accepted value is any string up to 128 characters.

access

SNMPv1 or SNMPv2c community access level.

Accepted values can be one of read-only or read-write. The default value is read-only.

Examples

- ```
  snmp-community 1 community public
  ```

  Set the first SNMPv1 or SNMPv2c community name to 'public.'

- ```
  snmp-community 1 access read-write
  ```

  Set the first SNMPv1 or SNMPv2c community access level to 'read-write.'

snmp-user

Configures SNMPv3 users.

Syntax

```
snmp-user <1 - 10> <parameter> <value>
```

Parameters

user

SNMPv3 user name.

Accepted value is any string up to 32 characters.

authentication

SNMPv3 authentication type.

Accepted values can be one of none, md5 or sha1. The default value is none.

privacy

SNMPv3 privacy type. To use SNMPv3 privacy (that is, Data Encryption Standard (DES) or Advanced Encryption Standard (AES)) for the SNMP user, the SNMPv3 authentication type must be set to MD5 or SHA1.

Accepted values can be one of none, aes or des. The default value is none.

access

SNMPv3 user access level.

Accepted values can be one of read-only or read-write. The default value is read-only.

authentication-password

SNMPv3 authentication password. The password is stored in encrypted form.

Accepted value is any string up to 64 characters.

privacy-password

SNMPv3 privacy password. The password is stored in encrypted form.

Accepted value is any string up to 64 characters.

sntp

Configures system date and time using Simple Network Time Protocol (SNTP). SNTP continually polls an external NTP time server on either a private company network or the internet at a configured interval rate.

Syntax

```
sntp <parameter> <value>
```

Parameters

state

Enables or disables SNTP to set the system date and time.

Accepted values can be one of off or on. The default value is on.

server

The SNTP server to use for setting system date and time.

Value should be a fully qualified domain name. The default value is time.devicecloud.com.

update-interval

The interval, in minutes, at which the device checks the SNTP server for date and time.

Accepted value is any integer from 1 to 10080. The default value is 1440.

ssh

Configures Secure Shell (SSH) server settings.

Syntax

```
ssh <parameter> <value>
```

Parameters

server

Enables or disables the SSH server.

Value is either on or off. The default value is on.

port

The port number for the SSH Server.

Accepted value is any integer from 1 to 65535. The default value is 22.

ca-key

The base64 encoded public key for the certificate authority trusted to sign SSH certificates for user authentication.

This element is available to super users only.

Accepted value is any string up to 716 characters.

ca-key-type

The key type of the CA public key

This element is available to super users only.

Accepted values can be one of none, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, ssh-ed25519 or ssh-rsa. The default value is none.

syslog

Configures remote syslog servers

Syntax

```
syslog <1 - 2> <parameter> <value>
```

Parameters

server

Set the syslog server ip address. You can configure the syslog to log remotely to this ip address.

Value should be a fully qualified domain name.

server-port

This is the port that syslog server uses to report events.

Accepted value is any integer from 0 to 65535. The default value is 514.

mode

This allows you to send syslog messages with either TCP or UDP.

Accepted values can be one of udp or tcp. The default value is udp.

system

Configures system settings.

Syntax

```
system <parameter> <value>
```

Parameters

prompt

The prompt displayed in the command-line interface. You can configure the system prompt to use the device's serial number by including '%s' in prompt value. For example, a 'prompt' parameter value of 'LR54_%s' resolves to 'LR54_LR123456.'

Accepted value is any string up to 16 characters. The default value is digi.router>.

timeout

The time, in seconds, after which a web or command-line interface session times out if there is no activity.

Accepted value is any integer from 60 to 3600. The default value is 300.

loglevel

The minimum event level that is logged in the event log.

Accepted values can be one of emergency, alert, critical, error, warning, notice, info or debug. The default value is info.

name

The name of this device.

Accepted value is any string up to 255 characters.

location

The location of this device.

Accepted value is any string up to 255 characters.

contact

Contact information for this device.

Accepted value is any string up to 255 characters.

page

Sets the page size for command-line interface output.

Accepted value is any integer from 0 to 100. The default value is 40.

device-specific-passwords

Enables or disables device-specific passwords. Encrypted passwords can be device-specific or not. When encrypted passwords are device-specific, they are more secure, but cannot be copied onto another device.

Value is either on or off. The default value is off.

description

A description of this device.

Accepted value is any string up to 255 characters.

passthrough

The TCP port used for passthrough. The value 0 disables passthrough mode. A reboot is required for changes to this setting to take effect.

Accepted value is any integer from 0 to 65535. The default value is 0.

wizard

Enables or disables the Getting Started Wizard. To skip the wizard, disable this option.

Value is either on or off. The default value is on.

ipsec-debug

Enables or disables display of IPsec debugging messages. These messages help diagnose issues with IPsec configuration and interoperability.

Accepted values can be one of off or on. The default value is off.

log-to-file

Enables or disables logging TLR events to a file. If disabled, the log is created in RAM, and is lost when the device is rebooted. If enabled, the log is created to flash and is saved on reboot. Saving event logs to files and keeping them resident for some time is not recommended for normal operations, as this practice can lead to additional wear to the device's flash memory.

Value is either on or off. The default value is off.

log-system-to-file

If enabled, log system/kernel events to system.log (on flash, will be saved on reboot). This is not recommended for normal operations, as this practice can lead to additional wear to the device's flash memory.

Value is either on or off. The default value is off.

timezone

Sets the system timezone. When the date and time is set using SNTP, the system time is set to Universal Coordinated Time (UTC) and not to your local time. In addition, the date and time, whether it is set manually or using SNTP, does not automatically change to reflect Daylight Saving Time (DST). By setting the time zone, the device displays the local time for that time zone and automatically adjusts for daylight saving time.

Accepted values can be one of none, canada-atlantic, canada-central, canada-eastern, canada-mountain, canada-newfoundland, canada-pacific, europe-central, europe-eastern, europe-western, uk-ireland, us-alaska, us-arizona, us-central, us-eastern, us-hawaii, us-indiana, us-mountain or us-pacific. The default value is none.

log-to-syslog

Enables logging TLR events to a syslog server

Accepted values can be multiple values of syslog1, syslog2 and off. The default value is off.

log-system-to-syslog

Enables logging system events to a syslog server

Accepted values can be multiple values of syslog1, syslog2 and off. The default value is off.

traceroute

Traces the network route to a remote IP host.

Syntax

```
traceroute [src-ip <ip-address>] [interface <interface>] [hops <n>] [timeout
<secs>] [size <bytes>] host
```

Parameters

src-ip

Use this source IP address for outgoing packets.

interface

The interface from which traceroute messages are sent.

hops

The maximum number of hops to allow.

timeout

The maximum number of seconds to wait for a response from a hop.

size

The size, in bytes, of the message to send.

host

The IP address of the destination host.

Examples

- ```
  traceroute 8.8.8.8
  ```

  Finds the network route to IP address 8.8.8.8
  ```

unlock

Unlock a SIM card and set a new SIM card PIN code.

This command is available to super users only.

Syntax

```
unlock <sim1 | sim2> <puk code> <new sim pin>
```

Parameters

sim

The SIM slot number in which the SIM card is inserted. Enter sim1 if the SIM card is inserted in slot SIM1, or sim2 if the SIM card is inserted in slot SIM2.

puk_code

The PUK code for the SIM card. This code can be between 8 and 10 digits long.

new_sim_pin

The new SIM card PIN. This PIN can be between 4 and 8 digits long.

Examples

- ```
  unlock sim1 12345678 1234
  ```

  Unlock the SIM card in SIM1 with PUK code 12345678 and set the new SIM PIN to 1234.

- ```
  unlock sim2 12345678 1234
  ```

  Unlock the SIM card in SIM2 with PUK code 12345678 and set the new SIM PIN to 1234.

update

Performs system updates, such as firmware updates, setting the cellular carrier, and setting the configuration file used at bootup and when saving configuration. Firmware update options include specifying the device system firmware or the cellular module firmware to load onto the device.

This command is available to super users only.

Syntax

```
update firmware <firmware-file>
update modem <firmware-images-path | carrier-name>
update config <configuration-file>
update carrier <carrier-name>
```

Parameters

firmware

Updates the device system firmware.

modem

Updates the cellular module firmware.

config

Sets the configuration filename.

carrier

Update the cellular module for a carrier. Current allowed carrier values are att, verizon, and generic.

Examples

- ```
  update config config.da1
  ```

  Set the configuration file to 'config.da1.'

- ```
  update firmware filename
  ```

  Initiate the device system firmware update process.

- ```
  update modem
  ```

  Initiate the cellular module firmware update process. This process retrieves image files from Digi International site and downloads the images to the module.
  ```

- ```
  update modem ./modem_fw
  ```

  Initiate the cellular module firmware update process. This process uploads firmware files from the directory ./modem_fw to the cellular module.

- ```
  update modem verizon
  ```

  Initiate the cellular module firmware update process. This process retrieves firmware files from the Digi repository of cellular module firmware files and uploads the images to the module.

- ```
  update carrier att
  ```

  Initiates the cellular module to use ATT.
  ```

user

Configures users and user access privileges.

Syntax

```
user <1 - 10> <parameter> <value>
```

Parameters

name

User names are case-insensitive strings, which must start with a letter or underscore (_), but otherwise can contain letters, digits, underscores (_), or hyphens (-). In addition, they can end with a dollar sign ($). No other characters are allowed.

Accepted value is any string up to 32 characters.

password

The password for the user.

Accepted value is any string up to 128 characters.

access

The user access level for the user. User access levels determine the level of control users have over device features and their settings. The 'super' access permission allows the most control over features and settings, and 'read-only' the lowest control over features and settings.

Accepted values can be one of read-only, read-write or super. The default value is super.

ssh-key

The base64 encoded SSH public key to use for authentication of this user

Accepted value is any string up to 716 characters.

ssh-key-type

The key type of the SSH public key

Accepted values can be one of none, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, ssh-ed25519 or ssh-rsa. The default value is none.

Examples

- ```
  user 1 username _Username1234$
  ```

  Valid user 1 username starting with _ and ending with $.

- ```
  user 3 username userName-1234
  ```

  Valid user 3 username containing a dash.

vrrp

Configures Virtual Router Redundancy Protocol (VRRP). This allows multiple routers to work together to provide a LAN with high-reliability routing to the Internet or another network.

Syntax

```
vrrp <parameter> <value>
```

Parameters

state

Enable or disable Virtual Router Redundancy Protocol (VRRP).

Value is either on or off. The default value is off.

initial-state

The initial VRRP state of this router when it is enabled.

Accepted values can be one of backup or master. The default value is backup.

interface

The LAN interface on which to run VRRP.

Accepted values can be one of lan1, lan2, lan3, lan4, lan5, lan6, lan7, lan8, lan9 or lan10. The default value is lan1.

ip-address

The virtual IP address assigned to the VRRP virtual router. Each client on the LAN should use this address as the default gateway. Typically, the DHCP server distributes this address to the each client.

Value should be an IPv4 address.

router-id

The ID of the VRRP virtual router.

Accepted value is any integer from 1 to 255. The default value is 1.

priority

The VRRP priority of this router.

Accepted value is any integer from 1 to 255. The default value is 100.

interval

The time in seconds betweeen VRRP advertisement packets. All of the routers in the VRRP group should use the same interval.

Accepted value is any integer from 1 to 60. The default value is 1.

wan

Configures a Wide Area Network (WAN). The physical communications interface for the WAN can be an Ethernet or cellular interface that connects to a remote network, such as the internet.

Syntax

```
wan <1 - 10> <parameter> <value>
```

Parameters

interface

The physical interface to use for the WAN.

Accepted values can be one of none, eth1, eth2, eth3, eth4, cellular1 or cellular2. The default value is none.

nat

Enables Network Address Translation (NAT) for outgoing packets on the WAN. NAT is a mechanism that allows sending packets from a private network (for example, 10.x.x.x or 192.168.x.x) over a public network. The device changes the source IP address of the packet to be the address for the WAN interface, which is a public IP address. This allows the device on the public network to know how to send responses.

Value is either on or off. The default value is on.

timeout

The time, in seconds, to wait for the physical interface to connect and to receive a probe response before failing over to a lower priority interface.

Accepted value is any integer from 10 to 3600. The default value is 180.

probe-host

The IPv4 or fully qualified domain name (FQDN) of the address of the device itself. The WAN failover feature sends probe packets over the WAN to the IP address of this device.

Value should be a fully qualified domain name.

probe-timeout

Timeout, in seconds, to wait for a response to a probe. The value for this parameter must be smaller than the probe-interval and timeout parameter values or the configuration is considered invalid, and an error message is written to the system log.

Accepted value is any integer from 1 to 60. The default value is 5.

probe-interval

Interval, in seconds, between sending probe packets. The value for probe-interval must be larger than the probe-timeout value. If not, the WAN failover configuration is considered invalid, and an error message is written to the system log.

Accepted value is any integer from 2 to 3600. The default value is 60.

probe-size

Size of probe packets sent to detect WAN failures.

Accepted value is any integer from 64 to 1500. The default value is 64.

activate-after

The time, in seconds, that the primary interface needs to be up before switching back to it as the active interface. If probing is active, no probes are permitted to be lost during this period. Otherwise, the timer is restarted.

Accepted value is any integer from 0 to 3600. The default value is 0.

retry-after

The time, in seconds, to wait before retrying this interface after failing over to a lower priority one. Use a large retry timeout when both interfaces are cellular interfaces.

Accepted value is any integer from 10 to 3600. The default value is 180.

dhcp

Enables or disables the DHCP client. The DHCP client is used to automatically get an IP address for the interface from a DHCP server.

Value is either on or off. The default value is on.

ip-address

The IPv4 address to be statically assigned to this WAN if DHCP is disabled.

Value should be an IPv4 address.

mask

The IPv4 mask to be statically assigned to this WAN if DHCP is disabled.

Value should be an IPv4 address. The default value is 255.255.255.0.

gateway

The gateway to use for the default route.

Value should be an IPv4 address.

dns1

The IPv4 address of the preferred DNS server. This value overrides the value assigned by DHCP.

Value should be an IPv4 address.

dns2

The IPv4 address of the alternate DNS server used if the device cannot communicate with the preferred server.

Value should be an IPv4 address.

allow-ssh-access

Allow SSH access on this WAN interface. Custom firewall rules may affect the behavior of this parameter.

Value is either on or off. The default value is off.

allow-https-access

Allow HTTPS access on this WAN interface. Custom firewall rules may affect the behavior of this parameter.

Value is either on or off. The default value is off.

state

Enables or disables a WAN interface

Value is either on or off. The default value is on.

ipv6-state

Enables or disables IPv6 support on this WAN interface

Value is either on or off. The default value is off.

ipv6-prefix-length

Set the length, in bits, of the IPv6 address prefix to request from the upstream router for this WAN. The size of the prefix determines how many LANs can support IPv6. Request a prefix length of 60 bits or less to support up to 16 LANs.

Accepted value is any integer from 48 to 64. The default value is 60.

qos

Enables or disables Quality of Service (QoS) on this WAN interface

Value is either on or off. The default value is off.

bandwidth-upstream

Sets the upstream bandwidth of the WAN interface in kbps.

Accepted value is any integer from 1 to 1000000. The default value is 1000000.

web-filter

Configures the web filtering service to be used for all WAN traffic. Use of a web filtering service like Cisco Umbrella may provide content filtering, security, privacy, and monitoring features. If web filtering is enabled, all DNS requests passing through the router are redirected to the selected web filtering service, ensuring that computers on the LAN cannot bypass the web filter.

Syntax

```
web-filter <parameter> <value>
```

Parameters

state

Enables or disables the use of a web filtering service for all WAN traffic.

Value is either on or off. The default value is off.

service

Selects the web filtering service that the router uses for all WAN traffic.

Accepted values can be one of umbrella. The default value is umbrella.

token

The customer-specific API token for the Cisco Umbrella service. This token can be found on the Cisco Umbrella dashboard under the Network Devices area. The router uses this token to automatically obtain a device ID using the Network Device Registration API.

Accepted value is any string up to 255 characters.

wifi

Configures a Wi-Fi 2.4 GHz interface.

Syntax

```
wifi <1 - 4> <parameter> <value>
```

Parameters

state

Enables or disables the Wi-Fi 2.4 GHz interface.

Accepted values can be one of off or on. The default value is off.

description

A descriptive name for the Wi-Fi 2.4 GHz interface.

Accepted value is any string up to 255 characters.

ssid

Service Set Identifier (SSID) for the Wi-Fi 2.4 GHz interface. You can configure the SSID to use the device's serial number by including '%s' in the SSID. For example, an 'ssid' parameter value of 'LR54_%s' resolves to 'LR54_LR123456.'

Accepted value is any string up to 32 characters.

security

Security for the Wi-Fi 2.4 GHz interface.

Accepted values can be one of none, wpa2-personal, wpa-wpa2-personal, wpa2-enterprise or wpa-wpa2-enterprise. The default value is wpa2-personal.

password

Password for the Wi-Fi 2.4 GHz interface. The password must be 8-63 ASCII or 64 hexadecimal characters

Accepted value is any string up to 132 characters.

broadcast-ssid

Enables or disables broadcasting the SSID in beacon packets. Disabling the SSID prevents clients from easily detecting the presence of this access point.

Accepted values can be one of off or on. The default value is on.

isolate-clients

Enables or disables Wi-Fi client isolation, which prevents clients connected to the Wi-Fi access point from communicating with each other.

Accepted values can be one of off or on. The default value is on.

isolate-ap

Enables or disables clients on a Wi-Fi access point from communicating with clients on other Access Points.

Accepted values can be one of off or on. The default value is on.

radius-server

The IP address for the RADIUS server for WPA/WPA2-Enterprise.

Value should be an IPv4 address.

radius-server-port

The port for the RADIUS server.

Accepted value is any integer from 1 to 65535. The default value is 1812.

radius-password

The password for the RADIUS server.

Accepted value is any string up to 64 characters.

pmf

Enables or disables Protected Management Frames for the Wi-Fi 2.4 GHz interface. Enabling this feature is currently not recommended, as it will prevent most clients from being able to connect to the Wi-Fi access point.

Accepted values can be one of off or on. The default value is off.

wifi5g

Configures a Wi-Fi 5 GHz interface.

Syntax

```
wifi5g <1 - 4> <parameter> <value>
```

Parameters

state

Enables or disables the Wi-Fi 5 GHz interface.

Accepted values can be one of off or on. The default value is off.

description

A descriptive name for the Wi-Fi 5 GHz interface.

Accepted value is any string up to 255 characters.

ssid

Service Set Identifier (SSID) for the Wi-Fi 5 GHz interface. You can configure the SSID to use the device's serial number by including '%s' in the SSID. For example, an 'ssid' parameter value of 'LR54_%s' resolves to 'LR54_LR123456.'

Accepted value is any string up to 32 characters.

security

Security for the Wi-Fi 5 GHz interface.

Accepted values can be one of none, wpa2-personal, wpa-wpa2-personal, wpa2-enterprise or wpa-wpa2-enterprise. The default value is wpa2-personal.

password

Password for the Wi-Fi 5 GHz interface. The password must be 8-63 ASCII or 64 hexadecimal characters

Accepted value is any string up to 132 characters.

broadcast-ssid

Enables or disables broadcasting the SSID in beacon packets. Disabling the SSID prevents clients from easily detecting the presence of this access point.

Accepted values can be one of off or on. The default value is on.

isolate-clients

Enables or disables Wi-Fi client isolation, which prevents clients connected to the Wi-Fi access point from communicating with each other.

Accepted values can be one of off or on. The default value is on.

isolate-ap

Enables or disables clients on a Wi-Fi access point from communicating with clients on other Access Points.

Accepted values can be one of off or on. The default value is on.

radius-server

The RADIUS server for WPA/WPA2-Enterprise.

Value should be an IPv4 address.

radius-server-port

The port for the RADIUS server.

Accepted value is any integer from 1 to 65535. The default value is 1812.

radius-password

The password for the RADIUS server.

Accepted value is any string up to 64 characters.

pmf

Enables or disables Protected Management Frames for the Wi-Fi 5 GHz interface. Enabling this feature is currently not recommended, as it will prevent most clients from being able to connect to the Wi-Fi access point.

Accepted values can be one of off or on. The default value is off.

wifi-global

Configures global settings for Wi-Fi interfaces.

Syntax

```
wifi-global <parameter> <value>
```

Parameters

wifi-channel

The channel to use for Wi-Fi 2.4 GHz interfaces.

Accepted values can be one of auto, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 or 11. The default value is auto.

wifi5g-channel

The channel to use for Wi-Fi 5 GHz interfaces.

Accepted values can be one of auto, 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136 or 140. The default value is 36.

wifi-txpower

The TX power to use for Wi-Fi 2.4 GHz interfaces by percentage.

Accepted value is any integer from 1 to 100. The default value is 100.

wifi5g-txpower

The TX power to use for Wi-Fi 5 GHz interfaces by percentage. Need reboot after change.

Accepted value is any integer from 1 to 100. The default value is 100.

Advanced topics

Using firewall and firewall6 commands

The TransPort firewall is a full stateful firewall that controls which packets are allowed into and out of the device. Firewalls can filter packets based on the IP address, protocol, TCP ports, and UDP ports.

You can either:

- Allow TransPort to automatically manage firewall rules using built-in features, such as port forwarding and IP filters.

  or

- Directly manage firewalls using the firewall and firewall6 commands.

This section describes how to manage firewalls using the firewall and firewall6 commands. Use the firewall command to manage IPv4 traffic, and use the firewall6 command to manage IPv6 traffic. Both firewall commands function in the same manner except the firewall6 command does not manage a **nat** table.

For details on how to manage firewalls using built-in TransPort features, see Understanding system firewall rules.

TransPort firewalls based on iptables firewall

The TransPort firewall and firewall6 commands are based on the open-source firewall named **iptables**. Both commands use the same syntax as **iptables**, except the rules start with the keyword **firewall** or **firewall6** instead of **iptables**. The firewall syntax is case-sensitive.

For more information on configuring the firewall, see www.netfilter.org/documentation and IptablesHowTo.

Note TransPort automatically manages some **iptables** rules, referred to as **system firewall rules**. Some system firewall rules are added when the device starts; other system firewall rules are added and removed when built-in features are configured. For example, when you use port forwarding, the TransPort adds system firewall rules based on your port forwarding rules. Take care when directly modifying firewall rules using firewall and firewall6 commands. The system may reapply unmodified rules when you use certain commands, the system restarts, or other configuration changes are made. See Understanding system firewall rules for details.

Tables and chains in firewall rules

Depending on their function, firewall rules are organized into tables and chains. The tables define the function of the rule. The chains define when the rule is applied in relation to when a packet is being received, sent or forwarded.

Tables

Firewall tables are as follows:

filter
The filter table filters packets being sent, received, and forwarded by the device. This is the default table if one is not specified in the firewall rule. The filter table supports these chains: **INPUT**, **OUTPUT**, **FORWARD**.

nat
The nat table modifies the source and destination IP addresses and TCP and UDP ports so that traffic can be sent between private IP networks such as a company network and public IP

networks such as the Internet. The nat table supports these chains: **OUTPUT**, **PREROUTING**, **POSTROUTING**.

mangle
The mangle table modifies a packet being sent, received, or forwarded by the device. The mangle table supports these chains: **INPUT**, **OUTPUT**, **FORWARD**, **PREROUTING**, **POSTROUTING**.

raw
The raw table marks packets for special treatment. When a packet is received, the raw table is processed first. The raw table supports these chains: **INPUT**, **OUTPUT**, **FORWARD**, **PREROUTING**, **POSTROUTING**.

Chains

By default, there are multiple chains for directing packets:

INPUT
For packets destined for the device.

OUTPUT
For packets generated by the device.

FORWARD
For packets forwarded by the device.

PREROUTING
For packets before the device has decided to forward the packet, or if the packet has been defined for the device.

POSTROUTING
For packets that have been forwarded by the device, or if the packet has been generated by the device.

tlr_port_forward
Used by the nat table. Contains rules associated with port forwarding. Reserved for use by the TransPort system only. Do not modify these rules.

tlr_wan_input
Used by the filter table. Contains rules associated with WAN configuration. Reserved for use by the TransPort system only. Do not modify these rules.

tlr_ip_filter_input
Used by the filter table. Contains rules associated with ip-filter for data destined to the device. Reserved for use by the TransPort system only. Do not modify these rules.

tlr_ip_filter_output
Used by the filter table. Contains rules associated with ip-filter for data originating from the device. Reserved for use by the TransPort system only. Do not modify these rules.

tlr_ip_filter_forward
Used by the filter table. Contains rules associated with ip-filter for data routing through the device. Reserved for use by the TransPort system only. Do not modify these rules.

tlr_ip_priority_output
Used by the filter table. Contains rules associated with services on the device that require outgoing access for correct operation. Reserved for use by the TransPort system only. Do not modify these rules.

Policy rules

A policy rule defines the default action for a chain; for example **ACCEPT** or **DROP**.

For example, the policy could be to drop all inbound packets that do not explicitly match any of the chain rules.

Using a policy rule is better than simply defining a normal rule that matches all packets. Policy rules are the last rule tested for a chain, while a normal rule could appear anywhere in the list of rules, depending how rules were added.

Default firewall configuration

To provide a secure device out-of-the-box, the LR54 firewall is configured for the following default behavior:

- Block all traffic received on the physical interfaces for WANs (**eth1**, **cellular1**, **cellular2**) except for traffic for established connections or related data.
- Allow all traffic from the physical interfaces for LANs to be forwarded by the device.
- Only allow ICMP, SSH, HTTP, HTTPS, DNS and DHCP traffic to be received on the physical interfaces for LANs.
- All other traffic is blocked.

The default settings allows devices connected on the physical interfaces for LANs to make connections over the physical interfaces for WANs, but remote devices cannot make a connection to the device or devices connected on the physical interfaces for LANs.

This means that by default it is not possible to make an HTTPS or SSH connection via a WAN. To allow HTTPS or SSH connections over a WAN, see Allow HTTPS access on a WAN and Allow SSH access on a WAN to change the default firewall behavior.

Example firewall rules

```
Filter Table
 ------------
 Chain INPUT (policy DROP xx packets, xxx bytes)
 num   pkts bytes target     prot opt in     out     source               destination
[....snip....]
 5        0     0 ACCEPT     icmp --  lan+   any     anywhere             anywhere             /* (autogenerated)
lan */
 6        0     0 ACCEPT     tcp  --  lan+   any     anywhere             anywhere             tcp dpt:22 /*
(autogenerated) lan */
 7        0     0 ACCEPT     tcp  --  lan+   any     anywhere             anywhere             tcp dpt:http /*
(autogenerated) lan */
 8        0     0 ACCEPT     tcp  --  lan+   any     anywhere             anywhere             tcp dpt:443 /*
(autogenerated) lan */
 9        0     0 ACCEPT     udp  --  lan+   any     anywhere             anywhere             udp dpt:67 /*
(autogenerated) lan */
 10       0     0 ACCEPT     udp  --  lan+   any     anywhere             anywhere             udp dpt:53 /*
(autogenerated) lan */
[....snip....]
```

Allow SSH access on a WAN

To allow SSH access on a WAN interface:

1. Open the command-line interface, either from a command prompt or the web interface **System > Device Console** option.
2. Use the wan command **allow-ssh-access** option to toggle SSH access on a WAN. For example, to allow SSH access on WAN 1:

```
digi.router> wan 1 allow-ssh-access on
```

3. Save the configuration.

```
digi.router> save config
```

Allow SSH access for only a specific source IP address

To allow SSH access for only a specific IP address:

1. Open the command-line interface, either from a command prompt or the web interface **System > Device Console** option**.**
2. Use the ip-filter command to allow incoming connections from hosts on the 10.20 network to SSH (port 22). For example, assuming port **22** is the SSH port, enter commands similar to the following:

```
digi.router> ip-filter 1 description Allow WAN SSH only from 10.20 network
digi.router> ip-filter 1 action accept
digi.router> ip-filter 1 src any-wan
digi.router> ip-filter 1 src-ip-address 10.20.0.0/16
digi.router> ip-filter 1 dst-ip-port 22
digi.router> ip-filter 1 state on
```

3. Use the wan command **allow-ssh-access** option to prohibit SSH access on a WAN. For example, to turn off SSH access on WAN 1:

WARNING! Before turning off ssh access for a WAN, make sure your device can accept traffic other than ssh traffic. Otherwise, when you turn off ssh access, you may remove your ability to access the device.

```
digi.router> wan 1 allow-ssh-access off
```

4. Save the configuration.

```
digi.router> save config
```

Allow HTTPS access on a WAN

To allow HTTPS access on a WAN interface:

1. Open the command-line interface, either from a command prompt or the web interface **System > Device Console** option.
2. Use the wan command **allow-https-access** option to toggle HTTPS access on a WAN. For example, to allow HTTPS access on **WAN 1**:

```
digi.router> wan 1 allow-https-access on
```

3. Save the configuration.

```
digi.router> save config
```

Allow HTTPS access on a WAN from only a specific source IP address

To allow HTTPS access on a WAN interface:

1. Open the command-line interface, either from a command prompt or the web interface **System > Device Console** option.
2. Use the ip-filter command to allow incoming connections from hosts on the 10.20 network to HTTPS (port 443). For example, assuming port **443** is the HTTPS port, enter commands similar to the following:

```
digi.router> ip-filter 1 description Allow WAN HTTPS only from 10.20
network
digi.router> ip-filter 1 action accept
digi.router> ip-filter 1 src any-wan
digi.router> ip-filter 1 src-ip-address 10.20.0.0/16
digi.router> ip-filter 1 dst-ip-port 443
digi.router> ip-filter 1 state on
```

3. Use the wan command **allow-https-access** option to prohibit HTTPS access on a WAN. For example:

```
digi.router> wan 1 allow-https-access off
```

4. Save the configuration.

```
digi.router> save config
```

Add a firewall rule

Note Take care when inserting or updating rules. The number of rules and the position of system rules may change when you configure some TransPort components. See Understanding system firewall rules for details.

Add a rule to the bottom of the firewall

To add a rule to the bottom of the firewall, use the firewall or firewall6 command **–A** option, using the following syntax. The command syntax is case-sensitive.

```
firewall [-t table] -A <chain> <rule>
```

If you do not specify a table (**-t**), the default table is the **filter** table.

For example, to append a rule to the bottom of the **filter** table, the firewall command is:

```
digi.router> firewall -A INPUT -i lan1 -p icmp --icmp-type echo-request -j DROP
digi.router>
```

The show firewall output for the **filter** table created by the above command is:

```
digi.router> show firewall filter

Filter Table
------------
Chain INPUT (policy DROP 4 packets, 256 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        3   152 DROP       tcp  --  any    any     anywhere             anywhere             tcp dpt:22
2        0     0 DROP       icmp --  lan1   any     anywhere             anywhere             icmp echo-request

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 4 packets, 256 bytes)
num   pkts bytes target     prot opt in     out     source               destination

digi.router>
```

Insert a rule at any position of the firewall

To insert rules into the firewall at any position, the firewall or firewall6 command **–I** option, using the following syntax:

```
firewall [-t table] -I <chain> <position> <rule>
```

For example, to insert a rule before the second rule, specify a position of **2**.

```
digi.router>

digi.router> show firewall filter

Filter Table
------------
Chain INPUT (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        3   152 DROP       tcp  --  any    any     anywhere             anywhere             tcp dpt:22
2       74  4440 DROP       icmp --  lan1   any     anywhere             anywhere             icmp echo-request

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination

digi.router>
digi.router> firewall -I INPUT 2 -i cellular1 -p udp --dport 7 -j ACCEPT
digi.router>
digi.router> show firewall filter

Filter Table
------------
Chain INPUT (policy DROP 4 packets, 256 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        3   152 DROP       tcp  --  any    any     anywhere             anywhere             tcp dpt:22
2        0     0 ACCEPT     udp  --  cellular1 any  anywhere             anywhere             udp dpt:7
3       74  4440 DROP       icmp --  lan1   any     anywhere             anywhere             icmp echo-request

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 4 packets, 256 bytes)
num   pkts bytes target     prot opt in     out     source               destination

digi.router>
```

For more information on configuring the firewall, see www.netfilter.org/documentation and IptablesHowTo.

Update a firewall rule

Note Take care when inserting or updating rules. The number of rules and the position of system rules may change when you configure some TransPort components. See Understanding system firewall rules for details.

To update a firewall rule, use the firewall or firewall6 command **–R** option, using the following syntax:

```
firewall [-t table] -R <chain> <position> <rule>
```

For example, to update the second rule, specify a position of **2**.

```
digi.router> firewall -R INPUT 2 -i cellular1 -p udp --dport 123 -j ACCEPT
```

The show firewall output for the filter table created by the above command looks like this:

```
digi.router> show firewall filter

Filter Table
------------
Chain INPUT (policy DROP 2 packets, 130 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        3   152 DROP       tcp  --  any    any     anywhere             anywhere             tcp dpt:22
2        0     0 ACCEPT     udp  --  cellular1 any     anywhere          anywhere             udp dpt:123
3       74  4440 DROP       icmp --  lan1   any     anywhere             anywhere             icmp echo-request

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 2 packets, 130 bytes)
num   pkts bytes target     prot opt in     out     source               destination

digi.router>
```

Delete a firewall rule

Note Take care when inserting or updating rules. The number of rules and the position of system rules may change when you configure some TransPort components. See Understanding system firewall rules for details.

To delete a firewall rule, use the firewall or firewall6 command **–D** option. You can delete a single firewall rule or all firewall rules.

Delete a single firewall rule

For example, suppose the following firewall rule exists to block incoming SSH traffic over the **cellular1** interface. The firewall rule is displayed here through the output from a show config command:

```
[FIREWALL]
*filter
-A INPUT -i cellular1 -p tcp -m tcp --dport 22 -j DROP
COMMIT
[FIREWALL_END]
```

The command to delete this firewall rule is:

```
firewall -D INPUT -i cellular1 -p tcp -m tcp --dport 22 -j DROP
```

Delete all firewall rules

To remove all firewall rules, use the firewall or firewall6 command **-F** option. If you do not specify a table, all the rules in the filter table are deleted.

```
firewall -F [-t <table>]
```

WARNING! Using **firewall -F -t nat** to clear entries in the NAT table removes entries that perform NAT operations on WAN interfaces. Clearing such entries could leave the device unreachable if you are remotely accessing it over a WAN interface.

Show firewall rules and counters

To display all firewall rules and counters, use the show firewall or show firewall6 command.

For example:

Display all firewall rules

```
digi.router> show firewall

 Filter Table
 ------------
 Chain INPUT (policy DROP 0 packets, 0 bytes)
 num    pkts bytes target     prot opt in      out     source          destination
 1         3   272 ACCEPT     all  --  eth+    any     anywhere        anywhere            state RELATED,ESTABLISHED
/* (autogenerated) wan */
 2         0     0 ACCEPT     all  --  cellular1 any      anywhere     anywhere            state RELATED,ESTABLISHED
/* (autogenerated) wan */
 3         0     0 ACCEPT     all  --  cellular2 any      anywhere     anywhere            state RELATED,ESTABLISHED
/* (autogenerated) wan */
 4        33  2412 tlr_wan_input  all  --  any     any      anywhere     anywhere            /* (autogenerated) wan */
 5         0     0 ACCEPT     icmp --  lan+    any     anywhere        anywhere            /* (autogenerated) lan */
 6         0     0 ACCEPT     tcp  --  lan+    any     anywhere        anywhere            tcp dpt:22 /*
(autogenerated) lan */
 7         0     0 ACCEPT     tcp  --  lan+    any     anywhere        anywhere            tcp dpt:http /*
(autogenerated) lan */
 8         0     0 ACCEPT     tcp  --  lan+    any     anywhere        anywhere            tcp dpt:443 /*
(autogenerated) lan */
 9         0     0 ACCEPT     udp  --  lan+    any     anywhere        anywhere            udp dpt:67 /*
(autogenerated) lan */
 10        0     0 ACCEPT     udp  --  lan+    any     anywhere        anywhere            udp dpt:53 /*
(autogenerated) lan */
 11       33  2412 ACCEPT     all  --  lo      any     anywhere        anywhere            /* (autogenerated) core */

 Chain FORWARD (policy DROP 0 packets, 0 bytes)
 num    pkts bytes target     prot opt in      out     source          destination
 1         0     0 REJECT     tcp  --  lan+    any     anywhere        anywhere   state INVALID /*
(autogenerated)core */ reject-with tcp-reset
 2         0     0 DROP       all  --  lan+    any     anywhere        anywhere            state INVALID /*
(autogenerated) core */
 3         0     0 TCPMSS     tcp  --  any     any     anywhere        anywhere            tcp flags:SYN,RST/SYN /*
(autogenerated) core */ TCPMSS clamp to PMTU
 4         0     0 ACCEPT     all  --  eth+    any     anywhere        anywhere            state RELATED,ESTABLISHED
/* (autogenerated) wan */
 5         0     0 ACCEPT     all  --  cellular1 any   anywhere        anywhere            state RELATED,ESTABLISHED
/* (autogenerated) wan */
 6         0     0 ACCEPT     all  --  cellular2 any   anywhere        anywhere            state RELATED,ESTABLISHED
/* (autogenerated) wan */
 7         0     0 ACCEPT     all  --  any     any     anywhere        anywhere            ctstate DNAT /*
(autogenerated) port-forward */
 8         0     0 ACCEPT     all  --  lan+    any     anywhere        anywhere            /* (autogenerated) lan */

 Chain OUTPUT (policy ACCEPT 8 packets, 576 bytes)
 num    pkts bytes target     prot opt in      out     source          destination

 Chain tlr_wan_input (1 references)
 num    pkts bytes target     prot opt in      out     source          destination


 Raw Table
 ---------
```

```
Chain PREROUTING (policy ACCEPT 116 packets, 17802 bytes)
num   pkts bytes target     prot opt in     out     source          destination

Chain INPUT (policy ACCEPT 36 packets, 2684 bytes)
num   pkts bytes target     prot opt in     out     source          destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source          destination

Chain OUTPUT (policy ACCEPT 36 packets, 2620 bytes)
num   pkts bytes target     prot opt in     out     source          destination

Chain POSTROUTING (policy ACCEPT 36 packets, 2620 bytes)
num   pkts bytes target     prot opt in     out     source          destination


NAT Table
---------
Chain PREROUTING (policy ACCEPT 2 packets, 120 bytes)
num   pkts bytes target     prot opt in     out     source          destination
1       38 10641 tlr_port_forward  all  --  any     any     anywhere anywhere          /* (autogenerated) port-
forward */

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source          destination

Chain OUTPUT (policy ACCEPT 1 packets, 72 bytes)
num   pkts bytes target     prot opt in     out     source          destination

Chain POSTROUTING (policy ACCEPT 1 packets, 72 bytes)
num   pkts bytes target     prot opt in     out         source      destination
1        3   208 MASQUERADE  all  --  any    eth1       anywhere    anywhere
2        0     0 MASQUERADE  all  --  any    cellular1  anywhere    anywhere
3        0     0 MASQUERADE  all  --  any    cellular2  anywhere    anywhere

Chain tlr_port_forward (1 references)
num   pkts bytes target     prot opt in     out     source          destination
```

Display a specific firewall table

To display individual firewall tables, specify the table name on the show firewall or show firewall6 command. In the command output, the policy for each chain is also displayed in brackets after the chain name. For example:

```
digi.router> show firewall filter

Filter Table
------------
Chain INPUT (policy ACCEPT 1732 packets, 117K bytes)
num   pkts bytes target     prot opt in     out     source          destination
1       16   960 DROP       tcp  --  cellular1 any  anywhere        anywhere             tcp dpt:22

Chain FORWARD (policy ACCEPT 788 packets, 82764 bytes)
num   pkts bytes target     prot opt in     out     source          destination

Chain OUTPUT (policy ACCEPT 1646 packets, 110K bytes)
num   pkts bytes target     prot opt in     out     source          destination

digi.router>
```

Display and clear firewall rule counters

The firewall keeps a counter for each rule that counts the number of packets and bytes that have been matched against the rule. This is a useful tool to determine if a rule is correctly detecting packets.

To clear the counters, use the **clear firewall** and **clear firewall6** commands.

```
digi.router> show firewall filter

Filter Table
------------
Chain INPUT (policy ACCEPT 1732 packets, 117K bytes)
num   pkts bytes target     prot opt in     out     source          destination
1        3   152 DROP       tcp  --  cellular1 any  anywhere        anywhere             tcp dpt:22
2       23  1380 DROP       icmp --  lan1   any     anywhere        anywhere             icmp echo-request
```

```
Chain FORWARD (policy ACCEPT 788 packets, 82764 bytes)
num   pkts bytes target     prot opt in     out     source           destination

Chain OUTPUT (policy ACCEPT 1646 packets, 110K bytes)
num   pkts bytes target     prot opt in     out     source           destination

digi.router>
digi.router> clear firewall

Filter Table
------------
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source            destination
1        0     0 DROP       tcp  --  cellular1 any     anywhere       anywhere             tcp dpt:22
2        0     0 DROP       icmp --  lan1   any     anywhere          anywhere             icmp echo-request

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source            destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source            destination

digi.router>
```

Understanding system firewall rules

This section explains how TransPort built-in components automatically create and apply system firewall rules transparently when you configure system components.

Who should read this section

Do this ...	If you
Skip this section	If you do not use the firewall or firewall6 commands or you use the commands only to create simple firewall rules that allow greater access to device features, skip this section.
Continue reading this section	If you use the firewall or firewall6 commands to create or manage firewall rules on your TransPort device, read this section to understand how TransPort components automatically create and manage system firewall rules and how all firewall rules—both system-generated and command-generated—are saved and applied.

What are system firewall rules?

System firewall rules are automatically created and managed when you configure various TransPort components. For example, the WAN, LAN, and port-forward components create and manage system firewall rules when you configure the components, either from the web interface or the command line.

System firewall rules are applied when the TransPort device starts and anytime you configure a TransPort component that creates or modifies a system firewall rule.

Demonstration

For example, if you enter the following command to allow HTTPS access on WAN 1:

```
wan 1 allow-https-access on
```

TransPort automatically creates a new system firewall rule in the **tlr_wan_input** section of the **iptables** chain. See Using firewall and firewall6 commands for more information about tables and chains.

The new rule might look like this:

```
Chain tlr_wan_input (1 references)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 ACCEPT     tcp  --  eth1   any     anywhere             anywhere             tcp dpt:443 /* (autogenerated) wan 1 */
```

The WAN firewall rule will be re-applied anytime the WAN configuration is changed from the web interface or the command line.

Testing new firewall rules

When you create or modify firewall rules using the firewall or firewall6 commands, save the new rules using the **save config** command and then reboot the TransPort device to test the new rules.

The **FIREWALL** section of the configuration file **config.da0** is saved based on **iptables** save support, and the **FIREWALL** section is executed after the system firewall rules.

Using the autorun command to force firewall rule precedence

If you have difficulty with the saved rule set or the order in which rules are executed, you can use the autorun command to work around these issues. Use an **autorun** command to apply a firewall rule after system startup and after all firewall rules have been applied.

For example, the following **autorun** command applies a DROP to all ICMP requests for the LAN after system startup and after all the firewall rules have been applied. Note the example rule is marked with the **donotsave** comment to prevent it from being saved to the **FIREWALL** section of the **config.da0** file.

```
autorun 1 command firewall -I INPUT 1 -i lan+ -p icmp -j DROP -m comment --comment (donotsave)
```

The result is that the autorun firewall rule is inserted before all of the user and system rules in the **INPUT** chain.

Demonstration

For example, enter the following command to configure the WAN to allow HTTPS connections:

```
wan 1 allow-https-access on
```

A user rule to drop HTTPS traffic on any Ethernet interface might look like this:

```
firewall -A INPUT -i eth+ -p tcp -m tcp --dport 443 -m comment --comment BLOCK-HTTPS-EXAMPLE -j DROP
```

And the result may not be as expected. HTTPS traffic to eth1 (on a device where eth1 is part of wan 1) will not be dropped. The reason can be demonstrated in the following snippet of lines from the show firewall command.

Input packets are processed by the **INPUT** chain in the filter table. When rule 4 is encountered, the system chain **tlr_wan_input** is processed, accepting packets destined for HTTPS (port 443). The appended rule 12 to drop HTTPS packages is never processed because the packet was already accepted due to the system rule created by **wan 1 allow-https-access on**.

```
digi.router> show firewall

 Filter Table
 ------------
```

```
Chain INPUT (policy DROP 8 packets, 2523 bytes)
num   pkts bytes target     prot opt in     out     source               destination
...
4      798 92581 tlr_wan_input  all  --  any    any     anywhere          anywhere             /* (autogenerated) wan */
...
12       0     0 DROP       tcp  --  eth+   any     anywhere             anywhere             tcp dpt:443 /* BLOCK-HTTPS-EXAMPLE */
...
Chain tlr_wan_input (1 references)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 ACCEPT     tcp  --  eth1   any     anywhere             anywhere             tcp dpt:443 /* (autogenerated) wan 1 */
...
```

System chains

The system creates **iptables** chains named with the prefix **tlr_**.

- Do not modify rules in **tlr** chains using the firewall or firewall6 commands. Changes will be discarded.
- Do not modify rules jumping to or from **tlr** chains. Changes will be discarded or negatively affect the system configuration.

Migration of rules from older firmware

Prior to TransPort **1.4.0.0** firmware, all firewall rules (both user and system) were saved in the **FIREWALL** section of the configuration file **config.da0**. The rules were restored as one unit during startup as part of system initialization.

With TransPort firmware **1.4.0.0** and later, any firewall rules recognized as system firewall rules are migrated out of the configuration file and are now managed by the system. The system firewall rules run each time the device is started or when configuration changes result in new or modified system firewall rules.

Future releases

System firewall rules will continue to change and be restructured as subsequent versions of the TransPort firmware are released. If you create or modify firewall rules using the firewall command, be aware of the relationship between system-managed rules and the rules you create.