



Digi TransPort® LR

User Guide

Revision history—90001461

Revision	Date	Description
A	August 2016	Initial revision.
B	October 2016	Added features for TransPort LR firmware 1.2.0.
C	January 2017	Added supportability and usability features: traceroute, show dhcp , show tech-support , and traffic and data packet capture/traffic analyzer features, and documentation for configuring and managing devices from the web interface.
D	April 2017	Added the port forwarding feature. 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 the Configure a user topic and the user command with restrictions on characters in usernames. Updated several hardware specifications. Addressed several issues with display of examples.
E	June 2017	Added IP filtering feature; 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.

Trademarks and copyright

Digi, Digi International, and the Digi logo are trademarks or registered trademarks in the United States and other countries worldwide. All other trademarks mentioned in this document are the property of their respective owners.

© 2017 Digi International Inc. All rights reserved.

Disclaimers

Information in this document is subject to change without notice and does not represent a commitment on the part of Digi International. Digi provides this document “as is,” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranties of fitness or merchantability for a particular purpose. Digi may make improvements and/or changes in this manual or in the product(s) and/or the program(s) described in this manual at any time.

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@digicom.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.digicom.com/support.

Contents

Hardware

TransPort LR54/LR54W hardware overview	12
Hardware specifications	13
Serial connector pinout	14
TransPort LR54 LEDs	15
Regulatory and safety statements	17
Certifications	22

Management and status

Managing devices from the web interface	24
Log in to the web interface	27
The Dashboard	28
Log out of the web interface	30
Managing devices from the command line	31
Interfaces	32
Ethernet interfaces	33
Cellular interfaces	39
Wi-Fi interfaces	49
Serial interface	60
Local Area Networks (LANs)	64
Example LAN	64
Configure a LAN	65
Show LAN status and statistics	69
Delete a LAN	70
Local Networks page	70
DHCP servers	72
Wide Area Networks (WANs)	76
Using Ethernet interfaces in a WAN	76
Using cellular interfaces in a WAN	76
WAN priority, default routes, and metrics	76
Handling WAN failures	76
Wide Area Networks (WAN) page	78
Configure a Wide Area Network (WAN)	82
WAN failover	86
Show WAN status and statistics	89
Delete a WAN	92
Security	93
User management	94
Firewall management with IP filters	100

Services and applications	118
Auto-run commands	119
Port forwarding	120
SSH server	127
Remote management	131
Digi Remote Manager	132
Simple Network Management Protocol (SNMP)	137
Routing	141
IP routing	142
Virtual Private Networks (VPN)	148
IPsec	149
System administration	163
Configure system settings	164
Show system information settings	167
Set system date and time	168
Show system date and time	170
Updating firmware	171
Managing configuration files	177
Reboot the device	183
Reset the device to factory defaults	185
Diagnostics	186
Event and system logs	187
Analyze traffic	202
Use the "ping" command to troubleshoot network connections	210
Use the "tracert" command to diagnose IP routing problems	211
Use the "show tech-support" command	213

File system

File management page	215
Create a directory	217
From the web interface	217
From the command line	217
Display directory contents	219
From the web interface	219
From the command line	219
Change the current directory	220
From the web interface	220
From the command line	220
Delete a directory	222
From the web interface	222
From the command line	222
Display file contents	224
From the web interface	224
From the command line	224
Copy a file	225
From the web interface	225
From the command line	225
Rename a file	227
From the web interface	227
From the command line	227
Delete a file	229
From the web interface	229
From the command line	229
Upload and download files	231

From the web interface	231
From the command line	231

Troubleshooting

Troubleshooting tools and resources	235
Digi support site	235
Digi knowledge base	235
Troubleshooting Ethernet interfaces	236
Ethernet LED does not illuminate	236
Device cannot communicate on WAN/ETH1 port	238
Device cannot communicate on ETH2, ETH3, or ETH4 ports	241
Troubleshooting cellular interfaces	245
Verify cellular connectivity	246
Check cellular signal strength	249
Troubleshooting the serial interface	250
Verify serial connectivity	251
TransPort LR54 model-specific troubleshooting	255
Check TransPort LR54 LEDs	256
Recover a Transport LR54 device	257

Command reference

Command-line interface basics	263
Command line interface access options	264
Log in to the command line interface	265
Exit the command line interface	266
Execute a command from the web interface	267
Display command and parameter help using the ? character	268
Revert command settings using the ! character	269
Auto-complete commands and parameters	270
Enter configuration commands	271
Save configuration settings to a file	272
Switch between configuration files	273
Display status and statistics using "show" commands	275
? (Display command help)	276
! (Revert command settings)	277
analyzer	278
Syntax	278
Parameters	278
autorun	279
Syntax	279
Parameters	279
Examples	279
cd	280
Syntax	280
Parameters	280
cellular	281
Syntax	281
Parameters	281
Examples	282
clear	283
Syntax	283
Parameters	283

Examples	283
cloud	284
Syntax	284
Parameters	284
copy	285
Syntax	285
Parameters	285
date	286
Syntax	286
Parameters	286
Examples	286
del	287
Syntax	287
Parameters	287
dhcp-server	288
Syntax	288
Parameters	288
dir	289
Syntax	289
Parameters	289
eth	290
Syntax	290
Parameters	290
Examples	290
exit	291
Syntax	291
firewall	292
Syntax	292
Parameters	292
ip	293
Syntax	293
Parameters	293
ip-filter	293
Syntax	293
Parameters	293
ipsec	296
Syntax	296
Parameters	296
Examples	299
lan	300
Syntax	300
Parameters	300
mkdir	302
Syntax	302
Parameters	302
more	303
Syntax	303
Parameters	303
ping	304
Syntax	304
Parameters	304
Examples	304
port-forward	304
Syntax	304
Parameters	305

Examples	305
pwd	306
Syntax	306
Parameters	306
reboot	307
Syntax	307
Parameters	307
rename	308
Syntax	308
Parameters	308
rmdir	309
Syntax	309
Parameters	309
route	310
Syntax	310
Parameters	310
save	311
Syntax	311
Parameters	311
Examples	311
serial	312
Syntax	312
Parameters	312
show analyzer	313
Parameters	313
show cellular	314
Parameters	314
show cloud	317
Parameters	317
show config	318
Parameters	318
show dhcp	319
Parameters	319
show eth	320
Parameters	320
show firewall	323
Parameters	323
show ip-filter	323
Parameters	323
show ipsec	325
Parameters	325
show ipstats	327
Parameters	327
show lan	329
Parameters	329
show log	330
Parameters	330
show port-forward	330
Parameters	330
show route	331
Parameters	331
show serial	332
Parameters	332
show system	333
Parameters	333

show tech-support	335
Parameters	335
show wan	336
Parameters	336
show wifi	338
Parameters	338
show wifi5g	341
Parameters	341
snmp	344
Syntax	344
Parameters	344
Examples	344
snmp-community	345
Syntax	345
Parameters	345
Examples	345
snmp-user	346
Syntax	346
Parameters	346
sntp	347
Syntax	347
Parameters	347
ssh	348
Syntax	348
Parameters	348
syslog	348
Syntax	348
Parameters	348
system	349
Syntax	349
Parameters	349
traceroute	352
Syntax	352
Parameters	352
Examples	352
unlock	353
Syntax	353
Parameters	353
Examples	353
update	354
Syntax	354
Parameters	354
Examples	354
user	356
Syntax	356
Parameters	356
Examples	356
wan	357
Syntax	357
Parameters	357
wifi	360
Syntax	360
Parameters	360
wifi5g	362
Syntax	362

Parameters	362
wifi-global	364
Syntax	364
Parameters	364

Advanced topics

Using the firewall command	365
Firewall design is based on iptables	365
Tables and chains in firewall rules	365
Policy rules	366
Allow SSH access on a WAN	368
Allow SSH access for only a specific source IP address	368
Allow HTTPS access on a WAN	370
Allow HTTPS access on a WAN from only a specific source IP address	370
Add a firewall rule	372
Update a firewall rule	375
Delete a firewall rule	377
Show firewall rules and counters	379
Understanding system firewall rules	383
Who should read this section	383
What are system firewall rules?	383
Testing new rules	384
Using the autorun command to force rule precedence	384
System chains	385
Migration of rules from older firmware	385
Future releases	385

Hardware

This section provides hardware specifications, reviews key hardware features, and lists regulatory statements and certifications for TransPort LR Family products.

TransPort LR54/LR54W hardware overview	12
--	----

TransPort LR54/LR54W hardware overview

The following figures show front and back views of the TransPort LR.



1. Enclosure
2. Power
3. Ethernet connectors
4. SIM card slots
5. Cellular antennas
6. Wi-Fi antennas (Wi-Fi models only)
7. Serial port connector See [Serial connector pinout](#)

8. LEDs. See [TransPort LR54 LEDs](#)
9. Reset button. See [Reset the device to factory defaults](#)
10. Internal temperature sensor

Hardware specifications

For a detailed list of TransPort LR hardware specifications, see [TransPort LR54 specifications](#).

Serial connector pinout

TransPort LR54 products are DCE devices. The pinout for the DB9 serial connector is as follows:

Signal name	RS232 signal	DCE signal direction	DB9 pin number
Transmit Data	TxD	In	3
Receive Data	RxD	Out	2
Ready To Send	RTS	In	7
Clear to Send	CTS	Out	8
Data Set Ready	DSR	Out	6
Ground	GND	N/A	5
Data Carrier Detect	DCD	Out	1
Data Terminal Ready	DTR	In	4
Ring Indicate	RI	Out	Not connected

TransPort LR54 LEDs

The TransPort LR54 has LEDs on the top front panel. The number of LEDs varies by model. During bootup, the front-panel LEDs light up in sequence to indicate boot progress. For example, here are the LEDs for a TransPort LR54W (Wi-Fi model):



There are also several LEDs on the rear WAN/LAN connectors that indicate network link and activity.

Power

- **Off:** No power.
- **Blue:** Unit has power.

WWAN Signal

Indicates strength of cellular signal.

- **Off:** No service.
- **Yellow:** Poor / Fair signal.
- **Green:** Good / Excellent signal.

[Signal strength for 4G cellular connections](#)

[Signal strength for 3G and 2G cellular connections](#)

[Tips for improving cellular signal strength](#)

WWAN Service

Indicates the presence and level of cellular service running on the device.

- **Off:** No service.
- **Blinking Green:** 2G/3G/4G connection is coming up.
- **Solid Yellow:** 2G or 3G connection is up.
- **Solid Green:** 4G connection is up.

SIM 1

Indicates use of the SIM card installed in SIM slot 1.

- **Off:** SIM 1 is not being used.
- **Solid green:** SIM 1 is being used or is coming up.

SIM 2

Indicates use of the SIM card installed in SIM slot 2.

- **Off:** SIM 2 is not being used.
- **Solid green:** SIM 2 is being used or is coming up.

Note SIM1 and SIM2 are never both on at the same time.

Wi-Fi 2.4 GHz LED (Wi-Fi models only)

Indicates state and activity on the Wi-Fi 2.4 GHz interface.

- **Off:** Wi-Fi 2.4 GHz interface is disabled.
- **Solid green:** Wi-Fi 2.4 GHz interface is enabled.

Wi-Fi 5 GHz LED (Wi-Fi models only)

Indicates state of and activity on the Wi-Fi 5 GHz interface.

- **Off:** Wi-Fi 5 GHz interface is disabled.
- **Solid green:** Wi-Fi 5 GHz interface is enabled.

Ethernet 1-4 Link and Activity (on rear panel)

The LEDs on the **WAN/ETH1**, **ETH2**, **ETH3**, and **ETH4** ports indicate that the Ethernet network interface is up and there is activity on the network interface.

- **Off:** No Ethernet link detected.
- **Solid green:** Ethernet link detected.
- **Blinking green:** Indicates Ethernet traffic.

Regulatory and safety statements

The following regulatory and safety statements apply to TransPort LR54 devices.

[RF exposure statement](#)

[Federal Communication \(FCC\) Part 15 Class B](#)

[European Community - CE Mark Declaration of Conformity \(DoC\)](#)

[Industry Canada \(IC\) certifications](#)

[RoHS compliance statement](#)

[Safety statements](#)

RF exposure statement

In order to comply with RF exposure limits established in the ANSI C95.1 standards, the distance between the antenna or antennas and the user should not be less than **20 cm**.

Federal Communication (FCC) Part 15 Class B

Radio Frequency Interference (RFI) (FCC 15.105)

TransPort LR has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet that is on a circuit different from the receiver.
- Consult the dealer or an experienced radio/TV technician for help.

Labeling Requirements (FCC 15.19)

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

If the FCC ID is not visible when installed inside another device, then the outside of the device into which the module is installed must also display a label referring to the enclosed module FCC ID.

Modifications (FCC 15.21)

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

European Community - CE Mark Declaration of Conformity (DoC)

Digi has issued Declarations of Conformity for TransPort LR concerning emissions, EMC, and safety. For more information, see www.digi.com/resources/certifications.

Important note

Digi customers assume full responsibility for learning and meeting the required guidelines for each country in their distribution market. Refer to the radio regulatory agency in the desired countries of operation for more information.

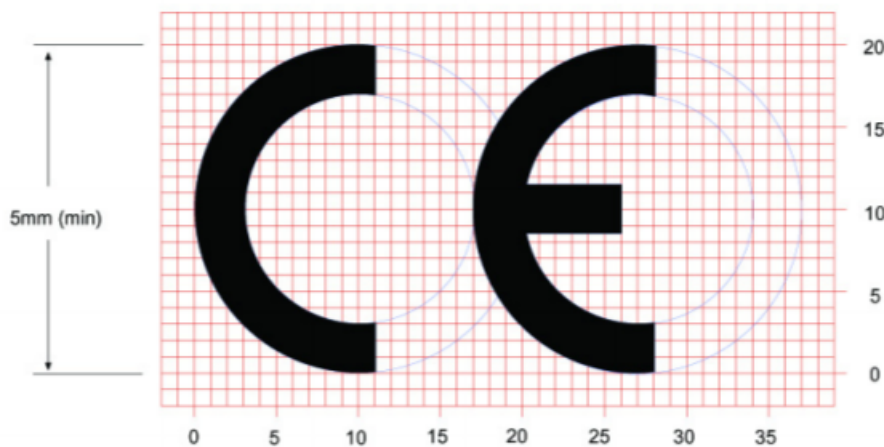
CE mark (Europe)

The TransPort LR is certified for use in several European countries. For information, visit www.digi.com/resources/certifications.

If the TransPort LR is incorporated into a product, the manufacturer must ensure compliance of the final product with articles 3.1a and 3.1b of the RE Directive (Radio Equipment Directive). A Declaration of Conformity must be issued for each of these standards and kept on file as described in the RE Directive (Radio Equipment Directive). Furthermore, the manufacturer must maintain a copy of the (product name) user manual documentation and ensure the final product does not exceed the specified power ratings, antenna specifications, and/or installation requirements as specified in the user manual.

OEM labeling requirements

The 'CE' marking must be affixed to a visible location on the OEM product.

CE labeling requirements

The CE mark shall consist of the initials “CE” taking the following form:

- If the CE marking is reduced or enlarged, the proportions given in the above graduated drawing must be respected.
- The CE marking must have a height of at least 5mm except where this is not possible on account of the nature of the apparatus.
- The CE marking must be affixed visibly, legibly, and indelibly.

Maximum transmit power for radio frequencies

The following table shows the maximum transmit power for frequency bands.

Frequency bands	Maximum transmit power
Cellular LTE 700 MHz Cellular LTE 800 MHz Cellular LTE 850 MHz Cellular LTE 900 MHz Cellular LTE 1700 MHz Cellular LTE 1800 MHz Cellular LTE 1900 MHz Cellular LTE 2100 MHz	200mW
Cellular LTE 2600 MHz Cellular LTE 2300 MHz Cellular LTE 2500 MHz	158.49mW
13 overlapping channels at 22 MHz or 40 MHz wide spaced at 5 MHz Centered at 2.412MHz to 2.472MHz	651.784mW
165 overlapping channels at 22 MHz or 40 MHz or 80 MHz wide spaced at 5 MHz Centered at 5180 MHz to 5825 MHz	351.295mW

Industry Canada (IC) certifications

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

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la class B prescrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

RoHS compliance statement

All Digi International Inc. products that are compliant with the RoHS Directive (EU Directive 2002/95/EC and subsequent amendments) are marked as **RoHS COMPLIANT**. RoHS COMPLIANT means that the substances restricted by the EU Directive 2002/95/EC and subsequent amendments of the European Parliament are not contained in a finished product above threshold limits mandated by EU Directive 2002/95/EC and subsequent amendments, unless the restrictive substance is subject of an exemption contained in the RoHS Directive. Digi International Inc., cannot guarantee that inventory held by distributors or other third parties is RoHS compliant.

Safety statements

Important Safety Information

To avoid contact with electrical current:

- Never install electrical wiring during an electrical storm.
- Never install an Ethernet connection in wet locations unless that connector is specifically designed for wet locations.
- Use caution when installing or modifying lines.
- Use a screwdriver and other tools with insulated handles.
- Wear safety glasses or goggles.
- Do not place Ethernet wiring or connections in any conduit, outlet or junction box containing electrical wiring.
- Installation of inside wire may bring you close to electrical wire, conduit, terminals and other electrical facilities. Extreme caution must be used to avoid electrical shock from such facilities. Avoid contact with all such facilities.
- Ethernet wiring must be at least 6 feet from bare power wiring or lightning rods and associated wires, and at least 6 inches from other wire (antenna wires, doorbell wires, wires from transformers to neon signs), steam or hot water pipes, and heating ducts.
- Do not place an Ethernet connection where it would allow a person to use an Ethernet device while in a bathtub, shower, swimming pool, or similar hazardous location.
- Protectors and grounding wire placed by the service provider must not be connected to, removed, or modified by the customer.
- Do not touch uninsulated Ethernet wiring if lightning is likely!
- External Wiring: Any external communications wiring installed needs to be constructed to all relevant electrical codes. In the United States this is the National Electrical Code Article 800. Contact a licensed electrician for details.



5.10 Ignition of Flammable Atmospheres

Warnings for Use of Wireless Devices



Observe all warning notices regarding use of wireless devices.

Potentially Hazardous Atmospheres

Observe restrictions on the use of radio devices in fuel depots, chemical plants, etc. and areas where the air contains chemicals or particles, such as grain, dust, or metal powders, and any other area

where you would normally be advised to turn off your vehicle engine.

Safety in Aircraft

Switch off the wireless device when instructed to do so by airport or airline staff. If the device offers a 'flight mode' or similar feature, consult airline staff about its use in flight.

Safety in Hospitals

Wireless devices transmit radio frequency energy and may affect medical electrical equipment. Switch off wireless devices wherever requested to do so in hospitals, clinics, or health care facilities. These requests are designed to prevent possible interference with sensitive medical equipment.

Pacemakers

Pacemaker manufacturers recommended that a minimum of 15 cm (6 inches) be maintained between a handheld wireless device and a pacemaker to avoid potential interference with the pacemaker. These recommendations are consistent with independent research and recommendations by Wireless Technology Research.

Persons with Pacemakers:

- Should ALWAYS keep the device more than 15 cm (6 inches) from their pacemaker when turned ON.
- Should not carry the device in a breast pocket.
- If you have any reason to suspect that the interference is taking place, turn OFF your device.

Certifications

International EMC (Electromagnetic Compatibility) and safety standards

This product complies with the requirements of following Electromagnetic Compatibility standards. There are no user-serviceable parts inside the product. Contact your Digi representative for repair information.

Certification category	Standards
Electromagnetic Compatibility (EMC) compliance standards	■ EN 300 328 v1.8.1 ■ EN 301 893 v1.7.2 ■ EN 301 489 ■ FCC Part 15 Subpart B Class B ■ FCC Part 15 Subpart C certification (Integrated Wi-Fi + Cellular Modules)
Safety compliance standards	EN 62368
E-UTRA CA, E-UTRA FDD, E-UTRA TDD, UMTS FDD	PTCRB
Cellular carriers	See the current list of carriers on the TransPort LR54 datasheet, available on the TransPort LR54 Specifications page .

Management and status

These topics show how to manage your TransPort LR devices, including configuring and viewing the status of various TransPort LR features, performing system administration tasks, and performing diagnostics.

Managing devices from the web interface	24
Managing devices from the command line	31
Interfaces	32
Local Area Networks (LANs)	64
Wide Area Networks (WANs)	76
Security	93
Services and applications	118
Remote management	131
Routing	141
Virtual Private Networks (VPN)	148
System administration	163
Diagnostics	186

Managing devices from the web interface

The TransPort LR web interface supports how users typically set up and manage TransPort LR devices.

The first time you power on a TransPort LR device, the **Getting Started Wizard** steps you through the process of initial configuration. After the Getting Started Wizard completes, the next time you access the device, a login prompt appears:

Device Login

Username

Password

Click LOGIN to login to device

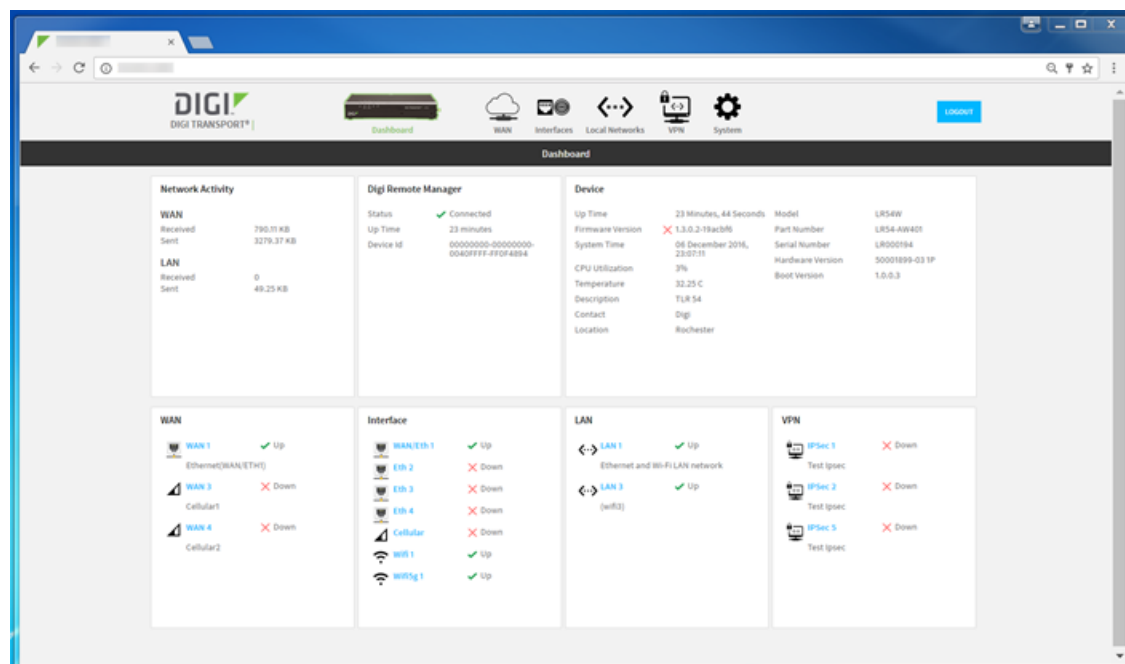
LOGIN

See [Log in to the web interface](#) for login instructions.

After you log in, the TransPort LR **Dashboard** appears. The **Dashboard** provides a snapshot of current activity for the device, including:

- Network statistics over Wide Area Networks and Local Area Networks
- The current connection status to Digi Remote Manager
- Basic device configuration and identifying information
- Summary information for local area network status and the status of physical interfaces

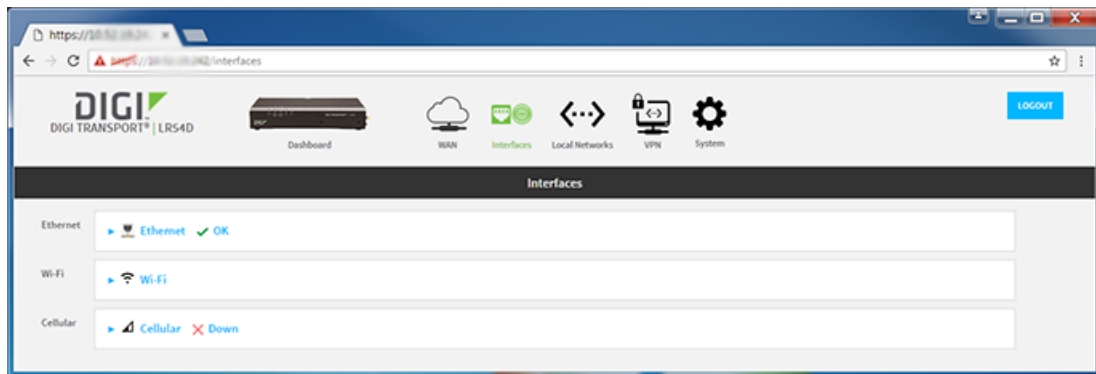
For more information, see [The Dashboard](#).



The web interface menu, at the top of the interface view, organizes information by virtual and physical interfaces that represent the private and public sides of the TransPort LR device. Clicking the items on the menu displays information below the menu.

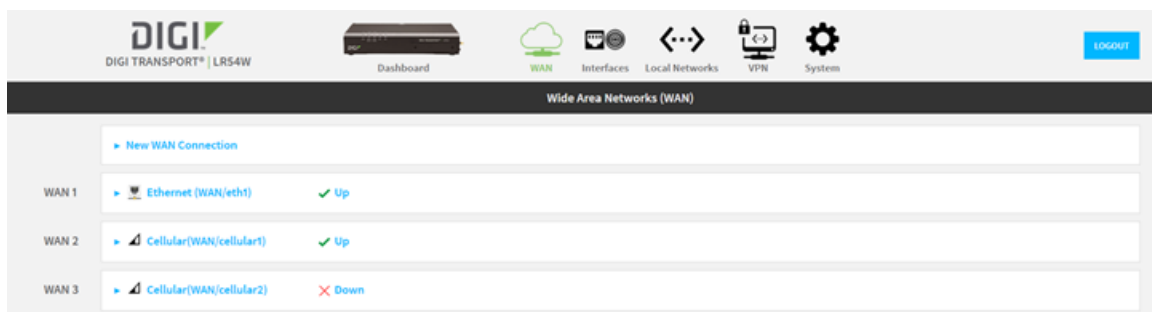


Clicking the **Interfaces** menu item  displays the physical interfaces for your device. From this view, you can configure settings that are specific to the non-networking characteristics of those interfaces, such as Ethernet interface speed, Wi-Fi security, and cellular APN settings. For example:

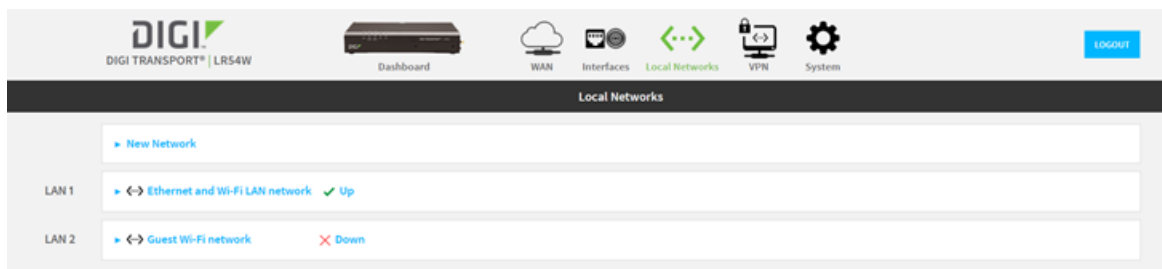


Clicking the **WAN**  and **Local Networks**  menu items display views that are virtual representations of wide-area and local networks that use the physical interfaces in the device. From these views, you can view and change configuration settings for the networking capabilities of the router such as IP, failover, and DHCP server settings.

For example, here is the WAN view for a device:



And here is the Local Networks view for the same device:



Clicking the **System** menu item displays links to pages for displaying pages for performing administrative tasks, such as updating firmware, configuring users, and displaying the event log. From

this menu, you can also open the **Device Console** from this control, to execute commands from within the web interface.

Related topics

[Log in to the web interface](#)

[The Dashboard](#)

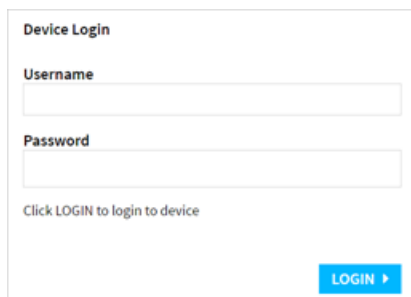
[Execute a command from the web interface](#)

[Log out of the web interface](#)

Log in to the web interface

The first time you access a TransPort LR 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.

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:

A screenshot of the 'Device Login' web interface. It features a title 'Device Login' at the top. Below it are two input fields: 'Username' and 'Password'. Under the password field is a link that says 'Click LOGIN to login to device'. At the bottom right is a blue button labeled 'LOGIN ►'.

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

Use the default 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 LR device appears. See [The Dashboard](#) for more information about this view.

Related topics

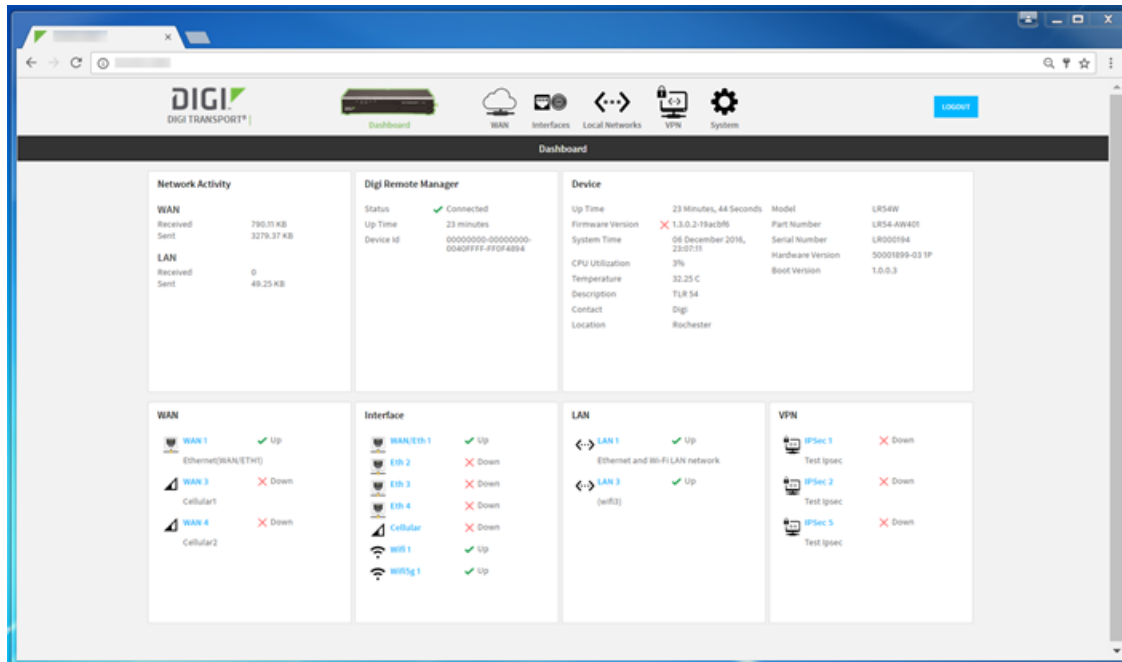
[Managing devices from the web interface](#)

[The Dashboard](#)

[Log out of the web interface](#)

The Dashboard

Clicking **Dashboard** on the web interface menu displays the **Dashboard**.



This display shows the current state of the device in several key areas:

- **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 configured and active WANs and LANs and those that have been disabled or are inactive.
- **Digi Remote Manager:** Displays the status of the device's connection to Digi Remote Manager, the amount of time the connection has been up, and the device's registration ID in Digi Remote Manager. For more information on the Digi Remote Manager connection, see [Remote management](#).
- **Device:** Displays device status, statistics, and identifying information. For descriptions of these fields, see the [show system](#) command description. For the **Firmware Version** field, a green checkmark ✓ indicates that the device's operating system firmware is up to date, and a red x ✗ indicates that a more recent firmware version than the one currently loaded is available.
- **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. For more information on WANs, see [Wide Area Networks \(WANs\)](#).
- **Interface:** Displays all configured and available physical interfaces for the device and their current states. For more information on interfaces, see [Interfaces](#).

- **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. For more information on LANs, see [Local Area Networks \(LANs\)](#).
- **VPN:** Displays all configured Virtual Private Network (VPN) tunnels. For more information, see [Virtual Private Networks \(VPN\)](#).

Related topics[Managing devices from the web interface](#)[Log in to the web interface](#)[Log out of the web interface](#)

Log out of the web interface

Click the **Logout** button in the upper right corner of the web interface. The **Device Login** prompt is displayed again.

Related topics

[Managing devices from the web interface](#)

[The Dashboard](#)

[Log in to the web interface](#)

Managing devices from the command line

TransPort LR devices have a command-line interface from which you can configure features, display current feature status and statistics, and perform action commands, such as updating firmware or performing file management tasks.

The help topics in the rest of this section show how to perform tasks both from the web interface and command line. Look for the heading **From the command line** for the steps to perform each task from the command line interface.

Related topics

[Command-line interface basics](#)

Command descriptions in the [Command reference](#)

Interfaces

TransPort LR 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](#)

[Cellular interfaces](#)

[Wi-Fi interfaces](#)

[Serial interface](#)

Related topics

[Local Area Networks \(LANs\)](#)

[Wide Area Networks \(WANs\)](#)

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.

Related topics

[Configure Ethernet interfaces](#)

[Show Ethernet status and statistics](#)

[Troubleshooting Ethernet interfaces](#)

For more information on WANs, see [Wide Area Networks \(WANs\)](#).

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

Related commands

[eth](#)

[show eth](#)

Configure Ethernet interfaces

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

Required configuration items

- 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 options

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 LR 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.

From the web interface

1. On the menu, click **Interfaces**.
2. Click  **Ethernet**. The available Ethernet interfaces display, along with the current LAN or WAN to which the interface belongs, and its state.
3. Select the Ethernet interface to configure.
4. 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.
5. Click **Apply**.

From the command line

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

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

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

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

- Optional: Set the duplex mode.

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

- Optional: Set the speed.

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

Related topics[Ethernet interfaces](#)[Show Ethernet status and statistics](#)[Troubleshooting Ethernet interfaces](#)[Local Area Networks \(LANs\)](#)[Configure a LAN](#)[Wide Area Networks \(WANs\)](#)[Configure a Wide Area Network \(WAN\)](#)**Related commands**[eth](#)[show eth](#)

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 and statistics from the **Interfaces** page or the **Dashboard**.

From the Interfaces panel

1. On the menu, click **Interfaces**. The **Ethernet** section displays all Ethernet interfaces and their configured states.
2. If an interface is assigned to a WAN, click the **WAN** link. Information about the Ethernet interface displays below the WAN name.
3. On the rightmost side of the page, view the Ethernet status and statistics.

From the Dashboard

1. On the menu, click **Dashboard**.
2. In the **WAN** panel, click the WAN associated with an Ethernet interface for which you want to display status and statistics.
3. On the rightmost side of the page, view the Ethernet status and statistics.

From the 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

```

-----
Rx Unicast Packet    : 0
Rx Broadcast Packet   : 0
Rx Multicast Packet   : 0
Rx CRC Error         : 0
Rx Drop Packet       : 0
Rx Pause Packet      : 0
Rx Filtering Packet   : 0
Rx Alignment Error    : 0
Rx Undersize Error    : 0
Rx Fragment Error     : 0
Rx Oversize Error     : 0
Rx Jabber Error       : 0

```

Sent

```

-----
Tx Unicast Packet    : 0
Tx Broadcast Packet   : 0
Tx Multicast Packet   : 0
Tx CRC Error         : 0
Tx Drop Packet       : 0
Tx Pause Packet      : 0
Tx Collision Event    : 0

```

```

digi.router>

```

Related topics

[Ethernet interfaces](#)

[Configure Ethernet interfaces](#)

[Troubleshooting Ethernet interfaces](#)

Related commands

[eth](#)

[show eth](#)

Cellular interfaces

The TransPort LR 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 LR 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 LR failover, the cellular interface must be assigned to a WAN.

Related topics

[Configure cellular interfaces](#)

[Show cellular status and statistics](#)

[Switch the cellular carrier](#)

[Unlock a SIM card](#)

[Update cellular modem firmware](#)

[Signal strength for 3G and 2G cellular connections](#)

[Signal strength for 4G cellular connections](#)

[Tips for improving cellular signal strength](#)

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

[TransPort LR54 LEDs](#) - See the discussion of the **WWAN Signal** and **WWAN Service** LEDs.

[Troubleshooting cellular interfaces](#)

Related commands

[cellular](#)

[show cellular](#)

[unlock](#)

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](#).

From the web interface

1. Click **Interfaces**. The configurable interfaces for the device displays.
2. Click  **Cellular**. The available cellular interfaces to configure display.
3. Select an interface.

4. 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.
5. Click **Apply**.

From the 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
```

Related topics[Cellular interfaces](#)[Show cellular status and statistics](#)[Switch the cellular carrier](#)[Unlock a SIM card](#)[Update cellular modem firmware](#)[Troubleshooting cellular interfaces](#)[Wide Area Networks \(WANs\)](#)[Configure a Wide Area Network \(WAN\)](#)**Related commands**[cellular](#)[show cellular](#)[unlock](#)

Show cellular status and statistics

From the web interface

The web interface displays the status and statistics for cellular interfaces on the Wide Area Networks (WAN) page for the WAN to which the cellular interface belongs.

To view cellular status and statistics from the interface panel

1. On the menu, click  **WAN**. The **Wide Area Networks (WAN)** page displays all configured WANs and their configured state.
2. If a cellular interface is assigned to a WAN, click the **WAN** link. Information about the cellular interface displays below the WAN name.
3. On the rightmost side of the page, view the cellular status and statistics.
4. Optional: Click the WAN name again to close the display of cellular interface information.

To view cellular status and statistics from the Dashboard

1. On the menu, click **Dashboard**.
2. In the **WAN** panel, click the WAN associated with cellular interface for which you want to display status and statistics. The **WAN** page is displayed.
3. On the rightmost side of the page, view the cellular status and statistics.

From the 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

Related topics[Cellular interfaces](#)[Configure cellular interfaces](#)[Switch the cellular carrier](#)[Unlock a SIM card](#)[Update cellular modem firmware](#)[Troubleshooting cellular interfaces](#)**Related commands**[cellular](#)[show cellular](#)[unlock](#)

Switch the cellular carrier

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

From the command line

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>
```

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 modem firmware](#).

Related topics

[Cellular interfaces](#)

[Configure cellular interfaces](#)

[Show cellular status and statistics](#)

[Unlock a SIM card](#)

[Update cellular modem firmware](#)

[Troubleshooting cellular interfaces](#)

Related commands

[cellular](#)

[show cellular](#)

[unlock](#)

[update](#)

Unlock a SIM card

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 LR 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             :
:
```

From the 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. The syntax for this command is:

```
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.

Related topics

[Cellular interfaces](#)
[Configure cellular interfaces](#)
[Show cellular status and statistics](#)
[Switch the cellular carrier](#)
[Update cellular modem firmware](#)
[Troubleshooting cellular interfaces](#)

Related commands

[cellular](#)
[show cellular](#)
[unlock](#)

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

Related topics

[Cellular interfaces](#)
[TransPort LR54 LEDs](#)
[Check cellular signal strength](#)
[Tips for improving cellular signal strength](#)
[Troubleshooting cellular interfaces](#)

Related commands

[show cellular](#)

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

Related topics

[Cellular interfaces](#)

[TransPort LR54 LEDs](#)

[Check cellular signal strength](#)

[Tips for improving cellular signal strength](#)

[Troubleshooting cellular interfaces](#)

Related commands

[show cellular](#)

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 LR 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](#)

Related topics

[Cellular interfaces](#)

[TransPort LR54 LEDs](#)

[Check cellular signal strength](#)

[Signal strength for 4G cellular connections](#)

[Signal strength for 3G and 2G cellular connections](#)

[Troubleshooting cellular interfaces](#)

Related commands

[show cellular](#)

Wi-Fi interfaces

Wi-Fi-enabled TransPort LR 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.

Related topics

[Configure a channel for Wi-Fi 2.4 GHz interfaces](#)

[Configure a channel for Wi-Fi 5 GHz interfaces](#)

[Configure an access point](#)

[Configure an access point with enterprise security](#)

[Show Wi-Fi status and statistics](#)

Related commands

[wifi](#)

[wifi5g](#)

[wifi-global](#)

[show wifi](#)

[show wifi5g](#)

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 LR 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**.

From the web interface

1. On the menu, click **Interface > Wi-Fi**. The available Wi-Fi interfaces appear.
2. In the **Wi-Fi Options** box, select a channel on the **2.4 GHz Channel** setting, or select **auto** to let the device select the channel.
3. Click **Apply**.

From the 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
```

Related topics

[Wi-Fi interfaces](#)

[Configure a channel for Wi-Fi 5 GHz interfaces](#)

[Configure an access point](#)

[Configure an access point with enterprise security](#)

[Show Wi-Fi status and statistics](#)

Related commands

[wifi](#)

[wifi5g](#)

[wifi-global](#)

[show wifi](#)

[show wifi5g](#)

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 LR 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.

From the web interface

1. On the menu, click **Interfaces > Wi-Fi**. The available Wi-Fi interfaces appear.
2. In the **Wi-Fi Options** box, select a channel on the **5 GHz Channel** setting, or select **auto** to let the device select the channel.
3. Click **Apply**.

From the 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
```

Related topics

[Wi-Fi interfaces](#)

[Configure a channel for Wi-Fi 2.4 GHz interfaces](#)

[Configure an access point](#)

[Configure an access point with enterprise security](#)

[Show Wi-Fi status and statistics](#)

Related commands

[wifi](#)

[wifi5g](#)

[wifi-global](#)

[show wifi](#)

[show wifi5g](#)

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](#).

From the web interface

1. On the menu, click **Interfaces > Wi-Fi**. The available Wi-Fi interfaces appear.
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**.

From the 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
```

Related topics[Wi-Fi interfaces](#)[Configure a channel for Wi-Fi 2.4 GHz interfaces](#)[Configure a channel for Wi-Fi 5 GHz interfaces](#)[Configure an access point with enterprise security](#)[Show Wi-Fi status and statistics](#)[Local Area Networks \(LANs\)](#)[Configure a LAN](#)**Related commands**[wifi](#)[wifi5g](#)[wifi-global](#)[show wifi](#)[show wifi5g](#)

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 a 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 LR 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](#).

From the web interface

1. On the menu, click **Interfaces**.
2. Click  **Wi-Fi**. The available Wi-Fi interfaces display, along with the current LAN to which the interface belongs, and its state.
3. Select a Wi-Fi interface to configure.
4. 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.
5. Click **Apply**.

From the 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
```

Related topics[Wi-Fi interfaces](#)[Configure a channel for Wi-Fi 2.4 GHz interfaces](#)[Configure a channel for Wi-Fi 5 GHz interfaces](#)[Configure an access point](#)[Show Wi-Fi status and statistics](#)**Related commands**[wifi](#)[wifi5g](#)[wifi-global](#)[show wifi](#)[show wifi5g](#)

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.

From the web interface

The web interface displays the status and statistics for Wi-Fi interfaces on **Interfaces** page.

To view Wi-Fi status and statistics from the Interface panel

1. On the menu, click **Interfaces**. The Interfaces page displays sections for **Ethernet**, **Wi-Fi**, and **Cellular** interfaces.
2. Click **Wi-Fi** to display all available Wi-Fi interfaces, along with status and statistics.

To view cellular status and statistics from the Dashboard

1. On the menu, click **Dashboard**.
2. In the **Interface** panel, click the Wi-Fi interface you want to display.

From the 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>
```

Related topics

[Wi-Fi interfaces](#)

[Configure a channel for Wi-Fi 2.4 GHz interfaces](#)

[Configure a channel for Wi-Fi 5 GHz interfaces](#)

[Configure an access point](#)

[Configure an access point with enterprise security](#)

Related commands

[wifi](#)

[wifi5g](#)

[wifi-global](#)

[show wifi](#)

[show wifi5g](#)

Serial interface

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

Related topics

[Configure the serial interface](#)

[Show serial status and statistics](#)

[Troubleshooting the serial interface](#)

[Command-line interface basics](#)

Related commands

[serial](#)

[show serial](#)

Configure the serial interface

By default, the serial interface is **enabled**, with the following configuration, which you can modify as needed:

- Baud rate: **115200**
- Data bits: **8**
- Stop bits: **1**
- Parity: **None**
- Flow control: **None**

From the command line

To change serial configuration settings, use the **serial** command.

- Disable the serial interface.

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

- Enter a description for the serial interface.

```
digi.router> serial description "Command line access"
```

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

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

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

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

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

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

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

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

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

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

Related topics

[Serial interface](#)

[Show serial status and statistics](#)

[Troubleshooting the serial interface](#)

Related commands

[serial](#)

[show serial](#)

Show serial status and statistics

From the command line

To show the status and statistics for the serial interface, use the [show serial](#) command. For example:

```
dig1.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

dig1.router>
```

Related topics

[Serial interface](#)

[Configure the serial interface](#)

[Troubleshooting the serial interface](#)

Related commands

[serial](#)

[show eth](#)

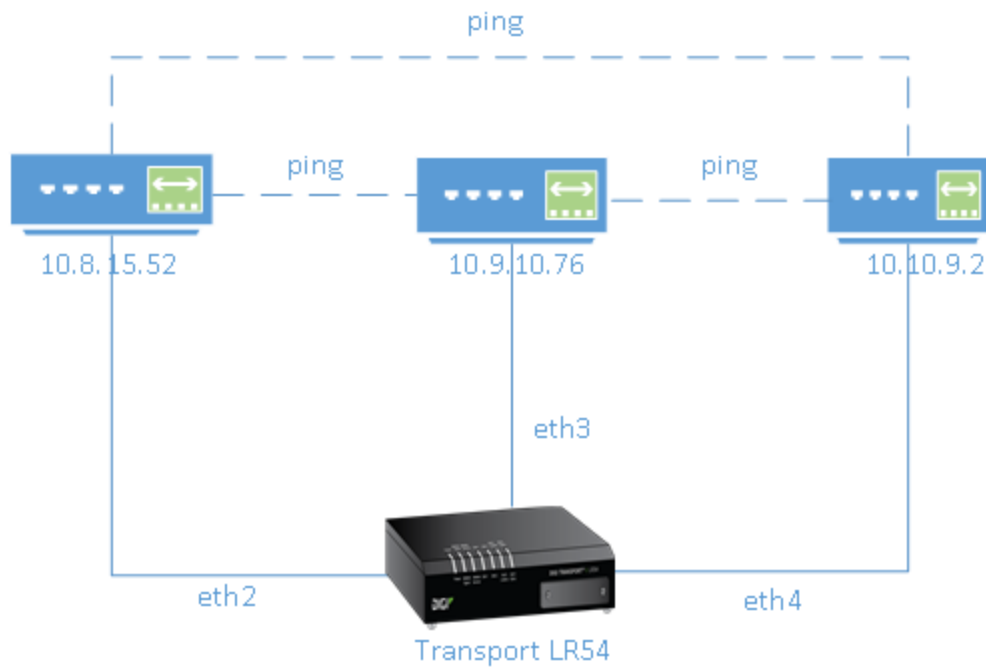
Local Area Networks (LANs)

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.

Example LAN

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.



Related topics

- [Configure a LAN](#)
- [Show LAN status and statistics](#)
- [Delete a LAN](#)
- [DHCP servers](#)

Related commands

- [lan](#)
- [show lan](#)

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.

Additional configuration options

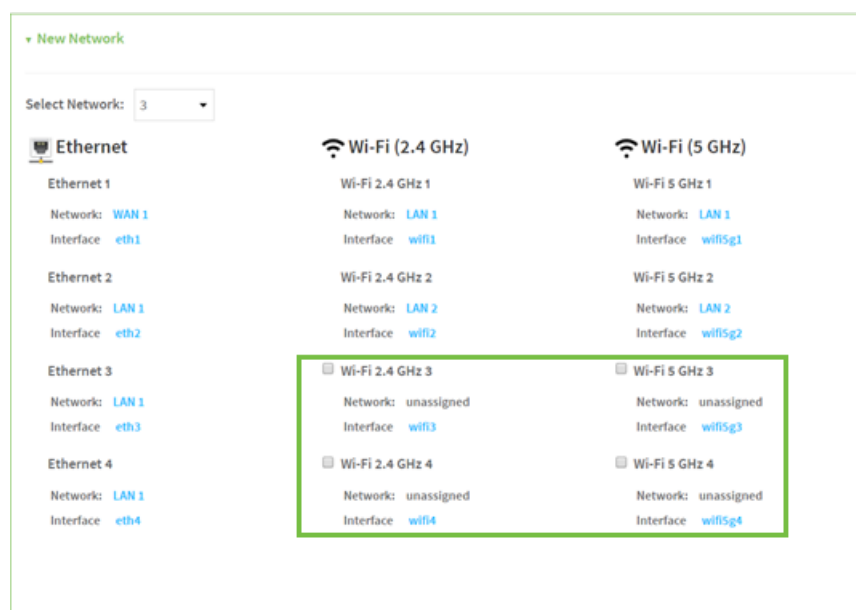
- Setting a descriptive name for the LAN.
- Setting the Maximum Transmission Unit (MTU), or packet size, for packets sent over the LAN.

From the web interface

Create a new LAN

1. On the menu, click  **Local Networks**. The **Local Networks** page shows the default LAN configuration, including the physical interfaces assigned to the LANs and their states.
2. Click **New Network**.
3. In the **Select Network** field, assign an index number to the LAN.

The interfaces shown below the index number are the interfaces available for use by the LAN. Interfaces displayed with an empty checkbox are available. Select one or more interfaces to assign to the LAN. For example, in the following **New Network** display, several Wi-Fi 2.4 GHz and 5 GHz interfaces are available for a new LAN:



New Network			
Select Network: 3			
Ethernet	Wi-Fi (2.4 GHz)	Wi-Fi (5 GHz)	
Ethernet 1	Wi-Fi 2.4 GHz 1	Wi-Fi 5 GHz 1	
Network: WAN 1	Network: LAN 1	Network: LAN 1	
Interface: eth1	Interface: wifi1	Interface: wifi5g1	
Ethernet 2	Wi-Fi 2.4 GHz 2	Wi-Fi 5 GHz 2	
Network: LAN 1	Network: LAN 2	Network: LAN 2	
Interface: eth2	Interface: wifi2	Interface: wifi5g2	
Ethernet 3	☐ Wi-Fi 2.4 GHz 3	☐ Wi-Fi 5 GHz 3	
Network: LAN 1	Network: unassigned	Network: unassigned	
Interface: eth3	Interface: wifi3	Interface: wifi5g3	
Ethernet 4	☐ Wi-Fi 2.4 GHz 4	☐ Wi-Fi 5 GHz 4	
Network: LAN 1	Network: unassigned	Network: unassigned	
Interface: eth4	Interface: wifi4	Interface: wifi5g4	

4. Optional: In the **Description** setting, enter a description for the LAN.
5. In the **Enable** setting, enable or disable the LAN after it is configured.
6. In the **IPv4** and **Netmask** fields, enter the IPv4 address for the LAN, and the subnet mask for the LAN.
7. In the **MTU** field, enter the Maximum Transmission Unit (MTU), or packet size, for packets sent over the LAN.
8. Configure the DHCP server. You can enable the DHCP server feature in a TransPort LR device to assign IP addresses and other IP configuration to other hosts on the same local network. Addresses are assigned from a specified pool of IP addresses.
 - **DHCP Server:** Enable or disable the DHCP server. The DHCP server is disabled by default.

- **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.

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 web interface's **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.

9. Click **Apply**. The new LAN is added to the **LAN** page.

Modify an existing LAN

1. On the menu, click **Local Networks**. The **Local Networks** page shows the default LAN configuration for the TransPort LR device, including the physical interfaces assigned to the LANs and their states. A checkmark next to the interfaces indicates that the interface is a part of a LAN.
2. Select a LAN.
3. Modify the settings as needed; for example:
 - In the interfaces list, assign different physical interfaces to the LAN.
 - In the **Configuration** settings, change the description of the LAN.
 - Enable or disable the LAN.
 - Change the IP address and netmask values.
 - Change the Maximum Transmission Unit (MTU).
 - Change the DHCP server settings.
4. Click **Apply**.

From the 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
```

Related topics

[Local Area Networks \(LANs\)](#)
[Show LAN status and statistics](#)
[Delete a LAN](#)
[DHCP servers](#)

Related commands

[lan](#)
[show lan](#)

Show LAN status and statistics

From the web interface

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.

From the command line

To show the status and statistics for a LAN, use the [show lan](#) command. For example, here is **show lan** output before and after enabling **lan1**.

```
digi.router> show lan 1
```

LAN 1 Status and Statistics

Admin Status : Up

Oper Status : Up

Description : Ethernet and Wi-Fi LAN

Interfaces : eth2,eth3,eth4,wifi1,wifi5g1

MTU : 1500

IP Address : 192.168.1.1

Network Mask : 255.255.255.0

	Received	Sent
	-----	----
Packets	624	6
Bytes	48632	468

```
digi.router>
```

Related topics

[Local Area Networks \(LANs\)](#)

[Configure a LAN](#)

[Delete a LAN](#)

[DHCP servers](#)

Related commands

[lan](#)

[show lan](#)

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.

From the web interface

1. On the menu, click  **Local Networks**.
2. On the **LAN** page, select the LAN to delete.
3. Click **Delete**.

From the command line

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

```
wan <wan-number> interfaces !
```

Related topics

[Wide Area Networks \(WANs\)](#)

[WAN failover](#)

[Configure a Wide Area Network \(WAN\)](#)

[Show WAN status and statistics](#)

Related commands

[show wan](#)

[wan](#)

Local Networks page

Use the Local Networks page to configure and manage local networks. For each network, you can configure the following options.

Configuration options

Option	Description
Description	Displays the description for the network.
Enable	Enable or disable the network .he default is disabled.
IPv4	Specifies the IP address for the network in IPv4 format.
Netmask	Specifies the netmask for IP address in IPv4 format.
MTU	Specifies the maximum Transmission Unit (MTU), or packet size, for packets sent over the LAN.

Option	Description
DHCP server	Enables or disables a DHCP server. The default is disabled.
IP start	Specifies the starting 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.

Related topics

[Local Area Networks \(LANs\)](#)
[Show LAN status and statistics](#)
[Delete a LAN](#)
[DHCP servers](#)

Related commands

[lan](#)
[show lan](#)

DHCP servers

You can enable the DHCP server feature in a TransPort LR device to assign IP addresses and other IP configuration 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 web interface's **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.

Related topics

[Configure DHCP server settings](#)

[Show DHCP server settings](#)

Related commands

[dhcp-server](#)

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.

From the web interface

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

From the 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
```

Related topics[DHCP servers](#)[Show DHCP server settings](#)**Related commands**[dhcp-server](#)

Show DHCP server settings

You can view the DHCP status to monitor which devices have been given IP configuration by the TransPort LR device and diagnose any issues.

From the web interface

In the web interface, DHCP server settings are displayed in the LAN configuration settings.

1. On the menu, click  **Local Networks**.
2. Select a LAN.
3. In the **Configuration** settings, the DHCP server settings for the LAN are:
 - **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.

From the 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>
```

Related topics

[DHCP servers](#)

[Configure DHCP server settings](#)

Related commands

[dhcp-server](#)

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, described below

Using Ethernet interfaces in a WAN

Depending on model type, TransPort LR 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 LR 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 LR 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 LR 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 LR device automatically starts to use the cellular interface until the Ethernet interface becomes active again.

For more information on WAN failover, see [WAN failover](#).

Related topics

[Configure a Wide Area Network \(WAN\)](#)

[WAN failover](#)

[Show WAN status and statistics](#)

[Delete a WAN](#)

Related commands

[wan](#)

[show wan](#)

Wide Area Networks (WAN) page

Use the Wide Area Networks (WAN) page to configure and manage WANs. For each WAN, you can configure the following options.

Ethernet interface options

Column	Description
Network	
Enable	Enable or disable the network. The default is Enabled .
Interface	Specifies the Ethernet interface associated with the WAN. By default: ■ wan1 is assigned eth1
Interface status	Displays the current status of the specified interface: Up or Down .
Description	Displays the description for the Ethernet interface.
Speed	Displays the speed for the ethernet interface: Automatic , 10Mbps , 100Mbps , 1000Mbps . The default is Automatic .
Duplex	Displays the duplex mode for the ethernet interface: Automatic , Full , or Half . The default is Automatic .
Configure using	Specifies how the IP address is configured: Manually or DHCP . The default is Manually .
IPv4	If Configured using is set to Manually , specifies the IP address for the interface in IPv4 format.
Netmask	If Configured using is set to Manually , specifies the netmask for IP address in IPv4 format.
Gateway	If Configured using is set to Manually , specifies the gateway for the IP address in IPv4 format.
DNS1	Specifies the IP address of the primary Domain Name System (DNS) in IPv4 format.
DNS2	Specifies the IP address of the secondary Domain Name System (DNS) in IPv4 format.
Inbound remote access	
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.

Column	Description
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 .
Ethernet status and statistics	
IP address	Display the IP address of the Ethernet interface.
Netmask	Displays the netmask of the Ethernet interface IP address.
Gateway	Displays the gateway of the Ethernet interface IP address.
DNS servers	Displays the DNS servers for the Ethernet interface.
Packets	Displays the number of Received and Sent packets.
Bytes	Displays the number Received and Sent bytes.

Cellular interface options

Column	Description
Network	
Enable	Enable or disable the network. The default is Enabled.

Column	Description
Interface	Specifies the cellular interface associated with the WAN. By default: ■ wan2 is assigned cellular1 ■ wan3 is assigned cellular2
Inbound remote access	
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 .
Interface status and statistics	
	Shows status and statistics for the interface assigned to the WAN.

Buttons

Button	Action
Delete	Delete the WAN.
Cancel	Cancel changes.
Apply	Apply and save configuration changes.

Related topics

[Configure a Wide Area Network \(WAN\)](#)

[WAN failover](#)

[Show WAN status and statistics](#)

[Delete a WAN](#)

Related commands

[wan](#)

[show wan](#)

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.

Assigning priority to WANs

You can assign priority to WANs based on the behavior you desire for primary and backup for 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 LR 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**.

Required configuration items

- Assign an Ethernet, or Cellular interface to the WAN. By default, WANs are assigned the following physical interfaces:
 - **wan1: eth1**
 - **wan2: cellular1**
 - **wan3: cellular2**

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 statically configured IP configuration 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 \(WANs\)](#).

From the web interface

Create a new WAN

1. On the menu, click  **WAN**. The **Wide Area Networks (WAN)** page shows the current WAN configuration for the TransPort LR device, including the physical interfaces assigned to the WANs and their states.
2. Click **New WAN Connection**.
3. In the **Select WAN** field, assign an index number to the WAN. This number sets the WAN priority for the WAN.
4. Select an interface to assign to the WAN.
5. Click **Apply**. The new WAN is displayed in an edit dialog, where you can configure additional options, such as IP address settings and WAN failover.

Modify an existing WAN

1. On the menu, click **WAN**. The **Wide Area Networks (WAN)** page shows the current WAN configuration for the TransPort LR device displays, including the physical interfaces assigned to the WANs, plus any additional WANs that have been created.
2. Select a WAN.
3. Modify the settings as needed; for example:
 - Assign a different physical interface
 - Change the IP configuration
 - Disable DHCP client
 - Change the Maximum Transmission Unit (MTU)
 - Modify the IP probe settings for WAN failover. For more information on these settings, see [WAN failover](#).
4. Click **Apply**.

From the command line

Configure basic WAN settings

1. Assign an interface to the WAN interface.

```
digirouter> wan 1 interface eth1
```

2. Optional: Disable DHCP client mode.

```
digirouter> wan 1 dhcp off
```

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

```
digirouter> wan 1 ip-address 10.1.2.2
digirouter> wan 1 mask 255.255.255.252
digirouter> wan 1 gateway 10.1.2.1
digirouter> wan 1 dns1 10.1.2.1
digirouter> wan 1 dns2 8.8.8.8
```

4. Optional: Set the speed.

```
digirouter> 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.

```
digirouter> wan 1 timeout 60
```

2. Configure the IP host to probe.

```
digirouter> 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.

```
digirouter> 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.

```
digirouter> 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
```

Related topics

[Wide Area Networks \(WANs\)](#)
[WAN failover](#)
[Show WAN status and statistics](#)
[Delete a WAN](#)
[Allow SSH access on a WAN](#)
[Allow HTTPS access on a WAN](#)

Related commands

[show wan](#)
[wan](#)

WAN failover

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

For example, if you use an Ethernet interface as your main 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 LR device automatically starts to use 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 LR to switch to another interface include:

- On an Ethernet interface, the cable for the Ethernet interface is broken or disconnected, or 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

Sometimes, problems can occur beyond the immediate WAN connection that prevent some IP traffic reaching their 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 LR 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 LR 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:

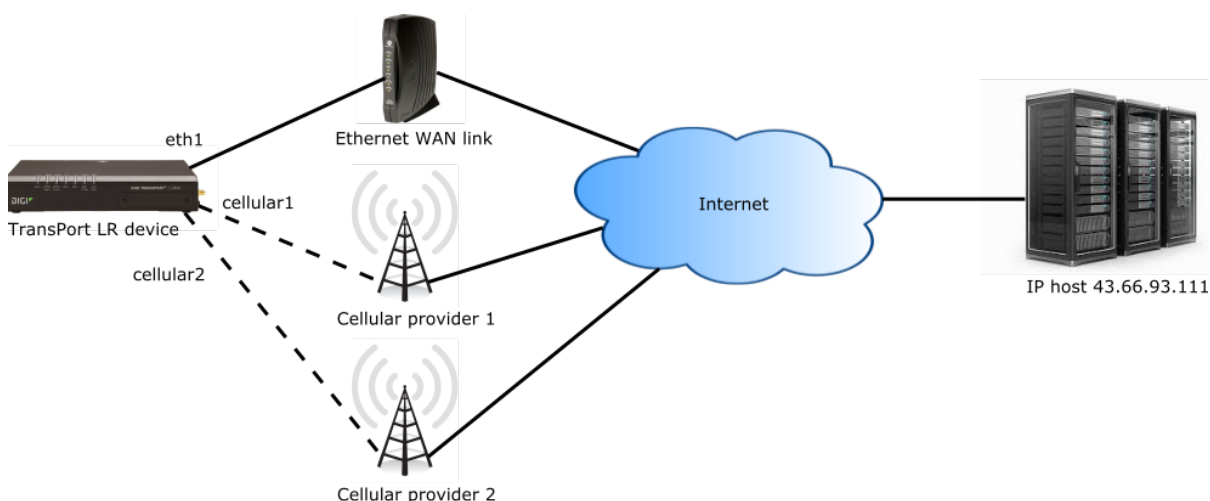
- **timeout:** The time, in seconds, to wait for this interface to connect and to receive a probe response before failing over to a lower priority interface.
- **probe-host:** The IPv4 or fully qualified domain name (FQDN) of the address of the device itself. The WAN failover feature sends probe packets 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 LR 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 LR device brings the **eth1** interface down and starts using the **wan2** (**cellular1**) interface.

If the TransPort LR 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 LR 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
```

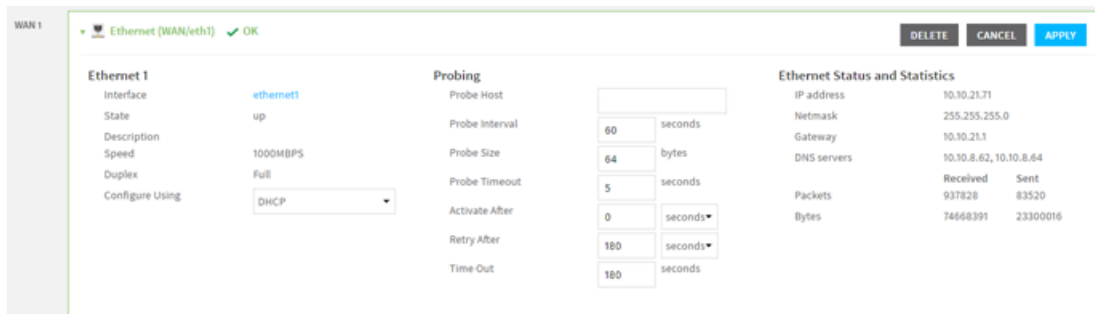
```
digi.router> wan 1 timeout 60
digi.router> wan 1 probe-host 43.66.93.111
digi.router> wan 1 probe-interval 10
digi.router> wan 1 probe-size 256
digi.router> wan 1 activate-after 120
digi.router> wan 2 interface cellular1
digi.router> wan 2 retry-after 1800
digi.router> wan 3 interface cellular2
```

Related topics[Wide Area Networks \(WANs\)](#)[Configure a Wide Area Network \(WAN\)](#)[Show WAN status and statistics](#)[Delete a WAN](#)**Related commands**[wan](#)[show wan](#)

Show WAN status and statistics

From the web interface

1. On the menu, click  **WAN**. The WANs configured for the TransPort LR device appear.
2. Select a WAN.
3. The WAN display expands to show the configuration parameters and the status and statistics for the interface assigned to the WAN. For example, for a WAN using interface **eth1** the Ethernet parameters, status, and statistics are as follows:



From the command line

To show the status and statistics for a WAN, use the `show wan` command. For a description of the output fields, see the `show wan` command.

For example, here is the `show wan` command output with **eth1** and **cellular1** configured as WAN interfaces.

```
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>
```

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`.

To show detailed status for a WAN, enter the `show wan` command, specifying the WAN interface number. For example:

```
digi.router> show wan 1

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

```

IP Address   : 192.168.13.103
Mask        : 255.255.255.0
Gateway     :
DNS Server(s) : 192.168.11.1, 192.168.13.1

```

	Received	Sent
	-----	----
Packets	932	272
Bytes	79464	39425

```
digi.router>
```

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

Related topics[Wide Area Networks \(WANs\)](#)[Configure a Wide Area Network \(WAN\)](#)[WAN failover](#)[Delete a WAN](#)**Related commands**[wan](#)[show wan](#)[show cellular](#)[show eth](#)

Delete a WAN

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

From the web interface

1. On the menu, click  **WAN**.
2. On the **WAN** page, select the WAN to delete.
3. Click **Delete**.

From the command line

Use the `wan` command to set the **interface** parameter value to **none**:

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

Related topics

[Wide Area Networks \(WANs\)](#)

[WAN failover](#)

[Configure a Wide Area Network \(WAN\)](#)

[Show WAN status and statistics](#)

Related commands

[show wan](#)

[wan](#)

Security

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

[User management](#)

[Firewall management with IP filters](#)

User management

To access a TransPort LR 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 LR user model, as well as how to create, modify, and delete users.

Maximum number of users

TransPort LR 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 LR 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**

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

User access levels

TransPort LR 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 LR 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.

Access level	Permissions allowed
read-only	The user can view device configuration and status, but cannot change the configuration or status.

Related topics[Configure a user](#)[Delete a user](#)[Change a user's password](#)[Reset the device to factory defaults](#)**Related commands**[user](#)

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.

From the web interface

1. Click  **System**.
2. Select **User Management**. The **User Management** page shows all defined users and a link to create a new user. The indicator **Active User** displays next to the currently logged-on user.
3. Click **New User**.

Note When you add a new user using the web interface, TransPort LR 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.

4. 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.
5. Click **Apply**.

From the 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
```

Related topics

[User management](#)

[Delete a user](#)

[Change a user's password](#)

Related commands

[user](#)

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.

From the web interface

1. Click **System**.
2. Select **User Management**. The **User Management** page shows currently defined users.
3. Select the user to delete.
4. Click **Delete** and respond to the confirmation prompt.

From the command line

Enter the following command:

```
dig1.router> user n name !
```

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

```
dig1.router> user 1 name !
```

Related topics

[User management](#)

[Configure a user](#)

[Change a user's password](#)

Related commands

[user](#)

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.

From the web interface

1. Click  **System**. The **User Management** page lists currently defined users.
2. Select the user.
3. Enter the new password.
4. Confirm the new password.
5. Click **Apply**.

From the command line

Enter the user command, specifying the new password value:

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

For example:

```
user 6 password tester
```

Related topics

[User management](#)

[Configure a user](#)

[Delete a user](#)

Related commands

[user](#)

Firewall management with IP filters

TransPort LR 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](#)

Related topics

[Allow HTTPS access on a WAN](#)

[Allow HTTPS access on a WAN from only a specific source IP address](#)

[Allow SSH access on a WAN](#)

[Allow SSH access for only a specific source IP address](#)

[Firewall page](#)

[Wide Area Networks \(WAN\) page](#)

Related commands

[ip-filter](#)

[show ip-filter](#)

[port-forward](#)

[show port-forward](#)

[wan](#)

[show wan](#)

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 (Dest)**, 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](#).

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.

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

Column	Description
Enabled	Shows the current state of the IP filter rule: ☒ Rule is enabled (on). ☐ Rule is disabled (off). 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 IPv4 source IP address for incoming packets. If you do not specify an address, the filter is applied to all addresses.
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

Column	Description
Enabled	Shows the current state of the IP filter rule: ☒ Rule is enabled (on). ☐ Rule is disabled (off). The default is enabled.

Column	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 IPv4 source IP address for incoming packets. If you do not specify an address, the filter is applied to all addresses.
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 IPv4 destination IP address for incoming packets. If you do not specify an address, the filter is applied to all addresses.
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.

Buttons

Button	Action
+ Add Rule	Adds an IP filter rule. To specify where to insert the rule, select an existing rule and use the drop-down menu to Add to end , Add before , or Add after .
 Edit	Edit the selected rule.
↓ Down ↑ Up	Move the selected rule down in the list. Move the selected rule up in the list.
 Delete Rule	Delete the selected IP filter rule.
Apply	Apply and save all changes.
Cancel	Cancel current changes.

Related topics

[Add an IP filter rule](#)

[Delete an IP filter rule](#)

[Edit an IP filter rule](#)

[Enable or disable an IP filter rule](#)

[Show IP filter rules](#)

Related commands

[ip-filter](#)

[show ip-filter](#)

Add an IP filter rule

From the web interface

To add one or more IP filter rules:

1. On the menu, click **System**.
2. Click **Firewall**. The **Firewall** page appears. There are two sets of rules: Input IP filter rules and Routing IP filter rules.
3. Within the set of rules you want to add, click **+** (Add Rule) to create a new rule. See [Firewall page](#) for field descriptions.
4. When you have finished adding rules, click **Apply**.

From the 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
```

Related topics

[Delete an IP filter rule](#)

[Edit an IP filter rule](#)

[Enable or disable an IP filter rule](#)

[Show IP filter rules](#)

[Firewall page](#)

Related commands

[ip-filter](#)

[show ip-filter](#)

Delete an IP filter rule

From the web interface

To delete one or more IP filter rules:

1. On the menu, click  **System**.
2. Click **Firewall**. The **Firewall** page appears.
3. Select the rule you want to remove, and click .
4. Click **Apply**.

From the 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
```

Related topics

[Add an IP filter rule](#)

[Edit an IP filter rule](#)

[Enable or disable an IP filter rule](#)

[Show IP filter rules](#)

[Firewall page](#)

Related commands

[ip-filter](#)

[show ip-filter](#)

Edit an IP filter rule

From the web interface

To edit an IP filter rule:

1. On the menu, click  **System**.
2. Click **Firewall**. The **Firewall** page appears. There are two sets of rules: Input IP filter rules and Routing IP filter rules.
3. Select the rule you want to edit and click  **Edit Rule**.
4. When you have finished editing the rule, click **Apply**.

From the 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
```

Related topics

[Add an IP filter rule](#)

[Delete an IP filter rule](#)

[Enable or disable an IP filter rule](#)

[Show IP filter rules](#)

[Firewall page](#)

Related commands

[ip-filter](#)

[show ip-filter](#)

Enable or disable an IP filter rule

From the web interface

To enable or disable an IP filter rule:

1. On the menu, click **System**.
2. Click **Firewall**. The **Firewall** page appears. There are two sets of rules: Input IP filter rules and Routing IP filter rules.
3. Select the rule you change and enable or disable the rule.
4. When you have finished, click **Apply**.

From the 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
```

Related topics

[Add an IP filter rule](#)

[Delete an IP filter rule](#)

[Edit an IP filter rule](#)

[Show IP filter rules](#)

[Firewall page](#)

Related commands

[ip-filter](#)

[show ip-filter](#)

Show IP filter rules

From the web interface

To show IP filter rules:

1. On the menu, click  **System**.
2. Click **Firewall**. The **Firewall** page appears, displaying all configured IP filter rules.

From the 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        none
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

Related topics

[Add an IP filter rule](#)

[Delete an IP filter rule](#)

[Edit an IP filter rule](#)

[Enable or disable an IP filter rule](#)

[Firewall page](#)

Related commands

[ip-filter](#)

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 for WANs, traffic to the TransPort LR 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.

```
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
```

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.

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

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 LR 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 WiFi 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.

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

```
ip-filter 6 description Restrict LAN1 from Accessing Other LANs
ip-filter 6 action Reject
ip-filter 6 src lan1
ip-filter 6 dst any-lan
ip-filter 6 protocol any
ip-filter 6 state on
```

Services and applications

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

[Auto-run commands](#)

[Port forwarding](#)

[Firewall management with IP filters](#)

[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 LR supports up to **10** auto-run commands.

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 test configuration on a remote device that could potentially cause the device to stay offline.

Using the command line

Use the [autorun](#) command.

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"
```

Related topics

[Use multiple configuration files to test configurations on remote devices](#)

[Managing configuration files](#)

[Save configuration settings to a file](#)

[Switch between configuration files](#)

[Reboot the device](#)

Related commands

[autorun](#)

[reboot](#)

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.

Related topics

[Add a port forwarding rule](#)

[Delete a port forwarding rule](#)

[Enable or disable a port forwarding rule](#)

[Show port forwarding rules](#)

[Port forwarding page](#)

[Using the firewall command](#)

[Understanding system firewall rules](#)

Related commands

[port-forward](#)

[show port-forward](#)

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.

Columns

Each port forwarding rule shows the following fields:

Column	Description
Enabled	Shows the current state of the port forwarding rule: ☒ Rule is enabled (on). ☐ Rule is disabled (off). 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.
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. If the IP address is not configured, omit this parameter.
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) .

Buttons

Button	Action
+ Add Rule	Adds a new port forwarding rule to the end of the list.

Button	Action
 Insert Rule	Inserts a new port forwarding rule before the selected rule.
 Delete Rule	Delete the selected port forwarding rule.
Apply	Apply and save all changes.
Cancel	Cancel current changes.

Related topics[Add a port forwarding rule](#)[Delete a port forwarding rule](#)[Enable or disable a port forwarding rule](#)[Show port forwarding rules](#)[Using the firewall command](#)[Understanding system firewall rules](#)**Related commands**[port-forward](#)[show port-forward](#)

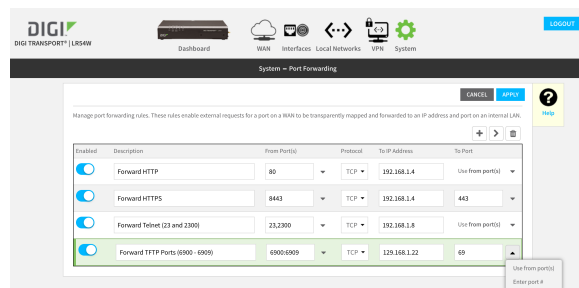
Add a port forwarding rule

From the web interface

To add one or more port forwarding rules:

1. On the menu, click **System**.
2. Click **Port Forwarding**. The **Port Forwarding** page appears.
3. 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.
4. When you have finished adding rules, click **Apply**.

Here's a sample of port forwarding rules:



From the 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

```

Related topics

- [Delete a port forwarding rule](#)
- [Enable or disable a port forwarding rule](#)
- [Show port forwarding rules](#)
- [Port forwarding page](#)
- [Using the firewall command](#)
- [Understanding system firewall rules](#)

Related commands

- [port-forward](#)
- [show port-forward](#)

Delete a port forwarding rule

From the web interface

To delete one or more port forwarding rules:

1. On the menu, click  **System**.
2. Click **Port Forwarding**. The **Port Forwarding** view appears.
3. Select the rule you want to remove, and click .
4. Click **Apply**.

From the 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
```

Related topics

[Add a port forwarding rule](#)

[Enable or disable a port forwarding rule](#)

[Show port forwarding rules](#)

[Port forwarding page](#)

[Using the firewall command](#)

[Understanding system firewall rules](#)

Related commands

[port-forward](#)

[show port-forward](#)

Enable or disable a port forwarding rule

From the web interface

To enable or disable a port forwarding rule:

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

From the command line

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

For example, to enable port forwarding rule 4:

```
digirouter> port-forward 4 state on
digirouter> save config
```

To disable port forwarding rule 4:

```
digirouter> port-forward 4 state off
digirouter> save config
```

Related topics

[Add a port forwarding rule](#)

[Delete a port forwarding rule](#)

[Show port forwarding rules](#)

[Port forwarding page](#)

[Using the firewall command](#)

[Understanding system firewall rules](#)

Related commands

[port-forward](#)

[show port-forward](#)

Show port forwarding rules

From the web interface

To show port forwarding rules:

1. On the menu, click  **System**.
2. Click **Port Forwarding**. The **Port Forwarding** page appears. See [Port forwarding page](#) for field descriptions.

From the command line

To show port forwarding rules, use the [show port-forward](#) command.

For example:

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

Related topics

[Add a port forwarding rule](#)

[Delete a port forwarding rule](#)

[Enable or disable a port forwarding rule](#)

[Port forwarding page](#)

[Using the firewall command](#)

[Understanding system firewall rules](#)

Related commands

[port-forward](#)

[show port-forward](#)

[show port-forward](#)

SSH server

TransPort LR 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, as earlier versions of SSH protocol are no longer considered secure.

[Configure a Secure Shell \(SSH\) server](#)

[Use SSH to connect to the TransPort LR command-line interface](#)

[Terminate an SSH connection](#)

Configure a Secure Shell (SSH) server

This section describes how to configure an SSH server.

Required configuration items

Enable the SSH server. It is enabled by default.

Additional configuration options

SSH server port. By default the port is **22**, the standard SSH port, but this setting can be configured as needed.

From the 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
```

Related topics

[Use SSH to connect to the TransPort LR command-line interface](#)

[Terminate an SSH connection](#)

Related commands

[ssh](#)

[exit](#)

Use SSH to connect to the TransPort LR command-line interface

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

The following example shows a user using 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>
```

Related topics

[Configure a Secure Shell \(SSH\) server](#)

[Terminate an SSH connection](#)

Related commands

[ssh](#)

[exit](#)

Terminate an SSH connection

To terminate an SSH connection, exit the command-line interface using the [exit](#) command.

Related topics

[Configure a Secure Shell \(SSH\) server](#)

[Use SSH to connect to the TransPort LR command-line interface](#)

Related commands

[ssh](#)

[exit](#)

Remote management

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

[Digi Remote Manager](#)

[Simple Network Management Protocol \(SNMP\)](#)

Digi 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](#).

Related topics

[Configure Digi Remote Manager](#)

[Show Digi Remote Manager connection status](#)

[Remote Manager User Guide](#)

Related commands

[cloud](#)

[show cloud](#)

Configure Digi Remote Manager

Digi Remote Manager is enabled by default. Once the TransPort LR 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.

From the web interface

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**.
2. Select **Digi Remote Manager**.
3. On the **Digi Remote Manager** page, enter your credentials to log in to your Digi Remote Manager account and click **Log In**.
4. Select a group for your device in your Digi Remote Manager account, then click **Register Device**.
5. 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**.
2. Select **Digi Remote Manager**.
3. On the **Digi Remote Manager** page, enter the settings.
 - Enable or disable the TransPort LR device's 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.
4. Click **Apply**.

From the command line

- Disable the Digi Remote Manager connection.

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

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

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

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

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

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

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

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

```
digirouter> cloud keepalive-count 5
```

Related topics[Digi Remote Manager](#)[Show Digi Remote Manager connection status](#)[Remote Manager User Guide](#)**Related commands**[cloud](#)[show cloud](#)

Show Digi Remote Manager connection status

From the web interface

1. On the menu, click  **System**.
2. Select **Digi Remote Manager**.

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

From the 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:

```
digirouter> 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

digirouter>
```

Related topics

[Digi Remote Manager](#)

[Configure Digi Remote Manager](#)

[Remote Manager User Guide](#)

Related commands

[cloud](#)

[show cloud](#)

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

- Standard SNMP MIBs
- An enterprise-specific MIB, specific to 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.

Related topics

[Configure SNMPv1 and SNMPv2](#)

[Configure SNMPv3](#)

Related commands

[snmp](#)

[snmp-community](#)

[snmp-user](#)

Configure SNMPv1 and SNMPv2

Configuring SNMPv1 or SNMPv2c support involves configuring the following items:

- Enabling the desired SNMP version.
- Whether to configure SNMPv1/v2c communities.
- If configuring SNMPv1/v2c communities, the community access level.

From the 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
```

Related topics

[Simple Network Management Protocol \(SNMP\)](#)

[Configure SNMPv3](#)

Related commands

[snmp](#)

[snmp-community](#)

[snmp-user](#)

Configure SNMPv3

Configuring SNMPv3 support involves configuring the following items:

- Enabling SNMPv3.
- Configuring the SNMPv3 users. Up to **10** SNMPv3 users can be configured.
- Configuring SNMPv3 user authentication type and password, privacy type and password, and user access level.

From the 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 authentication 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
```

Related topics

[Simple Network Management Protocol \(SNMP\)](#)

[Configure SNMPv3](#)

Related commands

[snmp](#)

[snmp-community](#)

[snmp-user](#)

Routing

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

[IP routing](#)

IP routing

The TransPort LR device uses IP routes to decide where to send a packet it receives for a remote network.

Process for determining IP route

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.

Configuring and managing IP routing

Configuring and managing IP routing involves the following tasks:

[Configure general IP settings](#)

[Configure a static route](#)

[Show the IPv4 routing table](#)

[Delete a static route](#)

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**.

From the web interface

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 \(WAN\)](#).

From the 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
```

Related topics

[IP routing](#)

[Configure a static route](#)

[Show the IPv4 routing table](#)

[Delete a static route](#)

Related commands

[ip](#)

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 LR 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.

From the command line

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
```

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
```

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

Related topics

[IP routing](#)

[Configure general IP settings](#)

[Show the IPv4 routing table](#)

[Delete a static route](#)

Related commands

[ip](#)

[route](#)

[show route](#)

Show the IPv4 routing table

From the command line

To display the IPv4 routing table, use the [show route](#) command.

```
digirouter> 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

```
digirouter>
```

Related topics

[IP routing](#)

[Configure general IP settings](#)

[Configure a static route](#)

[Delete a static route](#)

Related commands

[ip](#)

[route](#)

[show route](#)

Delete a static route

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

From the command line

to revert the settings for the route destination, enter the [route](#) command, specifying the interface number, the destination parameter, and the ! character. For example:

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

Related topics[IP routing](#)[Configure general IP settings](#)[Configure a static route](#)[Show the IPv4 routing table](#)**Related commands**[ip](#)[route](#)[show route](#)

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 from the web interface and command line.

[IPsec](#)

IPsec

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

TransPort LR devices support up to **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 LR 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.

Related topics

[Configure an IPsec tunnel](#)

[Example: IPsec tunnel between a TransPort LR54 and TransPort WR44](#)

[Debug an IPsec configuration](#)

[Show IPsec status and statistics](#)

Related commands

[ipsec](#)

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 LR 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.

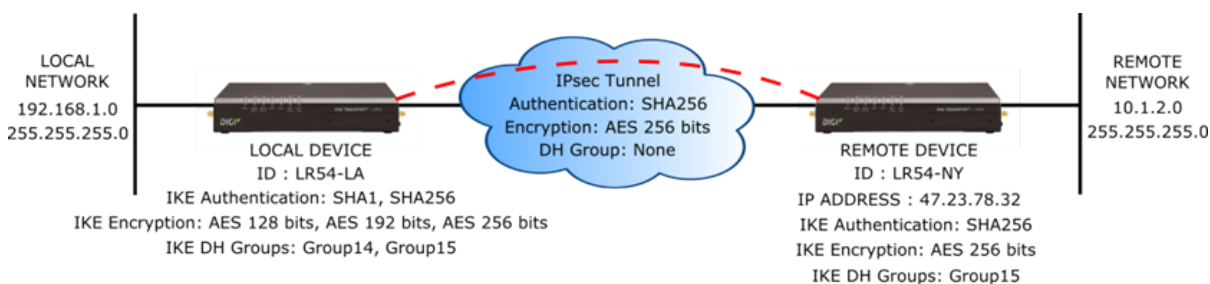
- The number of bytes, also known as lifebytes, sent on the IPsec tunnel before it is renegotiated. By default, this setting is disabled, but can be configured up to **4 GB**. This setting does not need to match the setting on the remote device.
- The IKE lifetime before the keys are renegotiated. This 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:



From the web interface

Configure a new IPsec tunnel

1. **Prerequisite:** Configuring an IP tunnel requires an configured LAN to be available for use in the IPsec tunnel. The default configuration for TransPort LR devices includes a LAN, but if that LAN has been deleted or is unavailable, you will need to configure a LAN for use in the IPsec tunnel. See [Configure a LAN](#).

2. On the menu, click  **VPN**.

3. Click **New IPsec Tunnel**. The **VPN** 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  **VPN**. The existing IPsec tunnels and their current states are displayed.
2. Select an IPsec tunnel and click **Edit**.
3. Modify the **Network**, **Encryption**, **Negotiation**, and **Lifetime** settings as needed.
4. Click **Apply**.

From the 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
```

Related topics

[IPsec](#)

[Example: IPsec tunnel between a TransPort LR54 and TransPort WR44](#)

[Debug an IPsec configuration](#)

[Show IPsec status and statistics](#)

Related commands

[ipsec](#)

[show ipsec](#)

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
margin-time	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=
```

Related topics

[IPsec](#)

[Configure an IPsec tunnel](#)
[Debug an IPsec configuration](#)
[Show IPsec status and statistics](#)

Related commands

[ipsec](#)

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.

IPsec tunnel debug messages are disabled by default. Once enabled, the debug messages are displayed in the file **ipsec.debug**.

Enable IPsec debug messages

From the command line

To enable IPsec debugging, use the [system](#) command's **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
```

Related topics

[IPsec](#)

[IPsec tunnel failover](#)

[Configure an IPsec tunnel](#)

[Example: IPsec tunnel between a TransPort LR54 and TransPort WR44](#)

[Show IPsec status and statistics](#)

[Event and system logs](#)

Related commands

[ipsec](#)

[ipsec-failover](#)

[show ipsec](#)

[system](#)

Show IPsec status and statistics

From the web interface

On the menu, click  **VPN**. The **VPN** page displays IPsec status and statistics for IPsec tunnels.

From the 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>
```

Related topics

[IPsec](#)

[Configure an IPsec tunnel](#)

Example: IPsec tunnel between a TransPort LR54 and TransPort WR44

Debug an IPsec configuration

Related commands

ipsec

show ipsec

System administration

These topics cover administration and management tasks that need to be performed on TransPort LR devices periodically.

[Configure system settings](#)

[Show system information settings](#)

[Set system date and time](#)

[Show system date and time](#)

[Updating firmware](#)

[Managing configuration files](#)

[Reboot the device](#)

Configure system settings

The TransPort LR device has several settings that control the general behavior of the device, and information displayed about the device.

From the web interface

Click  **System**. The choices on the **System** menu are:

- **Firmware Update:** Updates operating system firmware and other device firmware. See [Updating firmware](#).
- **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 [Event and system logs](#).
- **File Management:** Displays the local file system for the TransPort LR device and allows you to perform file management operations. See [File system](#).
- **User Management:** Creates and manages device users and their access permissions. See [User management](#).
- **Digi Remote Manager:** Configures the connection to Digi Remote Manager. See [Digi Remote Manager](#).
- **Reboot:** Reboots the device. See [Reboot the device](#).

From the command line

Required configuration items

- None. Most system settings either have defaults. The informational settings default to blank if no value is specified.

Additional configuration options

- The system prompt displayed in the command-line interface. The default system prompt is **digirouter>**. 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**.
- The command-line interface 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.
- 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 [Event and system logs](#), [Event log levels](#), and [Configure options for event and system logs](#).
- The name of this device.
- The location of this device.

- Contact information for this device.
- 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**.
- Enabling 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.
- A description of this device.
- The TCP port used for passthrough. 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.
- Disabling the 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.
- Enabling display of 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](#).

Examples of changing system settings

- Change the system prompt.

```
digi.router> system prompt "LR54_%s"
```

- Set the command-line interface timeout. For example, to set the timeout to 60 seconds, enter:

```
digi.router> system timeout 60
```

- Configure the event log level. For example, to set the event log level to **warning**, enter:

```
system log-level warning
```

- Specify a name for the device.

```
digi.router> system name "Wireless router"
```

- Specify the location of the device.

```
digi.router> system name "Second floor"
```

- Specify contact information for the device.

```
digi.router> system contact "John Doe at x3749"
```

- Set the page size for command-line interface output. For example, to set the output to **30** lines:

```
digi.router> system page 30
```

- Enable device-specific passwords.

```
digi.router> system device-specific-passwords on
```

- Specify a description of the device.

```
digi.router> system description "Engineering department wireless router"
```

- Specify the TCP port used for passthrough.

```
digi.router> system passthrough 5000
```

- Disable the Getting Started Wizard.

```
digi.router> system wizard off
```

- Enable IPsec debugging.

```
digi.router> system ipsec on
```

Related topics[System administration](#)[Show system information settings](#)**Related commands**[system](#)[show system](#)

Show system information settings

From the web interface

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.

From the 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>
```

Related topics

[System administration](#)

[Configure system settings](#)

Related commands

[system](#)

[show system](#)

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.

Methods for setting system date and time

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

Required configuration items

- None.

Additional configuration options

- The SNTP server. By default, SNTP is configured to use Digi's SNTP server, **time.devicecloud.com**.
- The SNTP update interval. This is the interval at which the TLR device 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.

From the 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
```

Set the date and time manually

From the command line

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**.

From the command line

Optional: Set the time zone. For example, to set the time zone to US Eastern:

```
digi.router> system timezone us-eastern
```

Related topics

[Show system date and time](#)

Related commands

[date](#)

[sntp](#)

Show system date and time

From the web interface

1. On the menu, click **Dashboard**.
2. In the **Device** panel, view the **System Time** field.

From the 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>
```

Related topics

[Set system date and time](#)

Related commands

[date](#)

[sntp](#)

Updating firmware

Maintaining your TransPort LR device involves periodic updates to firmware for the main operating system and several subsystems.

[Update system firmware](#)

[Update cellular modem firmware](#)

Update system firmware

This topic shows how to update the TransPort LR operating system firmware.

System firmware files

The TransPort LR 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 LR device validates the system firmware image as part of the update process and only successfully updates if the system firmware image can be authenticated.

Handling of multiple system firmware images

The TransPort LR 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 LR device automatically switches to boot the new system firmware image when it is next rebooted. This means that the TransPort LR 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.

Digi Remote Manager recommended for managing firmware updates

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](#).

From the web interface

Digi maintains a repository of available TransPort LR 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. From the menu, click **⚙ System** and select **Firmware Update**. The **Firmware** view displays the current firmware version running on the TransPort LR device.
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 LR 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**.

From the command line

1. Download the TransPort LR 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>
```

Related topics

[Update cellular modem firmware](#)

[Reboot the device](#)

Related commands

[reboot](#)

[show system](#)

[update](#)

Update cellular modem firmware

Digi provides the cellular modem files for all certified cellular carriers for TransPort LR devices on the [Digi repository of cellular modem firmware files](#).

From the command line

Update cellular modem firmware from a file on the Digi repository

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
```

Related topics

[Update system firmware](#)

[Reboot the device](#)

[Switch the cellular carrier](#)

Related commands

[copy](#)

[reboot](#)

[show system](#)

[update](#)

Managing configuration files

The configuration file for TransPort LR devices holds all of the configuration for a device that is applied when the device boots up. The configuration file contains the commands required to configure the device to the user's needs.

When the device boots up, the configuration file is read and each of the commands are processed in order.

Configuration file name

By default, the configuration file is named **config.da0**. You can change the name of the configuration file if desired. For more information, see [Switch between configuration files](#).

Factory default configuration file

The device has a factory default configuration file, named **config.fac**. This file contains the configuration that is applied when the device is factory defaulted. You can customize the **config.fac** file, so that a factory-defaulted device boots up with the your custom configuration.

Saving configuration changes

Configuration changes are **not automatically saved** to the configuration file. You must explicitly save all configuration changes; the changes are lost when the device is next rebooted. For more information on saving configurations, see [Save configuration settings to a file](#).

Key sections of the configuration file

There are several sections of note in the configuration file.

Timestamp section

The first part of the configuration file includes a **timestamp** of when the configuration file was saved, and by which user:

```

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, containing the commands and parameters required to configure features.

- Any passwords in the file are stored in encrypted form. It is not possible to display passwords in clear-text form.
- To include comments in the file, begin the line with a # 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+uGGAqPg0F8iU="
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$61hWHSy071CYMrIOdUMUSB9vq7powrwcMftGAL912MLQutR9LHhW2k1LQrsZxETCz3sAw4DL4vZU20b1ZxxC."
:
```

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 the firewall command](#).

```
[FIREWALL]
*nat
-A POSTROUTING -o eth1 -j MASQUERADE
COMMIT
[FIREWALL_END]

digi.router>
```

Device-specific passwords and sharing configuration files among devices

Passwords are stored in the configuration file in an encrypted form. It is not possible to read the password in clear-text form once it has been configured.

By default, passwords are stored in a form that allows another device to decipher the encrypted form of the password. This allows for sharing and copying configuration files between devices, but only if device-specific passwords have not been enabled.

If sharing the configuration file is not required, you can encrypt passwords in a device-specific manner. This means that only the device on which the password is configured can decipher the password. To enable device specific passwords, use the **system device-specific-passwords** command.

Related topics

[Save configuration settings to a file](#)

[Switch between configuration files](#)

[Use multiple configuration files to test configurations on remote devices](#)

[Reset the device to factory defaults](#)

[File system](#)

Save configuration settings to a file

Configuration changes are **not** automatically saved. This means that the device will lose any unsaved changes when it is next rebooted.

To save configuration settings to a file:

From the web interface

On configuration pages, clicking **Apply** saves your changes to the configuration file immediately.

From the command line

Enter the **save config** command.

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

Related topics

[Managing configuration files](#)

[Switch between configuration files](#)

[Use multiple configuration files to test configurations on remote devices](#)

[File system](#)

Related commands

[save](#)

Switch between configuration files

You can have multiple configuration files stored on the device, although the device uses only one configuration file when it reboots.

From the command line

Identify the current configuration file

If necessary, identify the current configuration file the TransPort LR device is using. Enter the [show system](#) command and note the file listed after **Using Config File:**. 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>
```

Change the configuration file name

1. Change the name of the configuration file to be used at boot-up and when the configuration is saved.

```
digi.router> update config <filename>
```

2. If the new configuration file does not exist, enter the [save](#) command to create and save the configuration file.

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

Related topics

[Managing configuration files](#)

[Save configuration settings to a file](#)

[Use multiple configuration files to test configurations on remote devices](#)

[File system](#)

Related commands

[save](#)

[show system](#)

Use multiple configuration files to test configurations on remote devices

You can use multiple configuration files, along with the [autorun](#) command, to 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 desired configuration changes to test. In addition to the desired configuration changes, the file should contain 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 create a new test configuration file named **test.cfg**

This **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 LR 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 then 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
```

Related topics

[Managing configuration files](#)

[Save configuration settings to a file](#)

[Switch between configuration files](#)

[File system](#)

Related commands

[autorun](#)

[copy](#)

[reboot](#)

[save](#)

[update](#)

Reboot the device

You can reboot the TransPort LR 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](#).

From the web interface

1. Click  **System**.
2. Select **Reboot**. A message displays the maximum time expected for the reboot operation. When the device reboot operation completes, the device reconnects and the **Device Login** page displays.

From the 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
```

Related topics

[Set system date and time](#)

[Save configuration settings to a file](#)

[Reset the device to factory defaults](#)

Related commands

[reboot](#)

[save](#)

Reset the device to factory defaults

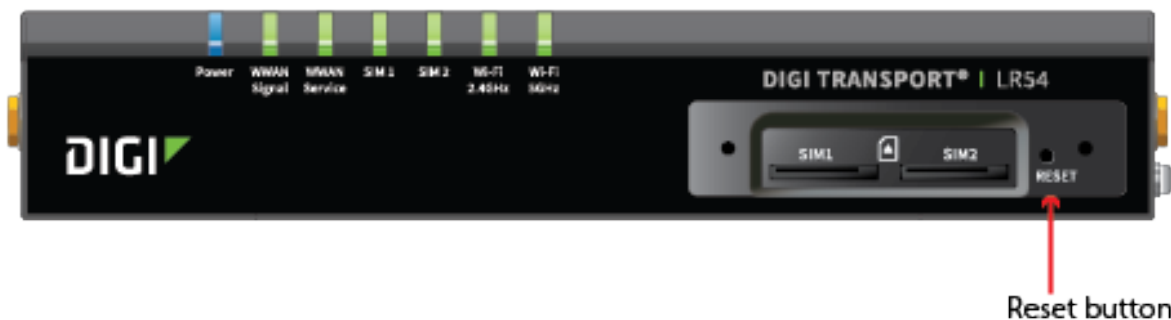
Resetting the device to factory defaults performs the following actions:

- 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.

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 is now reset back to factory defaults. Follow the instructions on the TransPort device's Quick Start Guide to reconfigure the device.

Related topics

[Managing configuration files](#)

[Save configuration settings to a file](#)

[Reboot the device](#)

[Recover a TransPort LR54 device](#)

Diagnostics

These topics cover the diagnostics capabilities available for TransPort LR devices.

[Event and system 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](#)

Event and system logs

The **event log** contains events related to the functionality of the TransPort LR device. These events include information about configuration changes, interface state changes, user access, etc.

The **system log** contains events related to the device's low-level system. While these events are typically not useful to device 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.

Related topics

[Event log levels](#)

[Log viewer page](#)

[Log configuration page](#)

[Configure options for event and system logs](#)

[Display logs](#)

[Find and filter log file entries](#)

[Save logs to a file](#)

[Download log files](#)

[Clear logs](#)

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.

From the web interface

1. On the menu, click **System > 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**.

From the command line

Enter the system log-level command, specifying the event log level.

```
system log-level <level>
```

For example:

```
system log-level warning
```

Related topics

[Event and system logs](#)

[Event log levels](#)

[Log viewer page](#)

[Log configuration page](#)

[Display logs](#)

[Find and filter log file entries](#)

[Save logs to a file](#)

[Download log files](#)

[Clear logs](#)

Related commands

[clear](#)

[show log](#)

[system](#)

Configure syslog servers

You can configure up to two syslog servers for storing event and system logs.

From the web interface

1. On the menu, click **System > 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**.

From the 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
```

Related topics

[Event and system logs](#)[Event log levels](#)[Log viewer page](#)[Log configuration page](#)[Display logs](#)[Find and filter log file entries](#)[Save logs to a file](#)[Download log files](#)[Clear logs](#)

Related commands

[clear](#)[show log](#)[system](#)

Display logs

From the web interface

1. On the menu, click **System > 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](#).

From the 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>
```

Related topics

[Event and system logs](#)

[Event log levels](#)

[Log viewer page](#)

[Log configuration page](#)

[Configure options for event and system logs](#)

[Find and filter log file entries](#)

[Save logs to a file](#)

[Download log files](#)

[Clear logs](#)

Related commands

[clear](#)

[show log](#)

[system](#)

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.

From the web interface

1. Click **System > 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.

Related topics

[Event and system logs](#)

[Event log levels](#)

[Log viewer page](#)

[Log configuration page](#)

[Configure options for event and system logs](#)

[Display logs](#)

[Save logs to a file](#)

[Download log files](#)

[Clear logs](#)

Related commands

[clear](#)

[show log](#)

[system](#)

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 device's flash memory.

From the web interface

1. Click **System**.
2. Select **Logs**.
3. On the **System - Logs** page, click **Log Configuration**.
4.
 - 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**.
5. Click **Apply**.

From the 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
```

Related topics

[Event and system logs](#)

[Event log levels](#)

[Log viewer page](#)

[Log configuration page](#)

[Configure options for event and system logs](#)

[Display logs](#)

[Find and filter log file entries](#)

[Download log files](#)

[Clear logs](#)

[File system](#)

Related commands

[clear](#)

[show log](#)

[system](#)

Download log files

From the web interface

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 Management** download function. See [Upload and download files](#).

1. On the menu, click **System > 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.

From the command line

See [Upload and download files](#).

- To download the event log, download file **event.log**.
- To download the system log, download file **system.log**.

Related topics

[Event and system logs](#)

[Event log levels](#)

[Log viewer page](#)

[Log configuration page](#)

[Configure options for event and system logs](#)

[Display logs](#)

[Find and filter log file entries](#)

[Save logs to a file](#)

[Clear logs](#)

[Upload and download files](#)

Related commands

[clear](#)

[show log](#)

[system](#)

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.

From the command line

To clear the event log, use the **clear log** command. For example:

```
digirouter> clear log
```

To clear the system log, use the **clear log system** command. For example:

```
digirouter> clear log system
```

Related topics

[Event and system logs](#)

[Event log levels](#)

[Log viewer page](#)

[Log configuration page](#)

[Configure options for event and system logs](#)

[Display logs](#)

[Find and filter log file entries](#)

[Save logs to a file](#)

[Download log files](#)

[File system](#)

Related commands

[clear](#)

[show log](#)

[system](#)

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

Column	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 .

Related topics

[Event and system logs](#)

[Event log levels](#)

[Log configuration page](#)

[Configure options for event and system logs](#)

- Display logs
- Find and filter log file entries
- Save logs to a file
- Download log files
- Clear logs

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.

Related topics

[Event and system logs](#)

[Event log levels](#)

[Log viewer page](#)

[Configure options for event and system logs](#)

[Display logs](#)

[Find and filter log file entries](#)

[Save logs to a file](#)

[Download log files](#)

[Clear logs](#)

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. For each server, configure the following 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 .

Related topics

[Event and system logs](#)

[Event log levels](#)

[Log viewer page](#)

[Configure options for event and system logs](#)

[Display logs](#)

[Find and filter log file entries](#)

[Save logs to a file](#)

[Download log files](#)

[Clear logs](#)

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](#).

Related topics

[Event and system logs](#)

[Log viewer page](#)

[Log configuration page](#)

[Configure options for event and system logs](#)

[Display logs](#)

[Find and filter log file entries](#)

[Save logs to a file](#)

[Download log files](#)

[Clear logs](#)

Related commands

[clear](#)

[show log](#)

[system](#)

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.



Related topics

[Capture data traffic](#)

[Example filters for capturing data traffic](#)

[Show captured data traffic](#)

[Clear captured data traffic](#)

[Save captured data traffic to a file](#)

Related commands

[analyzer](#)

[clear](#)

[show analyzer](#)

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.



From the command line

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>
```

Related topics

[Analyze traffic](#)

[Example filters for capturing data traffic](#)

[Show captured data traffic](#)

[Clear captured data traffic](#)

[Save captured data traffic to a file](#)

Related commands

[analyzer](#)

[clear](#)

[show analyzer](#)

Example filters for capturing data traffic

To filter captured data, use the **analyzer** command's filter parameter. For example:

```
digi.router> analyzer filter ip host 192.168.1.1
```

Following are examples of the syntax for 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
```

Related topics

For more information on filtering, see <http://www.tcpdump.org/manpages/pcap-filter.7.html>

[Analyze traffic](#)

[Capture data traffic](#)

[Show captured data traffic](#)

[Clear captured data traffic](#)

[Save captured data traffic to a file](#)

Related commands

[analyzer](#)

[clear](#)

[show analyzer](#)

Show captured data traffic

From the command line

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  qrstuvw abcdefghi

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  qrstuvw bcdefghi

```

dig1.router>

Related topics

[Analyze traffic](#)

[Capture data traffic](#)

[Example filters for capturing data traffic](#)

[Clear captured data traffic](#)

[Save captured data traffic to a file](#)

Related commands

[analyzer](#)

[clear](#)

[show analyzer](#)

Clear captured data traffic

To clear the captured data traffic, use the [clear](#) command, specifying **clear analyzer**.

```
digi.router> clear analyzer  
digi.router>
```

Related topics[Analyze traffic](#)[Capture data traffic](#)[Show captured data traffic](#)[Save captured data traffic to a file](#)**Related commands**[analyzer](#)[clear](#)[show analyzer](#)

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.

From the command line

Use the **show analyzer <filename>** command. For example:

```
digi.router> save analyzer lan1.pcapng  
digi.router>
```

Related topics[Analyze traffic](#)[Capture data traffic](#)[Show captured data traffic](#)[Clear captured data traffic](#)[File system](#)**Related commands**[analyzer](#)[clear](#)[show analyzer](#)

Use the "ping" command to troubleshoot network connections

Use the [ping](#) command from the command line or web interface Device Console to help 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
```

Related topics

[Use the "traceroute" command to diagnose IP routing problems](#)

[Use the "show tech-support" command](#)

[Diagnostics](#)

[Troubleshooting](#)

[Execute a command from the web interface](#)

Related commands

[ping](#)

[traceroute](#)

Use the "traceroute" command to diagnose IP routing problems

Use the **traceroute** command from the command line or web interface Device Console 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 LR 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 LR device.
- 2. **192.168.8.1**: 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**.

Related topics

[Use the "ping" command to troubleshoot network connections](#)

[Use the "show tech-support" command](#)

[Diagnostics](#)

[Troubleshooting](#)

[Execute a command from the web interface](#)

Related commands

[ping](#)

[traceroute](#)

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:

```
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 tech-support**

In the output, each executed command's output is prefixed with the command's name; for example:

```
show system  
=====
```

Related topics

[Diagnostics](#)

[Use the "ping" command to troubleshoot network connections](#)

[Use the "traceroute" command to diagnose IP routing problems](#)

[Troubleshooting](#)

[Execute a command from the web interface](#)

Related commands

[show tech-support](#)

File system

The TransPort LR 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.

For information on managing configuration files, see [Managing configuration files](#) in [System administration](#).

You can manage the file system from the web interface or the command line. Common operations for directories and files include:

File management page	215
Create a directory	217
Display directory contents	219
Change the current directory	220
Delete a directory	222
Display file contents	224
Copy a file	225
Rename a file	227
Delete a file	229
Upload and download files	231

File management page

Use the **File management** page to display and manage the files and directories in the local file system of your TransPort LR device.

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 LR 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 LR 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.

Related topics

[File system](#)

[Create a directory](#)

[Display directory contents](#)

- Change the current directory
- Delete a directory
- Display file contents
- Copy a file
- Rename a file
- Delete a file
- Upload and download files

Create a directory

From the web interface

1. Click **System**.
2. Click **File Management**. The **System - File Management** page displays.
3. Navigate to the file system location where you want to create a directory and click . The **New Directory** dialog displays.
4. 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.
 - If you enter an invalid character for a directory name, an error message displays.
 - If you try to create a directory that already exists, an error message displays.

From the command line

To make a new directory, use the `mkdir` command, specifying the name of the directory.

For example:

```
dig1.router> mkdir test
dig1.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

```
dig1.router>
```

Related topics

[File system](#)

[File management page](#)

[Create a directory](#)

[Display directory contents](#)

[Change the current directory](#)

[Delete a directory](#)

[Display file contents](#)

[Copy a file](#)

[Rename a file](#)

[Delete a file](#)

[Upload and download files](#)

Related commands

[mkdir](#)

Display directory contents

From the web interface

1. Click **System**.
2. Select **File Management**. The **System - File Management** page appears.
3. Double-click the directory row to navigate to a sub-directory and display contents.

From the 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>
```

Related topics

[File system](#)

[File management page](#)

[Create a directory](#)

[Change the current directory](#)

[Delete a directory](#)

[Display file contents](#)

[Copy a file](#)

[Rename a file](#)

[Delete a file](#)

[Upload and download files](#)

Related commands

[dir](#)

Change the current directory

From the web interface

1. Click  **System**.
2. Select **File Management**. The **System - File Management** page appears.
3. Navigate to the desired directory or subdirectory.
4. To return to the home directory, click .

From the 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>
```

Related topics

[File system](#)

[File management page](#)

[Create a directory](#)

[Display directory contents](#)

[Delete a directory](#)

[Display file contents](#)

[Copy a file](#)

[Rename a file](#)

[Delete a file](#)

[Upload and download files](#)

Related commands

[cd](#)

Delete a directory

From the web interface

1. Click  **System**.
2. Select **File Management**. The **System - File Management** page appears.
3. Select the directory to delete.
4. Click . A warning dialog displays.
5. Click **OK**.

Note This operation deletes any files in the directory along with the directory.

From the 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>

Related topics[File system](#)[File management page](#)[Create a directory](#)[Display directory contents](#)[Change the current directory](#)[Display file contents](#)[Copy a file](#)[Rename a file](#)[Delete a file](#)[Upload and download files](#)**Related commands**[rmdir](#)

Display file contents

From the web interface

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. Click  **System**.
2. Select **File Management**. The **System - File Management** page appears.
3. Select the file.
4. Click .
5. When the file is downloaded, open it with the desired file editor.

From the 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>
```

Related topics

[File system](#)
[File management page](#)
[Create a directory](#)
[Display directory contents](#)
[Change the current directory](#)
[Delete a directory](#)
[Rename a file](#)
[Delete a file](#)
[Upload and download files](#)

Related commands

[more](#)

Copy a file

From the web interface

The copy file operation is not available from the **System - File Management** page.

From the command line

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>
```

Related topics

- [File system](#)
- [File management page](#)
- [Create a directory](#)
- [Display directory contents](#)
- [Change the current directory](#)
- [Delete a directory](#)
- [Display file contents](#)
- [Rename a file](#)
- [Delete a file](#)
- [Upload and download files](#)

Related commands

[copy](#)

Rename a file

From the web interface

1. Click  **System**.
2. Click **File Management**. The **System - File Management** page appears.
3. Select the file to rename. Navigate to the file's directory location, if necessary.
4. Click . Enter the new file name.
5. Click **OK**.

From the 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>
```

Related topics

[File system](#)

[File management page](#)

[Create a directory](#)

[Display directory contents](#)

[Change the current directory](#)

[Delete a directory](#)

[Display file contents](#)

[Copy a file](#)

[Delete a file](#)

[Upload and download files](#)

Related commands

[rename](#)

Delete a file

From the web interface

1. Click  **System**.
2. Click **File Management**. The **System - File Management** page appears.
3. Select or navigate to the file to delete.
4. Click . A confirm delete dialog displays.
5. Click **OK**.

Note To delete all files in a directory, see [Delete a directory](#).

From the 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>
```

Related topics

[File system](#)

[File management page](#)

[Create a directory](#)

[Display directory contents](#)

[Change the current directory](#)

[Delete a directory](#)

[Display file contents](#)

[Copy a file](#)

[Rename a file](#)

[Upload and download files](#)

Related commands

[del](#)

Upload and download files

From the web interface

Upload files

1. Click  **System**.
2. Select **File Management**. The **System - File Management** page displays the local file system for the TransPort LR device.
3. Click .
4. 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.
5. A progress dialog appears. When the upload operation is complete, the file is displayed in the file list.

Download files

1. Click  **System**.
2. Select **File Management**. The **System - File Management** page displays the local file system for the TransPort LR device.
3. 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**.
4. Click . The file downloads to your system using your browser's download settings.

From the command line

You can download and upload files from and to a TransPort LR device, 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, the syntax is:

```
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, the syntax is:

```
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 LR 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
$
```

Related topics

[File system](#)

[File management page](#)

[Create a directory](#)

[Display directory contents](#)

[Change the current directory](#)

[Delete a directory](#)

[Display file contents](#)

[Copy a file](#)

[Rename a file](#)

[Delete a file](#)

Troubleshooting

Troubleshooting tools and resources	235
Troubleshooting Ethernet interfaces	236
Troubleshooting cellular interfaces	245
Troubleshooting the serial interface	250
TransPort LR54 model-specific troubleshooting	255

Troubleshooting tools and resources

There are several tools and resources available within your TransPort LR device and on Digi's website for dealing with configuration or other device issues.

[Event and system 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 LR 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 LR 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 LR device's hardware. Contact [Digi Technical Support](#).

Related topics

[TransPort LR54 LEDs](#)

[Device cannot communicate on WAN/ETH1 port](#)

[Device cannot communicate on ETH2, ETH3, or ETH4 ports](#)

[Ethernet interfaces](#)

[Configure Ethernet interfaces](#)

[Show Ethernet status and statistics](#)

Related commands

[eth](#)
[show eth](#)

Device cannot communicate on WAN/ETH1 port

Problem

The TransPort LR 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 LR 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](#).

Related topics

[TransPort LR54 LEDs](#)

[Ethernet LED does not illuminate](#)

[Device cannot communicate on ETH2, ETH3, or ETH4 ports](#)

[Ethernet interfaces](#)

[Configure Ethernet interfaces](#)

[Show Ethernet status and statistics](#)

Related commands

[eth](#)
[show eth](#)

Device cannot communicate on ETH2, ETH3, or ETH4 ports

Problem

The TransPort LR 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-PJAC01	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](#).

Related topics

[TransPort LR54 LEDs](#)

[Ethernet LED does not illuminate](#)
[Device cannot communicate on WAN/ETH1 port](#)
[Ethernet interfaces](#)
[Configure Ethernet interfaces](#)
[Show Ethernet status and statistics](#)
[Local Area Networks \(LANs\)](#)
[Configure a LAN](#)
[DHCP servers](#)

Related commands

[dhcp-server](#)
[lan](#)
[show dhcp](#)

Troubleshooting cellular interfaces

[Verify cellular connectivity](#)

[Check cellular signal strength](#)

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 LR device.
2. Access the TransPort LR 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 LR 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 LR 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 LR device that contains the same type of radio module in the same location. Make sure this known working TransPort LR 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**.

Related topic

[TransPort LR54 LEDs](#)

[Signal strength for 4G cellular connections](#)

[Signal strength for 3G and 2G cellular connections](#)

[Tips for improving cellular signal strength](#)

[Show cellular status and statistics](#)

Related commands

[show cellular](#)

Troubleshooting the serial interface

[Verify serial connectivity](#)

Verify serial connectivity

Problem

When using the command line interface, command output displays unusual or garbled characters.

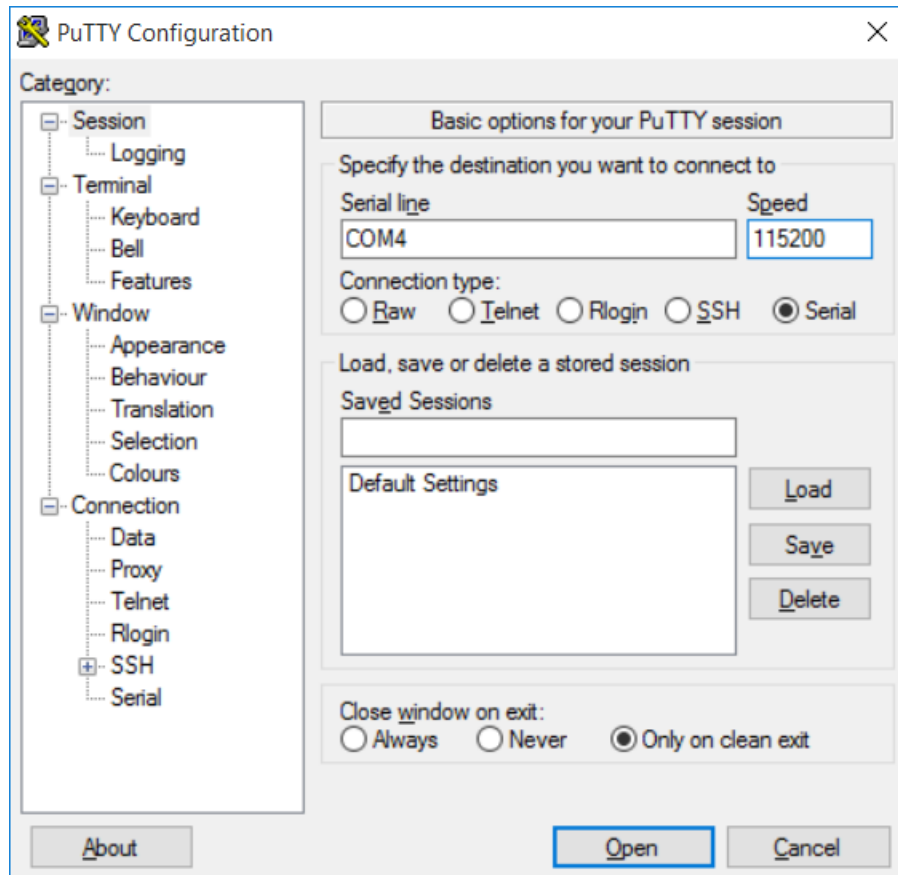
Probable causes

- 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

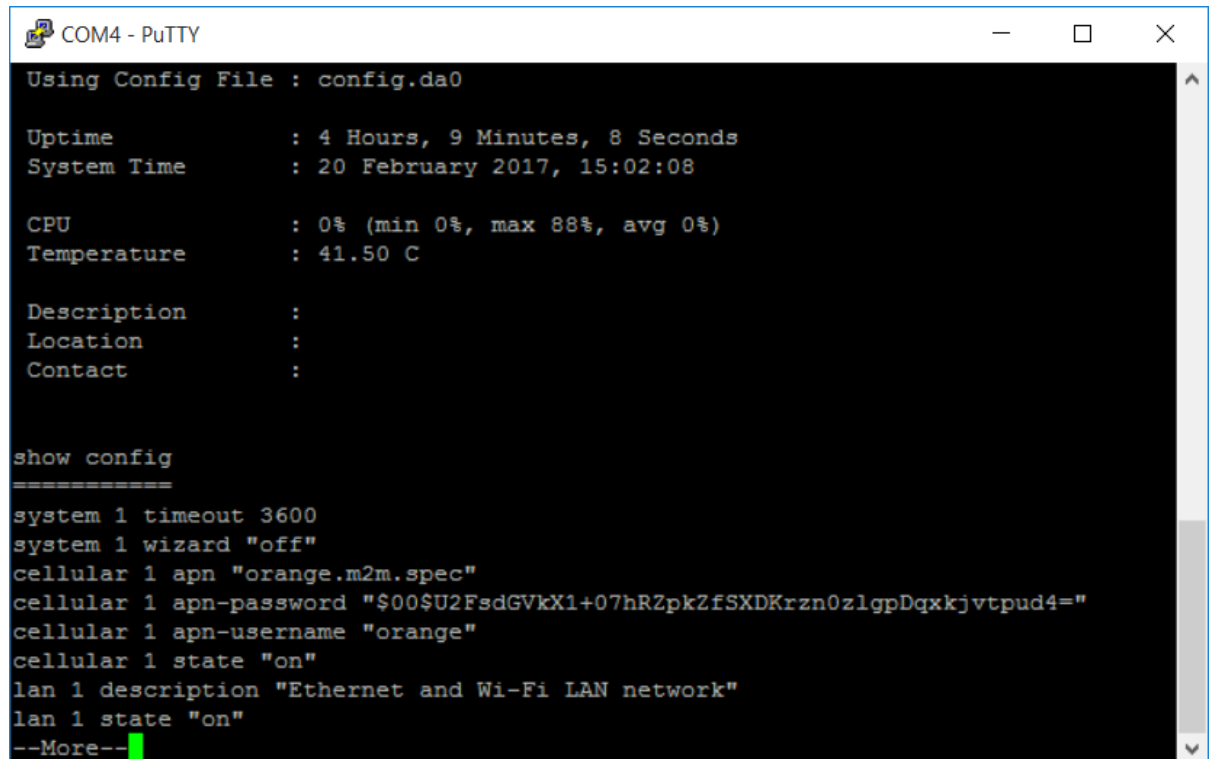
Test the serial connection.

1. Using a straight-through serial cable, connect a PC serial port to the TransPort LR device. For pinout details, see [Serial connector pinout](#).
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](#):



```

COM4 - PuTTY
Using Config File : config.da0

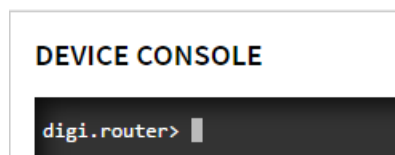
Uptime           : 4 Hours, 9 Minutes, 8 Seconds
System Time      : 20 February 2017, 15:02:08

CPU              : 0% (min 0%, max 88%, avg 0%)
Temperature      : 41.50 C

Description      :
Location         :
Contact          :

show config
=====
system 1 timeout 3600
system 1 wizard "off"
cellular 1 apn "orange.m2m.spec"
cellular 1 apn-password "$00$U2FsdGVkX1+07hRZpkZfSXDkrzn0zlgpDqxxkjtvpud4="
cellular 1 apn-username "orange"
cellular 1 state "on"
lan 1 description "Ethernet and Wi-Fi LAN network"
lan 1 state "on"
--More--
  
```

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 LR device's 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 LR 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**.

Related topics

[Log in to the web interface](#)

[Execute a command from the web interface](#)

[Serial interface](#)

[Configure the serial interface](#)

[Show serial status and statistics](#)

[Serial specifications](#)

[Serial connector pinout](#)

Related commands

[serial](#)

[show serial](#)

TransPort LR54 model-specific troubleshooting

The following topics apply to TransPort LR54 models only.

[Check TransPort LR54 LEDs](#)

[Recover a TransPort LR54 device](#)

Check TransPort LR54 LEDs

To check that all LEDs are working properly, set the device into recovery mode. See [Recover a TransPort LR54 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.

Related topics

[TransPort LR54 LEDs](#)

Recover a TransPort LR54 device

If other troubleshooting steps do not resolve issues you are experiencing with your TransPort LR54 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 LR 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 LR 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 LR 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.



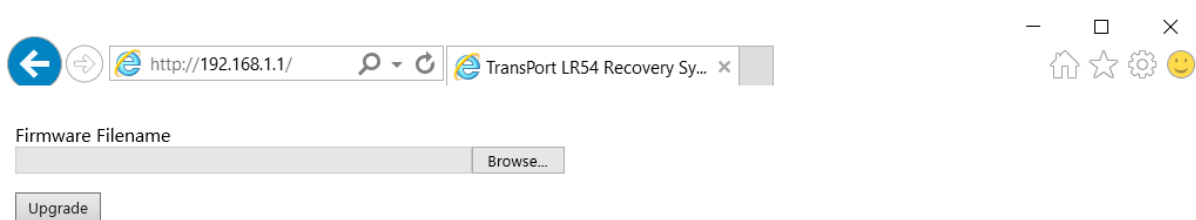
3. Press and hold the **Reset** button while connecting the power, and keep holding down the **Reset** button while the unit powers up.
4. Watch for all the LEDs on the device to blink.

- Wait for all the LEDs to turn off and the **Power** LED to be blink rapidly. The device is now in recovery mode.
- Now you can release the **Reset** button.



Upload new firmware

- Open a web browser and navigate to **http://192.168.1.1**. The TransPort LR54 Recovery System navigation window appears.



- Click the **Browse** button. Select or navigate to the previously downloaded firmware file.
- Click **Upgrade**.
- 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.



- Disconnect the power and reconnect it. The firmware has been successfully loaded on to TransPort LR54 device and is ready to use.

Related topics

[Update system firmware](#)
[Reset the device to factory defaults](#)
[Check TransPort LR54 LEDs](#)
[TransPort LR54 LEDs](#)
[Verify cellular connectivity](#)
[Check cellular signal strength](#)
[Troubleshooting Ethernet interfaces](#)

[Verify serial connectivity](#)

Command reference

These topics describe the command-line interface for TransPort LR devices and the commands entered through the command-line interface.

Command-line interface basics	263
? (Display command help)	276
! (Revert command settings)	277
analyzer	278
autorun	279
cd	280
cellular	281
clear	283
cloud	284
copy	285
date	286
del	287
dhcp-server	288
dir	289
eth	290
exit	291
firewall	292
ip	293
ip-filter	293
ipsec	296
lan	300
mkdir	302
more	303
ping	304
port-forward	304
pwd	306
reboot	307
rename	308
rmdir	309
route	310
save	311
serial	312
show analyzer	313
show cellular	314
show cloud	317
show config	318
show dhcp	319
show eth	320
show firewall	323
show ip-filter	323

show ipsec	325
show ipstats	327
show lan	329
show log	330
show port-forward	330
show route	331
show serial	332
show system	333
show tech-support	335
show wan	336
show wifi	338
show wifi5g	341
snmp	344
snmp-community	345
snmp-user	346
sntp	347
ssh	348
syslog	348
system	349
traceroute	352
unlock	353
update	354
user	356
wan	357
wifi	360
wifi5g	362
wifi-global	364

Command-line interface basics

Following are basic tasks you can perform within the command-line interface.

[Command line interface access options](#)

[Log in to the command line interface](#)

[Exit the command line interface](#)

[Execute a command from the web interface](#)

[Display command and parameter help using the ? character](#)

[Revert command settings using the ! character](#)

[Auto-complete commands and parameters](#)

[Enter configuration commands](#)

[Save configuration settings to a file](#)

[Switch between configuration files](#)

[Display status and statistics using "show" commands](#)

Command line interface access options

You can access the TransPort LR 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.

Related topics

[Log in to the command line interface](#)

[Use SSH to connect to the TransPort LR command-line interface](#)

[Execute a command from the web interface](#)

Log in to the command line interface

1. Connect to the TransPort LR 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. (For more information about access level and session command timeout, see [Related topics](#).)

```
Welcome admin
Access Level: super
Timeout      : 3600 seconds
digi.router>
```

Related topics

[Command line interface access options](#)

[User management](#)

[Use SSH to connect to the TransPort LR command-line interface](#)

Related commands

[system](#) - The **system timeout n** command changes the timeout for a command session.

Exit the command line interface

Enter the `exit` command.

Execute a command from the web interface

1. Click **System**.
2. Select **Device Console**. The Device Console displays.



3. To display the currently supported list of commands for the device, enter **?**
4. Enter the command.

Related topics

[Command-line interface basics](#)

[Command reference](#)

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.

Example

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 will lose any unsaved changes when it is next rebooted.

To save configuration settings to a file:

From the web interface

On configuration pages, clicking **Apply** saves your changes to the configuration file immediately.

From the command line

Enter the **save config** command.

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

Related topics

[Managing configuration files](#)

[Switch between configuration files](#)

[Use multiple configuration files to test configurations on remote devices](#)

[File system](#)

Related commands

[save](#)

Switch between configuration files

You can have multiple configuration files stored on the device, although the device uses only one configuration file when it reboots.

From the command line

Identify the current configuration file

If necessary, identify the current configuration file the TransPort LR device is using. Enter the [show system](#) command and note the file listed after **Using Config File:**. 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>
```

Change the configuration file name

1. Change the name of the configuration file to be used at boot-up and when the configuration is saved.

```
digi.router> update config <filename>
```

2. If the new configuration file does not exist, enter the [save](#) command to create and save the configuration file.

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

Related topics

[Managing configuration files](#)

[Save configuration settings to a file](#)

[Use multiple configuration files to test configurations on remote devices](#)

[File system](#)

Related commands

[save](#)

[show system](#)

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 starting a Python program, switching configuration files, or scheduling a reboot. You can configure up to 10 auto-run commands.

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 "python script.py"`
-

Automatically run a Python program.

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 8 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 log  
clear log system  
clear log all  
clear analyzer
```

Parameters

firewall

Clears firewall counters.

log

Clears event log.

analyzer

Clears the traffic analyzer log.

Examples

-
- `clear firewall`
-

Clear the packet and byte counters in all 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.

cloud

Configures Digi Remote Manager settings.

Syntax

```
cloud <parameter> <value>
```

Parameters

state

Enables or disables 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.

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.

gateway

The IP gateway address given to clients.

Value should be an IPv4 address.

dns1

Preferred DNS server address given to clients.

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).

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.

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 source address of the incoming packet. Use a simple IP address, or use CIDR notation (example: 192.168.100.0/24)

Accepted value is any string up to 18 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 destination address of the incoming packet. Use a simple IP address, or use CIDR notation (example: 192.168.100.0/24)

Accepted value is any string up to 18 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 or wan10. 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 or wan10. 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.

marginetime

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.

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.

ping

Sends ICMP echo (ping) packets to the specified destination address.

Syntax

```
ping [count n] [interface ifname] [size bytes] destination
```

Parameters

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 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

## 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.

## 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

## pwd

Displays the current directory name.

### Syntax

---

pwd

---

### Parameters

## 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, dsl, cellular1 or cellular2. 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.

This group is only supported in TransPort LR54, TransPort LR54W, TransPort LR54D, TransPort LR54DWC1, TransPort LR54-FIPS, TransPort LR54W-FIPS, Transport LR11, Transport LR21, Transport LR31 and Last Platform products.

### 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 modem.

#### ***firmware-version***

Manufacturer's version number for the software running on the cellular modem.

#### ***hardware-version***

Manufacturer's version number for the cellular modem hardware.

#### ***imei***

International Mobile Station Equipment Identity (IMEI) number for the cellular modem, 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 modem's connection to a cellular network.

#### ***network-provider***

Network provider for the cellular network.

**temperature**

Current temperature of the cellular modem, 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 modem is operating.

**channel**

The radio channel on which the cellular modem 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 modem during the current data session.

**tx-packets**

Number of packets transmitted by the cellular modem during the current data session.

**rx-bytes**

Number of bytes received by the cellular modem during the current data session.

**tx-bytes**

Number of bytes transmitted by the cellular modem during the current data session.

***attachment-status***

The status of the cellular modem'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 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

#### ***config***

The current firewall running on the device.

## 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.

#### ***mask***

Subnet mask for the LAN.

#### ***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.

## show log

Displays log(event or system/kernel).

### Parameters

#### ***system***

Display the system/kernel log.

## 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.

## 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.

This group is only supported in TransPort LR54, TransPort LR54W, TransPort LR54D, TransPort LR54DWC1, TransPort LR54-FIPS, TransPort LR54W-FIPS, Transport LR11, Transport LR21, Transport LR31 and Last Platform products.

### 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.

***temperature***

The current temperature of the device.

***core-temperature***

The current temperature of the CPU core.

***description***

Description for this device.

***location***

Location details for this device.

***contact***

Contact information for this device.

## 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 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***

Seconds since we received the last probe response, or -1 if probes are disabled, or -2 if we have not received any yet.

## show wifi

Displays status and statistics for a Wi-Fi 2.4 GHz interface.

This group is only supported in TransPort LR54, TransPort LR54W, TransPort LR54D, TransPort LR54DWC1, TransPort LR54-FIPS, TransPort LR54W-FIPS, Transport LR11, Transport LR21, Transport LR31 and Last Platform products.

### 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.

This group is only supported in TransPort LR54, TransPort LR54W, TransPort LR54D, TransPort LR54DWC1, TransPort LR54-FIPS, TransPort LR54W-FIPS, Transport LR11, Transport LR21, Transport LR31 and Last Platform products.

### 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.

## 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 the command-line interface times out if there is no activity.

Accepted value is any integer from 60 to 3600. The default value is 180.

#### ***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, the cellular module firmware, and the DSL modem 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 dsl <dsl-file>
update config <configuration-file>
update carrier <carrier-name>
```

---

### Parameters

#### ***firmware***

Updates the device system firmware.

#### ***modem***

Updates the cellular modem firmware.

#### ***dsl***

Updates the DSL modem 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 modem firmware update process. This process retrieves image files from Digi International site and downloads the images to the modem.

- 
- `update modem ./modem_fw`
- 

Initiate the cellular modem firmware update process. This process uploads firmware files from the directory `./modem_fw` to the cellular modem.

- 
- `update modem verizon`
- 

Initiate the cellular modem firmware update process. This process retrieves firmware files from the Digi repository of cellular modem firmware files and uploads the images to the modem.

- 
- `update dsl filename`
- 

Initiates the DSL modem firmware update process.

- 
- `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.

### 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.

## wan

Configures a Wide Area Network (WAN). The physical communications interface for the WAN can be an Ethernet, DSL, 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, dsl, 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 primary DNS server. This value overrides the value assigned by DHCP.

Value should be an IPv4 address.

***dns2***

The IPv4 address of the secondary DNS server used if the device cannot communicate with the primary 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.

## wifi

Configures a Wi-Fi 2.4 GHz interface.

This group is only supported in TransPort LR54, TransPort LR54W, TransPort LR54D, TransPort LR54DWC1, TransPort LR54-FIPS, TransPort LR54W-FIPS, TransPort LR11, TransPort LR21, TransPort LR31 and Last Platform products.

### 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 64 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.

This group is only supported in TransPort LR54, TransPort LR54W, TransPort LR54D, TransPort LR54DWC1, TransPort LR54-FIPS, TransPort LR54W-FIPS, TransPort LR11, TransPort LR21, TransPort LR31 and Last Platform products.

### 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 64 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.

This group is only supported in TransPort LR54, TransPort LR54W, TransPort LR54D, TransPort LR54DWC1, TransPort LR54-FIPS, TransPort LR54W-FIPS, Transport LR11, Transport LR21, Transport LR31 and Last Platform products.

## 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.

## Advanced topics

This section provides details on advanced topics for expert users who may need to fine-tune Transport LR features.

|                                           |     |
|-------------------------------------------|-----|
| Using the firewall command .....          | 365 |
| Understanding system firewall rules ..... | 383 |

## Using the firewall command

The TransPort LR 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 directly manage firewalls using the [firewall](#) command or you can manage firewall rules using built-in TransPort LR features, such as port forwarding and IP filters.

This section describes how to manage firewalls using the [firewall](#) command. For details on how to manage firewalls using built-in TransPort LR features, see [Understanding system firewall rules](#).

### Firewall design is based on iptables

The TransPort LR firewall is based on the open-source firewall named **iptables**. It uses the same syntax as **iptables**, except the rules start with the keyword **firewall** instead of **iptables**. The firewall syntax is case-sensitive.

For more information on configuring the firewall, see [www.netfilter.org/documentation](http://www.netfilter.org/documentation) and [IptablesHowTo](#).

---

**Note** TransPort LR 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 TransPort LR features are configured. For example, when you use port forwarding, the TransPort LR adds system firewall rules based on your port forwarding rules. Take care when directly modifying firewall rules. 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 LR 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 LR 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 LR 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 LR 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 LR 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 LR 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.

## Related topics

[Default firewall configuration](#)

[Allow SSH access on a WAN](#)

[Allow SSH access for only a specific source IP address](#)

[Allow HTTPS access on a WAN](#)

[Allow HTTPS access on a WAN from only a specific source IP address](#)

[Add a firewall rule](#)

[Update a firewall rule](#)

[Delete a firewall rule](#)

[Show firewall rules and counters](#)

[Understanding system firewall rules](#)

For more information on configuring the firewall, see [www.netfilter.org/documentation](http://www.netfilter.org/documentation) and [IptablesHowTo](#).

### **Related commands**

[firewall](#)

[show firewall](#)

## 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 Device Console.
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. Enter the **save config** command to save the new setting to the configuration file.

### Related topics

[Log in to the command line interface](#)

[Allow HTTPS access on a WAN](#)

[Allow HTTPS access on a WAN from only a specific source IP address](#)

[Configure a Wide Area Network \(WAN\)](#)

### Related commands

[wan](#)

[ip-filter](#)

[save](#)

[ssh](#)

## 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 Device Console.
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. Enter the **save config** command to save the new setting to the configuration file.

### **Related topics**

[Log in to the command line interface](#)

[Allow HTTPS access on a WAN](#)

[Allow HTTPS access on a WAN from only a specific source IP address](#)

[Configure a Wide Area Network \(WAN\)](#)

### **Related commands**

[wan](#)

[ip-filter](#)

[save](#)

[ssh](#)

## 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 Device Console.
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**:

---

```
digirouter> wan 1 allow-https-access on
```

---

3. Enter the **save config** command to save the new setting to the configuration file.

### Related topics

[Log in to the command line interface](#)

[Allow SSH access on a WAN](#)

[Allow SSH access for only a specific source IP address](#)

[Allow HTTPS access on a WAN](#)

[Allow HTTPS access on a WAN from only a specific source IP address](#)

[Allow SSH access for only a specific source IP address](#)

[Configure a Wide Area Network \(WAN\)](#)

### Related commands

[wan](#)

[ip-filter](#)

[save](#)

## 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 Device Console.
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. Enter the **save config** command to save the new setting to the configuration file.

#### Related topics

[Log in to the command line interface](#)

[Allow HTTPS access on a WAN](#)

[Allow SSH access on a WAN](#)

[Allow SSH access for only a specific source IP address](#)

[Configure a Wide Area Network \(WAN\)](#)

#### Related commands

[wan](#)

[ip-filter](#)

[save](#)

## 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 LR 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](#) command **-A** option, using the following syntax. The [firewall](#) 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, use the [firewall](#) 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>
```

**Related topics**

- [Using the firewall command](#)
- [Default firewall configuration](#)
- [Allow SSH access on a WAN](#)
- [Allow SSH access for only a specific source IP address](#)
- [Allow HTTPS access on a WAN](#)
- [Allow HTTPS access on a WAN from only a specific source IP address](#)
- [Update a firewall rule](#)
- [Delete a firewall rule](#)
- [Show firewall rules and counters](#)

### [Understanding system firewall rules](#)

For more information on configuring the firewall, see [www.netfilter.org/documentation](http://www.netfilter.org/documentation) and [IptablesHowTo](#).

#### **Related commands**

[firewall](#)

[show firewall](#)

## 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 LR components. See [Understanding system firewall rules](#) for details.

To update a firewall rule, use the [firewall](#) 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**.

```
digirouter> 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 is:

```
digirouter> 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

digirouter>
```

### Related topics

- [Using the firewall command](#)
- [Default firewall configuration](#)
- [Allow SSH access on a WAN](#)
- [Allow SSH access for only a specific source IP address](#)
- [Allow HTTPS access on a WAN](#)
- [Allow HTTPS access on a WAN from only a specific source IP address](#)
- [Add a firewall rule](#)

[Delete a firewall rule](#)

[Show firewall rules and counters](#)

[Understanding system firewall rules](#)

For more information on configuring the firewall, see [www.netfilter.org/documentation](http://www.netfilter.org/documentation) and [IptablesHowTo](#).

#### **Related commands**

[firewall](#)

[show firewall](#)

## 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 LR components. See [Understanding system firewall rules](#) for details.

To delete a firewall rule, use the [firewall](#) 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](#) command's **-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.

### Related topics

[Using the firewall command](#)

[Default firewall configuration](#)

[Allow SSH access on a WAN](#)

[Allow SSH access for only a specific source IP address](#)

[Allow HTTPS access on a WAN](#)

[Allow HTTPS access on a WAN from only a specific source IP address](#)

[Add a firewall rule](#)

[Update a firewall rule](#)

[Show firewall rules and counters](#)

[Understanding system firewall rules](#)

For more information on configuring the firewall, see [www.netfilter.org/documentation](http://www.netfilter.org/documentation) and [IptablesHowTo](#).

**Related commands**

[firewall](#)

[show firewall](#)

## Show firewall rules and counters

To display all firewall rules and counters, use the [show firewall](#) 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` 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 | 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** command.

```
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 tcp dpt:22
2 23 1380 DROP icmp -- lan1 any 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 tcp dpt:22
2 0 0 DROP icmp -- lan1 any 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>
```

**Related topics**

- [Using the firewall command](#)
- [Default firewall configuration](#)
- [Allow SSH access on a WAN](#)
- [Allow SSH access for only a specific source IP address](#)
- [Allow HTTPS access on a WAN](#)
- [Allow HTTPS access on a WAN from only a specific source IP address](#)
- [Add a firewall rule](#)
- [Update a firewall rule](#)
- [Delete a firewall rule](#)
  
- [Understanding system firewall rules](#)

For more information on configuring the firewall, see [www.netfilter.org/documentation](http://www.netfilter.org/documentation) and [IptablesHowTo](#).

**Related commands**

[clear](#) - the **clear firewall** command variant

[firewall](#)

[show firewall](#)

## Understanding system firewall rules

You can explicitly create and manage firewall rules using the `firewall` command. This section explains how TransPort LR built-in components automatically create and apply system firewall rules transparently when you configure system components.

### Who should read this section

If you do not use the `firewall` command or you use the command only to create simple firewall rules that allow greater access to device features, you can skip this section.

If you use the `firewall` command to create or manage firewall rules on your TransPort LR device, you should read this section to understand how Transport LR components automatically create and manage system firewall rules and how all firewall rules are saved and applied.

### What are system firewall rules?

System firewall rules are automatically created and managed when you configure various Transport LR 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 LR device starts and anytime you configure a Transport LR 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
```

The Transport LR automatically creates a new system firewall rule in the `tlr_wan_input` section of the `iptables` chain. See [Using the firewall command](#) 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 rules

When you create or modify firewall rules using the `firewall` command, save the new rules using the `save config` command and then reboot the Transport LR 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 rules.

## Using the autorun command to force 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**.

```
digirouter> 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](#) command. 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 LR **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 LR 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 LR 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.

### Related topics

- [Using the firewall command](#)
- [Default firewall configuration](#)
- [Allow SSH access on a WAN](#)
- [Allow SSH access for only a specific source IP address](#)
- [Allow HTTPS access on a WAN](#)
- [Allow HTTPS access on a WAN from only a specific source IP address](#)
- [Add a firewall rule](#)

[Update a firewall rule](#)

[Delete a firewall rule](#)

Save firewall rules

[Show firewall rules and counters](#)

For more information on configuring the firewall, see [www.netfilter.org/documentation](http://www.netfilter.org/documentation) and [IptablesHowTo](#).

### ***Related commands***

[firewall](#)

[show firewall](#)

[wan](#)