



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.

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.

© 2016 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:

<http://www.digi.com/howtobuy/terms>

Send comments

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

Customer support

Digi Technical Support: Digi offers multiple technical support plans and service packages to help our customers get the most out of their Digi product. For information on Technical Support plans and pricing, contact us at 877.912.3444 or visit us at www.digi.com/support.

Online: www.digi.com/support/eservice

Contents

TransPort LR Family User Guide

Hardware

TransPort LR54 hardware and specifications	10
Environmental specifications	12
Mounting options	13
Power requirements	15
Dimensions and weight	16
Ethernet specifications	17
Cellular specifications	18
Wi-Fi specifications	19
Serial specifications	20
Serial connector pinout	21
Processor, memory, and development specifications	22
Internal sensors	23
TransPort LR54 LEDs	24
Regulatory and safety statements	27
Certifications	32

Management and status

Managing devices from the web interface	34
Managing devices from the command line	36
Interfaces	37
Ethernet interfaces	38
Cellular interfaces	44
Wi-Fi interfaces	53
Serial interface	65
Local Area Networks (LANs)	68
Example LAN	68
Configure a LAN	69
Show LAN status and statistics	71
DHCP servers	72
Wide Area Networks (WANs)	75
WAN interface priority, default routes, and metrics	75
Using Ethernet interfaces in a WAN	75
Using cellular interfaces in a WAN	75
WAN failover	75
Configure a WAN interface	78
Example WAN failover: Ethernet to cellular	81
Show WAN status and statistics	83
Security	86
User management	87

Firewall	92
Services and applications	106
Auto-run commands	107
SSH server	108
Remote management	112
Digi Remote Manager	113
Simple Network Management Protocol (SNMP)	117
Routing	121
IP routing	122
Virtual Private Networks (VPN)	128
IPsec	129
System administration and management	140
Configure system settings	141
Show system information settings	144
Set system date and time	145
Show system date and time	147
Updating firmware	148
Managing configuration files	154
Reboot the device	160
Reset the device to factory defaults	161
Diagnostics	162
Using event and system logs	163
Use the "ping" command to troubleshoot network connections	169

File system

Make a directory	171
Display directory contents	172
Change the current directory	173
Remove a directory	174
Display file contents	176
Copy a file	177
Rename a file	179
Delete a file	180
Upload and download files	181
Upload files using SCP	181
Download files using SCP	181
Upload files using SFTP	181
Download files using SFTP	181

Command reference

Command-line interface basics	185
Command line interface access options	186
Log in to the command line interface	187
Exit the command line interface	188
Display command and parameter help using the ? character	189
Revert command settings using the ! character	190
Auto-complete commands and parameters	191
Enter configuration commands	192
Save configuration settings to a file	193
Switch between configuration files	194
Display status and statistics using "show" commands	196
Execute a command from the web interface	197

? (Display command help)	198
! (Revert command settings)	199
autorun	200
Syntax	200
Parameters	200
Examples	200
cd	201
Syntax	201
Parameters	201
cellular	202
Syntax	202
Parameters	202
Examples	203
clear	204
Syntax	204
Parameters	204
Examples	204
cloud	205
Syntax	205
Parameters	205
copy	206
Syntax	206
Parameters	206
date	207
Syntax	207
Parameters	207
Examples	207
del	208
Syntax	208
Parameters	208
dhcp-server	209
Syntax	209
Parameters	209
dir	210
Syntax	210
Parameters	210
eth	211
Syntax	211
Parameters	211
Examples	211
exit	213
Syntax	213
firewall	214
Syntax	214
Parameters	214
ip	215
Syntax	215
Parameters	215
ipsec	216
Syntax	216
Parameters	216
Examples	219
lan	220
Syntax	220
Parameters	220

mkdir	222
Syntax	222
Parameters	222
more	223
Syntax	223
Parameters	223
ping	224
Syntax	224
Parameters	224
Examples	224
pwd	225
Syntax	225
Parameters	225
reboot	226
Syntax	226
Parameters	226
rename	227
Syntax	227
Parameters	227
rmdir	228
Syntax	228
Parameters	228
route	229
Syntax	229
Parameters	229
save	230
Syntax	230
Parameters	230
Examples	230
serial	231
Syntax	231
Parameters	231
show cellular	232
Parameters	232
show cloud	235
Parameters	235
show config	236
Parameters	236
show eth	237
Parameters	237
show firewall	240
Parameters	240
show ipsec	241
Parameters	241
show ipstats	243
Parameters	243
show lan	245
Parameters	245
show log	246
Parameters	246
show route	247
Parameters	247
show serial	248
Parameters	248
show system	249

Parameters	249
show wan	251
Parameters	251
show wifi	253
Parameters	253
show wifi5g	256
Parameters	256
snmp	259
Syntax	259
Parameters	259
Examples	259
snmp-community	260
Syntax	260
Parameters	260
Examples	260
snmp-user	261
Syntax	261
Parameters	261
sntp	262
Syntax	262
Parameters	262
ssh	263
Syntax	263
Parameters	263
system	264
Syntax	264
Parameters	264
update	266
Syntax	266
Parameters	266
Examples	266
user	268
Syntax	268
Parameters	268
wan	269
Syntax	269
Parameters	269
wifi	271
Syntax	271
Parameters	271
wifi5g	273
Syntax	273
Parameters	273
wifi-global	275
Syntax	275
Parameters	275

TransPort LR Family User Guide

The TransPort LR Family is a family of routers designed for connecting distributed retail terminals (signs, kiosks, vending machines, point-of-care terminals) with business applications. Key features of TransPort LR routers include:

- High-speed CAT6 LTE
- Dual SIM cellular interfaces, providing redundancy
- Powerful 802.11ac Wi-Fi
- 4-port Gigabit Ethernet
- Automated Wide-Area Network (WAN) failover/failback
- Extended operating temperature
- Local command-line and web interfaces
- Superior network performance management through Digi Remote Manager (DRM)
- Global deployment support



Hardware

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

TransPort LR54 hardware and specifications	10
--	----

TransPort LR54 hardware and specifications



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

9. **Reset button.** See [Reset the device to factory defaults.](#)
10. **Internal temperature sensor.** See [Internal sensors.](#)

Environmental specifications

Specification	Value
Operating temperature	-20 C to +70 C (-4 F to 158 F)*  *Note: If you are installing this device above +60 C , it should be installed in a Restricted Access Location, to limit unintentional contact with hot surfaces.
Relative humidity	10% to 90% RH non-condensing
Storage and transport temperature	-40 C to 85 C (-40 F to 185 F)
Enclosure IP rating	IP30

Mounting options

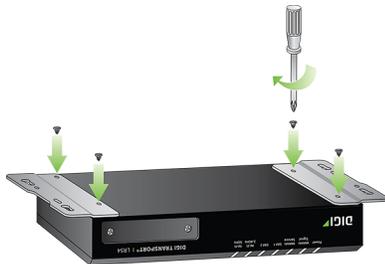
The TransPort LR54 Wall-Mount Kit (part number **78000001**) is available separately for wall-mounting. It contains two mounting brackets and four screws. You will need to supply additional self-tapping screws and sleeve anchors as needed.

Attach mounting brackets to the device

1. Remove the four rubber feet from the bottom of the TransPort LR54.

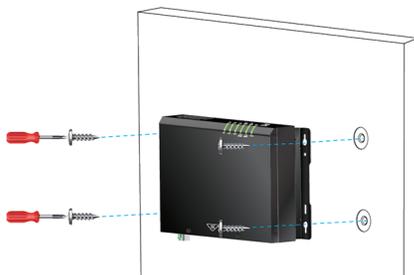


2. Using the four supplied M3x6mm screws, attach the mounting brackets.



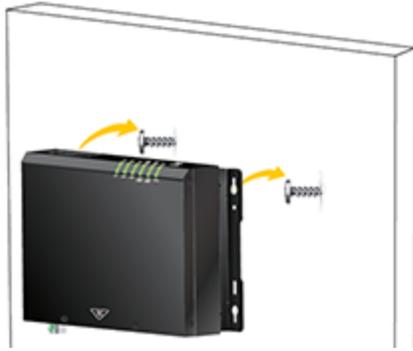
Mount the TransPort LR54 on a wall

1. Align the TransPort LR54 on wall.
2. Tighten self-tapping screws to wall through holes of mounting brackets. If mounting the device on a concrete wall, use sleeve anchors.



Hang the TransPort LR54 on a wall

Tighten two self-tapping screws to wall, but leave a small part of screw protruding from the wall. To hang the TransPort LR54 on the wall, center the holes of the mounting brackets on the two wall-mounted screws.



Power requirements

Specification	Value
Power input type	DC
Voltage input	12V +/- 10%
Power consumption	1.5A
Power connector	4-pin Molex connector. Two pins are used for power; the other two pins are no-connect.

Dimensions and weight

Specification	Value
Width	20.7 cm (8.15 in)
Depth	13.85 cm (5.45 in)
Height	3.8 cm (1.5 in)
Weight	1.41 kg (3.1 lb)

Ethernet specifications

Specification	Value
Ethernet ports	4 RJ45 shielded Ethernet ports
Physical layer	10/100 Base-T (Auto-MDIX)
Data rate	10Mbps, 100Mbps, 1Gbps
Mode	Full or half duplex (auto-sensing)
Ethernet isolation	2250 VDC

Cellular specifications

Model	Technology	Specification	Value
TransPort LR54-AA401 TransPort LR54-AW401	LTE	Downstream rate	300 Mbps
		Upstream rate	50 Mbps
		Frequency bands	800, 850, 900, 1800, 1900, 2100 AWS, 2300, 2600 MHz
	HSPA+	Downstream rate	42 Mbps
		Upstream rate	5.76 Mbps
		Frequency bands	850, 900, AWS 1700, 1900, 2100 MHz
	UMTS	Downstream rates	
		Upstream rates	
		Frequency bands	850, 900, AWS 1700, 1900, 2100 MHz

Wi-Fi specifications

Specification	Value
802.11	a/b/g/n/ac connections, dual band, dual concurrent 2.4 GHz and 5 GHz
Wi-Fi Modes	Wi-Fi access point mode
Wi-Fi Security	WPA2 Personal Mixed WPA/WPA2 Personal WPA2 Enterprise Mixed WPA/WPA2 Enterprise
Wi-Fi transmit power	2.4 GHz: US variant: 13 dBm (802.11g/n), 16 dBm (802.11b) EU variant: 11 dBm (802.11g/n), 14 dBm (802.11b) 5 GHz: 13 dBm for all modes
Wi-Fi maximum data rates	54 Mbps (802.11a) 11 Mbps (802.11b) 54 Mbps (802.11g) 300 Mbps (802.11n) 866 Mbps (802.11ac)
Wi-Fi receiver sensitivity	-87 dBm / 11 Mbps (802.11b) -71 dBm / 54 Mbps and -90 dBm / 6 Mbps (802.11a) -74 dBm / 54 Mbps and -92 dBm / 6 Mbps (802.11g) -66 dBm / 300 Mbps and -92 dBm / 6 Mbps (802.11n 2.4 GHz) -67 dBm / 300 Mbps and -89 dBm / 6 Mbps (802.11n 5 GHz) -57 dBm / 866 Mbps and -83 dBm / 29 Mbps (802.11ac)

Serial specifications

Specification	Value
Serial ports	1
Standard	RS232
Async/Sync	Async
DTE/DCE	DCE
Signal support	TXD, RXD, RTS, CTS, DTR, DCD, DSR, RI
Flow control	Software (XON/XOFF), Hardware supported
Connector	DB9 female

Related topics

[Serial connector pinout](#)

Serial connector pinout

TransPort LR54 products are DCE devices. The pinout for the DB9 and RJ45 serial connectors 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

Processor, memory, and development specifications

Specification	Value
Flash memory available for custom applications	100 MB
RAM	256 MB
System clock	Real Time Clock with super-cap backup
Random number generator	Hardware random number generator
Python version	2.7.11

Internal sensors

TransPort LR devices have an internal temperature sensor for sensing temperature on the main motherboard.

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 LR54 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)

These LEDs 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.

Signal strength for 4G cellular connections

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

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

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.

- **> -70 dBm:** Excellent
- **-70 dBm to -85 dBm:** Good
- **-86 dBm to -100 dBm:** Fair
- **< -100 dBm to -109 dBm:** Poor
- **-110 dBm:** No service

Tips for improving cellular signal strength

If the signal strength LEDs for your device indicate poor or no service, try the following things to improve signal strength:

- Move the TransPort LR device to another location.
- Purchase a Digi Antenna Extender Kit:
 - Antenna Extender Kit, 1m (**76000954**)
 - Antenna Extender Kit, 3m (**76000955**)
- Move the TransPort LR device to another location.
- Purchase a Digi Antenna Extender Kit:
 - Antenna Extender Kit, 1m (**76000954**)
 - Antenna Extender Kit, 3m (**76000955**)

Regulatory and safety statements

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

[RF exposure statement](#)

[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**.

FCC Part 15 Class B

Radio Frequency Interface (RFI) (FCC 15.105)

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

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

Labeling Requirements (FCC 15.19)

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

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)



EU Declaration Of Conformity

Manufacturer's Name: Digi International inc.

Manufacturer's Address: 11001 Bren Road East
Minnetonka, MN 55343

declare under our sole responsibility that the product:

Product Name: TransPort LR54

Model Number: 50001899-XX, (X=0-9)

to which this declaration relates are in conformity with the essential requirements and other relevant requirements of EU Directive 2014/30/EU (EMC), EU Directive 2014/35/EU (LV) and EU Directive 2011/65/EU (RoHS2)

Safety: EN 62368-1:2014
EN 50564:2011
EN 50385:2002

Comm: EN 50585:2014

EMC:	EN 300 328 v1.9.1 (2015-02)	EN 61000-3-2:2014, Class A
	EN 301 489-1 v1.9.2 (2011-09)	EN 61000-3-3:2013
	EN 301 489-7 v1.3.1 (2005-11)	EN 61000-4-2:2009
	EN 301 489-17 v2.2.1 (2012-09)	EN 61000-4-3:2006 + A1:2008 + A2:2010
	EN 301 489-24 v1.5.1 (2010-10)	EN 61000-4-4:2012
	EN 55024:2010	EN 61000-4-5:2014
	EN 55022:2010 + AC:2011, Class B	EN 61000-4-6:2014
	EN 300 386 v1.6.1 (2012-09)	EN 61000-4-11:2004

RoHS2: EN 50581:2012

Minnesota, USA, 15th, April 2016
(Place and date of issue)

Authorised signature for and on behalf of Digi International Inc.
Joel Young, VP, Engineering

European Representative :	Andreas Burghart Digi International GmbH Lise-Meitner-StraRe 9 85737 Ismaning Germany Telephone:+49-89-540-428-0
---------------------------	--

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 present appareil numerique n'emet pas de bruits radioelectriques depassant les limites applicables aux appareils numeriques de la class B prescrites dans le Reglement sur le brouillage radioelectrique edicte par le ministere 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	<ul style="list-style-type: none"> ■ 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
GSM/UMTS	PTCRB
Cellular carriers	See the current list of carriers on the TransPort LR54 datasheet, available from the Specifications link on the TransPort LR54 product page on www.digi.com .

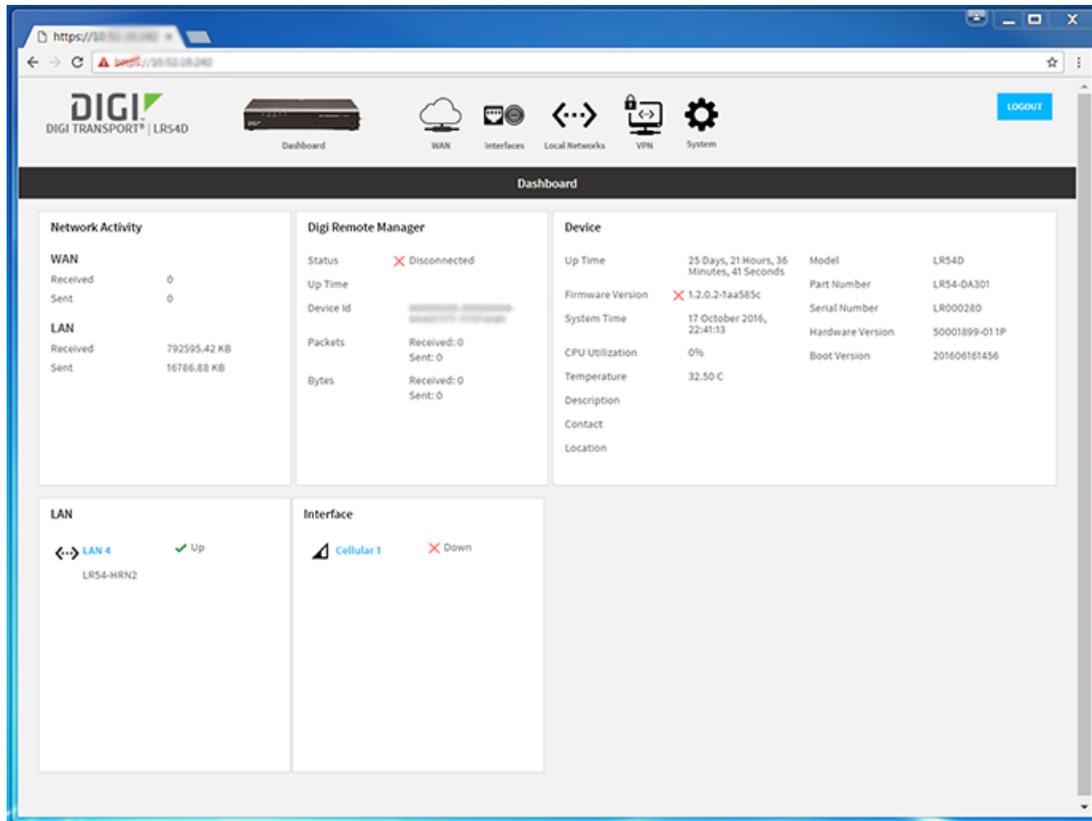
Management and status

These topics show how to configure and view the status of various TransPort LR features.

Managing devices from the web interface	34
Managing devices from the command line	36
Interfaces	37
Local Area Networks (LANs)	68
Wide Area Networks (WANs)	75
Security	86
Services and applications	106
Remote management	112
Routing	121
Virtual Private Networks (VPN)	128
System administration and management	140
Diagnostics	162

Managing devices from the web interface

The web user interface for TransPort LR products is designed around the way in which users typically use TransPort LR devices. For example, here is the top-level view of the web interface after you log in to the device.

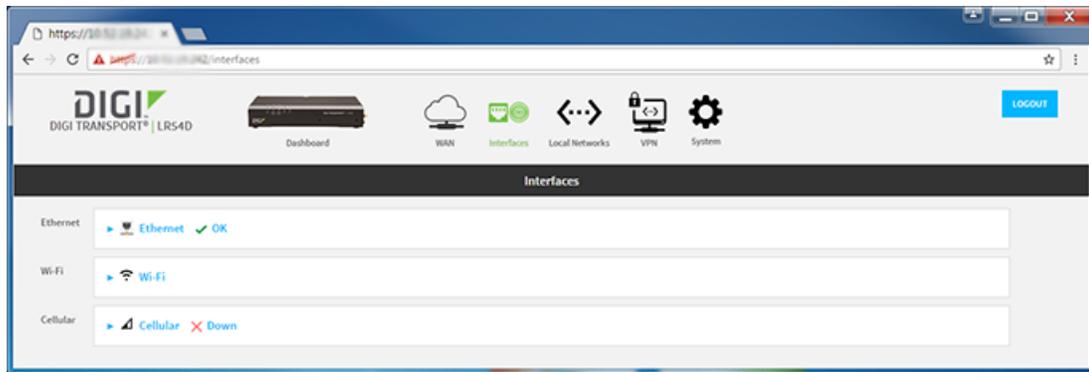


The web interface menu, at the top of the interface view, organizes information by virtual and physical interfaces that represent the “private” and “public” sides of the TransPort LR device. Clicking the items on the menu displays information below the menu.

Clicking the **Dashboard** menu item displays a snapshot of current activity for the device: network activity over wide-area and local networks, the current connection status to Digi Remote Manager, basic device configuration and identifying information, and summary info for local area network status and the status of physical interfaces.

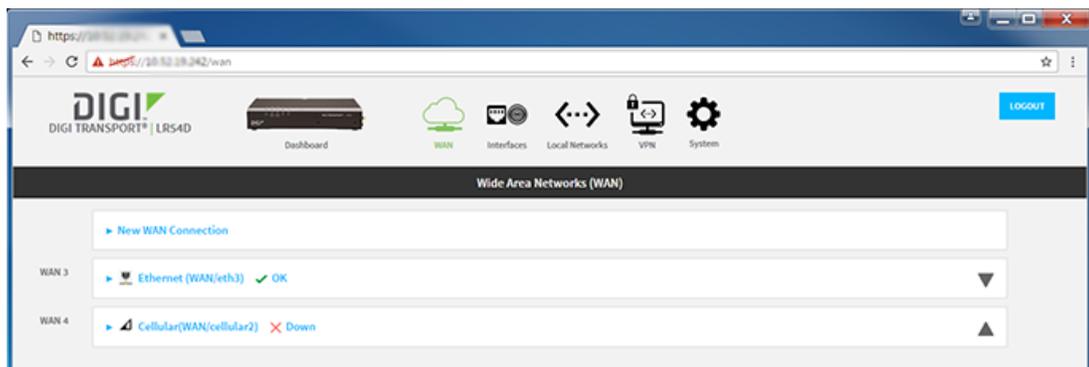


Clicking the **Interfaces** menu item displays the physical interfaces for your device. From this view, you can configure settings that are specific to the non-networking characteristics of those interfaces, such as Ethernet interface speed, Wi-Fi security, and cellular APN settings. For example:



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, fail-over and DHCP server settings.

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



Clicking the **System** menu item displays links to 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

The help topics in the **Management and status** section show how to perform tasks both from the web interface and command line. For the steps for each task from the web interface, see the heading **From the web interface**.

[Execute a command from 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 communications interfaces. The available interfaces vary by device model. This section covers configuring and managing interfaces.

[Ethernet interfaces](#)

[Cellular interfaces](#)

[Wi-Fi interfaces](#)

[Serial interface](#)

Ethernet interfaces

The Ethernet interfaces can be used as WAN or LAN interfaces. There is no IP configuration set on the individual Ethernet interfaces. Instead, the IP configuration is done on the WAN and LAN interfaces.

Related topics

[Configure Ethernet interfaces](#)

[From the command line](#)

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

For more information on LAN interfaces 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 **off**, **on**, or **on-demand**. The **on-demand** setting is a failover setting that causes the Ethernet interface to be brought up as needed if another interface with a higher priority goes down. For more information on the failover feature, see the discussion of WAN failover in [Wide Area Networks \(WANs\)](#).
- Once configured, the Ethernet interface must be assigned to a LAN interface or a WAN interface. For more information, see [Local Area Networks \(LANs\)](#) and [Configure a LAN](#) or [Wide Area Networks \(WANs\)](#) and [Configure a WAN interface](#).

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 WAN or LAN 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
```

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

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

3. Optional: Set the duplex mode.

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

4. Optional: Set the speed.

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

Related topics

[Ethernet interfaces](#)

[From the command line](#)

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

[Configure a LAN](#)

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

[Configure a WAN interface](#)

Related commands

[eth](#)

[show eth](#)

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             : 1000Base-T Full-Duplex

Received                               Sent
-----                                 ----
Rx Unicast Packet   : 5531             Tx Unicast Packet   : 2
Rx Broadcast Packet : 316403            Tx Broadcast Packet : 2
Rx Multicast Packet : 442694            Tx Multicast Packet : 2
Rx CRC Error        : 0                Tx CRC Error        : 0
Rx Drop Packet      : 0                Tx Drop Packet      : 0
Rx Pause Packet     : 0                Tx Pause Packet     : 0

```

```

Rx Filtering Packet : 0          Tx Collision Event : 0
Rx Alignment Error  : 0
Rx Undersize Error  : 0
Rx Fragment Error   : 0
Rx Oversize Error   : 0
Rx Jabber Error     : 0

Eth Status and Statistics Port 3
-----
Description      :
Admin Status     : Up
Oper Status      : Up
Up Time          : 1 Day, 13 Hours, 30 Minutes, 23 Seconds

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

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

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

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

Received                               Sent
-----                               ----
Rx Unicast Packet : 0                  Tx Unicast Packet : 0
Rx Broadcast Packet : 0                Tx Broadcast Packet : 0
Rx Multicast Packet : 0                Tx Multicast Packet : 0
Rx CRC Error       : 0                  Tx CRC Error       : 0
    
```

```
Rx Drop Packet      : 0          Tx Drop Packet      : 0
Rx Pause Packet     : 0          Tx Pause Packet     : 0
Rx Filtering Packet : 0          Tx Collision Event  : 0
Rx Alignment Error  : 0
Rx Undersize Error  : 0
Rx Fragment Error   : 0
Rx Oversize Error   : 0
Rx Jabber Error     : 0

digi.router>
```

Related topics[Ethernet interfaces](#)[Configure 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** respectively.

Both cellular interfaces cannot be up at the same time. If both cellular interfaces are enabled to **on**, then **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**.

For the TransPort LR device to automatically configure a default route for the cellular interface when it is up and for it to be able to failover to and from the cellular interface, it must be assigned to a WAN interface.

Related topics

[Configure cellular interfaces](#)

[Show cellular status and statistics](#)

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

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

Related commands

[cellular](#)

[show cellular](#)

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 **off**, **on**, or **on-demand**. The **on-demand** setting is a failover setting that causes the cellular interface to be brought up as needed if another interface with a higher priority goes down. For more information on the failover feature, see the discussion of WAN failover in [Wide Area Networks \(WANs\)](#).
- 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 WAN interface](#).

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.

From the web interface

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

4. In the **Edit Selected** box, enter the settings:
 - **Description:** Optional: Provide a description of the cellular interface.
 - **State:** Set the state to **On** to enable the cellular interface, **Off** to disable it, or **On-demand** to cause the cellular interface to be brought up as needed if another interface with a higher priority goes down.
 - **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. 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
```

4. Optional: Set a preferred mode.

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

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

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

6. 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
```

Related topics

[Cellular interfaces](#)

[Show cellular status and statistics](#)

[Switch the cellular carrier](#)

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

[Configure a WAN interface](#)

Related commands

[cellular](#)

[show cellular](#)

Show cellular status and statistics

From the command line

To show the status and statistics for a cellular interface, use the [show lan](#) 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               : 359072060051337
Temperature        : 32C

SIM status         : Using SIM2
ICCID              : 89014103278252818581

Signal strength    : Excellent (-80dBm)
Signal quality     : Excellent (-8dB)

Registration status : Registered
Attachment status  : Attached

Network provider   : AT&T, USA
Connection type    : 4G
Radio Band         : LTE 1900 PCS
Channel            : 700

APN in use         : Context 1: 12655.mcs

IP address         : 172.20.1.132
Mask               : 255.255.255.248
Gateway            :
DNS servers        : 10.10.8.62, 10.10.8.64

                Received          Sent
                -----          ----
Packets         2                  2
Bytes           612                656
```

Related topics

[Cellular interfaces](#)

[Configure cellular interfaces](#)

[Switch the cellular carrier](#)

Related commands

[cellular](#)

[show cellular](#)

Switch the cellular carrier

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.

Related topics

[Cellular interfaces](#)

[Configure cellular interfaces](#)

[Show cellular status and statistics](#)

Related commands

[cellular](#)

[show cellular](#)

[update](#)

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.

- **> -70 dBm**: Excellent
- **-70 dBm to -85 dBm**: Good
- **-86 dBm to -100 dBm**: Fair
- **< -100 dBm to -109 dBm**: Poor
- **-110 dBm**: No service

Signal strength for 4G cellular connections

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

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

Tips for improving cellular signal strength

If the signal strength LEDs for your device indicate poor or no service, try the following things to improve signal strength:

- Move the TransPort LR device to another location.
- Purchase a Digi Antenna Extender Kit:
 - Antenna Extender Kit, 1m (**76000954**)
 - Antenna Extender Kit, 3m (**76000955**)
- Move the TransPort LR device to another location.
- Purchase a Digi Antenna Extender Kit:
 - Antenna Extender Kit, 1m (**76000954**)
 - Antenna Extender Kit, 3m (**76000955**)

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 **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. 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.
4. 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**.
2. Click **Wi-Fi**. The available Wi-Fi interfaces display, along with the current LAN to which the interface belongs, and its state.
3. 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.
4. 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 options are as follows. By default, **WPA2-Personal** security is used.
 - **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**.
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 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.
5. 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
```

- Optional: Enter the RADIUS server port.

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

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

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

- Optional: Disable broadcasting the SSID in beacon packets.

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

- Optional: Disable Wi-Fi client isolation mode.

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

- 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 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](#)

[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](#)

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 descriptions of the output fields, see [show eth](#). For example:

```
digi.router> show serial

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

digi.router>
```

Related topics

[Serial interface](#)

[Configure the serial interface](#)

Related commands

[serial](#)

[show eth](#)

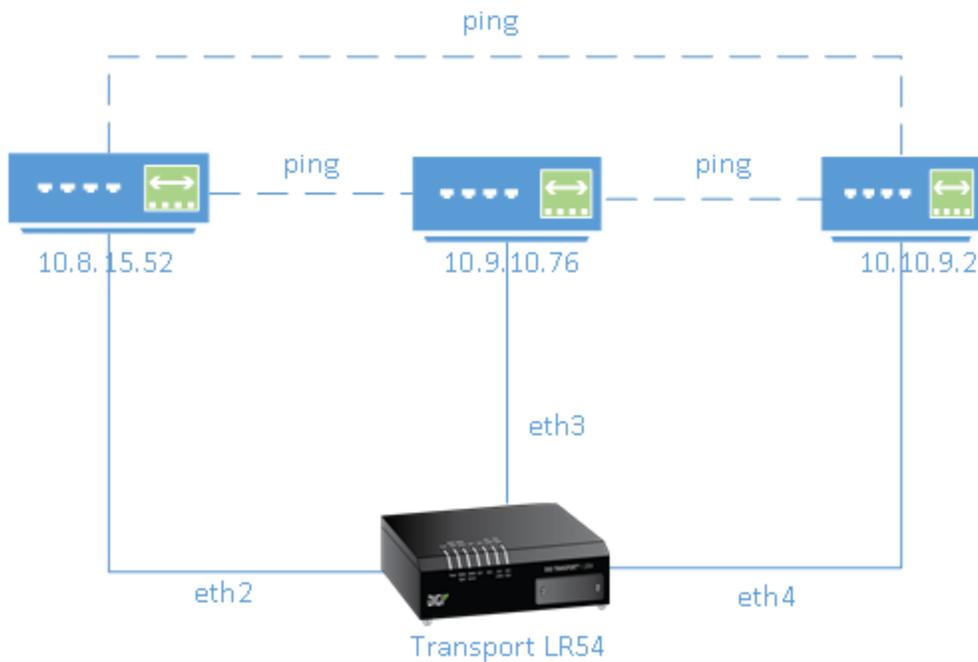
Local Area Networks (LANs)

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](#)

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

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](#)

Related commands

[lan](#)

[show lan](#)

Show LAN status and statistics

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](#)

Related commands

[lan](#)

[show lan](#)

DHCP servers

The DHCP server feature can be enabled 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.

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](#)

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 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 netmask 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](#)

Related commands

[dhcp-server](#)

Wide Area Networks (WANs)

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

- An 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

WAN interface 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 interface 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**.

Using Ethernet interfaces in a WAN

TransPort LR devices support four Ethernet interfaces, named **eth1**, **eth2**, **eth3**, and **eth4**. You can use these Ethernet interfaces as a WAN interface 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 interface 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 LAN interface. 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 interface, 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 failover

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

For example, if you use an Ethernet interface as your main WAN interface, and have a cellular interface configured as a backup WAN interface, if the Ethernet interface was to fail (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.

Detecting when an interface goes down: active and passive detection

There are two ways to detect when an interface 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 interface 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 interface going down by monitoring its link status by some means other than sending IP probe packets; for example, if the 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 interface 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 responses to these probe packets are not received, the TransPort LR device can bring down the WAN interface, and switch to using another WAN interface 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 interface 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 interface 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.

All of the IP probing configuration has 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.

To see an example of these IP probe settings in action, see [Example WAN failover: Ethernet to cellular](#).

Related topics

[Configure a WAN interface](#)

[Example WAN failover: Ethernet to cellular](#)

[Show WAN status and statistics](#)

Configure a WAN interface

You can configure up to **10** WAN interfaces.

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 interface 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 interface. By default, WAN interfaces are assigned the following 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:

- The IP configuration. WAN interfaces typically get their IP address configuration from the network, for example, cellular, to which they connect. 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 WAN interfaces, to create a default route over the WAN interface.
 - 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 network 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 interface failover feature, including sending of probe packets over the WAN interface to a specified device to determine whether the WAN interface 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.

Configure basic WAN settings

1. On the menu, click **WAN**.
2. Click **New WAN Connection**.
3. In the **Select WAN** field, assign a WAN number to the WAN.
4. Select an interface to assign to the WAN.
5. Click Apply.

From the command line**Configure basic WAN settings**

1. Assign an interface to the WAN interface.

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

2. Optional: Disable DHCP client mode.

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

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

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

4. Optional: Set the speed.

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

Configure IP probe settings

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

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

2. Configure the IP host to probe.

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

3. Optional: Configure the time, in seconds, to wait for a response to a probe. This value must be smaller than the probe-interval and timeout parameter values or the configuration is considered invalid, and an error message is written to the system log.

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

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

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

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

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

- Optional: Configure the time in, seconds, after which the WAN interface must receive all IP probe responses before reactivating the WAN interface.

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

- Optional: Configure the time, in seconds, after which to attempt to bring up the WAN interface.

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

Related topics

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

[Example WAN failover: Ethernet to cellular](#)

[Show WAN status and statistics](#)

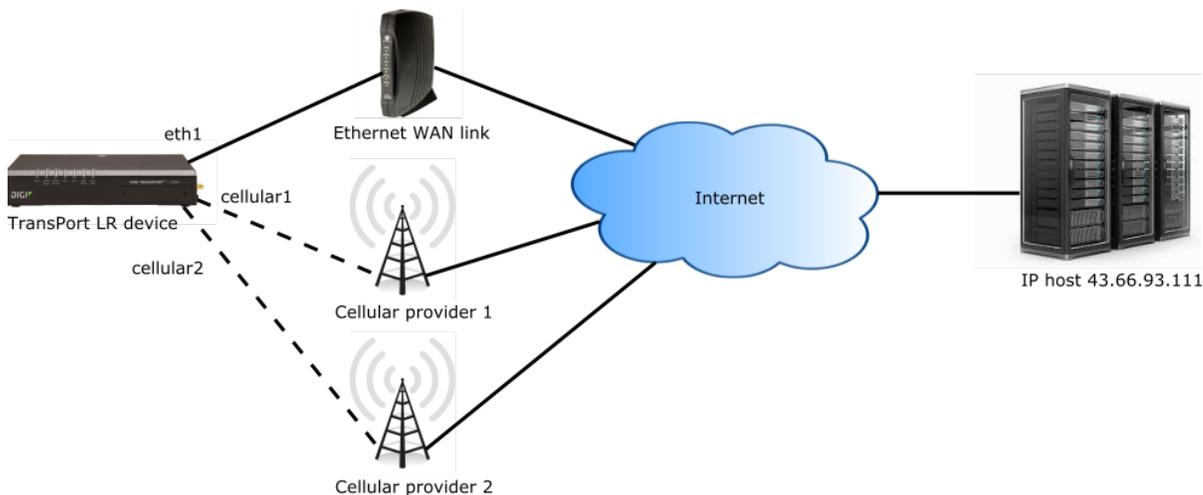
Related commands

[show wan](#)

[wan](#)

Example WAN failover: Ethernet to cellular

In this example, WAN, the **eth1** interface is the primary WAN, or **wan1**. **cellular1** and **cellular2** interfaces serve as backups to **eth1**. These interfaces are **wan2** and **wan3**, respectively.



To detect failover:

- The **eth1** interface uses IP probing to detect interface failure.
- The backup interfaces **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 WAN interface.

To achieve this WAN interface 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-demand
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 WAN interface](#)

[Show WAN status and statistics](#)

Related commands

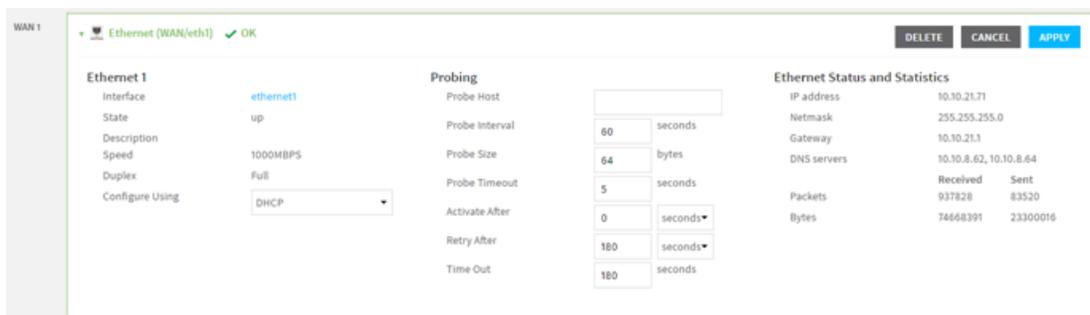
[wan](#)

[show wan](#)

Show WAN status and statistics

From the web interface

1. On the menu, click **WAN**.
2. The available WAN interfaces display. Select a WAN.
3. The WAN panel expands to display the configuration parameters and the status and statistics for the interface assigned to the WAN. For example, for a WAN using interface **eth1**:



From the command line

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

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 show detailed status for an interface, 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 detail about the host configured to probe, 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 WAN interface](#)[Example WAN failover: Ethernet to cellular](#)**Related commands**[wan](#)[show wan](#)

Security

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

[User management](#)

[Firewall](#)

User management

These topics cover configuring and managing TransPort LR device users, including their authentication credentials and access permissions.

Related topics

[Users and user access permissions](#)

[Configure a user](#)

Related commands

[user](#)

Users and user access permissions

To manage TransPort LR devices via the command-line interface or web interface, users must log in using a configured username and password.

This topic covers the TransPort LR user model and access permissions for users.

Number of supported users

Up to **10** administrative users are supported. Each user has a unique name, password and access level.

Default user

By default, TransPort LR devices have one user preconfigured. This default user is configured as **user 1**. Its default username is **admin**. Its default password is displayed on the label on the bottom of the device. For example:



You can change this **user 1** configuration to match your requirements.

User access permissions

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 their 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. A user with super access level must be present on a device, to allow editing user access levels. If you or any other device 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, etc.
read-only	The user can monitor device configuration and status, but cannot change the configuration or status of the TransPort LR device.

Related topics

[Configure a user](#)

[Delete a user](#)

[Reset the device to factory defaults](#)

Related commands

[user](#)

Configure a user

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

Required configuration items

- Username.
- Password. 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 permissions. The access level for users defaults to **super**. To restrict the access of this user to either read-write or read-only, you should configure the access level.

From the command line

The `user` command configures users.

1. Configure the username. 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

[Users and user access permissions](#)

[Delete a user](#)

Related commands

[user](#)

Delete a user

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

From the command line

Enter the following command:

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

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

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

Related topics

[Users and user access permissions](#)

[Configure a user](#)

Related commands

[user](#)

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; that is, forwarding a packet from a device on a public network to a device on a private network by modifying the destination IP address and/or TCP or UDP destination port.

Firewall design based on iptables

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 the keyword **firewall** instead of **iptables**. The firewall syntax is case-sensitive.

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

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 **5** 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.

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 automatically the last rule tested for a chain, while a normal rule could appear anywhere in the list of rules, depending how it and subsequent rules were added.

Related topics

[Default firewall configuration](#)

[Allow SSH access through the default firewall on WAN interfaces](#)

[Allow HTTPS access through the default firewall on WAN interfaces](#)

[Add a firewall rule](#)

[Update a firewall rule](#)

[Delete a firewall rule](#)

[Save firewall rules](#)

[Show firewall rules and counters](#)

[Example firewall rules](#)

Related commands

[firewall](#)

[show firewall](#)

Default firewall configuration

To provide a secure device “out of the box”, the firewall is configured for the following default behavior:

- Block all traffic received on the WAN interfaces (**eth1, cellular1, cellular2**) except for traffic for established connections or related data.
- Allow all traffic from the LAN interfaces to be forwarded by the device.
- Only allow ICMP, SSH, HTTP, HTTPS, DNS and DHCP traffic to be received on the LAN interfaces.
- All other traffic is blocked.

The default setting allows devices connected on the LAN interfaces to make connections over the WAN interfaces, but remote devices cannot make a connection to the device or devices connected on the LAN Interfaces.

This means that, by default, it is not possible to make an SSH or HTTPS connection via a WAN interface. To use SSH or HTTPS over a WAN interface, you must add a rule to the firewall to explicitly allow the connection.

[Allow SSH access through the default firewall on WAN interfaces](#)

[Allow HTTPS access through the default firewall on WAN interfaces](#)

Related topics

[Firewall](#)

[Add a firewall rule](#)

[Allow SSH access through the default firewall on WAN interfaces](#)

[Update a firewall rule](#)

[Delete a firewall rule](#)

[Save firewall rules](#)

[Show firewall rules and counters](#)

[Example firewall rules](#)

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

Related commands

[firewall](#)

[show firewall](#)

Allow SSH access through the default firewall on WAN interfaces

To allow SSH access through the default firewall on WAN interfaces:

1. Open the command-line interface, either from a command prompt or the web interface Device Console.
2. Depending on the interfaces you are using, copy and paste the following rules into the command line.
 - Port **22** is the default SSH port. If SSH has been configured to use a different port, using the `ssh` command, use that port instead of **22**.
 - To prevent other devices making SSH connections, specify the source IP address of the device making the SSH connection. If you do not want to specify the source IP address, remove `-s <source-ip-address>` from the rules.

```
firewall -A INPUT -i eth1 -s <source-ip-address> -p tcp --dport 22 -j ACCEPT
firewall -A INPUT -i cellular1 -s <source-ip-address> -p tcp --dport 22 -j ACCEPT
firewall -A INPUT -i cellular2 -s <source-ip-address> -p tcp --dport 22 -j ACCEPT
```

3. Enter the **save config** command to save the firewall rules to the configuration file.

Related topics

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

[Firewall](#)

[Default firewall configuration](#)

[Allow HTTPS access through the default firewall on WAN interfaces](#)

[Add a firewall rule](#)

[Update a firewall rule](#)

[Delete a firewall rule](#)

[Save firewall rules](#)

[Show firewall rules and counters](#)

[Example firewall rules](#)

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

Related commands

`firewall`

`show firewall`

`save`

`ssh`

Allow HTTPS access through the default firewall on WAN interfaces

To allow HTTPS access through the default firewall on WAN interfaces:

1. Open the command-line interface, either from a command prompt or the web interface Device Console.
2. Depending on the interfaces you are using, copy and paste the following rules into the command line. To prevent other devices making HTTPS connections, specify the source IP address of the device making the HTTPS connection. If you do not want to specify the source IP address, remove **-s <source-ip-address>** from the above rules.

```
firewall -A INPUT -i eth1 -s <source-ip-address> -p tcp --dport 443 -j ACCEPT
firewall -A INPUT -i cellular1 -s <source-ip-address> -p tcp --dport 443 -j ACCEPT
firewall -A INPUT -i cellular2 -s <source-ip-address> -p tcp --dport 443 -j ACCEPT
```

Related topics

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

[Firewall](#)

[Default firewall configuration](#)

[Allow SSH access through the default firewall on WAN interfaces](#)

[Add a firewall rule](#)

[Update a firewall rule](#)

[Delete a firewall rule](#)

[Save firewall rules](#)

[Show firewall rules and counters](#)

[Example firewall rules](#)

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

Related commands

[firewall](#)

[show firewall](#)

[save](#)

Add a firewall rule

From the command line

Use the `firewall` command to add rules to the firewall.

Add a rule to the bottom of the firewall

To add a rule to the bottom of the firewall, use the `firewall` command's `-A` option, using the following syntax. The `firewall` command syntax is case-sensitive.

```
firewall [-t table] -A <chain> <rule>
```

If no table is specified on the command, the `filter` table is used.

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)
  pkts bytes target    prot opt in     out     source      destination
  3    152 DROP      tcp  --  any     any     anywhere    anywhere    tcp
dpt:22
  0     0 DROP      icmp --  lan1    any     anywhere    anywhere    icmp
echo-request

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target    prot opt in     out     source      destination

Chain OUTPUT (policy ACCEPT 4 packets, 256 bytes)
  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's `-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)
  pkts bytes target    prot opt in     out     source      destination
  3    152 DROP      tcp  --  any     any     anywhere    anywhere    tcp
```

```
dpt:22
 74 4440 DROP      icmp -- lan1 any anywhere anywhere icmp
echo-request

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target    prot opt in     out     source destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
  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)
  pkts bytes target    prot opt in     out     source destination
    3  152 DROP      tcp  -- any   any     anywhere anywhere tcp
dpt:22
  0      0 ACCEPT    udp  -- cellular1 any anywhere anywhere
udp dpt:7
 74 4440 DROP      icmp -- lan1 any anywhere anywhere icmp
echo-request

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target    prot opt in     out     source destination

Chain OUTPUT (policy ACCEPT 4 packets, 256 bytes)
  pkts bytes target    prot opt in     out     source destination

digi.router>
```

Related topics

[Firewall](#)

[Default firewall configuration](#)

[Allow SSH access through the default firewall on WAN interfaces](#)

[Allow HTTPS access through the default firewall on WAN interfaces](#)

[Update a firewall rule](#)

[Delete a firewall rule](#)

[Save firewall rules](#)

[Show firewall rules and counters](#)

[Example firewall rules](#)

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

Related commands

[firewall](#)

[show firewall](#)

Update a firewall rule

To update a firewall rule, use the `firewall` command's `-R` option, using the following syntax:

```
firewall [-t table] -R <chain> <position> <rule>
```

For example, to update the second rule, specify a position of **2**.

```
digi.router> firewall -R INPUT 2 -i cellular1 -p udp --dport 123 -j ACCEPT
```

The `show firewall` output for the filter table created by the above command is:

```
digi.router> show firewall filter

Filter Table
-----
Chain INPUT (policy DROP 2 packets, 130 bytes)
  pkts bytes target    prot opt in     out     source            destination
    3  152 DROP      tcp  --  any    any    anywhere         anywhere         tcp
dpt:22
    0    0 ACCEPT    udp  --  cellular1 any    anywhere         anywhere
udp dpt:123
   74 4440 DROP      icmp --  lan1   any    anywhere         anywhere         icmp
echo-request

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target    prot opt in     out     source            destination

Chain OUTPUT (policy ACCEPT 2 packets, 130 bytes)
  pkts bytes target    prot opt in     out     source            destination

digi.router>
```

Related topics

[Firewall](#)

[Default firewall configuration](#)

[Allow SSH access through the default firewall on WAN interfaces](#)

[Allow HTTPS access through the default firewall on WAN interfaces](#)

[Add a firewall rule](#)

[Delete a firewall rule](#)

[Save firewall rules](#)

[Show firewall rules and counters](#)

[Example firewall rules](#)

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

Related commands

[firewall](#)

[show firewall](#)

Delete a firewall rule

To delete a firewall rule, use the `firewall` command's `-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

[Firewall](#)

[Default firewall configuration](#)

[Allow SSH access through the default firewall on WAN interfaces](#)

[Allow HTTPS access through the default firewall on WAN interfaces](#)

[Add a firewall rule](#)

[Update a firewall rule](#)

[Save firewall rules](#)

[Show firewall rules and counters](#)

[Example firewall rules](#)

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

Related commands

[firewall](#)

[show firewall](#)

Save firewall rules

To save the firewall rules in the configuration file, use the **save config** command.

For more information on the format of the configuration file and saving configuration, see [Managing configuration files](#).

Related topics

[Firewall](#)

[Default firewall configuration](#)

[Allow SSH access through the default firewall on WAN interfaces](#)

[Allow HTTPS access through the default firewall on WAN interfaces](#)

[Add a firewall rule](#)

[Update a firewall rule](#)

[Delete a firewall rule](#)

[Show firewall rules and counters](#)

[Example firewall rules](#)

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

Related commands

[save](#)

[firewall](#)

[show firewall](#)

Show firewall rules and counters

From the command line

To display the firewall, use the `show firewall` command.

For example:

```
digi.router> show firewall

Filter Table
-----
Chain INPUT (policy ACCEPT 1540 packets, 104K bytes)
  pkts bytes target    prot opt in     out     source        destination
    16  960 DROP      tcp  --  cellular1 any      anywhere
tcp dpt:22

Chain FORWARD (policy ACCEPT 704 packets, 76028 bytes)
  pkts bytes target    prot opt in     out     source        destination

Chain OUTPUT (policy ACCEPT 1466 packets, 97328 bytes)
  pkts bytes target    prot opt in     out     source        destination

Raw Table
-----
Chain PREROUTING (policy ACCEPT 3866 packets, 284K bytes)
  pkts bytes target    prot opt in     out     source        destination

Chain INPUT (policy ACCEPT 3599 packets, 255K bytes)
  pkts bytes target    prot opt in     out     source        destination

Chain FORWARD (policy ACCEPT 2020 packets, 202K bytes)
  pkts bytes target    prot opt in     out     source        destination

Chain OUTPUT (policy ACCEPT 3332 packets, 231K bytes)
  pkts bytes target    prot opt in     out     source        destination

Chain POSTROUTING (policy ACCEPT 5352 packets, 433K bytes)
  pkts bytes target    prot opt in     out     source        destination

NAT Table
-----
Chain PREROUTING (policy ACCEPT 143 packets, 14103 bytes)
  pkts bytes target    prot opt in     out     source        destination

Chain INPUT (policy ACCEPT 3 packets, 164 bytes)
  pkts bytes target    prot opt in     out     source        destination

Chain OUTPUT (policy ACCEPT 1248 packets, 82344 bytes)
  pkts bytes target    prot opt in     out     source        destination

Chain POSTROUTING (policy ACCEPT 1379 packets, 95795 bytes)
  pkts bytes target    prot opt in     out     source        destination
    0    0 MASQUERADE all  --  any      eth1      anywhere
```

```

0    0 MASQUERADE all -- any    cellular1 anywhere    anywhere
0    0 MASQUERADE all -- any    cellular2 anywhere    anywhere

digi.router>

```

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. For example:

```

digi.router> show firewall filter

Filter Table
-----
Chain INPUT (policy ACCEPT 1732 packets, 117K bytes)
  pkts bytes target    prot opt in     out     source    destination
   16  960 DROP      tcp  --  cellular1 any     anywhere  anywhere
tcp dpt:22

Chain FORWARD (policy ACCEPT 788 packets, 82764 bytes)
  pkts bytes target    prot opt in     out     source    destination

Chain OUTPUT (policy ACCEPT 1646 packets, 110K bytes)
  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 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.

```

digi.router> show firewall filter

Filter Table
-----
Chain INPUT (policy ACCEPT 1732 packets, 117K bytes)
  pkts bytes target    prot opt in     out     source    destination
    3   152 DROP      tcp  --  cellular1 any     anywhere  anywhere
tcp dpt:22
   23  1380 DROP      icmp --  lan1   any     anywhere  anywhere    icmp
echo-request

Chain FORWARD (policy ACCEPT 788 packets, 82764 bytes)
  pkts bytes target    prot opt in     out     source    destination

Chain OUTPUT (policy ACCEPT 1646 packets, 110K bytes)
  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)
  pkts bytes target    prot opt in     out     source    destination

```

```

0 0 DROP      tcp --  cellular1 any      anywhere      anywhere
tcp dpt:22
0 0 DROP      icmp --  lan1  any      anywhere      anywhere      icmp
echo-request

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out    source      destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out    source      destination

digi.router>
    
```

Related topics

[Firewall](#)

[Default firewall configuration](#)

[Allow SSH access through the default firewall on WAN interfaces](#)

[Allow HTTPS access through the default firewall on WAN interfaces](#)

[Add a firewall rule](#)

[Update a firewall rule](#)

[Delete a firewall rule](#)

[Show firewall rules and counters](#)

[Example firewall rules](#)

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

Related commands

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

[firewall](#)

[show firewall](#)

Example firewall rules

Define a policy to drop all packets if they do not match any other rule

```
digi.router> firewall -P INPUT DROP
```

Filter inbound SSH (port 22) traffic on the cellular1 interface

```
digi.router> firewall -A INPUT -i cellular1 -p tcp -dport 22 -j DROP
```

Block incoming ping requests on the eth1 interface

```
digi.router> firewall -A INPUT -i eth1 -p icmp --icmp-type echo-request -j DROP
```

Allow incoming HTTPS connections (port 443)

```
digi.router> firewall -A INPUT -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT
```

Allow outgoing ping requests and their incoming responses

```
digi.router> firewall -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT  
digi.router> firewall -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT
```

Block any inbound connection attempts over the cellular1 interface

```
digi.router> firewall -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT  
digi.router> firewall -A INPUT -m state --state NEW -i cellular1 -j DROP
```

Port forward any packet with TCP destination port 422 to IP address 192.168.1.47 port 22

```
digi.router> firewall -t nat -A PREROUTING -p tcp --dport 422 -j DNAT --to 192.168.1.47:22
```

Related topics

[Firewall](#)

[Default firewall configuration](#)

[Allow SSH access through the default firewall on WAN interfaces](#)

[Allow HTTPS access through the default firewall on WAN interfaces](#)

[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 and [IptablesHowTo](#).

Related commands

[firewall](#)

[show firewall](#)

Services and applications

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

[Auto-run commands](#)

[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](#)

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

To configure the 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.

Related topics

[Configure Digi Remote Manager](#)

[Show Digi Remote Manager connection status](#)

Related commands

[cloud](#)

[show cloud](#)

Configure Digi Remote Manager

Digi Remote Manager is enabled by default and should require no additional configuration. Once the device has a WAN connection, it should automatically connect 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.
- The reconnection timer can be changed. 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 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**:

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

Related topics

[Digi Remote Manager](#)

[Show Digi Remote Manager connection status](#)

Related commands

[cloud](#)

[show cloud](#)

Show Digi Remote Manager connection status

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:

```
digi.router> show cloud

Device Cloud Status
-----

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

Uptime      : 1 Minute, 9 Seconds

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

digi.router>
```

Related topics

[Digi Remote Manager](#)

[Configure Digi Remote Manager](#)

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. 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 will use the route with the lowest metric.

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 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 and DSL 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

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

```
digi.router> show route
```

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

```
digi.router>
```

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 is used by 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](#)

[show 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**, **on**, or **on-demand**. The **on-demand** setting is a failover setting that causes the IPsec tunnel to be brought up as needed if another IPsec tunnel with a higher priority goes down.
- 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.
- The local and remote IP networks.
- 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.
 - **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

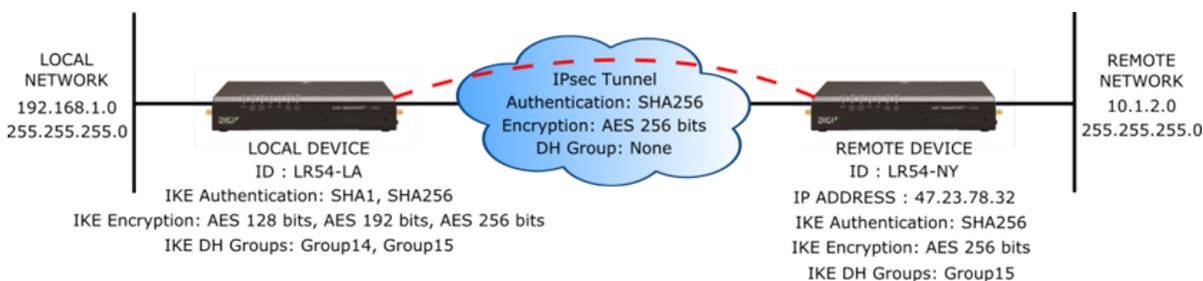
- The lifetime of the IPsec tunnel before it is renegotiated. This defaults to **1 hour (3600 seconds)**, and does not need to match the setting on the remote device.
- The number of bytes, also known as lifebytes, sent on the IPsec tunnel before it is renegotiated. By default, this setting is disabled, 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 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

Following an example IPsec configuration between an TransPort LR54 and a TransPort WR44.



The configuration settings for both devices are as follows:

TransPort LR54 configuration	TransPort WR44 configuration
<pre> digi.router> lan 1 state on description IPsec local net mtu 1500 interfaces eth2,eth3,eth4 ip-address 192.168.54.1 mask 255.255.255.0 dns1 dns2 dhcp-client off digi.router> lan 2 state on description Link to WR44 mtu 1500 interfaces eth1 ip-address 10.0.0.54 mask 255.255.255.0 dns1 dns2 dhcp-client off digi.router> ipsec 1 state on description Tunnel to WR44 peer 10.0.0.44 local-network 192.168.54.0 local-mask 255.255.255.0 remote-network 192.168.44.0 remote-mask 255.255.255.0 esp-authentication sha1 esp-encryption aes128 esp-diffie-hellman none auth-by psk psk <configured> local-id 10.0.0.54 remote-id 10.0.0.44 lifetime 3600 lifebytes 0 margintime 540 marginbytes 0 random 100 ike 1 ike-mode aggressive ike-encryption aes128 ike-authentication sha1 ike-diffie-hellman group5 ike-lifetime 3600 ike-tries 3 dpddelay 30 dpdtimeout 150 dpd off </pre>	<pre> # 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=" </pre>

Related topics

[IPsec](#)

[Configure an IPsec tunnel](#)

[Debug an IPsec configuration](#)

[Show IPsec status and statistics](#)

Related commands

[ipsec](#)

[show ipsec](#)

Show IPsec status and statistics

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 and management

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.

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 **dig.router>**. You can configure the system prompt to be any value of up to **16** characters. To use the device's serial number in the system prompt, include **%s** in the **prompt** parameter value. For example, a **prompt** parameter value of **LR54_%s** resolves to **LR54_LR123456**.
- 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 [Using event and system logs](#), [Event log levels](#), and [Configure the event logging level](#).
- 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.

From the command line

- 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 and management](#)

[Show system information settings](#)

Related commands

[system](#)

[show system](#)

Show system information settings

From the command line

To show system settings, use the [show system](#) command. For descriptions of the output fields, see [show system](#). 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        :
```

Related topics

[System administration and management](#)

[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 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 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 the Digi Remote Manager Profile Manager to handle firmware updates. Profile Manager 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 [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 > 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 for each model 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.

If any errors occur during the firmware update process, see Firmware update issues.

```
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

Firmware update issues

[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|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

Firmware update issues

[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. Following is an example configuration file. The notes in red identify these key sections.

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+uGGAqPgOF8iU="
wifi5g 1 state on
wifi5g 1 ssid LR54-2.4G-%s
wifi5g 1 password "$00$U2FsdGVkX1/aQwCR/VgIcG0r/Un/Px9a3XBRkPI9euQ="
user 1 name "admin"
user 1 password

"$6$n8bHC46Qo.TQfT/r$61hWHSy071CYMrIOdUMUSB9vq7powrwcMftGAL912MLQutR9LHhW2k1LQrsZxETCz3sAw4DL4
vZU20b1ZxxC."
:

```

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 [Firewall](#).

```

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

digi.router&gt;

```

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 command line

Enter the **save config** command.

```
digirouter> save config
```

Related topics

[Managing configuration files](#)

[Switch between configuration files](#)

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

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](#)

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](#)

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 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. For TransPort LR54 devices, 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 **5** 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](#)

Diagnostics

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

[Using event and system logs](#)

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

[Execute a command](#)

Using 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 .

Format of event log entries

Event 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:

```
May 3 12:05:29 user.info CLI[admin]: system timeout 3600
```

Related topics

[Event log levels](#)

[Configure the event logging level](#)

[Display the event or system log](#)

[Save event or system logs to a file](#)

[Clear the event or system log](#)

Event log levels

Events can be logged at one of eight log levels. The log levels, from highest to lowest level of severity, are:

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.
notice	Events that are unusual, but are not error conditions.
info	Normal operational messages that require no action.
debug	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 the event logging level](#).

Related topics

- [Using event and system logs](#)
- [Configure the event logging level](#)
- [Save event or system logs to a file](#)
- [Display the event or system log](#)
- [Clear the event or system log](#)

Related commands

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

Configure the event logging level

You can change the level of events that are logged in the event log from its default, which is to log all events of level **informational** or higher.

To configure the event log level:

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

[Using event and system logs](#)

[Event log levels](#)

[Display the event or system log](#)

[Save event or system logs to a file](#)

[Clear the event or system log](#)

Related commands

[clear](#)

[show log](#)

[system](#)

Display the event or system log

To display the event or system log:

From the command line

Display the event log

To display the event log, use the [show log](#) command. For example:

```
digi.router> show log

Jun  8 16:54:39 user.info cellular_monitor[1245]: Model = HE910
Jun  8 16:54:39 user.info cellular_monitor[1245]: modem support = HE910 4G support = 0
Jun  8 16:54:47 user.notice CLI[]: Login failure by .
Jun  8 16:54:50 user.notice CLI[admin]: Login by admin.
```

Display the system log

To display the system log, use the **show log system** command variant. For example:

```
digi.router> show log system

Nov 18 12:07:43 kern.info kernel:device eth3 entered promiscuous mode
Nov 18 12:07:43 kern.info kernel:lan1: port 2(eth3) entering forwarding state
Nov 18 12:07:43 kern.info kernel:lan1: port 2(eth3) entering forwarding state
Nov 18 12:07:43 kern.info kernel:device eth4 entered promiscuous mode
Nov 18 12:07:43 kern.info kernel:lan1: port 3(eth4) entering forwarding state
Nov 18 12:07:43 kern.info kernel:lan1: port 3(eth4) entering forwarding state
Nov 18 12:07:43 kern.info kernel:device wifi1 entered promiscuous mode
Nov 18 12:07:43 kern.info kernel:device wifi5g1 entered promiscuous mode
Nov 18 12:07:45 kern.warning kernel:ESW: Link Status Changed - Port2 Link Down

digi.router>
```

Related topics

[Using event and system logs](#)

[Event log levels](#)

[Configure the event logging level](#)

[Save event or system logs to a file](#)

[Clear the event or system log](#)

Related commands

[clear](#)

[show log](#)

[system](#)

Save event or system logs to a file

By default, the event logs are stored in RAM. This means the event logs are lost when the device is rebooted. You can configure the device to store the event 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 event 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.

Note 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.

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

[Using event and system logs](#)

[Event log levels](#)

[Configure the event logging level](#)

[Display the event or system log](#)

[Clear the event or system log](#)

Related commands

[clear](#)

[show log](#)

[system](#)

Clear the event or system log

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.

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

[Using event and system logs](#)

[Event log levels](#)

[Configure the event logging level](#)

[Display the event or system log](#)

[Save event or system logs to a file](#)

Related commands

[clear](#)

[show log](#)

[system](#)

Use the "ping" command to troubleshoot network connections

You can use the [ping](#) command 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 commands

[ping](#)

File system

The TransPort LR 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.

Related topics

[Managing configuration files](#)

Following are common operations for directories and files in the TransPort LR Family file system:

Make a directory	171
Display directory contents	172
Change the current directory	173
Remove a directory	174
Display file contents	176
Copy a file	177
Rename a file	179
Delete a file	180
Upload and download files	181

Make a directory

To make a new directory, use the [mkdir](#) command, specifying the name of the directory.

For example:

```
digi.router> mkdir test
digi.router> dir

File                               Size  Last Modified
-----
test                               Directory
config.da0                         763   Sun Mar  5 12:36:20
config.fac                         186   Mon Feb 21 03:00:17

Remaining User Space: 102,457,344 bytes

digi.router>
```

Related topics

[File system](#)

[Display directory contents](#)

[Change the current directory](#)

[Remove a directory](#)

Related commands

[mkdir](#)

Display directory contents

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](#)

[Make a directory](#)

[Change the current directory](#)

[Remove a directory](#)

Related commands

[dir](#)

Change the current directory

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](#)

[Make a directory](#)

[Display directory contents](#)

[Remove a directory](#)

Related commands

[cd](#)

Remove a directory

To remove a directory:

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](#)

[Make a directory](#)

[Display directory contents](#)

[Change the current directory](#)

Related commands

[rmdir](#)

Display file contents

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](#)

[Copy a file](#)

[Rename a file](#)

[Delete a file](#)

[Upload and download files](#)

Related commands

[more](#)

Copy a file

To copy a file, use the [copy](#) command, specifying the existing file name, followed by the name of the new copy.

For example, to copy file **config.da0** to a file in the main directory named **backup.da0**, and then to a file named **test.cfg** in the **test** directory, enter the following:

```
>
digi.router> dir

File                               Size  Last Modified
-----
test                               Directory
config.da0                         763   Sun Mar  5 12:36:20
config.fac                          186   Mon Feb 21 03:00:17

Remaining User Space: 102,457,344 bytes
digi.router>
digi.router>
digi.router> copy config.da0 backup.da0
digi.router>
digi.router> dir

File                               Size  Last Modified
-----
test                               Directory
config.da0                         763   Sun Mar  5 12:36:20
config.fac                          186   Mon Feb 21 03:00:17
backup.da0                          763   Wed Apr  5 07:22:29

Remaining User Space: 102,457,344 bytes
digi.router>
digi.router> copy config.da0 test/test.cfg

digi.router>
digi.router> dir test

File                               Size  Last Modified
-----
test.cfg                           763   Wed Apr  5 07:24:45

Remaining User Space: 102,457,344 bytes

digi.router>
```

Related topics

[File system](#)

[Display file contents](#)

[Rename a file](#)

[Delete a file](#)

[Upload and download files](#)

Related commands

[copy](#)

Rename a file

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](#)

[Display file contents](#)

[Copy a file](#)

[Delete a file](#)

[Upload and download files](#)

Related commands

[rename](#)

Delete a file

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](#)

[Display file contents](#)

[Copy a file](#)

[Rename a file](#)

[Upload and download files](#)

Related commands

[del](#)

Upload and download files

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 TLR 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](#)

[Display file contents](#)

[Copy a file](#)

[Rename a file](#)

[Delete a file](#)

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	185
? (Display command help)	198
! (Revert command settings)	199
autorun	200
cd	201
cellular	202
clear	204
cloud	205
copy	206
date	207
del	208
dhcp-server	209
dir	210
eth	211
exit	213
firewall	214
ip	215
ipsec	216
lan	220
mkdir	222
more	223
ping	224
pwd	225
reboot	226
rename	227
rmdir	228
route	229
save	230
serial	231
show cellular	232
show cloud	235
show config	236
show eth	237
show firewall	240
show ipsec	241
show ipstats	243
show lan	245
show log	246
show route	247
show serial	248
show system	249
show wan	251
show wifi	253

show wifi5g	256
snmp	259
snmp-community	260
snmp-user	261
sntp	262
ssh	263
system	264
update	266
user	268
wan	269
wifi	271
wifi5g	273
wifi-global	275

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](#)

[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](#)

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

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](#)

Log in to the command line interface

1. Connect to the TransPort LR54 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 is displayed, 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](#)
- [Users and user access permissions](#)
- [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.

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
```

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 !
```

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 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](#)

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](#)

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 dsl** displays status and statistics for the DSL interface.
- **show cellular** displays status and statistics for specific or all cellular interfaces.

Execute a command from the web interface

1. Click .
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 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.

! (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:

```
digirouter> lan 1 interfaces !
```

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.

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, or enables it as an on-demand interface. The 'on-demand' setting allows configuring the cellular interface as an on-demand interface. An on-demand interface is brought up as needed if a higher priority goes down.

Accepted values can be one of off, on or on-demand. 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.

This element is available to all users.

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.

## Examples

- `cellular 1 state on`

Enable the Cellular 1 interface.

- `cellular 1 state off`

Disable the Cellular 1 interface.

- `cellular 1 state on-demand`

Disable Cellular 1 interface until the failover task brings it up.

- `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, etc.  
This command is available to super users only.

### Syntax

```
clear firewall
clear log
clear log system
clear log all
```

### Parameters

#### ***firewall***

Clears firewall counters.

#### ***log***

Clears event 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.

## 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 0 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 0 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 [file]
```

### Parameters

#### *file*

Lists information about the file (by default, the current directory).

## eth

Configures an Ethernet interface.

### Syntax

```
eth <1 - 4> <parameter> <value>
```

### Parameters

#### **state**

Enables or disables the Ethernet interface, or enables it as an on-demand interface. The 'on-demand' setting allows configuring the Ethernet interface as an on-demand interface. An on-demand interface is brought up as needed if a higher priority goes down.

Accepted values can be one of off, on or on-demand. 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.

- `eth 3 state on-demand`

Disable Ethernet interface 3 until the failover task brings it up.

## 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.

## 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.

This element is available to all users.

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 LAN interface. A LAN interface is a group of Ethernet and Wi-Fi interfaces.

### Syntax

```
lan <1 - 10> <parameter> <value>
```

### Parameters

#### **state**

Enables or disables a LAN interface.

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 member interfaces for the LAN.

Accepted values can be multiple values of eth1, eth2, eth3, eth4, wifi1, wifi2, wifi3, wifi4, wifi5g1, wifi5g2, wifi5g3 and wifi5g4.

#### **ip-address**

IPv4 address for the LAN. While it is not strictly necessary for a LAN interface to have an IP address, an IP address must be configured to send traffic from and to the LAN network.

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

## **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
```

### Parameters

#### *config*

Saves all configuration to flash memory.

### Examples

- ```
save config
```

Save the current configuration to flash memory.

serial

Configures a serial interface.

Syntax

```
serial <1 - 4> <parameter> <value>
```

Parameters

state

Enables or disables the serial interface.

Value is either on or off. The default value is on.

description

A description of the serial interface.

Accepted value is any string up to 63 characters.

baud

The data rate in bits per second (baud) for serial transmission.

Accepted values can be one of 110, 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400, 460800 or 921600. The default value is 115200.

databits

Number of data bits in each transmitted character.

Accepted values can be one of 8 or 7. The default value is 8.

parity

Sets the parity bit. The parity bit is a method of detecting errors in transmission. It is an extra data bit sent with each data character, arranged so that the number of 1 bits in each character, including the parity bit, is always odd or always even.

Accepted values can be one of none, odd or even. The default value is none.

stopbits

The number of stop bits sent at the end of every character.

Accepted values can be one of 1 or 2. The default value is 1.

flowcontrol

The type of flow control signals to pause and resume data transmission. Available options are software flow control using XON/XOFF characters, hardware flow control using the RS232 RTS and CTS signals, or no flow control signals.

Accepted values can be one of none, software or hardware. The default value is none.

show 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.

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 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.

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 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 LAN interface status and statistics.

Parameters

admin-status

Whether the LAN interface is sufficiently configured to be brought up.

oper-status

Whether the LAN interface is up or down.

description

Description of the LAN interface.

interfaces

The interfaces connected by 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 route

Displays all IP routes in the IPv4 routing table.

Parameters

destination

Destination of the route.

gateway

The gateway for the route.

metric

The metric assigned to the route.

protocol

The protocol for the route.

idx

The index number for the route.

interface

The interface for the route.

status

Status of the route.

show serial

Displays serial interface status and statistics.

Parameters

description

A description of the serial interface.

admin-status

Whether the serial interface is sufficiently configured to be brought up.

oper-status

Whether the serial interface is up or down.

uptime

Amount of time the serial interface has been up.

tx-bytes

Number of bytes transmitted over the serial interface.

rx-bytes

Number of bytes received over the serial interface.

overrun

Number of times the next data character arrived before the hardware could move the previous character.

overflow

Number of times the received buffer was full when additional data was received.

line-status

The current signal detected on the serial line.

show system

Displays system status and statistics.

Parameters

model

The model name for the device.

part-number

The part number for the device.

serial-number

The serial number for the device.

hardware-version

The hardware version for the device.

bank

The current firmware flash memory bank in use.

firmware-version

The current firmware version running on the device.

bootloader-version

The current bootloader version running on the device.

config-file

The current configuration file loaded on the device.

uptime

The time the device has been up.

system-time

The current time on the device.

cpu-usage

Current CPU usage.

cpu-min

Minimum CPU usage.

cpu-max

Maximum CPU usage.

cpu-avg

Average CPU usage.

temperature

The current temperature of the device.

description

Description for this device.

location

Location details for this device.

contact

Contact information for this device.

show wan

Displays WAN interface status and statistics.

Parameters

admin-status

Whether the WAN interface is sufficiently configured to be brought up.

oper-status

Whether the WAN interface is up or down.

interface

The 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 and TransPort LR54DWC1 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 and TransPort LR54DWC1 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.

This element is available to all users.

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.

This element is available to all users.

Accepted value is any string between 8 and 64 characters.

privacy-password

SNMPv3 privacy password. The password is stored in encrypted form.

This element is available to all users.

Accepted value is any string between 8 and 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.

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.

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.

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 ./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

The username for the user.

Accepted value is any string up to 32 characters.

password

The password for the user.

This element is available to all users.

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.

wan

Configures WAN interface settings. A WAN interface 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 WAN interface to configure.

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 interface. 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 this 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 interface 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 interface 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 interface if DHCP is disabled.

Value should be an IPv4 address.

mask

The IPv4 mask to be statically assigned to this WAN interface 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.

wifi

Configures a Wi-Fi 2.4 GHz interface.

This group is only supported in TransPort LR54, TransPort LR54W, TransPort LR54D and TransPort LR54DWC1 products.

Syntax

```
wifi <1 - 4> <parameter> <value>
```

Parameters

state

Enables or disables the Wi-Fi 2.4 GHz interface, or enables it as an on-demand interface. The 'on-demand' setting allows configuring the cellular interface as an on-demand interface. An on-demand interface is brought up as needed if a higher priority goes down.

Accepted values can be one of off, on or on-demand. 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

This element is available to all users.

Accepted value is any string between 8 and 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.

This element is available to all users.

Accepted value is any string between 1 and 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 and TransPort LR54DWC1 products.

Syntax

```
wifi5g <1 - 4> <parameter> <value>
```

Parameters

state

Enables or disables the Wi-Fi 5 GHz interface, or enables it as an on-demand interface. The 'on-demand' setting allows configuring the cellular interface as an on-demand interface. An on-demand interface is brought up as needed if a higher priority goes down.

Accepted values can be one of off, on or on-demand. 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 '.'

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

This element is available to all users.

Accepted value is any string between 8 and 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.

This element is available to all users.

Accepted value is any string between 1 and 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 and TransPort LR54DWC1 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.