Digi TransPort

User Guide

Digi TransPort User Guide

(Part number 90001019)

Revision	Date	Description
A	February, 2009	Initial Release.
B	February, 2009	Added bug fixes.
C	April, 2009	Revised with firmware updates.
D	October, 2009	Revised with firmware updates.
E	May, 2005	Added minor changes.
F	March, 2012	Changed default IP address and added temperature monitoring section.
G	May, 2012	Updated autosa and ouridtype parameters.
H	August, 2012	Added GPIO section.
K	April, 2013	Added several new commands including network status commands, GOBI image load selection and MultiTX.
L	February, 2015	Added PPP CLI commands and fixed errors.
M	December, 2015	Added TransPort WR31 product information. Created Hardware chapter to house all hardware content for models, including content migrated from Installation Guides. Addressed several technical issues. Reorganized content and deleted obsolete product information.
N	January, 2016	Updated TransPort WR31 serial pinout diagram and links to it. Updated links and information Dynamic DNS feature.

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.

Trademarks and copyright

Customer support

If you need assistance, contact technical support:

Telephone (8:00 am - 5:00 pm—U.S. Central Time):

    866.765.9885 toll-free U.S.A. & Canada

    801.765.9885 Worldwide

    Fax: 952.912.4952

Online: www.digi.com/support/eservice/

Mail:

    Digi International

    11001 Bren Road East

    Minnetonka, MN 55343 USA

Contents

Configure network interfaces

Configure DHCP servers

Configure network services

Configure DNS servers and Dynamic DNS

Configure IP routing and forwarding

Configure Virtual Private Networking (VPN)

Configure Secure Sockets Layer (SSL)

Configure Secure Shell (SSH) server and client

Configure FTP Relay

Configure IP passthrough

Configure UDP echo

Configure Quality of Service (QoS)

Configure time bands

Configure advanced network settings

Configure legacy protocols

Configure alarms

Configure system settings

Configure Remote Manager

Configure security settings

Configure position (GPS) settings

Manage applications

Glossary

Introduction to Digi TransPort routers

The Digi TransPort WR family of 3G/4G cellular routers offers an all-in-one mobile communications solution with true enterprise class routing, security and firewall. These multifunction cellular routers feature a flexible design with optional integrated Wi-Fi access point (with multi SSID) / client, USB, serial, VDSL, 1-, 2- or 4-port Ethernet switch with VLAN. Additional configuration options include multiple serial ports (async or sync), GPS or telemetry I/O.

The Digi TransPort family offers an advanced routing, security and firewall feature set including stateful inspection firewall and integrated VPN. Enterprise class protocols incorporate BGP, OSPF and VRRP+, a patented technology built upon the popular VRRP failover standard providing true auto-sensing, auto-failure and auto-recovery of any line drop.

Digi TransPort WR routers are ideal for transportation, POS, energy, medical, financial and digital signage as well as cellular backup and remote device connectivity applications.

Digi management solutions provide easy setup, configuration and maintenance of large installations of remote Digi TransPort devices. Digi Remote Manager offers web-based device management for remote Digi cellular routers and gateways. Digi TransPort routers have the following features:

- Enterprise class cellular routers with advanced dynamic routing, security and firewall features.
- High speed LTE/4G router with fall back to both GSM and CDMA 3G/2G technologies.
- Optional integrated Wi-Fi access point and multiport Ethernet switch.
- Flexible interfaces including serial (async/sync), GPS, VDSL, USB, CAN Bus and telemetry I/O, with flexible DC power options.
- Powerful integrated end user programming.
- Remote Management via windows remote management software or cloud hosted Remote Manager.

TransPort WR 11

Digi TransPort WR11 is a full-featured, cellular router offering the flexibility to scale from basic connectivity applications to enterprise class routing and security solutions. With its high performance architecture, Digi TransPort WR11 is designed for Wide Area Network connectivity including 2.5G, 3G and 4G networks.

TransPort WR21

Digi TransPort WR21 is a full-featured, cellular router offering the flexibility to scale from basic connectivity applications to enterprise class routing and security solutions. With its high performance architecture, Digi TransPort WR21 is designed for Wide Area Network connectivity including 2.5G/3G/4G networks.

Digi TransPort WR21 is available with a range of Ethernet, Serial (RS232, RS422/485) and Power connector options.

Digi TransPort WR21 also offers an optional advanced routing, security and firewall feature set including stateful inspection firewall and integrated VPN. Enterprise class protocols incorporate BGP, OSPF and VRRP+, a patented technology built upon the popular VRRP failover standard providing true auto sensing, auto failure and auto recovery of any line drop.

TransPort WR31

Digi's TransPort WR31 is an intelligent 4G LTE router designed for critical infrastructure and industrial applications.

Key features of the TransPort WR31 include:

- Global HSPA+ and 4G LTE support and certification on major carrier networks around the world

- Software defined multi-carrier networking with Gobi 4G LTE, meaning one device that operates in 2G, 3G, or 4G across all major North American carriers.

- Ethernet, serial, and I/O for connecting diverse field assets

- Extremely resilient cellular connection through Digi's patented SureLink™, VRRP+ protocol, and dual SIM slots

- Enterprise Routing features for security, logging, and redundancy (e.g. stateful firewall, VPN, SNMP); no annual enterprise software license required

- Digi Remote Manager provides mass configuration, device management, and troubleshooting tools

- Rugged aluminum enclosure, optimized for Din rail or shelf mounting
- Optional weatherproof enclosure
- 5 year warranty standard—no additional cost

The TransPort WR31 provides a secure, reliable connection to industrial controllers, process automation equipment, and smart grid assets on third party sites or remote locations. This drop-in connectivity gives operators a way to reduce the cost of downtime and service calls and also increase revenue by bringing distributed sites online faster.

The TransPort WR31 is ideal for connecting the following:

- Building and process automation controllers
- Smart grid assets (meters, switches, controllers)
- IP Cameras and access controllers
- Remote data loggers, flow meters, and sensing equipment
- Telco infrastructure
- Traffic and obstruction lighting

TransPort WR 41

The Digi TransPort WR family of cellular routers offers an all-in-one mobile communications solution with true enterprise class routing, security and firewall. These multifunction cellular routers feature a flexible design with an optional integrated Wi-Fi access point (with multi SSID) / Client, USB, serial, and Ethernet, as well as a variety of configuration options including multiple serial ports (async or sync), GPS or I/O telemetry modules.

The Digi TransPort family also offers an advanced routing, security and firewall feature set including stateful inspection firewall and integrated VPN. Enterprise class protocols incorporate BGP, OSPF and VRRP+, a patented technology built upon the popular VRRP failover standard providing true auto sensing, auto failure and auto recovery of any line drop.

Digi TransPort WR routers are ideal for transportation and mobile applications. Flexible power options include AC, DC and 4-pin Molex connectors for direct integration into vehicle applications. Also available is the Digi Remote Manager™ which provides easy setup, configuration and maintenance of large installations of Digi TransPort devices.

Model	GPRS	EDGE	UMTS	HSUPA	EVDO / 1xRTT
WR-41-E	✔	✔			
WR-41-G	✔				
WR41-U	✔	✔	✔	✔	
WR41-C					✔
WR41-U5	✔	✔	✔	✔	✔

TransPort WR44 / WR44 R

The Digi TransPort WR44 cellular router is an all-in-one mobile communications solution with true enterprise-class routing, security and firewall. This multifunction cellular router features a flexible design with integrated Wi-Fi access point, USB, serial and 4-port Ethernet switch, as well as a variety of configuration options including multiple serial ports (async or sync), GPS or I/O telemetry modules.

The Digi TransPort family offers an advanced routing, security and firewall feature set including stateful inspection firewall and integrated VPN. Enterprise-class protocols incorporate BGP, OSPF and VRRP+, a patented technology built upon the popular VRRP failover standard providing true auto sensing, auto failure and auto recovery of any line drop.

Digi TransPort WR44 is ideal for transportation and mobile applications. Flexible power options include 11-58 VDC barrel or molex connectors for direct integration into vehicle applications. Digi Remote Manager™ provides easy setup, configuration and maintenance of large installations of Digi TransPort devices.

Digi TransPort WR routers are available on the following networks:

Model	GPRS	EDGE	UMTS	HSUPA	EVDO / 1xRTT
WR-44-E	✓				
WR-41-G		✓			
WR44-U	✓				
WR44-C	✓	✓	✓	✓	✓
WR44-U5	✓	✓	✓	✓	✓

TransPort WR44 RR

Digi TransPort WR44 RR is a rugged enterprise-class cellular router designed for rail environments. Its rail industry ratings, versatility, security features and performance make it ideal for applications such as Positive Train Control (PTC), wayside device communications and on-board passenger Internet access.

Digi TransPort WR44 RR provides a reliable primary high speed cellular network connection or can act as a secure backup connection to the existing railroad network. It features a flexible communications design with 3G/4G multicarrier GSM/CDMA cellular, plus integrated Wi-Fi b/g/n access point, serial and 4-port Ethernet switch. It also features full on-board train certifications, including AREMA C/H and EN50155. Communications interfaces include hardened connectors, including M12 for Ethernet and serial, as well as TNC connectors for antenna connections.

Digi management solutions provide easy setup, configuration and maintenance of large installations of remote Digi TransPort devices. Digi Remote Manager offers web-based device management for remote Digi cellular routers and gateways.

Hardware

This section describes hardware specifications and features of TransPort products, presents pinout information, and covers regulatory and safety statements and certifications.

TransPort WR11 hardware

TransPort WR11 EVDO model hardware features

1. **LAN port**: This Ethernet port connects the device to a 10/100 base-T Local Area Network (LAN). The port is capable of auto-sensing for speed and wiring, so it can accept both straight-through or cross-over cable connections.

2. **Power cord input**: This locking power connector connects the device to a power source. The connector should be inserted and rotated to lock in place.

3. **LEDs:**

   - **Service LED**: Indicates the presence and level of cellular service running on the device.

     Off: No cellular service

     1 Blink: Device is running 1xRTT service

     2 Blinks: Device is running EDVO Rev 0 service

     3 Blinks: Device is running EDVO Rev A service

   - **Signal LED**: Indicates strength of cellular signal.

     Off: Poor or No signal. Place the device in a location where it gets a better signal.

     Amber: Fair

     Green: Good

   - **Power LED**

     Off: No power

     Green: TransPort device is powered

4. **Cellular antenna connector**: This SMA female connector connects the device's primary cellular antenna.

TransPort WR11 HSPA+ model hardware features
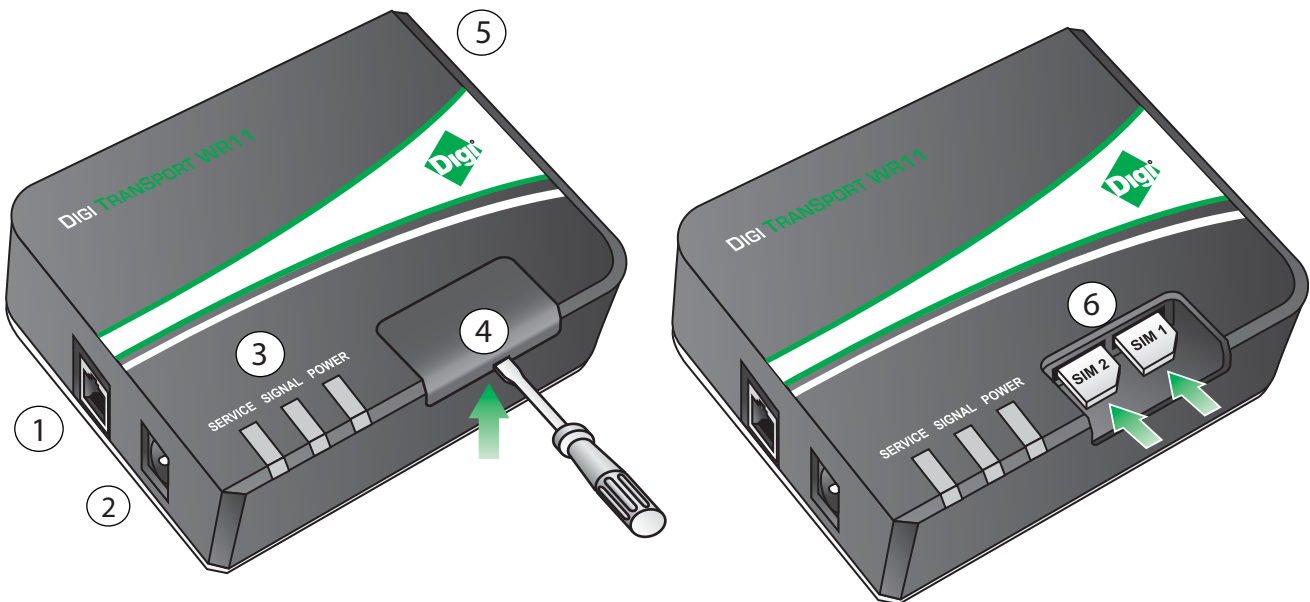
1. **LAN port**: This Ethernet port connects the device to a 10/100 base-T Local Area Network (LAN). The port is capable of auto-sensing for speed and wiring, so it can accept both straight-through or cross-over cable connections.

2. **Power cord input**: This locking power connector connects the device to a power source. The connector should be inserted and rotated to lock in place.

3. **LEDs:**

   • **SERVICE LED**: Indicates the presence and level of cellular service running on the device.

   Off: No cellular service

   1 Blink: GPRS mode

   2 Blinks: EDGE mode

   3 Blinks: UMTS mode

   4 Blinks: HSDPA mode

   5 Blinks: HSUPA mode

   • **SIGNAL LED**: Indicates strength of cellular signal.

   Off: Poor or No signal. Place the device in a location where it gets a better signal.

   Amber: Fair

   Green: Good

   • **POWER LED**:

   Off: No power

   Green: TransPort device is powered

4. **SIM door**: Encloses the SIM sockets. The SIM door must be removed to install the SIM cards
    For installation details, refer to the Quick Start Guide that came with your device.

Note To remove the SIM door, hold the device on a flat surface and using a screwdriver, firmly
pull the cover straight up.

5. **Cellular antenna connector**: This SMA female connector connects the device's primary
    cellular antenna.

6. **SIM Sockets**: SIM 1 and SIM 2 are for use with the Subscriber Identification Module(s) (SIMs).

TransPort WR11 LTE-MIMO hardware features

1. **LAN port:** This Ethernet port connects the device to a 10/100 base-T Local Area Network (LAN). The port is capable of auto-sensing for speed and wiring, so it can accept both straight-through or cross-over cable connections.

2. **Power cord input**: This locking power connector connects the device to a power source. The connector should be inserted and rotated to lock in place.

3. **LEDs:**

   - **SERVICE LED**: Indicates the presence and level of cellular service running on the device.

     Off: No cellular service

     1 Blink: GPRS mode

     2 Blinks: EDGE mode

     3 Blinks: UMTS mode

     4 Blinks: HSDPA mode

     5 Blinks: HSUPA mode

     6 Blinks: LTE mode

   - **SIGNAL LED**: Indicates strength of cellular signal.

     Off: Poor or No signal. Place the device in a location where it gets a better signal.

     Amber: Fair

     Green: Good

   - **POWER LED**:

     Off: No power

     Green: TransPort device is powered

4. **SIM door**: Encloses the SIM sockets. The SIM door must be opened to install the SIM cards. For installation details, refer to the Quick Start Guide that came with your device.

Note To open the SIM door, slide the SIM door out using your finger.

5. **SIM sockets**: SIM 1 and SIM 2 are for use with the Subscriber Identification Module(s) (SIMs).

6. **Primary LTE antenna connector**: This SMA female connector connects the device's primary cellular antenna.

7. **Secondary LTE antenna connector**: This SMA female connector connects the device's secondary cellular antenna.

TransPort WR11 XT

1. **LAN port:** This Ethernet port connects the device to a 10/100 base-T Local Area Network (LAN). The port is capable of auto-sensing for speed and wiring, so it can accept both straight-through or cross-over cable connections.

2. **Power cord input**: This locking power connector connects the device to a power source. The connector should be inserted and rotated to lock in place.

3. **LEDs:**

   • **SERVICE LED**: Indicates the presence and level of cellular service running on the device.

     Off: No cellular service

     1 Blink: GPRS mode

     2 Blinks: EDGE mode

     3 Blinks: UMTS mode

     4 Blinks: HSDPA mode

     5 Blinks: HSUPA mode

     6 Blinks: LTE mode

   • **SIGNAL LED**: Indicates strength of cellular signal.

     Off: Poor or No signal. Place the device in a location where it gets a better signal.

     Amber: Fair

     Green: Good

   • **POWER LED:**

     Off: No power

     Green: TransPort device is powered

4. **SIM door**: Encloses the SIM sockets. The SIM door must be opened to install the SIM cards. For installation details, refer to the Quick Start Guide that came with your device.

5. **SIM sockets**: SIM 1 and SIM 2 are for use with the Subscriber Identification Module(s) (SIMs). Insert SIM cards with the notch facing the bottom-right corner of the device. If you are using one SIM card only, insert it in the SIM 1 slot.

6. **Primary cellular antenna connector**: This SMA female connector connects the device's primary cellular antenna.

7. **Secondary cellular antenna connector**: This SMA female connector connects the device's secondary cellular antenna.

TransPort WR11 hardware specifications

Category	Specification	Value
General features	Dimensions (L x W x H)	3.9" x 5.2" x 1.3" (10 cm x 13.1 cm x 3.2 cm)
	Weight	0.85 lbs.
Cellular	EDGE	850, 900, 1800, 1900 MHz
	GSM	UMTS / HSPA 800/850, 900, 1700 (AWS), 1900, 2100 MHz
	CDMA	1xRTT 800, 1900 MHz
	EVDO	800, 1900 MHz
	LTE-AT&T	700 (B17) / 850 (B5) / AWS1700 (B4) / 1900 (B2)
	LTE-Verizon	700 (B13) / AWS1700 (B4)
	LTE-Worldwide	800 (B20) / 1800 (B3) / 2600 (B7)
Power requirements	Power input voltage	5V DC ± 5%
	Power	3.5W typical, 15W maximum
	Power connector	Locking barrel
Environmental	Operating temperature	0°C to 40°C required **TransPort WR11 XT only:** -30° to +70°C See also Restricted Access Location notice for TransPort WR11 XT on page 89
	Relative humidity	5% to 90% (non-condensing)
	Storage temperature	-40° C to +80° C **TransPort WR11 XT only:** -40°C to+85°C
	RoHS compliance	Yes

Category	Specification	Value
Approvals	Emissions/Immunity	EN 55022: 2010 Class B FCC 15.109(g):2014 Class B FCC 15.109:2014 Class B ICES-003:2012 Class B EN 55022: 2010 Class B FCC 15.107:2014 Class B ICES-003:2012 Class B EN 61000-3-2:2006 (Amended by A1:2009 and A2:2009) Class B EN 61000-3-3:2008 Class B EN 301 489-07 V1.3.1:2005 Class B EN 550024:2010 EN 301 489-07 V1.3.1:2005
	Safety	EN 60950-1: :2006 + A1:2010 + A11:2009 + A12:2011 IEC 60950-1:2005+ A1:2009 UL 60950-1 2nd Ed. Revised 2011-12-19 CSA C22.2 No. 60950-1 -07 + A1:2011
	Mobile certifications-GSM	AT&T & PTCRB
	Mobile certifications-EVDO	Sprint & Verizon
	Mobile certifications-LTE	AT&T; Verizon; PTCRB
	Wireless carrier certifications	Certified by most major carriers.

TransPort WR21 hardware

TransPort WR21 front panel features
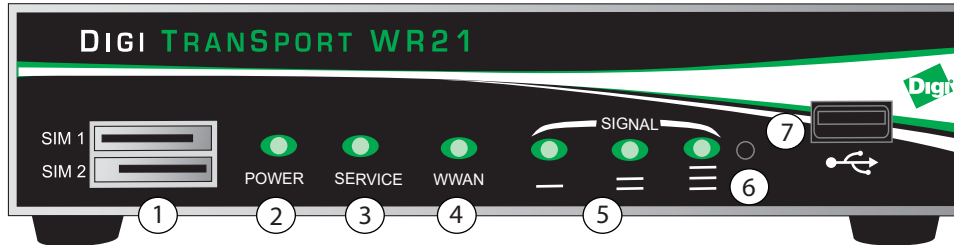
1. **SIM/R-UIM sockets (SIM card models only)**: SIM 1 and SIM 2 are for use with the Subscriber Identification Module(s) (SIMs) or Removable User Identification Module(s) (R-UIMs).

2. **POWER LED**:
    - **Off**: No power
    - **Green**: TransPort device is powered

3. **SERVICE LED**:
    - **Off**: No WWAN network connection
    - **Green**: WWAN network connection
    - **Flashing**: WWAN traffic being transmitted or received

4. **WWAN (Wireless Network) LED**: Indicates the presence and level of cellular service running on the device.
    - **Off**: No cellular service
    - **1 Blink**: GPRS mode
    - **2 Blinks**: EDGE mode
    - **3 Blinks**: UMTS mode
    - **4 Blinks**: HSDPA mode
    - **5 Blinks**: HSUPA mode
    - **6 Blinks**: LTE mode

5. **SIGNAL LED**: Indicate strength of cellular signal.
    - **3 LEDs**: Excellent
    - **2 LEDs**: Good
    - **1 LED**: Fair
    - **0 LEDs**: Poor or No signal

6. **Reset button**: Returns the router to its factory default settings.

7. **USB host connector**: Connects compatible USB 2.0 client devices such as memory sticks, and serial adapters. The total current available to power USB devices is 0.5A.

Reset the TransPort WR21

1. Turn the router on and wait 15 seconds for the router to complete its initialization process.

2. Press and hold the reset button gently for 5 seconds. After this time, the router will automatically re-boot and display a pattern of alternating LEDs flashing followed by the normal boot sequence.

CAUTION! Do not remove power from the router during this operation, as corruption of the flash memory may occur.

TransPort WR21 rear panel features
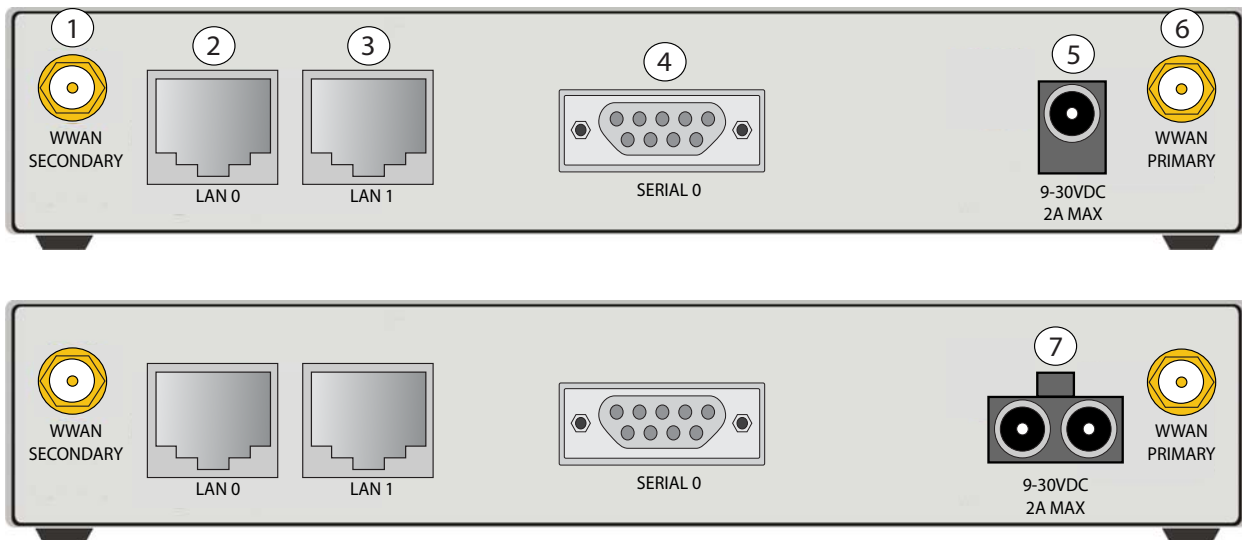
1. **Secondary cellular (WWAN) antenna connector**: This SMA female connector connects the router's secondary cellular antenna. It is highly recommended to use the secondary antenna for diversity. In most circumstances, dual antennas will provide improved signal strength thus better performance.

2. **LAN 0 port**: This RJ45 port connects the router to a 10/100 base-TLAN. The port is auto-sensing for speed and wiring (straight-through or cross-over).

3. **LAN 1 port** (optional): This RJ45 port connects the router to a 10/100 base-TLAN. The port is auto- sensing for speed and wiring (straight-through or cross-over).

4. **Serial 0 port**: This DB9 port provides an asynchronous RS232 (RS485 optional) serial port with optional RS422/485 support which may be which may be used to connect the router to a compatible serial device. This is a DCE serial port and allows CLI access to the device by default; the baud rate is 115200. For a pinout, see TransPort WR21 serial pinout on page 32.

5. **Power cord input**: This socket connects the router to a power source using either the supplied Power supply or DC power cord. The barrel plug connector can be secured by rotating it by 90 degrees once installed into the Digi TransPort router.

6. **Primary cellular (WWAN) antenna connector**: This SMA female connector connects the router's primary cellular antenna.

7. **Power cord input (terminal block variant)**: This socket connects the router to an alternative power source.

TransPort WR21 serial pinout

SERIAL 0

RS-232 pinout

Pin #	Direction	RS232 DCE	Description
1	Out	DCD	Data Carrier Detect
2	Out	RXD	Receive Data
3	In	TXD	Transmit Data
4	In	DTR	Data Terminal Ready
5	N/A	GND	Ground
6	Out	DSR	Data Set Ready
7	In	RTS	Ready To Send
8	Out	CTS	Clear To Send
9	Out	RI	Ring Indicate

RS422/ RS485 pinout

Pin #	Direction	RS422/ RS485	Description
1	Out	CTS-	Clear To Send -
2	Out	RD+	Receive Data +
3	In	TD+	Transmit Data +
4	In	RTS_B RTS-	Ready To Send -
5	N/A	GND	Ground
6	Out	RD-	Receive Data -
7	In	RTS+	Ready To Send +
8	Out	CTS+	Clear To Send +
9	In	TD-	Transmit -

Notes

- For true RS485 mode (2-wire half-duplex mode), the TD+ and RD+ pair and TD- and RD- pair should be connected together.
- The CTS and RTS signals for optional and not normally needed for RS485.

TransPort WR21 hardware specifications

Category	Specification	Value
General features	Dimensions (L x W x H)	3.9" x 5.2" x 1.3" (10 cm x 13.1 cm x 3.2 cm)
	Weight	0.85 lbs.
	Other	Standard dual SIM (SIM protection cover option)
RF features		
GSM models	GPRS	• GPRS Class 10 • Quad band 850/900/1800/1900 MHz
	EDGE	• GPRS Class 10/EDGE Class 10 • Quad band 850/900/1800/1900 MHz
	HSDPA/HSUPA/UMTS	850/900/1900/2100 MHz with Rx Diversity
CDMA models	CDMA/EV-DO Rev A	• Dual band 800/1900 MHz with Rx Diversity • Optional multi-mode GSM/ EV-DO Gobi support • 450 MHz, 3.1 Mbps down / 1.8 Mbps up • R-UIM support
Power requirements	Power input	9-30 VDC
	Power supply	• 100-240 VAC 50/60 Hz with barrel connector • Optional barrel connector with bare wire leads
	Power consumption	6W @ 12 VDC
Environmental	Operating temperature	-20° C to +55° C; -35° C to +75° C with reduced cellular performance
	Relative humidity	20% to 95% (non-condensing)
	Ethernet isolation	1.5 kV
	Serial port protection (ESD)	1.5 kV

Category	Specification	Value
Approvals	Emissions/Immunity	• CE • FCC Part 15 Class B • AS/NZS CISPR 22 • EN55022 Class B • EN55024
	Safety	• UL 60950 • CSA 22.2 No. 60950 • EN60950
	Mobile Certifications-GSM/UMTS	• R&TTE • EN 301 511
	Mobile Certifications-CDMA/EV-DO	• CDG TIA/EIA-690 • CDG TIA/EIA-98-E
	Wireless Carrier Certifications	Certified by most major carriers. See www.digi.com for current listing.
	Safety	• UL 60950 • CSA 22.2 No. 60950 • EN60950
	Emissions / Immunity	• CE, FCC Part 15 Class B • AS/NZS CISPR 22 • EN55022 Class A

TransPort WR31 hardware

TransPort WR31 hardware features
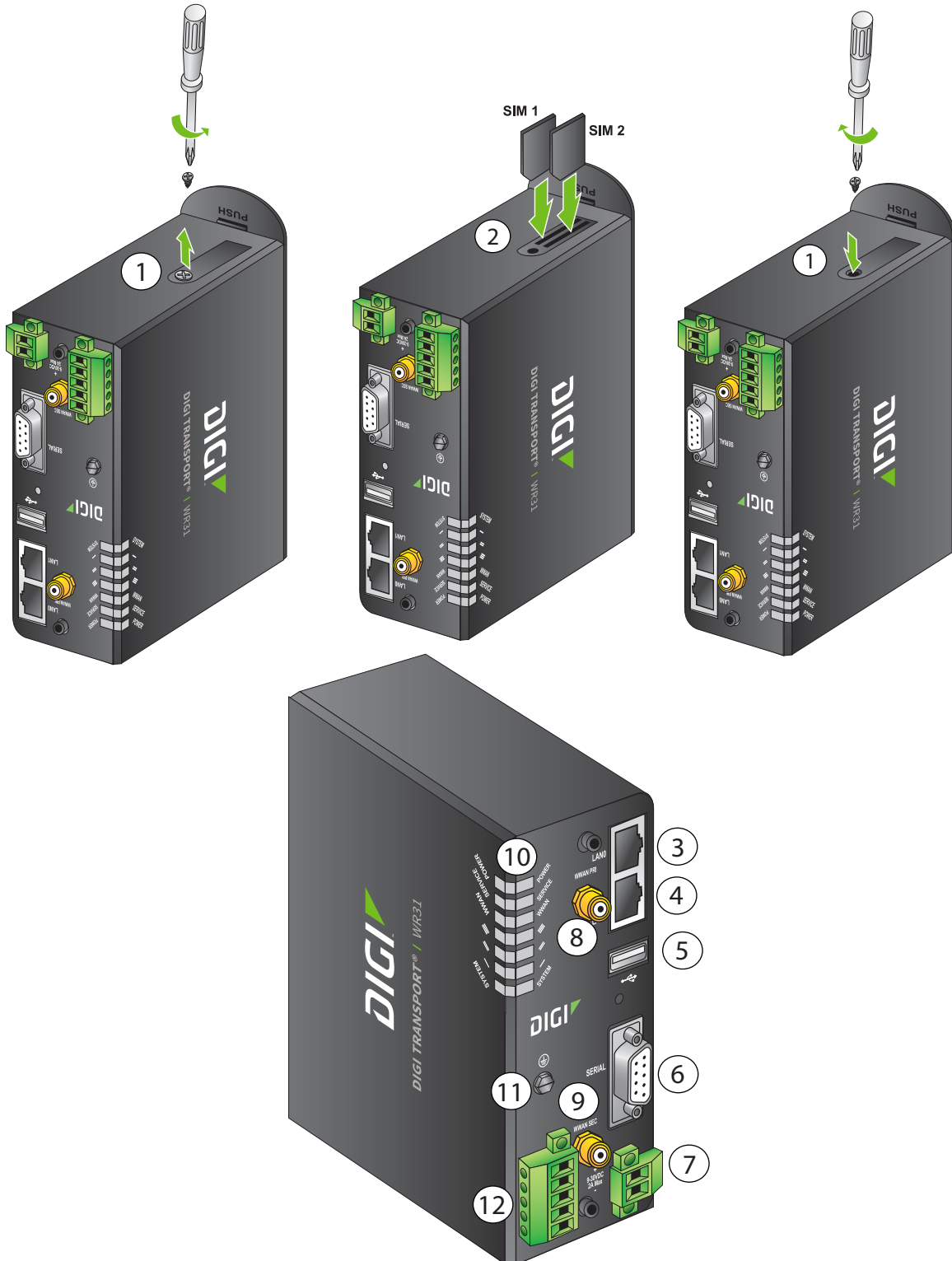
1. **SIM card slot cover**: On the underside of the router. Remove and replace with a Phillips-head screwdriver.

2. **SIM 1 and SIM 2 card slots**: On the underside of the router. SIM 1 and SIM 2 are for use with the Subscriber Identification Module(s) (SIMs) or Removable User Identification Module(s) (R-UIMs). when inserting the SIM card(s) into SIM sockets, SIM 1 is to the middle of the router, and SIM 2 is toward the outside of the router. In both cases, the end of the SIM card with the chamfered corner should be inserted first.

3. **LAN 0 port**: This RJ45 port connects the router to a 10/100 base-TLAN. The port is auto-sensing for speed and wiring (straight-through or cross-over).

4. **LAN 1 port**: This RJ45 port connects the router to a 10/100 base-TLAN. The port is auto-sensing for speed and wiring (straight-through or cross-over).

5. **USB host connector**: Connects compatible USB 2.0 client devices such as memory sticks, and serial adapters. The total current available to power USB devices is 0.5A.

WARNING! The USB port is for use in a normal location only, not a hazardous location.

6. **Serial connector**: This DB9 port provides an asynchronous RS232 (RS485 optional) serial port with optional RS422/485 support which may be which may be used to connect the router to a compatible serial device. This is a DCE serial port and allows CLI access to the device by default; the default serial baud rate is 115200. For a pinout, see TransPort WR31 serial pinout on page 39.

7. **Power connector**: A pluggable connector that connects the router to a power source using either the separately available power supply: Digi part number 76000736, or a DIN rail power supply.

8. **WWAN primary connector**: This SMA male connector connects the router's primary cellular antenna.

9. **WWAN secondary connector**: This SMA male connector connects the router's secondary cellular antenna. For multiple-input and multiple-output (MIMO), both cellular antennas are needed for downloading data.

10. **LEDs**: Indicate startup states and status for various signals and services:

- **POWER LED**:

  Off: No power

  Green: TransPort device is powered

- **SERVICE LED**:

  Off: No WWAN network connection

  Green: WWAN network connection

  Flashing: WWAN traffic being transmitted or received

- WWAN LED: Indicates the presence and level of cellular service running on the device.

  Off: No cellular service

  1 Blink: GPRS mode

  2 Blinks: EDGE mode

  3 Blinks: UMTS mode

4 Blinks: HSDPA mode

5 Blinks: HSUPA mode

6 Blinks: LTE mode

- **SIGNAL LEDs**: Indicate strength of cellular signal.

  3 LEDs: Excellent

  2 LEDs: Good

  1 LED: Fair

  0 LEDs: Poor or No signal

- **SYSTEM LED**: Reserved for user-defined functions.

11. **Earth ground**

12. **Digital/analog I/O connector**: An input/output connector with two digital input/output connections, and a single analog input connection. For more information and wiring diagrams, see TransPort WR31 digital and analog inputs and outputs on page 41.

TransPort WR31 mounting options

The TransPort WR31 can be mounted on a DIN rail, directly to a wall, or in a NEMA enclosure. For wall-mounting or NEMA enclosure installation, purchase the TransPort WR31 Wall Mount Bracket (Digi part number 76000963) and NEMA enclosure equipment, such as the NEMA enclosure, mounting plate, special cabling, and cable glands.

Hazardous Location installation

For Hazardous Location installation, see the *TransPort WR31 Hazardous Locations User Guide* (Digi part number 90001490) on www.digi.com.

TransPort WR31 serial pinout

RS-232 pinout

Pin #	Direction	RS232 DCE	Description
1	Out	DCD	Data Carrier Detect
2	Out	RXD	Receive Data
3	In	TXD	Transmit Data
4	In	DTR	Data Terminal Ready
5	N/A	GND	Ground
6	Out	DSR	Data Set Ready
7	In	RTS	Ready To Send
8	Out	CTS	Clear To Send
9	Out	RI	Ring Indicate

RS422/ RS485 pinout

Pin #	Direction	RS422/ RS485	Description
1	Out	CTS-	Clear To Send -
2	Out	RD+	Receive Data +
3	In	TD+	Transmit Data +
4	In	RTS_B RTS-	Ready To Send -
5	N/A	GND	Ground
6	Out	RD-	Receive Data -
7	In	RTS+	Ready To Send +
8	Out	CTS+	Clear To Send +
9	In	TD-	Transmit -

Notes

- For true RS485 mode (2-wire half-duplex mode), the TD+ and RD+ pair and TD- and RD- pair should be connected together.
- The CTS and RTS signals for optional and not normally needed for RS485.

TransPort WR31 digital and analog inputs and outputs

The TransPort WR31 has an input/output connector with two digital input/output connections, and a single analog input connection.

I/O connector pin assignments

The following figure and table shows the I/O connector, pin assignments, and the signals for each pin.

Pin 5

Pin 1
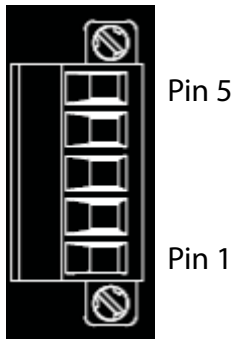
Pin #	Symbol	Description
5	AIN0	Analog Input 0
4	AGND	Analog Return
3	DIO0	Digital I/O 0
2	GND	Digital Return
1	DIO1	Digital I/O 1

TransPort WR31 digital input/output: representative circuit

WR31_3v3

Pull-up Enable Signal

Digital Input

DIGITAL INPUT

Digital Output Enable

DIGITAL RETURN
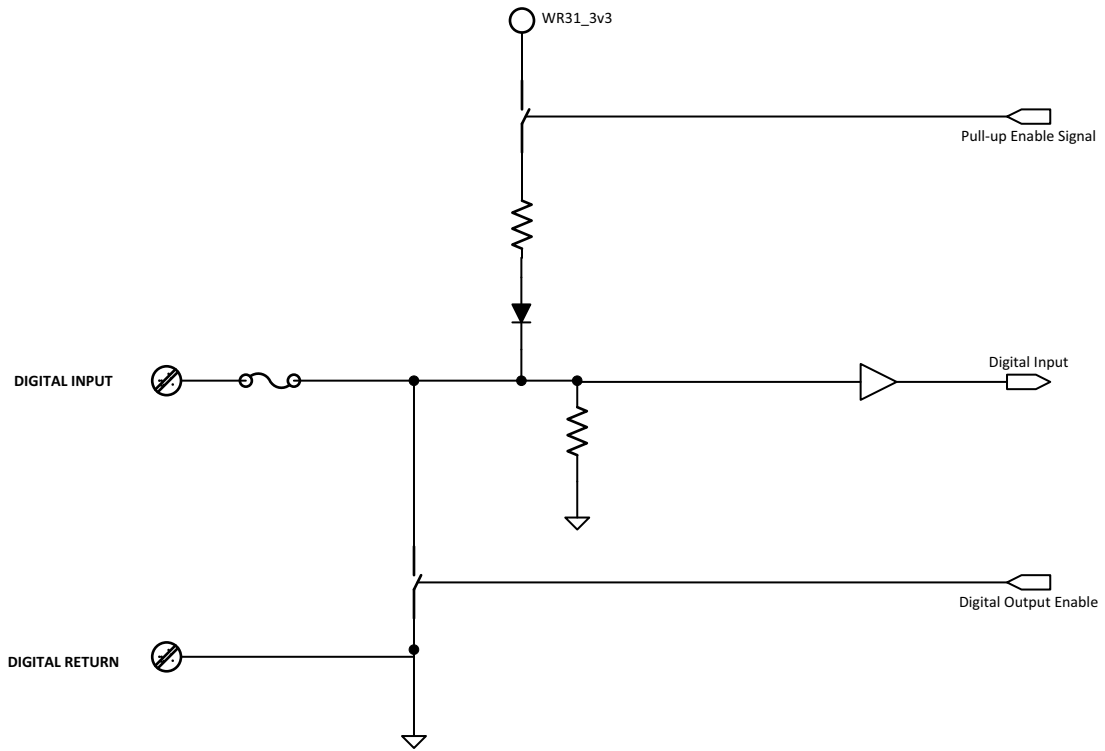
TransPort WR31 analog input: representative circuit

Analog Select Signal

Current Loop
Protector

200-Ohm

Current Loop Signal

Analog Input

Voltage Input Signal

ANALOG INPUT

ANALOG RETURN
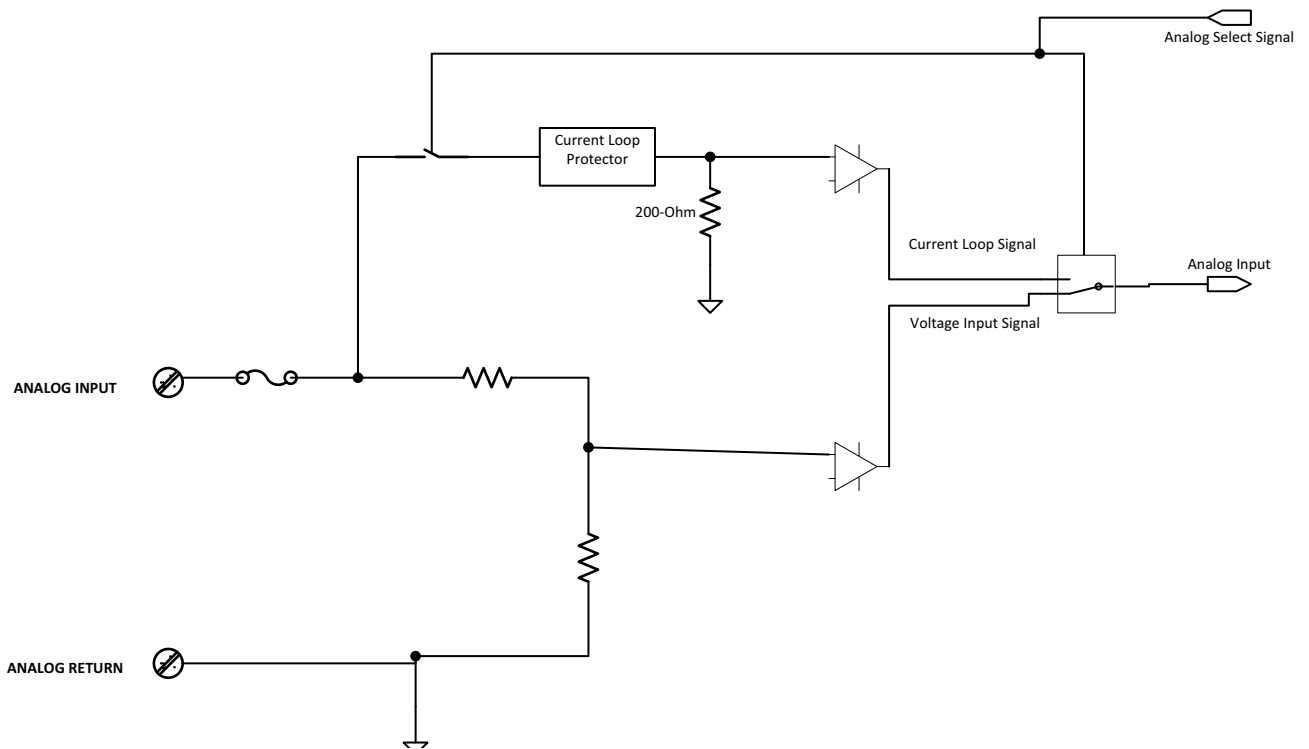
Example digital and analog I/O wiring

Digital input with pullup
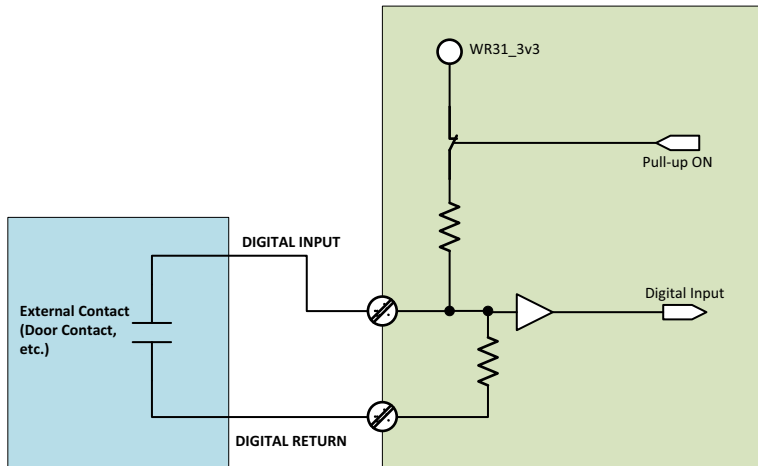
Digital input without pullup

Note that input is HIGH when contact is CLOSED.
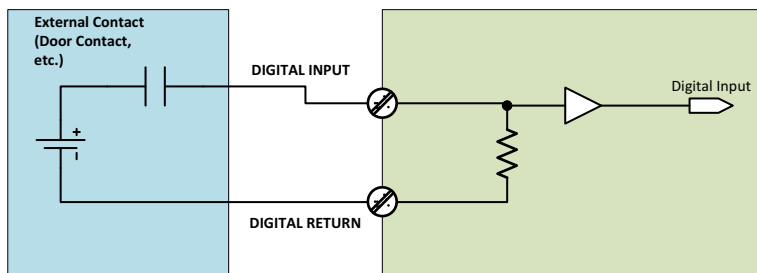
Digital output

The wiring diagram assumes a current-limiting resistor provided by installation or connected device is in use.
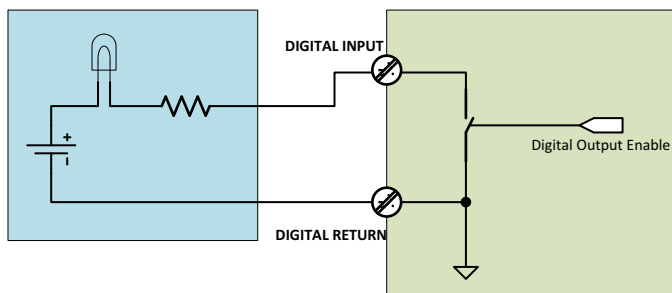
Analog input, 4-20mA input mode
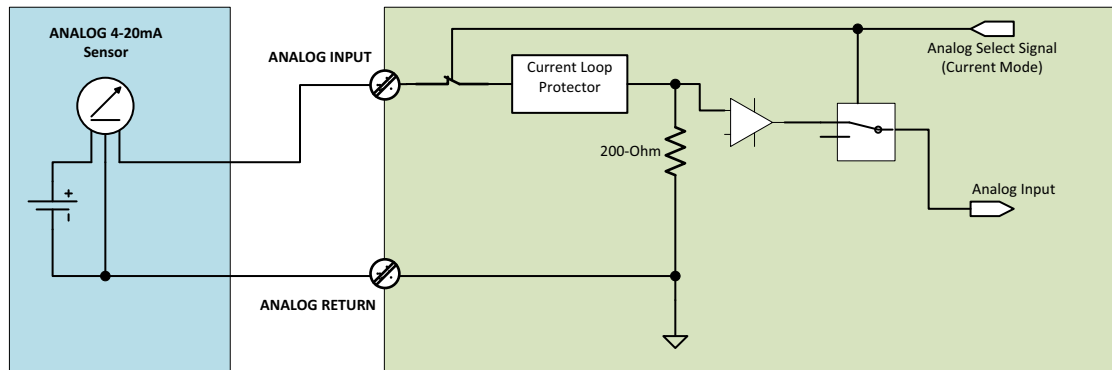
Analog input, 0-10V input mode
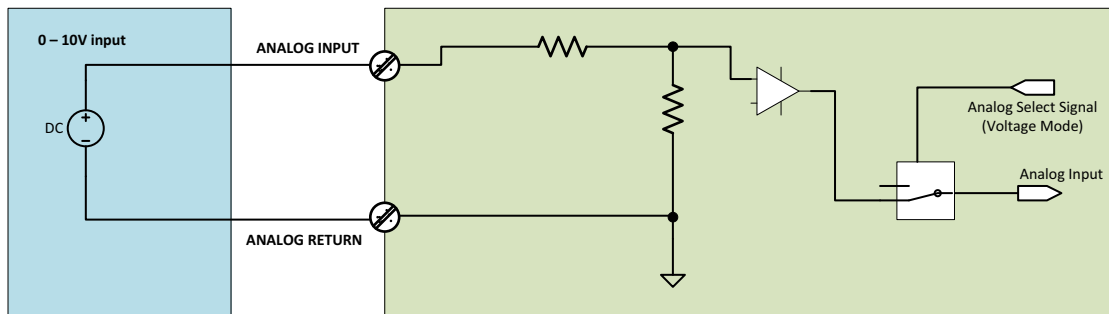
Digital and analog I/O specifications

Digital I/O specifications

Specification	MIN	NOM	MAX	UNITS
Rated Input Voltage	-0.2		30	V
Rated Input Current	-1.0		200	mA
Pull-Up Resistance		10 k		Ohms

Digital input specifications

- This input is a non-inverting Schmitt-trigger input.
- The default state at power-up with no voltage applied is LOW.

Specification	MIN	NOM	MAX	UNITS
+ Threshold	..	1.6	..	V
- Threshold	..	1.0	..	V
Input impedance		1 M		Ohms

Digital output

- This output is an open-collector, sinking driver output.
- The default state at power-up is OFF.

Specification	MIN	NOM	MAX	UNITS
Sink Current	..	..	200	mA
Pull-up Voltage		3		V

Analog input specifications

Specification	MIN	NOM	MAX	UNITS
Resolution	..	..	12	BITS
Accuracy	..	..	0.2	%
Rated Input Voltage	-0.2		30	V
Rated Input Current	0		40	mA

Voltage input mode (default)

Specification	MIN	NOM	MAX	UNITS
Input Voltage	-0.2	..	10.25	V
Input Impedance	..	291 K	..	Ohms

Current loop mode

Specification	MIN	NOM	MAX	UNITS
Minimum Input Voltage	..	2	..	V
Load Resistance	..	200	..	Ohms

TransPort WR31 hardware specifications

Category	Specification	Value
3G/4G LTE Specifications	LTE-North America(L5)	• Software-Defined Multi-Carrier (Verizon, AT&T, and Sprint) • 700/850/1700(AWS)/1900 MHz • 2G/3G GSM fall back to850/900/1700AWS/1800/1900/2100 MHz • 2G/3G CDMA fall back to 800/1900 MHz • Transfer Rate (max): 50 Mbps Up, 100 Mbps Down
	LTE-North America(L6)	• 700/850/1700 (AWS)/1900 MHz • 2G/3G fall back to 850/1900 MHz • Transfer Rate (max): 50 Mbps Up, 100 Mbps Down
	LTE-EMEA/APAC(L1)	• 800/850/900/1800/1900/2100/2600 MHz • 3G fall back to 850/900/1900/2100 MHz • 2G fall back to 850/900/1800/1900 MHz • Transfer Rate (max): 50 Mbps Up, 100 Mbps Down
	HSPA+ -(U9)	• 850/900/1700 (AWS)/1900/2100 MHz • Transfer Rate (max): 5.76 Mbps Up, 21 Mbps Down
	Connectors	• 1 x 50 Ω SMA (Center pin: female) • 2x connectors for LTE models
	SIM Slots	2
	SIM Security	Screw-down SIM cover
Software and Management	Remote Management	• Digi Remote Manager • SNMPv1/v2c/v3
	Local Management	• Web UI (HTTP/HTTPS) • CLI (Telnet, SSH, SMS)
	Management/ Troubleshooting tools	• FTP, SFTP, SCP • Protocol analyzer with PCAP for Wireshark • Event logging with Syslog and SMTP • NTP/SNTP
	Memory	• 20 MB RAM • 10 MB file space

Category	Specification	Value
Ethernet	Ports	(2) RJ-45ports
	Physical Layer	10/100Base-T
	Data Rate	10/100 Mbps (auto-sensing)
	Mode	Full or half duplex (auto-sensing)
	Interface	Auto MDI/MDIX
Serial	Ports	(1) RS-232/422/485
	DTE/DCE	DCE
	Signal Support	TXD, RXD, RTS, CTS, DTR, DCD, DSR, RI
	Flow Control	• Software (XON/XOFF) • Hardware supported
	COM Port Redirector	Digi RealPort®
Digital and analog I/O (see also TransPort WR31 digital and analog inputs and outputs on page 41)	Connector	(5) pin screw-down terminal block
	Digital	0-30VDC. (2) I/O, software-selectable
	Analog	• (1) analog input • 4-20mA or 0-10V • Software Selectable • 12 bit resolution
USB	Ports	(1) USB Type A
	Standard	USB2.0
Physical	Dimensions (L x W x H)	5 in x 3.5 in x 2 in (12.7 cm x 8.9 cm x 5.1cm);
	Weight	1.1 lb. (.5kg)
	Status LEDs	• Power • Service • WWAN • Signal strength (3x) • System (user-programmable LED)
	Enclosure	Aluminum
	Mounting	DIN rail, wall, shelf mount, or NEMA enclosure mount
Power requirements	Power input	9-30VDC
	Power connector	Screw down removable terminal block
	Power consumption	Typical 4 W (Max 6 W)

Category	Specification	Value
Environmental	Hazardous (Class 1 Div 2)	Yes
	Operating Temperature	-30° C to +70° C (-22° F to +158°F) Reduced cellular performance above 60°C
	Storage Temperature	-40° C to +85° C (-40° F to +185°F)
	Ethernet Isolation	1.5 kV RMS
	Serial Port Protection (ESD)	15kV
	Relative Humidity	5% to 95% (non-condensing)
Approvals	Safety	Hazardous Locations: • ANSI/ISA-12.12.01-2015 • CAN/CSA C22.2 NO.213-15 • EN 60079-0:2012+A11:2013 • EN 60079-15:2010 • See the *TransPort WR31 Hazardous Locations User Guide*, Digi part number 90001490. Ordinary Locations: • UL 60950-1, 2nd Edition, 2014-10-14
	Emissions/Immunity	• CE • FCC Part15 Class B • AS/NZS CISPR22 • EN55024 • EN55022 Class B
	GSM/UMTS	PTCRB
	Cellular Carriers	Certified by most major carriers. See www.digi.com for a full list.
Warranty	Product Warranty	5 years

TransPort WR41 hardware

TransPort WR41 front panel features
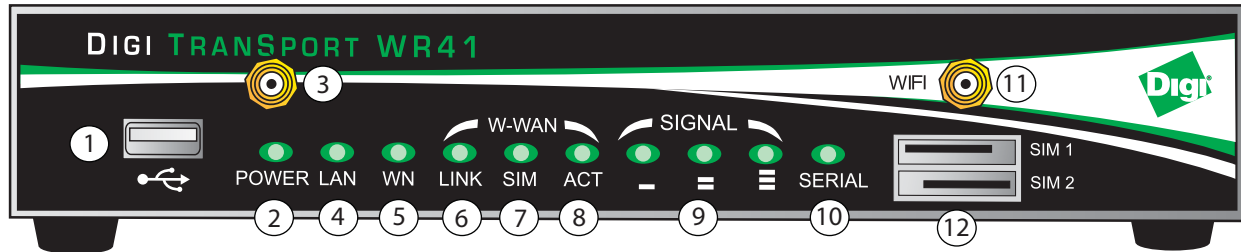
1. **USB host connector**: The USB host connector may be used to connect compatible USB 2.0 client devices such as memory sticks, and serial adapters. The total current available to power USB devices is 0.5A.

2. **POWER LED**:

- **Off**: No power

- **Green**: TransPort device is powered

3. **Secondary Wi-Fi antenna connector (Wi-Fi models only)**: This SMA connector is used to connect the router's secondary Wi-Fi antenna (if fitted).

4. **LAN LED**: Illuminates steadily when there is a network connection to the **LAN** port and flashes when data is transmitted or received.

5. **WN LED**:

- **Wi-Fi models**: Illuminates steady if Wi-Fi activity is present.

- **Non-Wi-Fi models**: Flashes to show which network mode the router is operating in:

    Off: No service

    1 blink: GPRS mode

    2 blinks: EDGE mode

    3 blinks: UMTS mode

    4 blinks: HSDPA mode

    5 blinks: HSUPA mode

    6 blinks: LTE mode

6. **LINK LED**: Illuminates steadily when a wireless WAN data connection has been established.

7. **SIM LED**: Illuminates steadily when a valid SIM card is installed.

8. **ACT LED**: Flashes to indicate that data is being transferred over the wireless WAN network.

9. **SIGNAL LEDs**: Indicate strength of cellular signal.

    - **3 LEDs**: Excellent

    - **2 LEDs**: Good

    - **1 LED**: Fair

    - **0 LEDs**: Poor or No signal

10. **SERIAL LED**: Illuminates steady if a terminal is connected to the **SERIAL** port and the DTR signal is on. Flashes when data is transmitted or received.

11. **Primary Wi-Fi antenna connector (Wi-Fi models only)**: This SMA connector is used to connect the router's primary Wi-Fi antenna.

12. **SIM / R-UIM Sockets (SIM card models only)**: SIM 1 and SIM 2 are for use with the Subscriber Identification Module(s) (SIMs) or Removable User Identification Module(s) (R-UIMs).

TransPort WR41 rear panel features
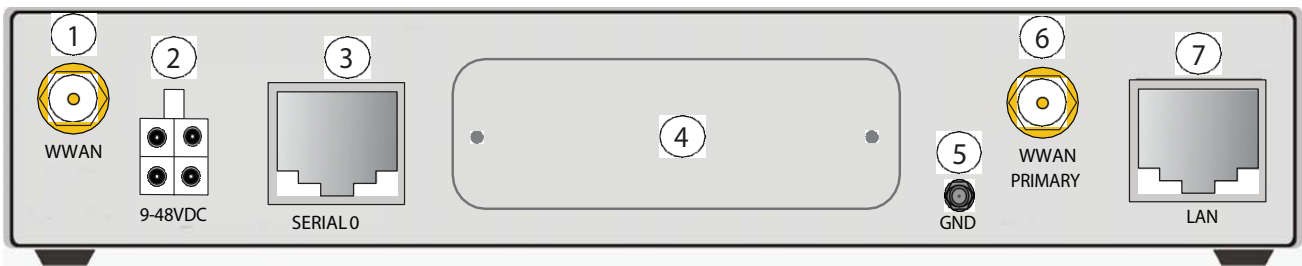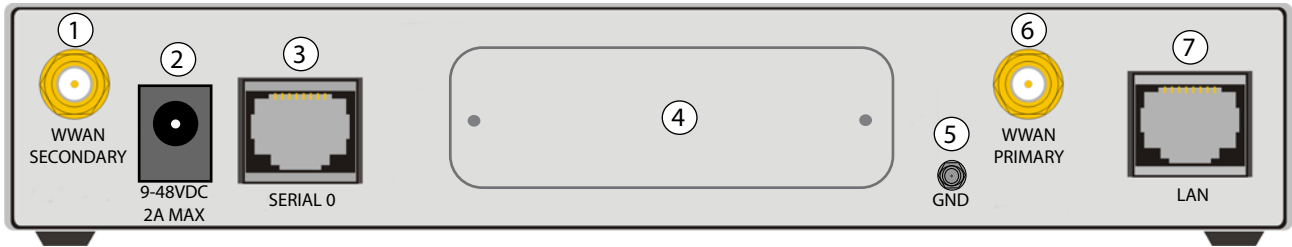
TransPort WR41 under-unit features
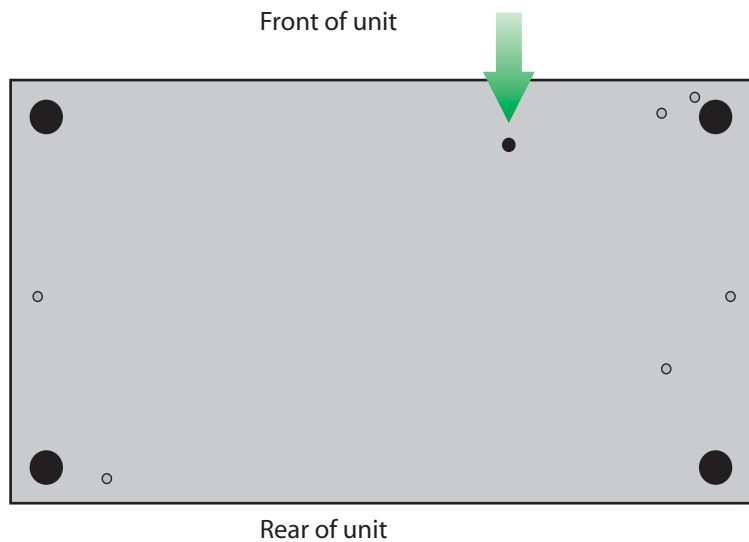
Front of unit

Rear of unit

Reset button

The reset button allows the user to return the router to its factory default settings. It is recessed [to avoid accidental reset], and can be accessed via a small 2.5mm hole located on the underside of the router.

Reset the router

1. Turn the router on and wait 15 seconds for the router to complete its initialization process.

2. Press and hold the reset button gently for 5 seconds. After this time, the router will automatically re-boot and display a pattern of alternating LEDs flashing followed by the normal boot sequence.

CAUTION! Do not remove power from the router during this operation, as corruption of the flash memory may occur.

TransPort WR41 additional hardware features
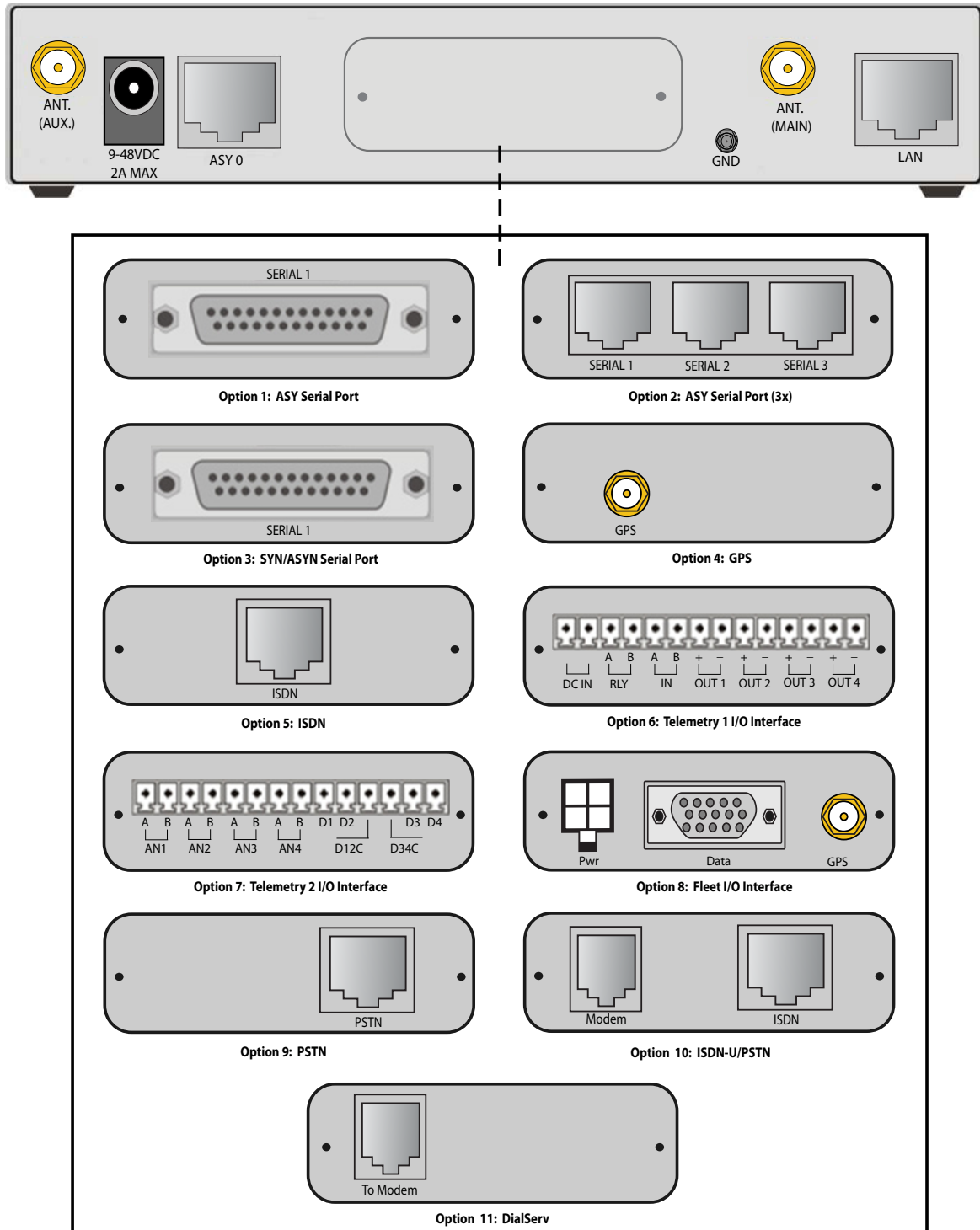
1. **ASY Serial Port**: Provides an additional asynchronous RS232 serial port using a DB25 connector.

2. **ASY Serial Port (3x)**: Provides three additional asynchronous RS232 serial ports using RJ45 connectors.

3. S**YN/ASYN Serial Port**: Provides an X.21/RS422/RS232 synchronous / asynchronous serial port using a DB25 connector.

4. **GPS**: Provides GPS capabilities using an SMA male connector.

5. **ISDN**: Provides an ISDN Basic Rate Interface (BRI) via an RJ45 port. This can be configured either as a TE (terminal endpoint) or as NT-1 (network termination). The option also includes an additional asynchronous serial port via a second RJ45 port.

6. **Telemetry 1 I/O Interface**: Provides 4 opto-isolated digital input ports and 1 opto-isolated digital output port. It also provides a relay I/O port, a voltage monitoring port, and internal temperature monitoring.

7. **Telemetry 2 I/O Interface**: Provides 4 isolated analog I/O ports and 4 non-isolated digital I/O ports.

8. **Fleet I/O Interface**: Provides CAN and J1708 interface, GPS, 4 non-isolated digital I/O ports, ignition sense port, and a 3 axis accelerometer.

9. **PSTN**: Provides a PSTN interface via an RJ45 connector that can be used to dial out and receive calls.

10. **ISDN-U/PSTN**: Provides an ISDN-U interface suitable for the USA plus PSTN interface. It can be configured for Bell-103 modulation in leased line mode as well as a normal PSTN interface.

11. **DialServ**: This RJ11/FXS connection converts a PSTN analog modem to a RS-232 serial signal.

For more information on the Telemetry 1, Telemetry 2, and the Fleet I/O Interfaces please see the product specific user's guides, available on www.digi.com on the TransPort WR41 product **Resources** page.

TransPort WR41 serial pinout
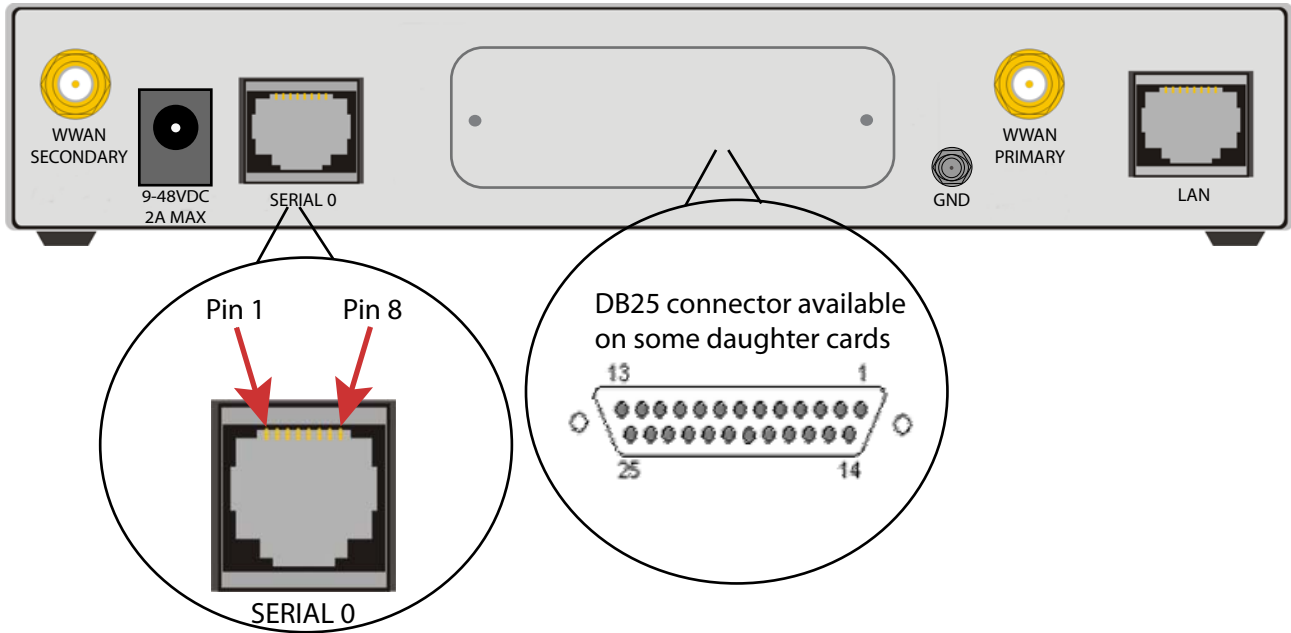
RS-232 port pinouts

Description	RS232 signal	Direction[1]	DB 25 Pin#	RJ45 Pin#
Transmit Data	TxD	in	2	6
Receive Data	RxD	out	3	3
Ready To Send	RTS	in	4	1
Clear To Send	CTS	out	5	8
Data Set Ready	DSR	out	6	n/a
Ground	GND	n/a	7	5
Data Carrier Detect	DCD	out	8	7
Transmitter Clock	TxC	out	15	n/a
Receiver Clock	RxC	out	17	n/a
Data Terminal Ready	DTR	in	20	2
Ring Indicate	RI	out	22	n/a
External Transmitter Clock	ETC	in	24	n/a

1 With respect to Digi routers

Asynchronous port (ASY 0) pinout
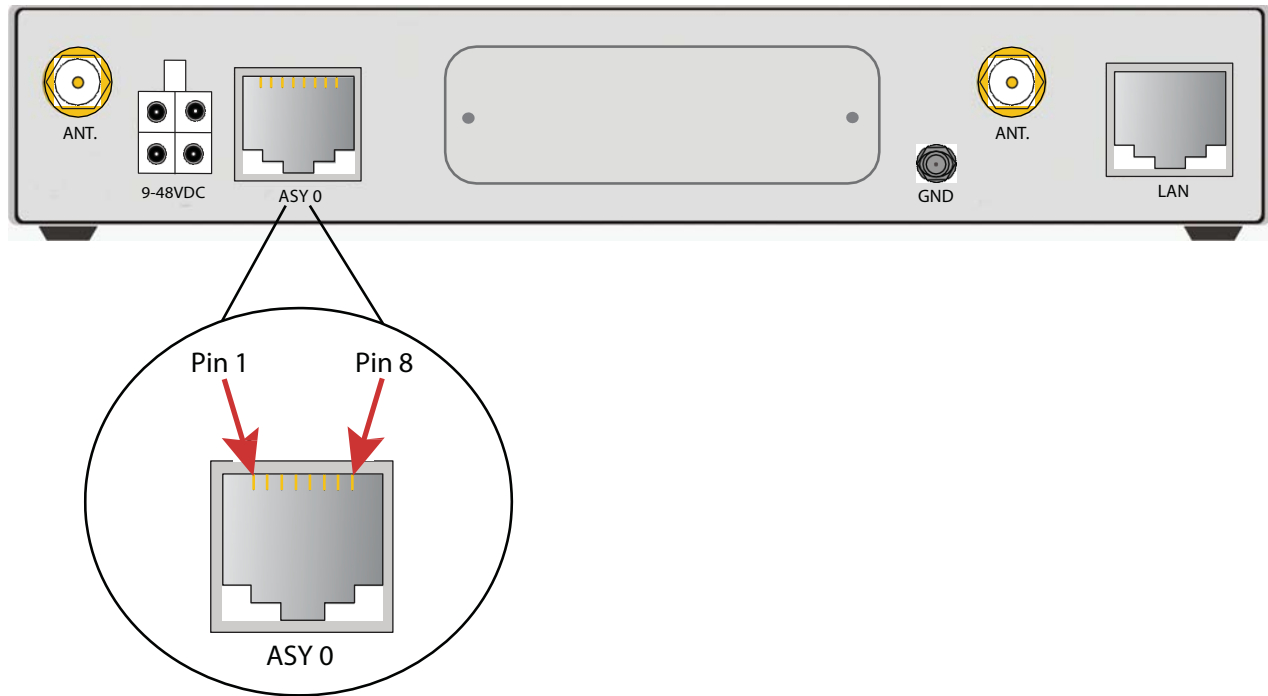
Pin #	Direction	RS232 DCE	Description
1	In	RTX	Ready To Send
2	In	DTR	Data Terminal Ready
3	Out	RxD	Receive Data
4	-	-	-
5	N/A	GND	Ground
6	In	TxD	Transmit Data
7	Out	DCD	Data Carrier Detect
8	Out	CTS	Clear To Send

TransPort WR41 hardware specifications

Category	Specification	Value
General features	Dimensions (L x W x H)	4.7" x 6.8" x 1.3" (12 cm x 17.3 cm x 3.2 cm)
	Weight	1.08 lb (0.49Kg)
	Other	Standard dual SIM (SIM protection cover option)
RF features: GSM Models	GPRS	• GPRS Class 10 • Quad band 850/900/1800/1900 MHz
	EDGE	• GPRS Class 10/EDGE Class 10 • Quad band 850/900/1800/1900 MHz
	HSDPA/HSUPA/UMTS	850/900/1900/2100 MHz with Rx Diversity
RF features: CDMA models	CDMA/EV-DO Rev A	• Dual band 800/1900 MHz with Rx Diversity • Optional multi-mode GSM/ EV-DO Gobi support • 450 MHz • 3.1 Mbps down / 1.8 Mbps up • R-UIM support
Power requirements	Power Input	8-48 VDC
	Power Supply	• 100-240 VAC 50/60 Hz with barrel connector • Optional barrel connector with bare wire leads
	Power Consumption	6W @ 12 VDC to WR41
Environmental	Operating Temperature	• -20° C to +55° C • -25° C to +70° C with reduced cellular performance **Wi-Fi models**: • -5° C to +55° C • -10° C to +70° C with reduced performance
	Relative Humidity	20% to 95% (non-condensing)
	Ethernet Isolation	1.5 kV
	Serial Port Protection (ESD)	1.5 kV

Category	Specification	Value
Approvals	Emissions/Immunity	• EN55022 Class B • CE • FCC Part 15 Class B • AS/NZS CISPR 22 • EN55024
	Safety	• UL 60950 • CSA 22.2 No. 60950 • EN60950
	Mobile Certifications-GSM/UMTS	• PTCRB • NAPRD.03 • GCF-CC • R&TTE • EN 301 511
	Mobile Certifications-CDMA/ EV-DO	• CDG TIA/EIA-690 • CDG TIA/EIA-98-E
	Wireless Carrier Certifications	Certified by most major carriers. See www.digi.com for current listing.
	Vehicle Related Certifications	• 2004/104/EC • 2005/49/EC • 2005/83/EC • 2006/28/EC • 72/245/EEC • ISO7637-2 Class C

TransPort WR44 / WR44 R hardware

TransPort WR44 enclosure features

TransPort WR44
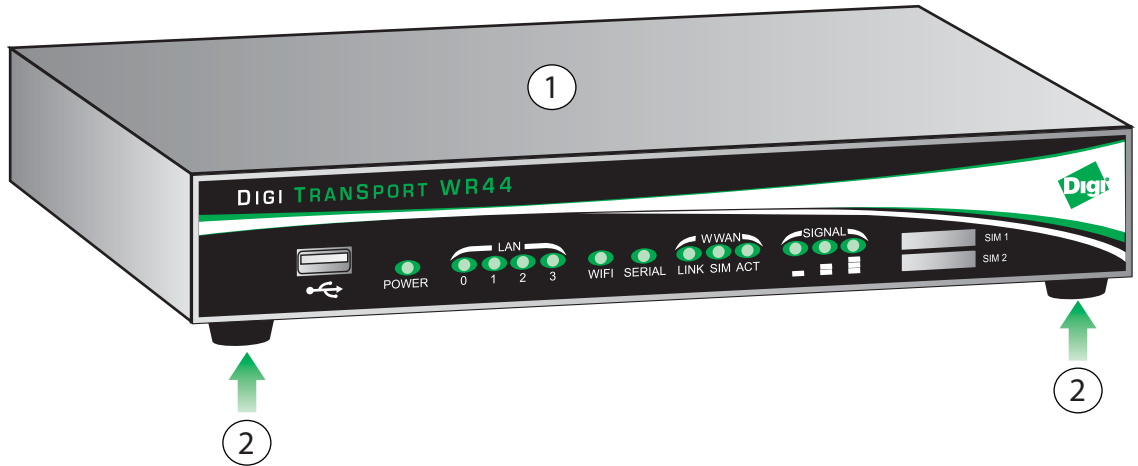
1. Commercial enclosure
2. Mounting feet

TransPort WR44 R
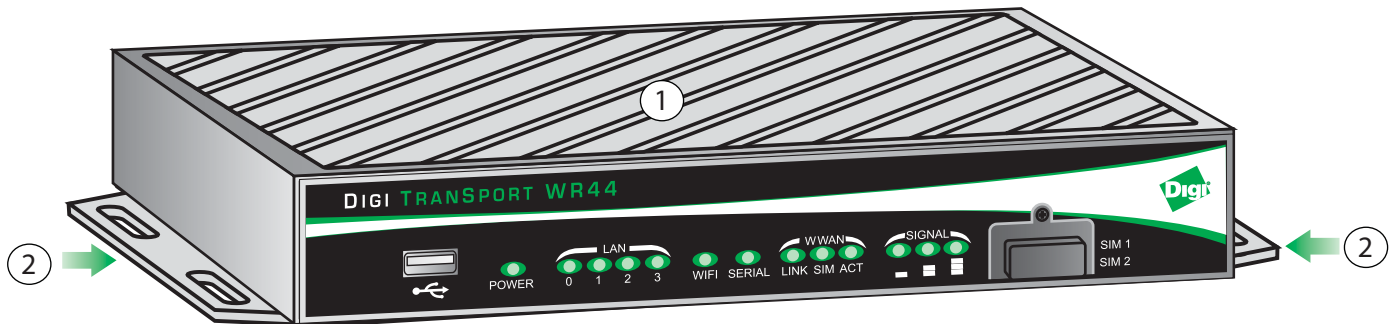
1. Rugged enclosure
2. Mounting tabs

TransPort WR44 front panel features

TransPort WR44 models with cellular interface
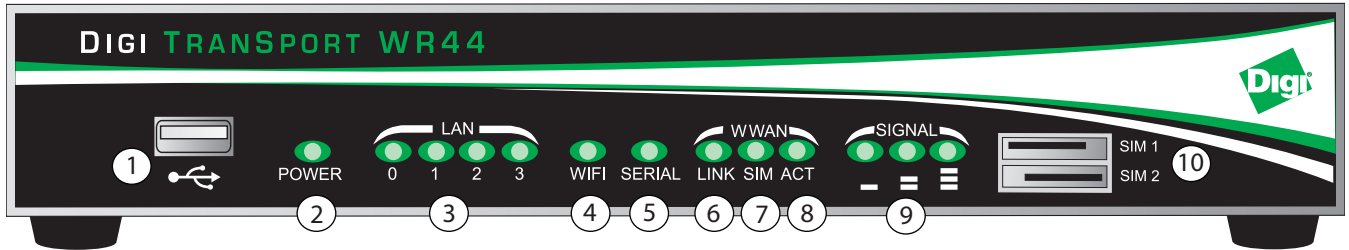
TransPort WR44 models without cellular interface
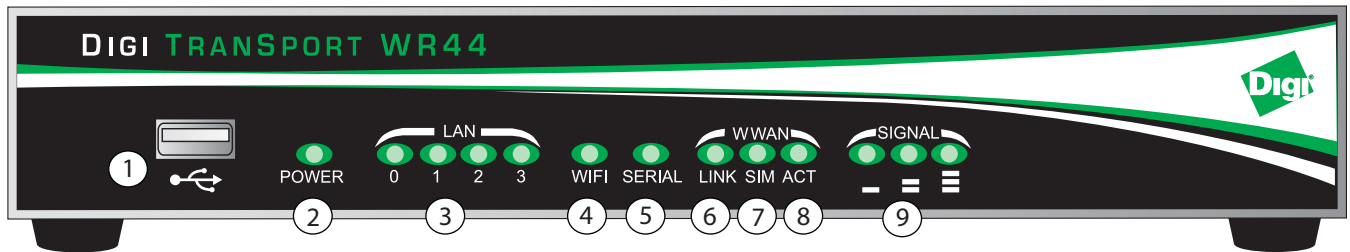
1. **USB host connector**: The USB host connector may be used to connect compatible USB 2.0 client devices such as memory sticks, and serial adapters. The total current available to power USB devices is 0.5A.

2. **POWER LED**:

   - **Off**: No power

   - **Green**: TransPort device is powered

3. **LAN (0, 1, 2, 3) LED**: Illuminates steadily when there is a network connection to the LAN port and flashes when data is transmitted or received.

4. **Wi-Fi LED**:

   - **Wi-Fi models**: Illuminates steady if Wi-Fi activity is present.

5. **SERIAL LED**: Illuminates steadily if a terminal is connected to the SERIAL port and the DTR signal is on. Flashes when data is transmitted or received.

6. **LINK LED**: Illuminates steadily when a wireless data connection has been established.

7. **SIM LED**:

   - **Cellular models**: Illuminates steadily when a valid SIM card is installed.

   - **Models without cellular interface**: Not operational.

8. **ACT LED**: Flashes to indicate that data is being transferred over the wireless network.

9. **SIGNAL LED**:

   - **Cellular models**: Indicate strength of cellular signal.

     3 LEDs: Excellent

     2 LEDs: Good

     1 LED: Fair

     0 LEDs: Poor or No signal

   - **Models without cellular interface**: Not operational.

10. **SIM / R-UIM Sockets**:

    - **Cellular SIM card models only)**: Illuminates steadily when a valid SIM card is installed.

    - **Models without cellular interface**: Not operational.

TransPort WR44 rear panel features
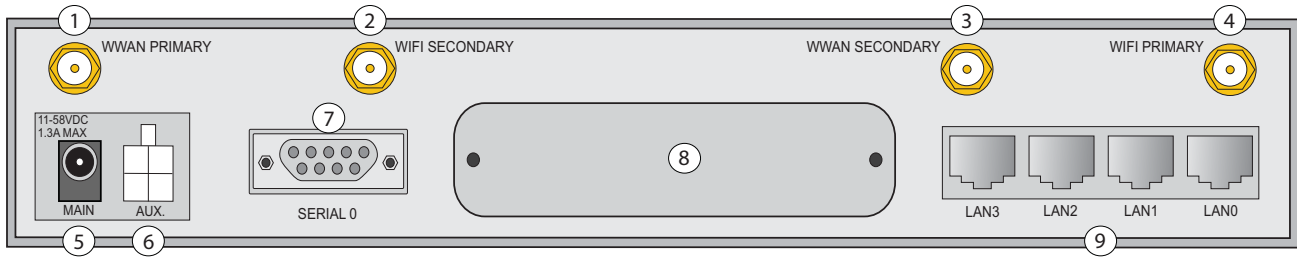
1. **Primary cellular (WWAN) antenna connector**: This SMA female connector is used to connect the router's primary cellular antenna.

2. **Secondary Wi-Fi (WLAN) Antenna connector (Wi-Fi models only)**: This SMA male connector is used to connect the router's secondary Wi-Fi antenna.

3. **Secondary cellular (WWAN) antenna connector (WR44-U and WR44-C models)**: This SMA female connector is used to connect the router's secondary cellular antenna. It is highly recommended to use   the secondary antenna for diversity. In most circumstances, dual antennas will provide improved signal strength thus better performance.

4. **Primary Wi-Fi (WLAN) antenna connector (Wi-Fi models only)**: This SMA male connector is used to connect the router's primary Wi-Fi antenna.

5. **Power cord input**: This socket is used to connect the router to a power source.

Note The power supply has a twist-lock connector which can be secured by rotating it 90 degrees once installed into the TransPort router.

---

6. **11-58VDC (Aux)**: This socket can be used to connect the router to an alternative 11-58VDC power supply (not supplied) using a fused power cable which can be purchased separately. This cable also contains two programmable IO signal lines, one is an input signal, and the other is an input/output signal.

7. **SERIAL 0 port**: This DB9 port provides an asynchronous RS232 serial port which may be used to connect the router to a compatible serial device. This is a DCE serial port and allows CLI access to the device by default; the baud rate is 115200.

8. **Hardware expansion port**: Various hardware upgrades are available for this router and are populated via this expansion port. See the TransPort WR44 additional hardware features on page 66 section for further information.

9. **LAN ports**: These RJ45 ports are used to connect the router to a 10/100 base-T LAN. These ports are auto- sensing for speed and wiring (straight-through or cross-over).

TransPort WR44 under unit features

TransPort WR44

[Front of Unit]

[Rear of Unit]

TransPort WR44 R

[Front of Unit]

[Rear of Unit]
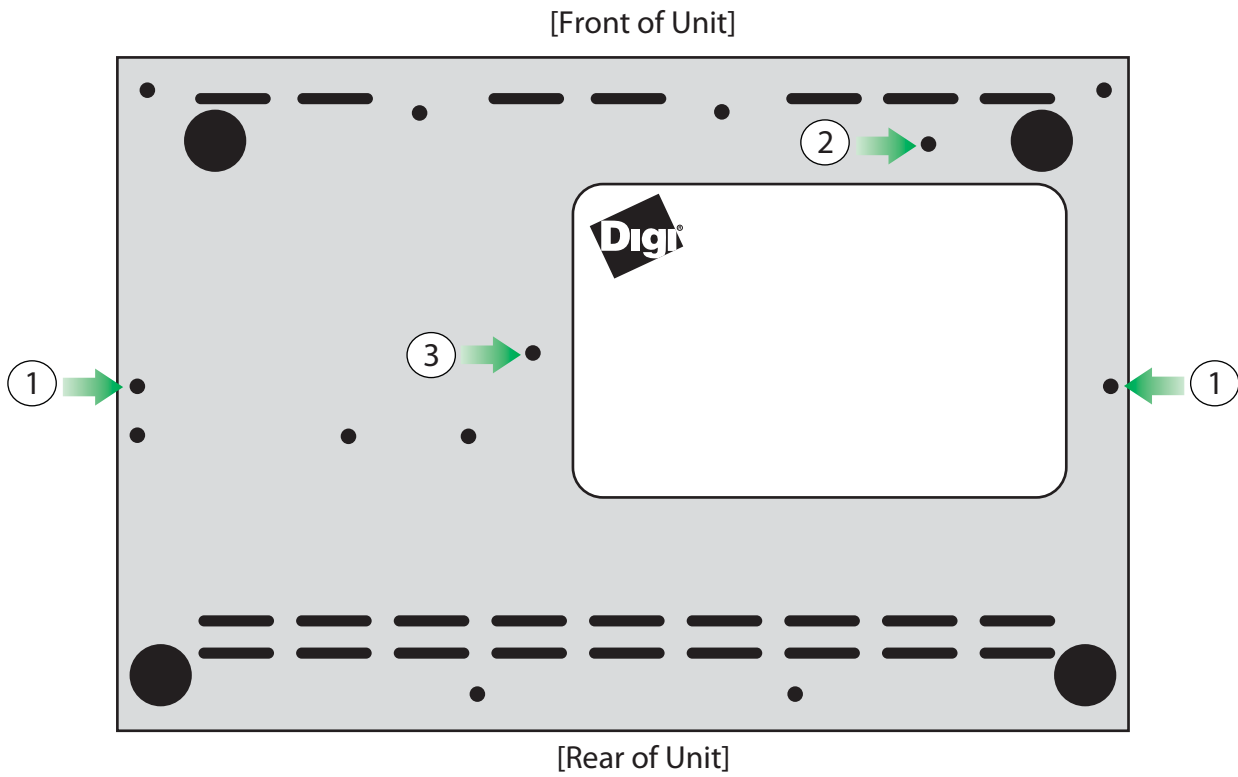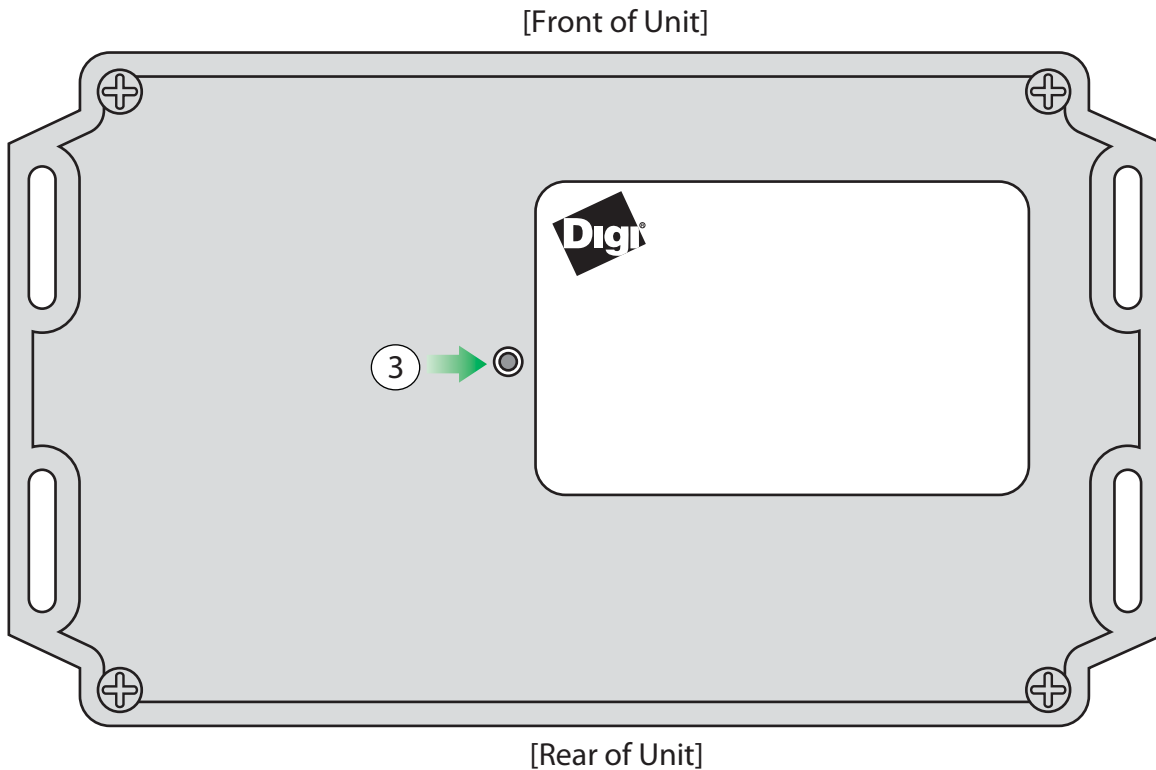
1. Mounting holes.

2. SIM slot cover plate mounting hole.

3. **Reset button**: The reset button allows the user to return the router to its factory default settings. It is recessed [to avoid accidental reset], and can be accessed via a small 2.5mm hole located on the underside of the router.

Reset the TransPort WR44/WR44 R

1. Turn the router on and wait 15 seconds for the router to complete its initialization process.

2. Press and hold the reset button gently for 5 seconds. After this time, the router will automatically re-boot and display a pattern of alternating LEDs flashing followed by the normal boot sequence.

CAUTION! Do not remove power from the router during this operation, as corruption of the flash memory may occur.

TransPort WR44 additional hardware features

The rear panel diagram shows:

- **WWAN PRIMARY** antenna connector
- **WIFI SECONDARY** antenna connector
- **WWAN SECONDARY** antenna connector
- **WIFI PRIMARY** antenna connector
- 11-58VDC 1.3A MAX power (MAIN / AUX.)
- SERIAL 0
- LAN3, LAN2, LAN1, LAN0

Option 1: ASY Serial Port (3x)
SERIAL 1, SERIAL 2, SERIAL 3

Option 2: SYN/ASYN Serial Port
SERIAL 1

Option 3: GPS
GPS

Option 4: ISDN
ISDN

Option 5: Telemetry 1 I/O Interface
DC IN, RLY (A B), IN (A B), OUT 1 (+ −), OUT 2 (+ −), OUT 3 (+ −), OUT 4 (+ −)

Option 6: Telemetry 2 I/O Interface
AN1 (A B), AN2 (A B), AN3 (A B), AN4 (A B), D12C (D1 D2), D34C (D3 D4)

Option 7: Fleet I/O Interface
Pwr, Data, GPS

Option 8: PSTN
PSTN

Option 9: ISDN-U/PSTN
Modem, ISDN

Option 10: DialServ
To Modem

1. **ASY serial port (3x)**: Provides three additional asynchronous RS232 serial ports using RJ45 connectors.

2. **SYN/ASYN serial port**: Provides an X.21/RS422/RS232 synchronous / asynchronous serial port using a DB25 connector.

3. **GPS antenna connector (GPS models only)**: Provides GPS capabilities using an SMA male connector.

4. **ISDN**: Provides an ISDN Basic Rate Interface (BRI) via an RJ45 port. This can be configured either as a TE (terminal endpoint) or as NT-1 (network termination). The option also includes an additional asynchronous serial port via a second RJ45 port.

5. **Telemetry 1 I/O interface**: Provides 4 opto-isolated digital input ports and 1 opto-isolated digital output port. It also provides a relay I/O port, a voltage monitoring port, and internal temperature monitoring.

6. **Telemetry 2 I/O interface**: Provides 4 isolated analog I/O ports and 4 non-isolated digital I/O ports.

7. **Fleet I/O interface**: Provides CAN and J1708 interface, GPS, 4 non-isolated digital I/O ports, ignition sense port, and a 3 axis accelerometer.

8. **PSTN**: Provides a PSTN interface via an RJ45 connector that can be used to dial out and receive calls.

9. **ISDN-U/PSTN**: Provides an ISDN-U interface suitable for the USA plus PSTN interface. It can be configured for Bell-103 modulation in leased line mode as well as a normal PSTN interface.

10. **DialServ**: This RJ11/FXS connection converts a PSTN analog modem to a RS-232 serial signal.

For more information on the Telemetry 1, Telemetry 2, and the Fleet I/O Interfaces please see the product specific user's guides, available on www.digi.com on the TransPort WR44 product **Resources** page.

TransPort WR44 / WR44 R serial pinout

RS-232 port Pin Outs

Description	RS232 signal	Direction[1]	DB 25 Pin#	DB 9 Pin#	RJ45 Pin #
Transmit Data	TxD	in	2	3	6
Receive Data	RxD	out	3	2	3
Ready To Send	RTS	in	4	7	1
Clear To Send	CTS	out	5	8	8
Data Set Ready	DSR	out	6	6	n/a
Ground	GND	n/a	7	5	5
Data Carrier Detect	DCD	out	8	1	7
Transmitter Clock	TxC	out	15	n/a	n/a
Receiver Clock	RxC	out	17	n/a	n/a
Data Terminal Ready	DTR	in	20	4	2
Ring Indicate	RI	out	22	9	n/a
External Transmitter Clock	ETC	in	24	n/a	n/a

1 With respect to Digi routers

TransPort WR44 / TransPort WR44 R hardware specifications

Category	Specification	Value
General features	Dimensions (L x W x H)	5.7" x 8.3" x 1.6" (145 mm x 210 mm x 40 mm)
	Weight	1.98 lb (0.9Kg)
	Other	Standard dual SIM (SIM protection cover option); Conformal coating (option)
RF features		
GSM models	GPRS	• GPRS Class 10 • Quad band 850/900/1800/1900 MHz
	EDGE	• GPRS Class 10/EDGE Class 10 • Quad band 850/900/1800/1900 MHz
	HSDPA/HSUPA/UMTS	850/900/1900/2100 MHz with Rx Diversity
CDMA models	CDMA/EV-DO Rev A	• Dual band 800/1900 MHz with Rx Diversity • Optional multi-mode GSM/EV-DO Gobi support • 450 MHz • 3.1 Mbps down / 1.8 Mbps up • R-UIM support
Power requirements	Power Input	11-58 VDC
	Power Supply	• 100-240 VAC 50/60 Hz with barrel connector • Optional Molex connector with bare wire leads
	Power Consumption	15W @ 12 VDC to WR44
Environmental	Operating Temperature	• WR44: 0° C to +60° C • WR44 Extended Temp/WR44R: -40° C to +75° C; -20° C to +75° C (Wi-Fi models only) • Reduced cellular performance may occur above +60° C
	Relative Humidity	20% to 95% (non-condensing)
	Ethernet Isolation	1.5 kV
	Serial Port Protection (ESD)	1.5 kV

Category	Specification	Value
Approvals	Emissions/Immunity	• CE • FCC Part 15 Class B • AS/NZS CISPR 22 • EN55024 • EN55022 Class B (WR44 models with VDSL are Class A)
	Safety	• UL 60950 • CSA 22.2 No. 60950 • EN60950
	Mobile Certifications-GSM/UMTS	• PTCRB • NAPRD.03 • GCF-CC • R&TTE • EN 301 511
	Mobile Certifications-CDMA/EV-DO	• CDG TIA/EIA-690 • CDG TIA/EIA-98-E
	Wireless Carrier Certifications	Certified by most major carriers. See www.digi.com for current listing.
	Safety	• UL 60950 • CSA 22.2 No. 60950 • EN60950
	Emissions / Immunity	• CE • FCC Part 15 Class B • AS/NZS CISPR 22 • EN55022 Class A
	Vehicle Related Certifications	• 2004/104/EC • 2005/49/EC • 2005/83/EC • 2006/28/EC • 72/245/EEC • ISO7637-2 Class C

TransPort WR44 RR hardware

TransPort WR44 RR enclosure features

1. Rugged Enclosure
2. Mounting Tabs

TransPort WR44 RR front panel features
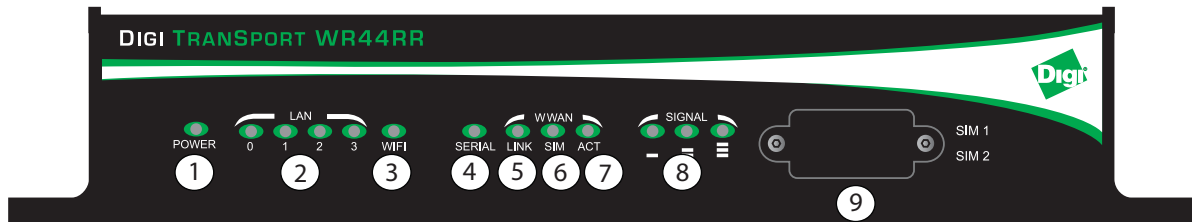
1. **POWER LED**:

    - **Off**: No power
    - **Green**: TransPort device is powered

2. **LAN (0, 1, 2, 3) LED**: Illuminates steadily when there is a network connection to the LAN port and flashes when data is transmitted or received.

3. **Wi-Fi LED**:

    - **Wi-Fi models only**: Illuminates steady if Wi-Fi activity is present.

4. **SERIAL LED**: Illuminates steadily if a terminal is connected to the **SERIAL** port and the DTR signal is on.

5. **LINK LED**: Illuminates steadily when a wireless WAN data connection has been established.

6. **SIM LED**: Illuminates steadily when a valid SIM card is installed.

7. **ACT LED**: Flashes to indicate that data is being transferred over the wireless WAN network.

8. **SIGNAL LEDs**: Indicate strength of cellular signal.

    - **3 LEDs**: Excellent
    - **2 LEDs**: Good
    - **1 LED**: Fair
    - **0 LEDs**: Poor or No signal

9. **SIM / R-UIM sockets (SIM card models only)**: SIM 1 and SIM 2 are for use with the Subscriber Identification Module(s) (SIMs) or Removable User Identification Module(s) (R-UIMs).

TransPort WR44 RR rear panel features
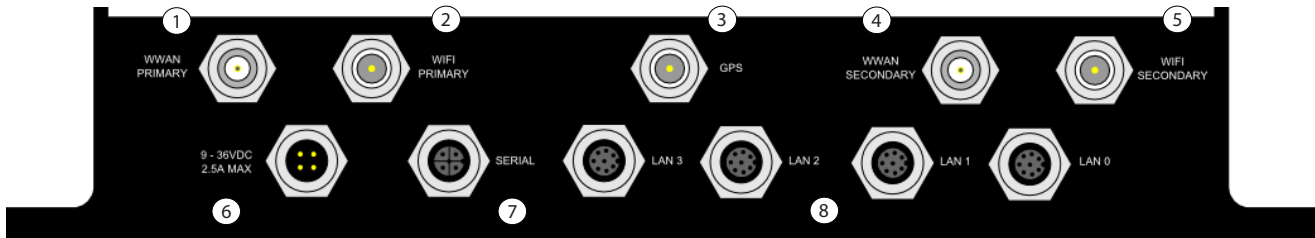
1. **Primary cellular (WWAN) antenna connector**: This TNC female connector is used to connect the router's primary cellular antenna.

2. **Primary Wi-Fi (WLAN) antenna connector (Wi-Fi models only)**: This TNC male connector is used to connect the router's secondary Wi-Fi antenna.

3. **GPS antenna connector (GPS models only)**: This TNC male connector is used to connector the connect the router's GPS antenna.

4. **Secondary cellular (WWAN) antenna connector**: This TNC female connector is used to connect the router's secondary cellular antenna. It is highly recommended to use the secondary antenna for diversity. In most circumstances, dual antennas will provide improved signal strength thus better performance.

5. **Secondary Wi-Fi (WLAN) antenna connector (Wi-Fi models only)**: This TNC male connector is used to connect the router's secondary Wi-Fi antenna.

6. **9-36VDC socket**: This M12 socket is used to connect the router to an alternative 9-36VDC power supply (not supplied) using the supplied fused power cable. This cable also contains two programmable GPIO signal lines.

7. **Serial port**: This M12 port provides an asynchronous RS232 serial port which may be used to connect the router to a compatible serial device. This is a DCE serial port and allows CLI access to the device by default; the baud rate is 115200.

8. **LAN ports**: These M12 ports are used to connect the router to a 10/100 base-T LAN. These ports are auto- sensing for speed and wiring (straight-through or cross-over).

TransPort WR44 RR connectors and pinouts

Pin locations

4 pin connector pin locations
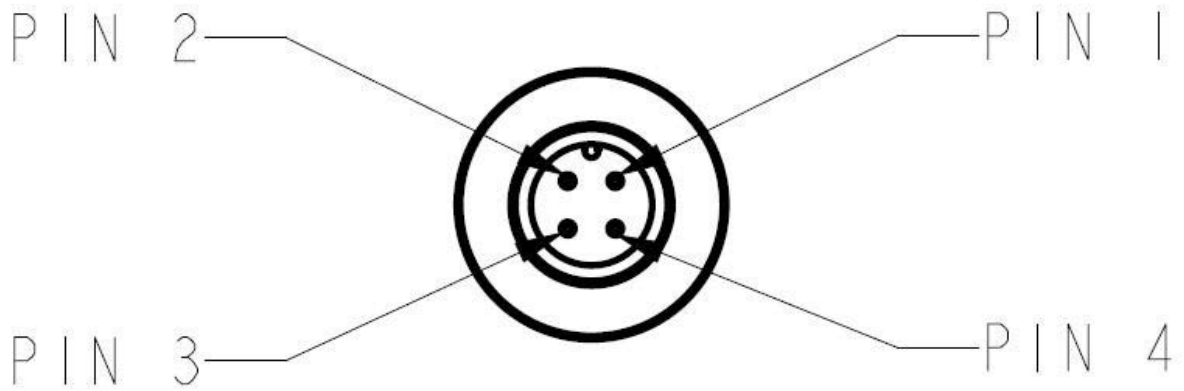
8-pin connector pin locations
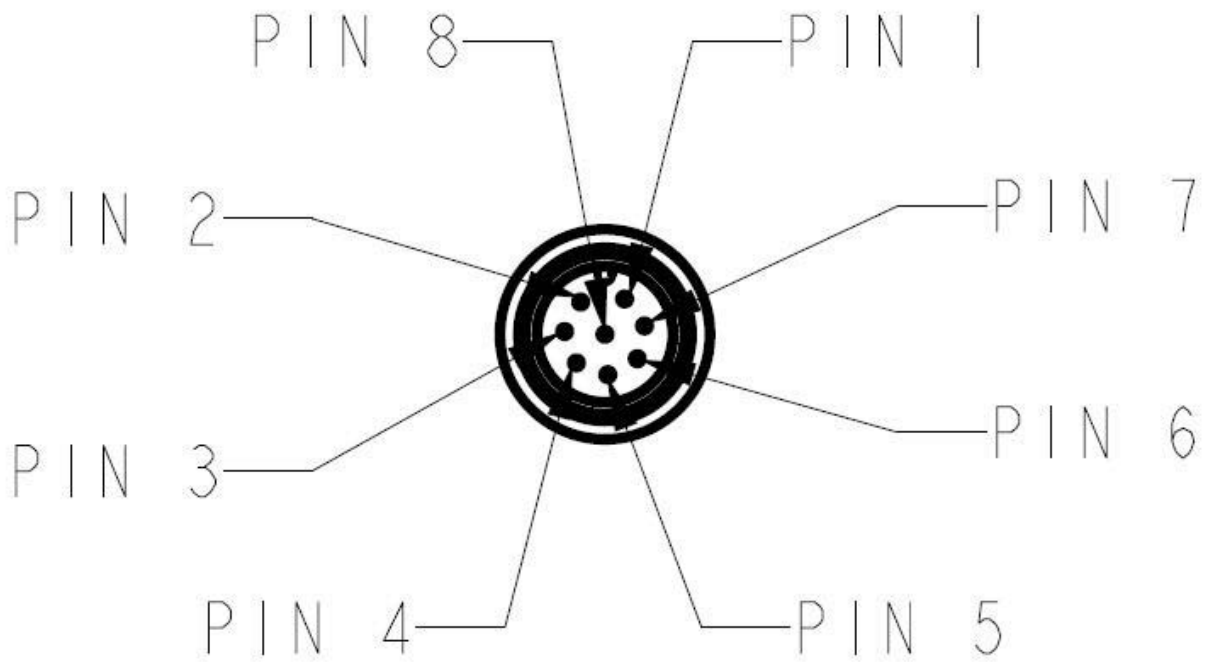
Power connector

The power connector is an M12-4 pin, A Coded connector. Pinout is as follows:

Pin	Signal
1	Power +ve
2	GPIO 0
3	Power -ve
3	GPIO 1

Serial connector

The serial connector is an M12-5 pin, A Coded connector. Pinout is as follows:

Pin	DB-9 (DCE)
1	2 (RXD)
2	3 (TXD)
3	8 (CTS)
4	7 (RTS)
5	5 (GTM)

Ethernet connectors

Ethernet connector M12-4 pin, D Coded

Pin	RJ45	Signal	Notes
1	1	TX+	Twisted Pair
2	2	TX-	
3	3	RX+	Twisted Pair
4	6	RX-	

Ethernet connector M12-8 pin, A Coded

Pin	RJ45	Signal	Notes
4	6	RX-	Twisted Pair
6	3	RX+	
5	1	TX+	Twisted Pair
8	2	TX-	
1	N/C		
2	N/C		
3	N/C		
7	N/C		

TransPort WR44 RR hardware specifications

Complete, updated specifications of the Digi TransPort WR44 RR device and accessories are available on the Digi website, www.digi.com.

- To view the Digi TransPort WR44 RR Hardware Specifications, go to the **Specifications** tab of the TransPort WR44 RR product page.

- To view available accessories, including cables and antennas for the Digi TransPort WR44 RR, go to the **Models** tab for the TransPort WR44 RR product page and click **View Accessories**.

LTE specifications

LTE type	Specification	Supported values
LTE-EMEA (L1)	Speed	800/850/900/1800/1900/2100/2600MHz
	Fall back	• 3G fall back to 850/900/1900/2100MHz • 2G fall back to 850/900/1800/1900MHz
	Maximum transfer rate	50 Mbps Up, 100 Mbps Down
LTE-North America (L5) Multi-Carrier (Verizon, AT&T, and Sprint)	Speed	700/850/1700(AWS)/1900 MHz
	Fall back	• 2G/3G GSM fall back to 850/900/1700AWS/1800/1900/2100MHz • 2G/3G CDMA fall back to 800/1900MHz
	Maximum transfer rate	50 Mbps Up, 100 Mbps Down
LTE-North America (L6)	Speed	700/850/1700(AWS)/1900MHz;
	Fall back	2G/3G fall back to 850/1900MHz
	Maximum transfer rate	50 Mbps Up, 100 Mbps Down
LTE-Verizon (L8)	Speed	700/1700(AWS)MHz
	Fall back	No 2G/3G fall back
	Maximum transfer rate	50 Mbps Up, 100 Mbps Down

Accessories

A variety of accessories are available for TransPort products. For the current list of accessories and their Digi part numbers, go to product page for your TransPort product on www.digi.com and click **Part Numbers & Accessories**.

Serial port connections and pinouts

Depending upon the model, the asynchronous serial ports on may be presented as DB 25 sockets, DB 9 sockets or 8-pin RJ45 sockets. On some models, a combination of the above may be used. The following tables list the pin designations of each type of connector for each Digi model.

The RS-232 port pinouts are suitable for both Async and Sync port connections. When used in Async mode the pins for TxC, RxC & ETC are not required, these are needed for Sync mode only.

The serial pinouts for all TransPort models are included with the hardware information for each model.

All TransPort serial ports are DCE

Note that **all TransPort serial ports are DCE**.

Purchase additional serial cables

For TransPort models that include serial ports with RJ45 connectors, Digi offers the following serial cables for connectivity:

Digi part number	Description
76000855	RJ45 to DB9 Female 6'
76000856	RJ45 to DB25 Male 6'
76000857	RJ45 to DB25 Female 6'

Signal strength indicators

On routers equipped with W-WAN modules, there are three LEDs on the front panel that will indicate the strength of the signal, as shown in the table below.

LEDs lit	Signal strength
None	Under -113 dBm (effectively no signal)
1	-112 dBm to -87 dBm (weak signal)
2	-86 dBm to -71 dBm (medium strength signal)
3	-70 dBm to -51 dBm (strong signal)

X.21 (RS-422)

Description	RS232 signal	Direction[1]	DB 25 Pin#	DB 9 Pin#
Transmit Data (A)	TxDA	in	2	1
Receive Data (A)	RxDA	out	3	2
Control (A)	CTLA	in	4	3
Indication (B)	INDA	out	5	4
Ground	GND	n/a	7	5
Clock (B)	CLKB	in or out[2]	9	n/a
Indication (B)	INDB	out	13	9
Transmit Data (B)	TxDB	in	14	6
Receive Data (B)	RxDB	out	16	7
Clock (A)	CLKA	in or out[2]	17	n/a
Control (B)	CTLB	in	19	8

1 With respect to Digi routers
2 Direction depends on whether the Digi router is clock sink or clock source.

RS-232 (V.24) serial cable wiring

The tables below detail the wiring required for the various types of serial cable that you may need.

Note Some products are able to operate both synchronously and asynchronously. When these products are operating asynchronously, it is strongly recommended that the clock pins (TxC, RxC and ETC) are left disconnected.

25-Pin to 25-Pin straight through cable

This cable is normally used to connect a V.24 synchronous terminal to a Digi router.

DB 25-Digi Side		DB 25	
Signal	Pin # (DCE)	Pin # (DTE)	Signal
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
TxD	2	2	TxD
RxD	3	3	RxD
RTS	4	4	RTS
CTS	5	5	CTS
DSR	6	6	DSR
GND	7	7	GND
DCD	8	8	DCD
RxC	17	17	RxC
DTR	20	20	DTR
ETC	24	24	ETC

Note Frame Ground is optional

25-Pin to 9-Pin straight through cable

This cable is normally used to connect a V.24 asynchronous terminal, such as a PC to a Digi router.

DB 25-Digi Side		DB 9	
Signal	Pin # (DCE)	Pin # (DTE)	Signal
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
TxD	2	3	TxD
RxD	3	2	RxD
RTS	4	7	RTS
CTS	5	8	CTS
DSR	6	6	DSR
GND	7	5	GND
DCD	8	1	DCD
DTR	20	4	DTR
RING	22	9	RING

RJ45 to 25-Pin straight through cable

This cable is normally used to connect a V.24 synchronous terminal to a Digi router.

RJ45-Digi Side		DB 25	
Signal	Pin # (DCE)	Pin # (DTE)	Signal
RTS	1	4	RTS
DTR	2	20	DTR
RxD	3	3	RxD
GND	5	7	GND
TxD	6	2	TxD
DCD	7	8	DCD
CTS	8	5	CTS

RJ45 to 9-Pin straight through cable

This cable is normally used to connect a V.24 asynchronous terminal, such as a PC to a Digi router.

RJ45-Digi Side		DB 9	
Signal	Pin # (DCE)	Pin # (DTE)	Signal
RTS	1	7	RTS
DTR	2	4	DTR
RxD	3	2	RxD
GND	5	5	GND
TxD	6	3	TxD
DCD	7	1	DCD
CTS	8	8	CTS

25-Pin to 25-Pin crossover cable

This cable is normally used to connect the router to a V.24 leased line.

DB 25-Digi Side		DB 25	
Signal	Pin # (DCE)	Pin # (DTE)	Signal
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
TxD	2	3	RxD
RxD	3	2	TxD
RTS	4	5	CTS
CTS	5	4	RTS
GND	7	7	GND
DCD	8	20	DTR
RxC	17	24	ETC
DTR	20	8	DCD
ETC	24	17	RxC

Note Frame Ground is optional.

25-Pin to 9-Pin crossover cable

This cable is normally used to connect the router to an external asynchronous modem.

DB 25-Digi Side		DB 9	
Signal	Pin # (DCE)	Pin # (DTE)	Signal
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
TxD	2	2	RxD
RxD	3	3	TxD
RTS	4	8	CTS
CTS	5	7	RTS
GND	7	5	GND
DCD	8	4	DTR
DTR	20	1	DCD

RJ45 to 25-Pin crossover cable

This cable is normally used to connect the router to a V.24 leased line.

RJ45-Digi Side		DB 25	
Signal	Pin # (DCE)	Pin # (DTE)	Signal
RTS	1	5	CTS
DTR	2	8	DCD
RxD	3	2	TxD
GND	5	7	GND
TxD	6	3	RxD
DCD	7	20	DTR
CTS	8	4	RTS

RJ45 to 9-Pin crossover cable

This cable is normally used to connect the router to an external asynchronous modem.

RJ45-Digi Side		DB 25	
Signal	Pin # (DCE)	Pin # (DTE)	Signal
RTS	1	8	CTS
DTR	2	1	DCD
RxD	3	3	TxD
GND	5	5	GND
TxD	6	2	RxD
DCD	7	4	DTR
CTS	8	7	RTS

Regulatory and safety statements

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.

Radio equipment-Canadian warning statements

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

This radio transmitter (identify the device by certification number, or model number if Category II) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Name / Model	Gain	Impedance
BEC C424-510065-A	1.8dBi	50Ω Nominal

OEM responsibilities

The WR44v2 Module has been certified for integration into products only by OEM integrators under the following conditions:

9. The antenna(s) must be installed such that a minimum separation distance of 20cm is maintained between the radiator (antenna) and all persons at all times.

10. The transmitter module must not be co-located or operating in conjunction with any other antenna or transmitter.

As long as the two conditions above are met, further transmitter testing will not be required. However, the OEM integrator is still responsible for testing their end-product for any additional compliance requirements required with this module installed (for example, digital device emissions, PC peripheral requirements, etc.).

Note In the event that these conditions can not be met (for certain configurations or co-location with another transmitter), then Industry Canada certification is no longer considered valid and the IC Certification Number can not be used on the final product. In these circumstances, the OEM integrator will be responsible for re-evaluating the end product (including the transmitter) and obtaining a separate Industry Canada authorization.

End product labeling

The WR44v2 Module is labeled with its own IC Certification Number. If the IC Certification Number is not visible when the module is 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. In that case, the final end product must be labeled in a visible area with either of the following:

• Contains Transmitter Module IC: 1846A-55M1644

• Contains IC: 1846A-55M1644

The OEM of the WR44v2 Module must only use the approved antenna(s) listed above, which have been certified with this module.

The OEM integrator has to be aware not to provide information to the end user regarding how to install or remove this RF module or change RF related parameters in the user's manual of the end product.

Note To comply with Industry Canada RF radiation exposure limits for general population, the antenna(s) used for this transmitter must be installed such that a minimum separation distance of 20cm is maintained between the radiator (antenna) and all persons at all times and must not be co-located or operating in conjunction with any other antenna or transmitter.

Radio equipment-FCC warning statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons.

Any product using the WR44v2 Wi-Fi module must have a label stating **Contains FCC ID: MCQ-55M1644B** placed on it in line with FCC labeling regulations.

Antenna specification: RP-SMA

This module obtained its complete certification by using the antenna described here. End users in North America should use an antenna that matches these specifications to maintain the module's certification. Antennas of the same type but operating with a lower gain may be used.

Attribute	Property
Frequency Range	2.4 to 2.5 GHz
Impedance	50 Ohm
VSWR	1.92 max
Return Loss	-10dB max
Gain	1.8 dBi
Polarization	Linear
Radiation Pattern	Near omni-directional in the horizontal plane
Admitted Power	1W
Electrical	1/2 λ Dipole

Restricted Access Location notice for TransPort WR11 XT

Because of the hot metal surface of the enclosure, installations with operating temperatures greater than 122F (50C) must be limited to Restricted Access Locations accessible only to trained service personnel.

Hazardous Location installation information for TransPort WR31

For Hazardous Location installation, see the *TransPort WR31 Hazardous Location User Guide* (Digi part number 90001490).

Safety notices

1. Please read all instructions before installing and powering the router. You should keep these instructions in a safe place for future reference.

2. If the power supply shows signs of damage or malfunction, stop using it immediately, turn off the power and disconnect the power supply before contacting your supplier for a repair or replacement.

3. Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. Use only the accessories, attachments, and power supplies provided by the manufacturer-connecting non-approved antennas or power supplies may damage the router, cause interference or create an electric shock hazard, and will void the warranty.

4. Do not attempt to repair the product. The router contains no electronic components that can be serviced or replaced by the user. Any attempt to service or repair the router by the user will void the product warranty.

5. Products in the TransPort WR family are designed for indoor use (except for the WR44 R) and should be used in an environment that is suitable for computers and other electronic equipment.

6. Ports that are capable of connecting to other apparatus are defined as SELV ports. To ensure conformity with IEC60950 ensure that these ports are only connected to ports of the same type on other apparatus.

Special notes on safety for wireless routers

Digi International products are designed to the highest standards of safety and international standards compliance for the markets in which they are sold. However, cellular-based products contain radio devices which require specific consideration. Please take the time to read and understand the following guidance. Digi International assumes no liability for an end user's failure to comply with these precautions.

Wireless routers incorporate a wireless radio module. Users should ensure that the antenna(s) is (are) positioned at least 1 meter away from themselves and other persons in normal operation.

When in a hospital or other health care facility, observe the restrictions on the use of mobile phones. Do not use the router in areas where guidelines posted in sensitive areas instruct users to switch off mobile phones. Medical equipment may be sensitive to RF energy.

The operation of cardiac pacemakers, other implanted medical equipment and hearing aids can be affected by interference from cellular terminals such as the wireless routers when places close to the device. If in doubt about potential danger, contact the physician or the manufacturer of the device to verify that the equipment is properly shielded. Pacemaker patients are advised to keep the wireless router away from the pacemaker while it is on.

Wireless routers must NOT be operated on aircraft. The operation of wireless appliances in an aircraft is forbidden to prevent interference with communications systems. Failure to observe these instructions may lead to the suspension or denial of cellular services to the offender, legal action, or both.

As with any electrical equipment, do not operate the router in the presence of flammable gases, fumes or potentially explosive atmospheres. Radio devices should not be used anywhere that blasting operations are taking place.

Wireless routers receive and transmit radio frequency energy when power is on. Interference can occur if used close to TV sets, radios, computers or inadequately shielded equipment. Follow any special regulations and always power off your router wherever forbidden or when it may cause interference or danger.

SOS IMPORTANT! Wireless routers operate using radio signals and cellular networks cannot be guaranteed to connect in all possible conditions. Therefore, never rely solely upon any wireless device for life critical communications.

Warning: For environments where the temperature is 55° C or above, this device must be installed in a restricted access area.

Product Disposal Instructions

The WEEE (Waste Electrical and Electronic Equipment: 2002/96/EC) directive has been introduced to ensure that electrical/ electronic products are recycled using the best available recovery techniques to minimize the impact on the environment.

This product contains high quality materials and components which can be recycled. At the end of its life this product MUST NOT be mixed with other commercial waste for disposal. Check with the terms and conditions of your supplier for disposal information.

Digi International Ltd WEEE Registration number: WEE/HF1515VU

EC Declaration of Conformity

Following are the EC Declaration of Conformity documents for the Digi TransPort products.

TransPort WR11Declaration of Conformity

EC Declaration Of Conformity

We,	**Manufacturer's Name:**	Digi International inc.
of	**Manufacturer's Address:**	11001 Bren Road East, Minnetonka, MN 55343 USA

declare under our sole responsibility that the product:

Product Name:	TransPort WR11
Model Number:	WR11-U900-DE1-SW

to which this declaration relates are in conformity with the essential requirements and other relevant requirements of EU Directive 1999/5/EC (R&TTE), EU Directive 2011/65/EU (RoHS2)

Safety: (article 3.1a)	EN 60950-1:2006 +A2:2013
	EN 50385:2002
EMC: (article 3.1b)	EN 301 489-1 V1.9.2 (2011-09)
	in accordance with the specific requirements of:
	EN 301 489-3 V1.6.1 (2013-08)
	EN 301 489-7 V1.3.1 (2005-11)
	EN 301 489-24 V1.5.1 (2010-10)
Spectrum: (article 3.2)	EN 300 440-2 V1.4.1
	EN 301 511 V9.0.2 (2003-03)
	EN 301 908-1 V6.2.1 (2013-04)
	EN 301 908-2 V5.4.1 (2012-12)
RoHS2	EN 50581:2012

Minnesota, USA July 24th, 2014

(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
	Joseph-von-Fraunhofer-Str.23, 44227 Dortmund, Germany
	Telephone: +49-7667-908-124

TransPort WR21Declaration of Conformity

EC Declaration Of Conformity

We,

Manufacturer's Name: Digi International

of

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

declare under our sole responsibility that the product:

Product Name: TransPort WR21

Model Numbers: WR21-NNHH-DFF-XX

Where
NN = C0, C3, C8, E1, U4, U5, U6, U7, U8
HH = 11, 12, 21, 22
FF = B1, E1
XX = SD, SF, SL, SN, SU, SW, XA, XB

to which this declaration relates are in conformity with the essential requirements and other relevant requirements of the *R&TTE Directive (1999/5/EC)*

Safety: (article 3.1a) EN60950-1:2006 + A11 (2009)

EMC: (article 3.1b) EN55022:2006 + A1 (2007) class B
EN55024:1998 + A1:2001 + A2:2003
EN61000-3-2:2006 + A1:2009 + A2:2009
EN61000-3-3:2008
EN301 489-7:v1.3.1
EN301 489-24:v1.5.1

Spectrum: (article 3.2) EN301511:v9.0.2
EN301526:v1.1.1
EN301908-1v:3.2.1

Minnesota, USA, 25 July, 2011

(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 Branch Breisach
Kueferstr. 8, 79206 Breisach, Germany
Telephone: +49-7667-908-124

TransPort WR31 Declaration of Conformity

DIGI ◢ **EU Declaration Of Conformity**

We, **Manufacturer's Name:** Digi International Inc.

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

declare under our sole responsibility that the product:

Product Name:	Transport® WR31
Model/Part Number:	WR31-L52A-DE1-TB – Huawei ME909u-521 PCIe
Description:	WR31-L12A-DE1-TB – Sierra Wireless MC7354
	WR31-U92A-DE1-TB – Telit HE910 Mini PCIe

to which this declaration relates are in conformity with the essential requirements and other relevant
requirements of EU Directive 1999/5/EC (R&TTE), EU Directive 2011/65/EU (RoHS2)

Safety: (article 3.1a)   IEC 60950-1:2006/A11:2009/A1:2010/A12:2011/A2:2013
IEC 62368-1:2014
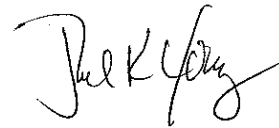
EMC: (article 3.1b)

EN55022/CISPR22	EN61000-4-5
EN55024:2010/CISR24	EN61000-4-6
EN61000-6-1:2007	EN61000-4-11
EN 61000-3-2:2014	EN 300 386
EN 61000-3-3:2013	ETSI EN 301 489-1
EN61000-4-2	ETSI EN 301 489-3
EN61000-4-3	ETSI EN 301 489-7
EN61000-4-4	EN 301 489-24 V1.5.1:2010

Spectrum: (article 3.2)

ETSI EN 301 908-2 V5.2.1 (2011-07)	ETSI EN 301 893 V1.8.1 (2015-03)
ETSI EN 301 511 V9.0.2 (2002-11)	ETSI EN 301 908-1 V1.7.1 (2015-03)
ETSI EN 300 328 V1.9.1 (2015-02)	ETSI EN 301 908-13 V6.2.1 (2013-10)

RoHS2: EN 50581

Minnesota, USA 2nd December 2015
(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
Joseph-von-Fraunhofer-Str.23, 44227 Dortmund, Germany
Telephone: +49-7667-908-124

TransPort WR41 Declaration of Conformity

EC Declaration Of Conformity

We,

    Manufacturer's Name: Digi International

of

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

declare under our sole responsibility that the product:

Product Name: TransPort WR41 v2

Model Numbers: Reference product list

to which this declaration relates are in conformity with the essential requirements and other relevant requirements of the Directive 2004/108/EC (EMC), Directive 2006/95/EC (LVD), and Council Directive 1999/5/EC R&TTE.

EMC: (article 3.1b)   EN55022:2006 + A1:2007
    EN55024:1998 + A1:2001 + A2:2003
    EN61000-3-2:2006
    EN61000-3-3:1995 + A1:2001 + A2:2005
    EN301489-7:v1.3.1 (not WR41-U)
    EN301489-24:v1.4.1 (WR41-U only)
    EN301489-17:v2.1.1
    EN301511:v9.0.2 (not WR41-C and WR41-U)
    EN301526:v1.1.1 (WR41-C only)
    EN301908-1:v3.2.1 (WR41-U only)

Safety: (article 3.1a)   EN60950-1:2006+A11:2009

Minnesota, USA, 16 November, 2010
(Place and date of issue)

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

EC Declaration Of Conformity

European
Representative:

Andreas Burghart
Digi International GmbH Branch Breisach
Kueferstr. 8, 79206 Breisach, Germany
Telephone: +49-7667-908-124

Part Number
WR41-X1X2-YZZ-AA
• Where X1 can be: 00, 01, C0, C1, C2, C5, C8, E1, G1, U0, U1, U2, U3, U4, U5
• Where X2 can be: 00, A1, A3, G1, I1, I3, P1, P3, S1, T1, T2
• Where Y can be: D or W
• Where ZZ can be: E1, E2, E3, E5, S1, S2, S3, S5, V1, V2, V3, V5, A1, A2, A3, A5, or any numeric value
• Where AA can be: SA, SB, SD, SF, SU, SN, SW, SL

TransPort WR44 Declaration of Conformity

EC Declaration Of Conformity

We,

Manufacturer's Name: Digi International

of

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

declare under our sole responsibility that the product:

Product Name: TransPort WR44

Model Numbers: Reference product list

to which this declaration relates are in conformity with the essential requirements and other relevant requirements of the Directive 2004/108/EC (EMC), and Directive 2006/95/EC (LVD).

EMC :(article 3.1b)   EN55022:2006 + A1:2007
EN55024:1998 + A1:2001 + A2:2003
EN61000-3-2:2006
EN61000-3-3:1995 + A1:2001 + A2:2005
EN301489-7:v1.2.1
EN301489-17:v2.1.1

Safety: (article 3.1a)   EN60950-1:2006+A11:2009

Minnesota, USA, 16 November, 2010
(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 Branch Breisach
Kueferstr. 8, 79206 Breisach, Germany
Telephone: +49-7667-908-124

TransPort WR44 RR Declaration of Conformity

EC Declaration Of Conformity

We,

Manufacturer's Name:	Digi International

of

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

declare under our sole responsibility that the product:

Product Name: TransPort WR44RR

Model Numbers: WR44-U8HH-WE1-MD

Where
HH = 04, 08, G4, G8
W   = C, N

to which this declaration relates are in conformity with the essential requirements and other relevant requirements of the Directive 2004/108/EC (EMC), Directive 2006/95/EC (LVD) and Council Directive 1999/5/EC R&TTE.

Safety: (article 3.1a)   EN60950-1:2006 + A11:2009 + A1:2010 + A12:2011

EMC: (article 3.1b)   EN 55022:2010
EN 55024:2010
EN 301 489-17:V2.1.1
EN 301 489-24:V1.5.1

Spectrum: (article 3.2)   EN 301 511:v9.0.2
EN 301526:v1.1.1
EN 301 908-1:v4.2.1
EN 301 908-2:v4.2.1

Minnesota, USA, 2nd July, 2012
(Place and date of issue)

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

91002268A   1 of 2   2/7/2012
Template 96000759B

EC Declaration Of Conformity

European Representative:	Andreas Burghart
	Digi International GmbH Branch Breisach
	Kueferstr. 8, 79206 Breisach, Germany
	Telephone: +49-7667-908-124

Use the Digi TransPort web interface

Digi TransPort routers have a built-in web interface for configuring the device, managing the network and connections, and managing applications. This section covers the following topics:

- Log in to the device on page 101
- Log out and return to the login page on page 103
- Accessing the web interface Via a LAN port on page 103
- Configure and test W-WAN models from the web interface on page 104
- Signal strength indicators on the Mobile status page on page 105
- Web interface wizards on page 106

Log in to the device

To configure the router via the Web interface, either establish a DUN connection to it and then open your web browser and enter 1.2.3.4 for the web address, or enter the router's Ethernet IP address (192.168.1.1) into your web browser after configuring your PC to have an address on the same subnet.

You will be presented with a login page similar to the following image.

The default Username and password are **username** and **password** respectively. Enter these and click the **Log in** button to access the configuration pages. The password will be displayed as a series of dots for security purposes.

> **Note** For security purposes, Digi recommends changing the username and password for all users away from their defaults. See Change the default username and password for a user on page 648.

After entering the username and password, the Home page is displayed. This page is the main operations page for the router.

Clicking on the **Click to load Applet graphics!** button displays a representation of the front panel of your router that will be updated every few seconds to show the actual status of the LED indicators. The model number of your router will be shown at the top of the screen. The router's serial number and ID are shown below the front panel representation.

In the left side of the page, you will see the main menu with subsections which further expand when clicking on them.

Log out and return to the login page

To log out the current user and return to the web interface login page, select **Logout**.

Accessing the web interface Via a LAN port

By default, the Digi Transport has a static IP address of 192.168.1.1 with DHCP server enabled. To access the router using a web browser (such as, Internet Explorer), simply connect an Ethernet cable between the LAN port on the Digi Transport and your PC. Make sure your PC is setup to automatically receive an IP address by selecting **Start > Control Panel > Network > Configuration** and verifying the configuration.

Note All models are auto-sensing for 10/100 operation. Most models are also auto MDI/MDX, such as will automatically work with either a straight-through or cross-over cable. The only exceptions are the IR2140 and GR2130, which are NOT auto MDI/MDX.

Configure and test W-WAN models from the web interface

1. To configure the TransPort router for the correct APN and PIN code, if any, see Configure mobile interfaces on page 189 section of this guide.

2. Power up the router and test connection to the wireless network.

3. If you have correctly configured everything, the W-WAN SIM indicator on the front panel should illuminate green to show that a W-WAN enabled SIM card is present.

4. The router will now attempt to log on to the specified mobile network. If it is able to do so, the W-WAN NET indicator will illuminate steady.

5. Data passing to and from the network is reflected by the status of the DAT indicator, which flash greens.

6. If you cannot connect to the network, go to the **Management > Network Status > Interfaces > Mobile** web page.

7. Click the **Refresh** button. A page similar to the following should be displayed. For more on the Signal Strength status and value displayed, see Signal strength indicators on the Mobile status page on page 105.

Signal strength indicators on the Mobile status page

On routers equipped with W-WAN modules, there are three LEDs on the front panel that indicates the strength of the signal, as shown in the following table.

The signal strength is shown in **negative dB**, which means that the stronger the signal, the lower the number. As a guide, -51dB is a very strong signal, normally only obtained very close to a cell site. -115dB represents no signal. If your router reports -115dB, try reorienting the antenna or consider adding an external antenna.

The following values are fairly specific to LTE. At 2G/3G technology, any strength lower than -100dBm becomes unusable.

LEDs lit	Signal Strength
None	Under -113 dBm (effectively no signal)
1	-112 dBm to -87 dBm (weak signal)
2	-86 dBm to -71 dBm (medium strength signal)
3	-70 dBm to -51 dBm (strong signal)

Web interface wizards

The wizards page contains wizards that simplify common configuration tasks. These wizards will change the minimum number of parameters to complete the required configuration task. Note that due to the generic nature of the wizards, they may not be suitable in all scenarios.

Wizards

Select the wizard you wish to run

- ○ Quick Start Wizard
- ○ Serial interface wizard
- ○ Create an aggressive mode LAN to LAN IPsec tunnel
- ○ SureLink wizard
- ○ GOBI module carrier wizard
- ○ Dual SIM wizard

Quick Start wizard

The Quick Start Wizard displays the options required for basic configuration of the **Eth 0**, WLAN and WWAN interfaces. This page allows you to set up your Ethernet LAN interface.

You can get IP settings assigned automatically if your network supports this capability. Otherwise you can assign the IP settings appropriate for your network.

○ Obtain an IP address automatically

⦿ Use the following IP address:

IP Address: 10.9.111.87
Subnet mask: 255.255.0.0
Default gateway: 10.9.1.1

○ Obtain a DNS server address automatically

⦿ Use the following DNS server addresses:

Preferred DNS Server: 10.10.8.62
Alternate DNS Server: 10.10.8.64

Next   Cancel

Serial Interface wizard

This wizard allows you to select a serial port and profile for your application.

Serial interface wizard

This wizard allows you to select a serial port and profile for your application.

Serial Port Configuration			
Port	**Description**	**Profile**	**Serial Configuration**
Port 0		None	115200 8N1
Port 1		None	115200 8N1
Port 2		modemcc(info) 0	115200 8N1
Port 3		None	115200 8N1
Port 4		modemcc 0	115200 8N1
Port 5		None	115200 8N1
Port 6		None	Auto 8N1
Port 7		None	Auto 8N1
Port 8		None	Auto 8N1

Edit Port profile for Port 0 ▾

Next   Cancel

Create an aggressive mode LAN to LAN IPsec Tunnel wizard

This wizard helps you configure an aggressive mode LAN to LAN IPsec tunnel to a remote host. The IPsec wizard can be used to help configure an aggressive mode LAN to LAN VPN tunnel.

The tunnel is configured as an initiator, this means it is responsible for starting the VPN connection.

Create an aggressive mode LAN to LAN IPsec tunnel

Provide a descriptive name for the tunnel.

Tunnel description:

Enter the WAN IP address of the other VPN router or concentrator.

Destination address:

SureLink wizard

This wizard configures your Digi TransPort router to stay connected to the W-WAN (Wireless Wide Area Network) under adverse conditions, using several features designed to recover from network and other problems. The wizard helps you choose the most appropriate set of features for you. Please read the following explanation carefully as it is important that you make the correct selection for your circumstances.

Automatic power cycling of the internal Wireless WAN radio will occur if ever the PPP link to the network cannot be established. In the event of a problem occurring when the PPP link is already up, some mechanism must be employed to detect the **dead link** and deactivate it. This wizard will help you configure the most appropriate dead link detection technique.

There are two types of dead link detection techniques: passive and active.

Passive techniques

Passive techniques work by monitoring data that would be sent over the W-WAN network anyway. As it is necessary for data to be sent in order to detect a problem, these techniques are only suitable if the equipment on the router's LAN (Local Area Network) regularly sends data over the W-WAN.

The main advantage of passive techniques are:

- No additional data charges (if your mobile operator charges you for data).
- In a hub and spoke deployment, no additional load will be placed on equipment at the hub.

The main disadvantages are:

- If the equipment on the LAN does not send data and a problem with the connection manifests, it will not be possible to connect to the router or the router's LAN remotely until the equipment on the LAN sends data.
- As equipment on the LAN needs to send data before some problems can be detected, if a problem does occur, the equipment on the LAN will be subject to delays when it first tries to send data. This is because it will take the Digi TransPort router a certain amount of time to detect and recover from the network problem.

Active techniques

Active techniques work by sending data to test the link. For example a ping, UDP packet or IPsec keep-alive (Dead Peer Detection) packet.

The main advantage of active techniques are:

- Problems are detected promptly and the availability of remote access to the router or its LAN is maximized.
- Problems can be repaired BEFORE equipment on the router's LAN needs to use the W-WAN resulting in no delays sending data.

The main disadvantages are:

- Some mobile operators charge for the data sent to test the link.
- In a hub-and-spoke deployment, additional load will be placed on equipment at the hub end by the test data.

GOBI Module Carrier wizard

GOBI Module Carrier wizard is used with routers that have a GOBI module installed, to configure the router for a specified WWAN carrier. This wizard allows you to select the GOBI module firmware to be used for your WWAN connection.

Changes to the router configuration will be also made depending on the firmware selection.

The router is currently configured to load firmware ID 0 (Generic UMTS).

Dual SIM wizard

This wizard will help you configure your router for dual SIM failover. It will determine the most appropriate configuration for your circumstances by explaining the options and then asking questions. Use this wizard to configure the router to detect a link failure and automatically switch to the second installed SIM. This wizard only helps to configure the most commonly used methods of link error detection.

Note that it is important that this wizard is run from a factory default configuration or close to a factory default configuration. If changes have been made to the W-WAN configuration other than username, password and APN, running this wizard could cause unanticipated behavior.

SIM weighting

There are two common dual SIM configurations:

- Both SIM cards/slots have equal weighting. In the event of a problem the router will fail over from one SIM to the other. Once it has failed over it will remain on the alternate SIM until another problem is detected in which case it will fail back to the original SIM. This method keeps down time to a minimum and is used when no SIM is to be given preference over the other.

- One SIM has a higher weighting than the other. After boot-up the primary SIM will be used if possible. In the event that a problem occurs the router will fail over to the secondary SIM. The secondary SIM will be used for a configurable period of time or until a problem is detected. When either a problem occurs or the time is up the router will attempt to fail back to the primary SIM. This is useful if one SIM needs to be preferred over another, for example if the data charges are cheaper on the primary SIM. Please note, however, that the internal radio module must be power cycled during SIM switchover. So attempting to revert to the primary SIM just because the secondary SIM has been used for the configured length of time will result in an outage. Also note that if the primary SIM still cannot be used there will be a further delay whilst the router reverts back to the secondary SIM.

Please make the appropriate selection:

◉ Equal weighting
○ SIM 1 has priority over SIM 2

[Next]   [Cancel]

Use the Digi TransPort command-line interface

This section describes the basics of using the command line interface, and provides descriptions of some key AT and application commands. It covers the following topics:

Additional commands and parameters are covered in the sections on configuring features, and in command-line examples throughout this guide.

About the Digi TransPort command line interface

Using a Web browser to modify text box or table values in the configuration pages is the simplest way to configure the router and this process is described in the next chapter. However, if you do not have access to a Web browser, the router can be configured using text commands. These commands may be entered directly at one of the serial ports or via a Telnet session. Remote configuration is also possible using Telnet or X.25.

> **Note** Low level permission users are designed to work in the web interface only. Command line use is not supported.

Supported command types

There are several types of text commands:

- **AT commands and S registers**: Digi TransPort supports AT commands and Special registers (S registers) to maintain compatibility with modems when the router is used as a modem replacement. For more information about the AT commands, see AT commands on page 116.

- **Application commands, also known as text commands**: Application commands are specific to Digi International products and control most features of the router when not using the Web interface. For more information about application commands, see Application commands on page 137.

- **X.3 commands**: These are standard X.3 commands which are used only in X.25 PAD mode. For more information on these commands, see Configure X.25 parameters on page 521.

- **TPAD commands**: These are used only in TPAD mode. For more information on these commands, see Configure TPAD parameters on page 509.

Required software for using the command line

To use the serial ports you will need:

- A PC connected to the TransPort router.

- Terminal emulation/communications software such as HyperTerminal ™ (supplied with Windows) or TeraTerm™. The same commands may also be used to configure the router remotely via Telnet, X.25 or V.120.

Connect to the TransPort router from a PC

If you ran the Getting Started Wizard at setup time, following instructions in the Quick Start Guide for your product, your router is already configured. To make configuration changes via the command line, follow these steps:

1. Make that the router is connected to a PC.

2. Make sure terminal emulation software, such as TeraTerm or HyperTerminal, is installed on the PC.

3. Using the terminal emulation software, configure the following settings for the router:

   - COM Port: select the appropriate port, typically **COM1**

   - Baud Rate: **11500**

   - Data Bits: **8**

   - Stop Bits: **1**

   - Parity: **No**

   - Parity: **No Parity**

   - Flow Control: **None**

4. Make sure the connection is active by entering the command AT. If the device is functioning properly, it will return the response OK. To learn more about the AT commands, see AT commands on page 116.

5. Make sure the COM port is set up correctly by entering the command **ATI5**.

Log in from the command line

When the login prompt appears on the command line, enter the default user name and password:

- Username: **username**
- Password: **password**

Note For security purposes, Digi recommends changing the username and password for all users away from their defaults. See Change the default username and password for a user on page 648.

Commands and the active port

When entering AT or text commands, in most cases, **the command only affects the settings for the active port**. This is usually the port to which you are physically connected but you may, if necessary, set the active port to another port of your choice using the **AT\PORT=N** command where **N** is 0-3.

When commands take effect

All entered commands take effect immediately.

View current configuration changes

To view the current configuration settings, enter the following command:

```
config c show
```

Save changes

To save changes made to the router, enter the following command:

```
config 0 save
```

Configure network settings

To configure the router with an IP address as part of an existing network, use the commands below.

Note The DHCP server will still operate unless it is disabled.

---

1. Set the IP address of Eth 0:

   ```
   eth 0 ipaddr xxx.xxx.xx.xxx
   ```

2. Set the subnet mask for Eth 0:

   ```
   eth 0 mask xxx.xxx.xx.xxx
   ```

   For example, to assign the IP address **192.168.10.254/24**, enter the following commands would be entered:

   ```
   eth 0 ipaddr 192.168.10.254
   eth 0 mask 255.255.255.0
   ```

Note When setting the mask in the above example to **255.255.255.0**, the mask's value will not be displayed in the output of the **config c show** command, as **255.255.255.0** is a default value.

---

3. To stop the DHCP server from serving addresses, use the following command:

   ```
   dhcp 0 ipmin x
   ```

   This command removes the minimum IP address that will be server via DHCP, disabling the DHCP server. For example, to stop the DHCP sever from DHCP requests, enter the command. Note that the variable **!** is used to remove a value or set it back to its default.

   ```
   dhcp 0 ipmin !
   ```

4. To retain the DHCP server, but on a different subnet, set the minimum IP address to assign, that is, the start of the DHCP pool:

   ```
   dhcp 0 ipmin x.x.x.x
   ```

5. Set the number of IP addresses in the DHCP pool:

   ```
   dhcp 0 iprange
   ```

6. Set the IP gateway address the DHCP clients should use (normally this router's LAN IP address):

   `dhcp 0 gateway x.x.x.x`

7. Set the subnet mask DHCP clients should use:

   `dhcp 0 mask x.x.x.x`

8. Set the DNS server DHCP clients should use:

   `dhcp 0 dns`

Establish a remote connection

Once you have finished configuring the router, there are several ways of establishing a link to a remote system:

- Use the **ATD** command to make an outgoing V.120 call.
- Initiate a DUN session to establish a dial-up PPP connection.
- Make an outgoing X.25 call using the **ATD** command followed by the X.28 **CALL** command.
- Make an outgoing TPAD (Transaction PAD) call using the TPAD **a** (address) command followed by the appropriate NUA. This is normally only carried out under software control.

Similarly, incoming calls are handled according to the protocols that have been bound to the ASY ports, and whether answering is enabled for each protocol.

AT commands

Digi TransPort supports AT commands and Special registers (S registers). Information and command descriptions in this section includes:

The AT command interface

The **AT** command prefix is used for those commands that are common to modems. To configure the router using AT commands, you must first connect it to a suitable asynchronous terminal.

1. You will first need to set the interface speed/data format for your terminal to 115,200bps, 8 data bits, no parity and 1 stop bit (these settings can be changed later if necessary).

2. When your terminal is correctly configured, apply power and wait for the B2 indicator to stop flashing.

   The device is now ready to respond to commands from an attached terminal and is in **command mode**. Alternatively, you can configure the router to automatically connect to a remote system on powerup,

3. Type **AT** (in upper or lower case), and press [**Enter**]. The router should respond with the message **OK**. This message is issued after successful completion of each command. If an invalid command is entered, the router will respond with the message **ERROR**.

   If there is no response, check that the serial cable is properly connected and that your terminal or PC communications software is correctly configured before trying again.

   If you have local command echo enabled on your terminal, you may see the AT command displayed as **AATT**. If this happens, use the **ATE0** command (which will appear as **AATTEE00**), to prevent the router from providing command echo. After this command has been entered, further commands will be displayed without the echo.

AT commands are case-insensitive

The **AT** command prefix and the commands that follow it can be entered in upper or lower case.

Entering multiple commands

After the prefix, you can enter one or more commands on the same line of up to 40 characters. When the line is entered, the router will execute each command in turn.

Escape sequences

If you enter a command such as **ATD**, which results in the router successfully establishing a connection to a remote system, it will issue a **CONNECT** result code and switch from command mode to on-line mode. This means that it will no longer accept commands from the terminal. Instead, data will be passed transparently through the router to the remote system. In the same way, data from the remote system will pass straight through to your terminal.

The router will automatically return to command mode if the connection to the remote system is terminated.

To return to command mode manually, you must enter a special sequence of characters called the escape sequence. This consists of three occurrences of the escape character, a pause (user configurable) and then AT. The default escape character is **+** so the default escape sequence is:

```
+++ {pause} AT
```

Entering this sequence when the router is on-line will cause it to return to command mode but it will NOT disconnect from the remote system unless you specifically instruct it to do so (using **ATH** or another method of disconnecting). If you have not disconnected the call, the **ATO** command may be used to go back on-line.

AT command result codes

Each time an AT command line is executed, the router responds with a result code to indicate whether the command was successful. If all commands entered on the line are valid, the **OK** result code will be issued. If any command on the line is invalid, the **ERROR** result code will be issued.

Result codes may take the form of an English word or phrase (verbose code) or an equivalent number (numeric code), depending on the setting of the **ATV** command. Verbose codes are used by default.

The **ATV0** command can be used to select numeric codes if required. The results from the text based commands can be numeric or verbose. A full list of the Result codes is provided in the following table:

Numeric Code	Verbose Code	Meaning
0	OK	Command line executed correctly
1	CONNECT ISDN	connection established
2	RING	Incoming ring signal detected
3	NO CARRIER X.25	service not available
4	ERROR	Error in command line
6	NO DIALTONE ISDN	service not available
7	BUSY	B-channel(s) in use
8	NO ANSWER	No response from remote

S registers

S (Special) registers are registers in the router that are used to store certain types of configuration information. They are essentially a legacy feature included to provide compatibility with software that was originally designed to interact with modems. A full list of the registers is provided under the S registers section.

D command: Dial a call

The ATD command causes the router to initiate an ISDN call. The format of the command depends on the mode of operation.

When using the router to make data calls on one of the ISDN B-channels, enter the ATD command followed by the telephone number. For example, to dial **01234 567890** enter the command:

```
atd01234567890
```

Spaces in the number are ignored. If the call is successful the router will issue the **CONNECT** result code and switch to on-line mode.

Dialing with a specified sub-address

The ATD command may also be used to route a call to an ISDN sub-address by following the telephone with the letter S and the required sub-address. The sub-address may be up to 15 digits long. For example:

```
atd01234567890s003
```

Dialing stored numbers

To dial numbers that have previously been stored within the router using the **AT&Z** command, insert the **S=** modifier within the dial string. For example, to dial stored number **3**, use the command:

```
atds=3
```

Combining ISDN and X.25 calls

A further option for the ATD command for X.25 applications is to combine the ISDN call and the subsequent X.25 CALL in the same command. To do this, follow the telephone number with the **=** symbol and the X.25 call string. For example:

```
atd01234 567890=123456789
```

Pressing any key while the **ATD** command is being executed will abort the call attempt.

H command: Hang-up

The **ATH** command is used to terminate an ISDN call. If the router is still on-line you must first switch back to command mode by entering the escape sequence, such as **+++**, wait 1 second and then enter an AT command or just **AT<CR>**.

After entering the **ATH** command, the call will be disconnected and the **NO CARRIER** result will be issued.

Z command: Reset

The **ATZ** command is used to load one of the stored profiles for the active ASY port. The command is issued in the format **ATZn** where **n** is the number (0 or 1) of the ASY port profile you wish to load.

&C command: DCD control

The **AT&C** command is used to configure the way in which the router controls the DCD signal to the terminal. There are three options:

- **&C0** DCD is always **On**
- **&C1** DCD is **On** only when an ISDN connection has been established (Layer 2 is UP)
- **&C2** DCD is always **Off**
- **&C3** DCD is normally **On** but pulses low for a time in 10 msec routers determined by S register **10**.

&F command: Load factory settings

The **AT&F** command is used to load a pre-defined default set of S-register and AT command settings (the default profile). These are:

E1, V1, &C1, &K1, &D2, S0=0, S2=43

All other values are set to 0.

&R command: CTS control

The **AT&R** command is used to configure the way in which the router controls the CTS signal to the terminal. There are three options:

- **&R0** CTS is always **On**.
- **&R1** CTS follows RTS. The delay between RTS changing and CTS changing is set in AT register **56** in multiples of 10msec.
- **&R2** CTS is always **Off**.

&V command: View profiles

The **AT&V** command displays a list of the current AT command and S register values, and the settings for the two stored profiles. For example:

```
at&v
CURRENT PROFILE:
&c1 &d2 &k1 &s1 &r0 e1 q0 v1 &y0
S0=0 S2=43 S12=50 S31=3 S45=5
states DTR:1 RTS:1

STORED PROFILE 0:
&c1 &d2 &k1 &s1 &r0 e1 q0 v1
S0=0 S2=43 S12=50 S31=3 S45=5

STORED PROFILE 1:
&c1 &d2 &k1 &s1 &r0 e1 q0 v1
S0=0 S2=43 S12=50 S31=3 S45=5
OK
```

&W command: Write SREGS.DAT file

The **AT&W** command is used to save the current command and S registers settings (for the active port), to the file **SREGS.DAT**. The settings contained in this file can be reloaded at any time using the ATZ command.

The **AT&W** command may be immediately followed by a profile number, either 0 or 1, to store the settings in the specified profile, for example:

```
at&w1
```

would store the current settings as profile **1**. If no profile number is specified, profile **0** is assumed.

All S register values and the following command settings are written by **AT&W**:

```
e, &c, &d, &k
```

&Y command: Set default profile

The **AT&Y** command is used to select the power-up profile (0 or 1). For example, to ensure that the router boots up using stored profile 1, enter the command:

```
at&y1
```

&Z command: Store phone number

The **AT&Z** command is used to store "default" telephone numbers within the router that may subsequently dialed when DTR dialing is enabled or by using the **S=** modifier in the ATD dial command. One telephone number may be stored for each ASY port. For example, to store the phone number **0800 123456** as the default number to be associated with **ASY 2**, use the command:

```
at&z2=0800123456
```

If the number of the ASY port is not specified, the number will be stored against the port from which the command was entered, such as entering the command:

```
at&z=0800123456
```

from ASY 3 has the same effect as:

```
at&z3=0800123456
```

from any port. Once a number has been stored it may be dialed from the command line using the ATD command with the **S=** modifier:

```
atds=3
```

This means that any stored number can be dialed from any port. If DTR dialing has been enabled by setting **S33=1** for the port, the number associated with that port will be dialed when the DTR signal for that port changes from **Off** to **On**, such as DTR dialing can only be used with the number associated with the port to which the terminal is connected.

\AT command: Ignore invalid AT commands

This command is a work-around for use with terminals that generate large amounts of extraneous text. If not ignored, this text can cause many error messages to be generated by the router, and may result in a communications failure. To turn on this feature, type the following command:

```
at\at=1
```

To turn off the feature, type the following command:

```
at\at=0
```

When this feature is turned on, the ASY port ignores all commands except real AT commands. As with other ASY modes this can be saved by **AT&W** but is not included in the **AT&V** status display. To determine whether or not this mode is enabled type:

```
at\at ?
```

The router will display 0 if the feature is Off, 1 if it is On.

\LS command: Lock speed

The **AT\LS** command is used to lock the speed and data format of the port at which it is entered to the current settings so that the non-AT application commands may be used.

\PORT command: Set the active port for text commands

Text commands which affect the settings associated with the serial ports normally operate on the port at which they are entered, such as entering the **AT&K** command from a terminal connected to ASY 1 will affect only the flow control settings for port 1.

The **AT\PORT** command is used to select a different "active" port from that at which the commands are entered. For example, if your terminal is connected to port **0** and you need to reconfigure the settings for port **2**, you would first enter the command:

```
at\port=2
PORT 2
OK
```

Port **2** is now the active port and any AT commands or changes to S registers settings which affect the serial ports will now be applied to port **2** only. This includes:

Commands: **Z**, **&D**, **&F**, **&K**, **&V**, **&Y**, **&W**

S registers: **S31**, **S45**

The **AT\PORT?** command will display the port to which you are connected and the active port for command/ S register settings. For example:

```
at\port?
PORT 2
ASY0
OK
```

Here, **ASY2** is the active port and **ASY0** is the port at which the command was entered. If the default port and the port to which you are connected are the same, only one entry will be listed.

To reset the default port to the one to which you are connected use the **AT\PORT** command without a parameter.

\smib commands

The **at\smib** command allows you to view a single standard MIB variable. To view the variable use the **at\smib=<mib_name>** command, where **<mib_name>** is the variable to be displayed. The variables are sorted according to the hierarchy shown below.

System hierarchy of smib commands

The system hierarchy consists of the following:

at\smib=mib-2.system.sysdescr

This variable shows the software version information; equivalent to what is shown on the **ati5** CLI command output.

```
mib-2.system.sysdescr =
Software Build Ver5121.  Jan 31 2011 12:26:04  9W
```

at\smib=mib-2.system.sysobjectid

The authoritative identification of the network management subsystem. TransPort does not support outputting OID variables. Instead, **oid** is output.

```
mib-2.system.sysobjectid = oid
```

at\smib=mib-2.system.sysuptime

The time the router has been running in 10msec units (hundredths of a second).

```
mib-2.system.sysuptime = 1806718
```

The above example shows that the router has been running for **5 hours, 1 minute and 7.18 seconds**.

at\smib=mib-2.system.syscontact

A description of the contact person for the router. For TransPort, this is always a zero-length string.

at\smib=mib-2.system.sysname

The name of the router. This is the name set in the **Router Identity** parameter on the **Configuration > System > Device Identity** page.

```
mib-2.system.sysname = digi.router
```

at\smib=mib-2.system.syslocation

The physical location of the router. For TransPort, this is always a zero-length string.

at\smib=mib-2.system.sysservices

This variable displays a value that represents the set of services the router provides. For each OSI layer, the router provides services for, **2(L-1)** is added to the value, where **L** is the layer. The layers are shown below. For TransPort, this value is always **7** (Physical layer (21-1)+Data Link layer (22-1)+Network layer (23-1)).

Layer	Functionality
1	Physical
2	Data Link
3	Network
4	Transport
5	Session
6	Presentation
7	Application

Interfaces hierarchy of smib commands

The Interfaces hierarchy consists of the **ifnumber** variable and the **iftable** node:

at\smib=mib-2.interfaces.ifnumber

The total number of interfaces on the router. This includes Ethernet, PPP and virtual interfaces (such as IPSec tunnels) and SYNC ports.

```
mib-2.interfaces.ifnumber = 52
```

at\smib=mib-2.interfaces.iftable

The iftable node contains **ifentry** nodes for each interface. For each table entry, an index specifier must be appended to the end of each variable (such as for PPP0, 1 must be appended).

at\smib=mib-2.interfaces.iftable.ifentry

at\smib=mib-2.interfaces.iftable.ifentry.ifindex

The unique index number of the interface.

at\smib=mib-2.interfaces.iftable.ifentry.ifdescr

This variable displays information about the interface. This information is displayed in the format **<interface type>-<instance>**, where:

<interface type> can be one of **PPP**, **ETH**, **TUN** (for IPSec tunnels), **SNAIP** (for SNAIP links) or **SYNC**, and

<instance> is the instance.

For example:

```
mib-2.interfaces.iftable.ifentry.ifdescr.1 = PPP-0
```

at\smib=mib-2.interfaces.iftable.ifentry.iftype

The type of interface, as described by the physical/link protocol below the network layer in the protocol stack. Values can be one of the following:

- PPP 23
- ETH 6
- IPSec Tunnel 131
- SNAIP 17
- SYNC port 118

For example:

```
mib-2.interfaces.iftable.ifentry.iftype.1 = 23
```

at\smib=mib-2.interfaces.iftable.ifentry.ifmtu

The size of the largest datagram (in octets) which can be sent on the interface. SNAIP and SYNC ports always return 0. IPSec tunnel interfaces will return the underlying interface if it can be located, otherwise 0 is returned. PPP interfaces will return the negotiated MTU if the link is connected, otherwise 0 is returned.

For example:

```
mib-2.interfaces.iftable.ifentry.ifmtu.21 = 1504
```

at\smib=mib-2.interfaces.iftable.ifentry.ifspeed

This variable displays an estimate of the interface's current bandwidth in bits per second. SNAIP and SYNC ports will always return 0. PPP ports will always return 64000.

For example:

```
mib-2.interfaces.iftable.ifentry.ifspeed.1 = 64000
```

at\smib=mib-2.interfaces.iftable.ifentry.ifphysaddress

The interface's address at the protocol layer immediately below the network layer in the protocol stack. For interfaces without such an address, a zero-length octet string is returned. For PPP, SNAIP and SYNC ports, a 0 length string is returned.

at\smib=mib-2.interfaces.iftable.ifentry.ifadminstatus

The desired state of the interface. The testing state (3) indicates no operational packets can be passed.

at\smib=mib-2.interfaces.iftable.ifentry.ifoperstatus

The current operational state of the interface. The testing state (3) indicates no operational packets can be passed.

at\smib=mib-2.interfaces.iftable.ifentry.ifinoctets

The total number of octets received on this interface, including framing characters.

at\smib=mib-2.interfaces.iftable.ifentry.ifinucastpkts

The number of subnetwork-unicast packets delivered by this interface to a higher-layer protocol.

at\smib=mib-2.interfaces.iftable.ifentry.ifinnucastpkts

The number of non-unicast (such as broadcast or multicast) packets delivered by this interface to a higher-layer protocol.

at\smib=mib-2.interfaces.iftable.ifentry.ifinerrors

The number of inbound packets received by this interface that contained errors preventing them from being delivered to a higher-level protocol.

at\smib=mib-2.interfaces.iftable.ifentry.ifoutoctets

The total number of octets transmitted by this interface, including framing characters.

at\smib=mib-2.interfaces.iftable.ifentry.ifoutucastpkts

The total number of packets that higher-level protocols requested this interface to transmit to a subnetwork-unicast address, including those that were discarded or not sent.

at\smib=mib-2.interfaces.iftable.ifentry.ifoutnucastpkts

The total number of packets that higher-level protocols requested this interface to transmit to a non-unicast (such as broadcast or multicast) address, including those that were discarded or not sent.

at\smib=mib-2.interfaces.iftable.ifentry.ifouterrors

The number of outbound packets that this interface could not transmit because of errors.

IP node

The IP node consists of the **ipforwarding** variable and the **ipaddrtable** and **iproutetable** nodes.

at\smib=mib-2.ip.ipforwarding

This variable indicates whether the router is acting as an IP gateway in respect to the forwarding of datagrams received by, but not addressed to, the router. IP gateways forward datagrams, IP hosts do not. For the router, this value is always 1.

at\smib=mib-2.ip.ipaddrtable

The ipaddrtable node contains **ipaddrentry** nodes for each IP address assigned to each interface of the router. For each table entry, an index specifier must be appended to the end of each variable that specifies the interface (such as for PPP0, 1 must be appended).

at\smib=mib-2.ip.ipaddrtable.ipaddrentry

at\smib=mib-2.ip.ipaddrtable.ipaddrentry.ipadentaddr

The IP address to which this entry's addressing information pertains.

at\smib=mib-2.ip.ipaddrtable.ipaddrentry.ipadentifindex

The index identifier for the interface associated with this IP address.

at\smib=mib-2.ip.ipaddrtable.ipaddrentry.ipadentnetmask

The subnet mask associated with the IP address.

at\smib=mib-2.ip.ipaddrtable.ipaddrentry.ipadentbcastaddr

The value of the least-significant bit in the IP broadcast address used for sending datagrams on the IP address of this interface.

at\smib=mib-2.ip.iproutetable

The iproutetable node contains **iprouteentry** nodes for each route defined on the router.

at\smib=mib-2.ip.iproutetable.iprouteentry

at\smib=mib-2.ip.iproutetable.iprouteentry.iproutedest

The destination IP address for the route. An entry with a value of 0.0.0.0 is considered the default route. Multiple routes to a single destination can appear in the routing table, but access to such multiple entries is dependent on the table-access mechanisms defined by the network management protocol in use.

at\smib=mib-2.ip.iproutetable.iprouteentry.iprouteifindex

The index value which uniquely identifies the local interface through which the next hop of the route should be reached.

at\smib=mib-2.ip.iproutetable.iprouteentry.iproutemetric1

The primary routing metric for the route.

at\smib=mib-2.ip.iproutetable.iprouteentry.iproutenexthop

The IP address of the next hop of the route.

at\smib=mib-2.ip.iproutetable.iprouteentry.iproutetype

The type of route. Valid values are:

    1   Valid

    2   Invalid

    3   Direct

    4   Indirect

at\smib=mib-2.ip.iproutetable.iprouteentry.iproutemask

The netmask for the route.

S register definitions

In addition to the AT commands there are a number of Special ("S") registers. These registers contain numeric values that may represent time intervals, ASCII characters or operational flags.

To display the contents of a particular "S" register, the ATS command is used in the form **ATSn?** where **n** is the number of the register whose contents are to be shown.

To store a new value into a register, use the S command in the form **ATSN=X** where **N** is the number of the register to be changed and **X** is the new value. For example, **ATS31=4** would store the value 4 in **S31**.

The router maintains one set of registers for each ASY port. By default, the S command operates ONLY on the S register set for the active port. To select an alternative default port, use the **AT\PORT** command first.

Each register can only be set to a limited range of values as shown in the table below:

Register	Description	Units	Default	Range
S0	V.120 Answer enable	Rings	0	0-255
S1	Ring count	Rings	n/a	n/a
S2	Escape character	ASCII	43	0-255
S9	DCD on delay	ms x 20	0	0-255
S10	Pulse time for DCD Low	ms x 10	0	0-255
S12	Escape delay	ms	50	0-255
S15	Data forwarding timer	ms	2	0-255
S16	RS422/485 serial port settings	N/A	0	0, 2, 3
S23	Parity	N/A	0	0-2 5 6
S31	ASY interface speed	refer to full description	n/a	0-11
S33	DTR dialing	N/A	0	0 1
S45	DTR loss de-bounce	0.05 seconds	(0.25s)	1-255

S0 V.120 Answer Enabled

Units: Rings
Default: 0
Range: 0-255

S0 is used only in V.120 mode to enable or disable automatic answering of incoming ISDN calls. Auto answering is disabled when **S0** is set to the default value of 0. Setting S0 to a non-zero value enables auto-answering.

The actual value stored determines the number of "rings" that the router will wait before answering. For example, the command **ATS0=2** enables auto-answering after two incoming rings have been detected.

With each ring the RING result code is issued and the value stored in **S1** is incremented. When the value in **S1** equals the value in **S0** the call is answered.

S1 Ring count

Units: Rings
Default: n/a
Range: n/a

When ADAPT detects an incoming ISDN call on an ASY port, it will print **RING** to the ASY port at 2 second intervals. It also increments the S1 register, counting how many times **RING** is printed.

S2 Escape Character

Units: ASCII
Default: 43
Range: 0-255

The value stored in **S2** defines which ASCII character is used as the Escape character, which by default is the **+** symbol. Entering this character three times followed by a delay of 1-2 seconds and then an AT command will cause the router to switch from on-line mode to command mode.

S12 Escape Delay

Units: ms
Default: 50
Range: 0-255

The value stored in **S12** defines the delay between sending the escape sequence and entering an AT command for the router to switch from on-line mode to command mode.

S15 Data Forwarding Timer

Units: 10ms
Default: 0
Range: 0-255

S15 is used to set the data forwarding timer for the ASY port in multiples of 10ms. The default data forwarding time is 20ms and in normal use this there should be no need to change this. However, setting **S15** to **1** enables a special mode of operation in which data is forwarded as fast as possible for the data rate for which the port is configured (at 115000bps, this will typically be 2-3ms).

Note that the default value of **0** is equivalent to setting the register to **2** in order to maintain compatibility with older systems.

S16 RS422/485 serial port settings

The RS485 option is only available on specific hardware versions.

Units: N/A
Default: 0
Range: 0,2,3, where **0**=RS232, **2**=RS485 full duplex, **3**=RS485 half duplex

Following example shows how to setup and save **ASY 0** in 485 half-duplex mode

```
AT\port=0
ATS16=3
AT&w
AT\port
```

The at\port=0 is needed to ensure that subsequent AT commands are directed to the right port (ASY0). The port settings can be saved permanently using AT&W.

Issue the command **ats16?** and check that the value of this S register is 3. To set it back to RS232 then set **ATS16** to zero and save it with the **&w** command.

S23 Parity

Units: N/A
Default: 0
Range: 0-2,5,6

The value stored in **S23** determines whether the parity used for the ASY port is set to **None** (**0**), **Odd** (**1**), **Even** (**2**), **8Data Odd** (**5**) or **8Data Even** (**6**).

S31 ASY Interface Speed

Units: N/A
Default: 0
Range: 0-11

Register **S31** is used to set the speed and data format for the ASY port to which you are currently connected.

The default value for **ASY 0** is 0, such as the port speed/data format is not set to a specific value, it is determined automatically from the AT commands that you enter.

The default value for ASY 1, 2 and 3 is **3**, such as the ports will only accept AT commands at 115,200bps (8 data bits, no parity and 1 stop bit).

To set the speed of one of the ports to a particular value, the appropriate register should be set to the required value from the following table:

S31	Port Speed (bps)	S31	Port Speed (bps)
0	Auto-detect	6	19200
1	Reserved	7	9600
2	Reserved	8	4800
3	115200	9	2400
4	57600	10	1200
5	38400	11	300

For example, to change the speed of **ASY 1** to **38,400bps**, connect your terminal to that port with the speed set to **9600bps**. Enter the command:

```
ats31=5
```

then change the speed of your terminal to **38,400bps** before entering any more AT commands.

The data format used when the **ATS31=n** command is entered is selected as the data format for all further commands.

The auto-detect option is only available for **ASY0** and **ASY1**.

S33 DTR Dialing

Units: N/A
Default: 0
Range: 0, 1

S33 is used to enable or disable DTR dialing for the port. When DTR dialing is enabled, the router will dial the number stored for that port (see **AT&Z**) when the DTR signal from the terminal changes from **Off** to **On**.

S45 DTR Loss De-Bounce

Units: 0.05 seconds
Default: 5
Range: 1-255

The value in **S45** determines the length of time for which the DTR signal from the terminal device must go off before the router acts upon any options that are set to trigger on loss of DTR. Increasing or decreasing the value in **S45** makes the router less or more sensitive to "bouncing" of the DTR signal respectively.

Application commands

The TransPort device also supports numerous text-based application commands that are specific to Digi International products, and do not require the AT prefix. Some of these are generic, such as they are related to the general operation of the router; others are application- or protocol-specific.

This section contains the following information about application commands:

- Lock the interface speed to the terminal on page 138
- Application commands are case-insensitive on page 138
- One command per line on page 138
- Application command syntax on page 138
- Using wildcards on page 139
- Using the CLI parameter tables in this guide on page 140
- reboot command: reboot router on page 141
- config command: show/save configuration on page 142
- ping command: Troubleshoot connectivity problems on page 143
- traceroute command: Troubleshoot connectivity problems on page 143
- ana command: Clear the Analyser Trace on page 143
- clear command: Clear the Event Log on page 143
- Activate and deactivate interfaces on page 144
- gpio command: General Purpose Input Output (GPIO) on page 145
- qdl command: Select cellular image to load on page 147
- tcpperm command: establish a permanent serial to IP connection on page 148
- tcpdial command: Establish a manually initiated serial to IP connection on page 150
- tcpdab command: Cancel a tcpdial connection on page 150

Lock the interface speed to the terminal

Application commands can be entered via any of the serial ports but if you are using ASY 0 or ASY 1 with auto-speed detection enabled (which is not possible on ports 2, 3, etc.), you must first lock the interface speed to the same as that of your terminal. To do this first ensure that the router is responding to AT commands correctly and then enter the command:

`AT\LS`

The speed will remain locked until the router goes on-line and then off-line again, the power is removed or the router is reset. Once the port speed has been locked, AT commands will still work but you may also use the application commands.

Remember that if you subsequently re-enable auto-speed detection on the port it will disable the use of application commands until the **AT\LS** command has been re-entered or the port speed has been set to a specific speed using **S31**. For example, to set the port speed at 19,200bps enter the command:

`ATS31=6`

And then change your terminal settings to match.

Note: Speed locking is not necessary when you use the text commands via a Telnet session.

Application commands are case-insensitive

Digi application commands (referred to just as **text commands** or **CLI commands** throughout the remainder of this guide), can be entered in upper or lower case.

One command per line

Unlike AT commands, only one command may be entered on a line. After each successful command, the **OK** result code will be issued. An invalid command will cause the **ERROR** result code to be issued.

Application command syntax

The general syntax for an application commands is:

`<entity> <instance> <param_name> <value>`

where:

`<entity>` is the name of the entity.

`<instance>` is the instance number for the entity that you are configuring.

`<param_name>` is the name of the parameter that you wish to configure.

`<value>` is the new value for the specified parameter.

For example, to set the window size to 5 for X.25 PAD instance 1 you would enter:

`pad 1 window 5`

Even if there is only once instance of particular entity, you should only enter 0 for the instance number.

Using wildcards

Wildcards can be used in the field **<param_name>** when viewing parameters (not setting them), for example, to view all PPP 1 parameters that start with **r**, as follows:

ppp 1 r* ?

The output will show:

```
ppp 1 r* ?
r_mru: 1500
r_acfc: OFF
r_pfc: OFF
r_pap: ON
r_chap: ON
r_accm: 0xffffffff
r_comp: OFF
r_addr: OFF
r_callb: 0
rxtimeout: 23
rdoosdly: 0
restdel: 2000
rebootfails: 0
rip: 0
ripip:
ripauth: 1
ripis: OFF
r_md5: 1
r_ms1: 1
r_ms2: 1
rbcast: OFF
OK
```

Using special usernames in commands

There are some special usernames that can also be used for both local and remote authentication, these are:

Username	Description
%s	Uses the serial number of the router as the username.
%i	Uses the IMEI of the cellular module as the username.
%c	Uses the ICCID of the SIM as the username.

If a **%** symbol is part of the username, it must be escaped with another **%** symbol. For example, **user%1** should be entered as **user%%1**.

Using the CLI parameter tables in this guide

Many sections in this guide include tables showing the CLI parameters that relate to the web-based settings. The CLI parameters nearly always take the following format; there are only a few exceptions.

`<entity> <instance> <parameter> <value>`

Where:

`<entity>`=eth, ppp, modemcc, wifi, ike, eroute, etc.

`<instance>`=0, 1, 2, 3, etc... Some entities only use 0. Others have multiple instances.

`<parameter>`=The parameter name, such as, ipaddr, mask, gateway, etc.

`<value>`=The value to set, such as, off, on, 192.168.1.1, username, free_text, etc.

For example, the following table is displayed for Ethernet parameters:

Entity	Instance	Parameter	Values	Equivalent Web Parameters
eth	n	descr	Free text field	Description
eth	n	ipaddr	Valid IP address	IP Address
eth	n	mask	Valid Subnet Mask	Mask
eth	n	gateway	IP address	Gateway
eth	n	dnsserver	IP address	DNS Server
eth	n	secdns	IP address	Secondary DNS Server
eth	n	dhcpcli	Off / On	On=Get an IP address automatically using DHCP Off=Use the following IP address

To use this table, read the row from left to right and replace values as appropriate. The first four columns only are needed for entering commands; the rightmost column shows the equivalent setting in the web interface.

If the **Instance** is **n** in the table, it is because there are multiple instances available. Use the instance number you need for your requirements. If the **Instance** is set to a specific number, such as **0**, use the number specified in the table.

For example, to set a **Description** of **Local LAN** on **Ethernet 0**, enter:

`eth 0 descr "Local LAN"`

Because of the space between **Local** and **LAN**, the wording is enclosed in double quotes.

To set an IP address on 192.168.1.1 on **Ethernet 0**:

`eth 0 ipaddr 192.168.1.1`

To set an IP address of 172.16.0.1 on **Ethernet 1**:

`eth 1 ipaddr 172.16.0.1`

To enable the DHCP client on Ethernet 2:

`eth 2 dhcpcli on`

reboot command: reboot router

The **reboot** command is used to reboot the router after altering the configuration. The **reboot** command executes a complete hardware reset, loading and running the main image from cold. It has three modes of operation:

- **reboot**: Reboots the router after any FLASH write operations have been completed. Also, 1 second each is allowed for the following operations to be completed before reboot will take place:

  - IPSec SA delete notifications have been created and sent

  - TCP sockets have been closed

  - PPP interfaces have been disconnected

- **reboot <n>**: A time reboot; reboots the router in **<n>** minutes where **n** is 1 to 65,535.

- **reboot cancel**: Cancels a timed reboot if entered before the time period has passed.

Reset the router to factory defaults

To reset router to factory defaults, see Reset the router to factory default settings on page 798.

Disable the reset button

Normally when the reset button is held in for 5 seconds the router is reset to factory defaults. The factory reset button functionality can be disabled/enabled, if required.

To disable the reset button, enter:

```
cmd 0 pbreset off
```

To re-enable the reset button functionality, enter:

```
cmd 0 pbreset on.
```

Note You can enable or disable the reset button from the web interface. For more information see Reset the router to factory default settings on page 798.

config command: show/save configuration

The **config** command is used for the following purposes to show current or stored configuration settings, to save the current configuration or to specify which configuration is to be used when the router is powered up or rebooted.

The format of the config command is:

```
config <0|1|c> <save|show|powerup>
```

Two separate configurations can be stored, numbered 0 and 1. The first parameter of the config command specifies to which configuration the command applies. The letter "c" denotes the current configuration settings, such as those currently in use.

The second parameter is one of the following keywords:

- **show** displays the specified configuration (either 0, 1 or c for the current configuration)
- **save** saves the current settings as the specified configuration (either 0 or 1)
- **powerup** sets the specified configuration (either 0 or 1) to be used at power-up or reboot

For example, to display the current configuration use the command:

```
config c show
```

The output will appear similar to the following example:

```
config c show
eth 0 descr "LAN 0"
eth 0 IPaddr "192.168.1.1"
eth 0 mask "255.255.255.0"
eth 0 bridge ON
eth 1 descr "LAN 1"
eth 2 descr "LAN 2"
eth 3 descr "LAN 3"
eth 4 descr "ATM PVC 0"
```

The config files only contain details of those settings that are different from the router's default settings. If you make a setting that is the same as the default setting, it will not appear in a stored configuration.

To save the current settings to configuration file 1, enter:

```
config 1 save
```

To use configuration 1 when the router is powered up or rebooted, enter:

```
config 1 powerup
```

config changes command: show number of changes counter

The **config changes** command shows the number of changes to the current configuration since the router has powered up and the initial configuration file run. Also shows the time when the configuration file was last saved.

ping command: Troubleshoot connectivity problems

From the CLI, the **ping** command can be used to help troubleshoot connectivity problems.

The syntax of the **ping** command is:

```
ping <ip address|FQDN> [n]
```

Where **n** (if used) is the number of ICMP echo requests to send. If not specified, only 1 echo request will be sent.

To stop pings when n has been set to a high value use **ping stop**.

traceroute command: Troubleshoot connectivity problems

From the CLI, the **traceroute** command can be used to help troubleshoot connectivity problems.

The syntax of the **traceroute** command is:

```
traceroute <ip address|FQDN>
```

To stop a failed trace if hosts can not be detected, use **traceroute stop**.

ana command: Clear the Analyser Trace

To clear the Analyser trace, the CLI command is:

```
ana 0 anaclr
```

clear command: Clear the Event Log

To clear the event log, the CLI command is:

```
clear_ev
```

Activate and deactivate interfaces

To manually activate (or raise) an interface, enter the following CLI command as an activation request:

`<entity> <instance> act_rq`

To manually deactivate (or lower) an interface, enter the following CLI command as an activation request:

`<entity> <instance> deact_rq`

Where *<entity>* can be:

PPP   for PPP interfaces

TUN   for GRE TUN interfaces

OVPN   for OpenVPN interfaces

And **<instance>** is the interface number, such as **0**, **1**, **2** etc

For example, to activate **PPP 1**, the CLI command is:

`ppp 1 act_rq`

and to deactivate **PPP 1**:

`ppp 1 deact_rq`

gpio command: General Purpose Input Output (GPIO)

GPIO commands are necessary to configure a WR44, which has one Digital Input/Output port and one Digital Input port. This command allows configuration of the I/O port either as an input port or an output port. For example:

Command	Description
gpio inout input	Configures the I/O port as an input.
gpio inout output	Configures the I/O port as an output.
gpio inout ON	Sets the I/O port to ON when configured as an output.
gpio inout OFF	Sets the I/O port to OFF when configured as an output.

The syntax of the command is as follows:

```
gpio [inout ON|OFF|input|output]
```

Display current status of ports

With no parameters, the **gpio** command displays the current status of the ports. For example:

```
gpio
Input(s):
        in : OFF
Output(s):
     inout : OFF
OK
```

Set the I/O port as an output

To set the I/O port to be an output:

```
gpio inout output
Input(s):
        in : OFF
Output(s):
     inout : OFF
OK
```

Set the I/O port to ON when configured as an output

To set the I/O port to **ON** when it is configured as an output:

```
gpio inout on
Input(s):
        in : OFF
Output(s):
     inout : ON
OK
```

The Input and Input/Output connections (pins **2** and **3**) are programmed via the command line using the **gpio** command. The default setting for pins **2** and **3** are **OFF** as seen in the above example.

Note Only one of the power connectors should be used. Never apply power to both the **MAIN** and **AUX** connectors at the same time.

Pin	Description
Pin 1	GROUND
Pin 2	INPUT
Pin 3	Input/ Output
Pin 4	Power

The following image shows the pins and the corresponding numbers:
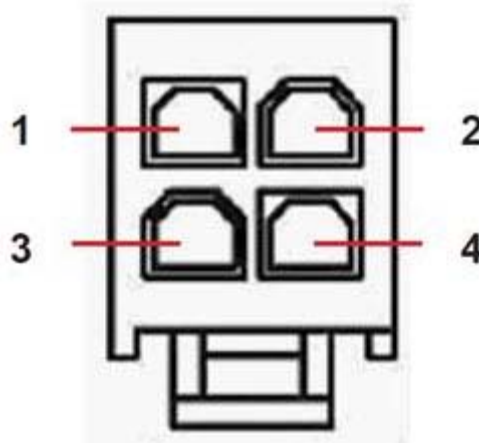
For more information on wiring and other details, see the *4-pin DC Power Cord User Guide*, Digi part number 90001246.

qdl command: Select cellular image to load

For the **qdl** command, it is used to specify which image to load onto a GOBI cellular module.

The syntax of the command is:

`qdl 0 fw <n>`

where **n** can be 0-14. The default value is **0**.

Instance	Value
0	Generic UMTS
1	Verizon
2	Sprint PCS
3	IUSACELL
4	Bell Mobility
5	Alltel
6	Cingular Blue
7	Cingular Orange
8	T-Mobile
9	Docomo
10	Orange
11	Vodafone
12	Telefonica
13	Telital
14	OMH

tcpperm command: establish a permanent serial to IP connection

The **tcpperm** command is available only as application commands, and has no equivalent web pages. **tcpperm** is used to establish a permanent "serial to IP" connection between one of the ASY ports and a remote IP host. After **tcpperm** has been executed, the router will automatically open a socket connection to the remote peer whenever data is received from a terminal attached to the specified ASY port. When the socket is first opened and the connection has been established, the router will issue a **CONNECT** message to the terminal and will subsequently relay data between the socket and the ASY port. The format of the **CONNECT** message can be modified using the standard AT commands (such as **ATV**, **ATE**, etc.) or using the **Configuration > Network > Interfaces > Serial > Serial Port n** web page.

Note The serial port should also be pre-configured to use the appropriate word format, speed and flow control.

While the serial-to-IP connection is established, if the attached serial device drops the DTR signal, then the socket connection will be terminated, much as with a standard modem or terminal adapter. Again this behavior can be modified via the **AT&D** command or the serial port settings.

The format of the command is:

```
TCPPERM <[ASY 0-1]> <Dest Host> <Dest Port> [UDP] [nodeact] [-l<listening port>] [-
i<inact_timeout>] [-f<fwd_time>] [-e<eth_ip>][-d(deact link)] [-k<keepalive_time>] [-
s<src_port>] [-ok] [-t<telnet_mode>] [-ho(host only)] [-ssl] [-ao(always open)] [-m<mhome
idx>]
```

The **tcpperm** parameters are as follows:

Parameter	Description
ASY	The number of the ASY port that the link will be made from/to.
Dest Host	The IP address (or name) of the remote peer.
Dest Port	The port number to use on the remote peer.
UDP	Open a UDP connection (the default is TCP).
-ao	Open socket immediately, and reopen if and when the socket is closed.
-e	Use the address of Ethernet port **n** for the socket connection rather than the default of the address of the interface over which the socket is opened (that is, **ppp 1**, **ppp 2**, etc.)
-d	Deactivate link. If non-zero, when the socket is closed and there are no other sockets using the interface then the interface connection is dropped (switched connections only).
-f	The forwarding time (**x10ms**) for packetizing data from the serial port.
-ho	Host. Indicates that the socket should only accept connections from the specified host.
-i	The inactivity timeout (s) after which the socket will be closed.
-k	Keep alive packet timer (s).
-l	Listening port. Allows the user to set a new TCP port number to listen on rather than the default value of **4000**+**ASY port #**.
-m	Multihome additional consecutive addresses index
-ok	Open socket in quiet mode, such as there is no **OK** response to the TCPPERM command.
-s	Source port number
-ssl	Use SSL mode
-t	Use Telnet mode. Opens socket in the corresponding Telnet mode (port **23** default), **0**=raw, **1**=Telnet Mode, **2**=Telnet Mode with null stuffing. If this is not specified, then the mode specified for the associated ASY port in general setup is used. If the **-t** option is specified then the **ok** option is always used.

The **tcpperm** command can also be made to execute automatically on power-up by using the **cmd n autocmd 'cmd'** macro command, such as

```
cmd 0 autocmd 'tcpperm asy 0 192.168.0.1 -f3 -s3000 -k10 -e1'
```

Considerations for use with VPN or GRE tunnels

When the socket used by TCPPERM is opened the default behavior is to use the address of the interface over which the socket is carried (**ETHn** or **PPPn**) as the source address of the socket. If the socket data is to be tunneled then it may be necessary to use the -en modifier so that the source address of the socket matches the local subnet address specified in the appropriate Eroute. A similar effect can also be achieved by setting the parameter Default source IP address interface: Ethernet n in the Web interface on the **Configuration > Network > Advanced Network Settings**.

tcpdial command: Establish a manually initiated serial to IP connection

The **tcpdial** command is available only as application commands, and has no equivalent web pages. **tcpdial** operates in an identical manner to **tcpperm**, except that establishment of the socket connection is not automatic and must be initiated by the **tcpdial** command. The simplest method of achieving this is to map a command using the **Configuration > Network > Interfaces > Serial > Command Mappings**, such as, Command to Map **ATDT0800456789** maps to **tcpdial asy 1 217.36.133.29 -e0**. Now, whenever the attached terminal device attempts to dial the number defined the router will map it to an IP socket connection.

In this way, multiple dial commands can be directed to the same or different IP hosts with other simple command mappings.

tcpdab command: Cancel a tcpdial connection

The **tcpdab** command can be used to cancel a TCPDIAL connection before the connection has been made. It can also be used from a command session to disconnect an existing TCPDIAL connection on another ASY port.

The format of the command is:

```
tcpdab <instance> ATH
```

where **<instance>** is the number of the ASY port.

Configure network interfaces

The **Configuration > Network > Interfaces** menu configures settings for several network interfaces. The configurable network interfaces available depend on the TransPort router model. This section covers configuring network interfaces from the web interface and command line. It covers the following topics:

- Configure Ethernet interfaces on page 152
- Configure Wi-Fi interfaces on page 177
- Configure mobile interfaces on page 189
- Configure GRE interfaces on page 223
- Configure ISDN interfaces on page 228
- Configure PSTN interfaces on page 250
- Configure DialServ interfaces on page 258
- Configure serial interfaces on page 267
- Configure Advanced interfaces settings on page 287

Configure Ethernet interfaces

The **Configuration > Network > Interfaces > Ethernet** page opens to list configuration pages for each of the available Ethernet instances on the router. Each page allows the user to configure parameters such as the IP address, mask, gateway, and others.

On routers with only one Ethernet port, if more than one Ethernet instance exist these are treated as logical Ethernet ports. These instances can be used to assign more than one Ethernet IP address to a router.

On routers with more than one physical Ethernet port, the Ethernet instances refer to the different physical Ethernet ports. These routers can be configured for either **HUB** mode or **Port Isolate** mode.

In HUB mode all the Ethernet ports are linked together and behave like an Ethernet hub or switch. This means that the router will respond to all of its Ethernet IP addresses on all of its ports (as the hub/ switch behavior links the ports together).

In Port Isolate mode, the router will only respond to its **Ethernet 0** IP address on physical port **LAN 0**, its **Ethernet 1** IP address on physical port **LAN 1**, etc. The router will not respond to its Ethernet 1 address on port **LAN 0** unless routing has been configured appropriately.

When configured for HUB mode it is important that no more than one of the router's ports is connected to another hub or switch on the same physical network otherwise an Ethernet loop can occur. The default behavior is **HUB** rather than **Port Isolate**.

VLAN tagging is not available when the router is configured for Port Isolate mode.

ETH n

This initial view only shows basic IP address parameters. The choice is to obtain an IP address by using a DHCP server or to manually configure the IP addressing for this interface.

Description

A memorable name for this Ethernet instance, to make it easier to identify.

Get an IP address automatically using DHCP

Enables the DHCP client on this interface.

Use the following IP address

Enables manual configuration of the IP addressing parameters

IP Address

This parameter specifies the IP address of this Ethernet port on your LAN.

Mask

The subnet mask of the IP subnet to which the router is attached via this Ethernet port. Typically, this would be **255.255.255.0** for a Class C network.

Gateway

The IP address of a gateway to be used by the router. IP packets whose destination IP addresses are not on the LAN to which the router is connected will be forwarded to this gateway.

DNS Server / Secondary DNS Server

The IP address of DNS servers to be used by the router for resolving IP hostnames.

Note If the IP address, Mask, Gateway, DNS server or Secondary DNS server parameters are specified manually, but the option to use a DHCP server is later selected, any existing manually specified parameters will override the DHCP supplied parameters. To change from manual configuration to DHCP, be sure to remove all manually specified parameters first.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameters
eth	n	descr	Free text field	Description
eth	n	ipaddr	Valid IP address	IP Address
eth	n	mask	Valid Subnet Mask	Mask
eth	n	gateway	IP address	Gateway
eth	n	dnsserver	IP address	DNS Server
eth	n	secdns	IP address	Secondary DNS Server
eth	n	dhcpcli	on, off	On=Get an IP address automatically using DHCP Off=Use the following IP address

Advanced Ethernet parameters

On routers with only one Ethernet port, there may be multiple configurable Ethernet instances. Ethernet 0 is the physical interface. These extra instances are treated as logical Ethernet ports and can be used to assign more than one Ethernet IP address to a router.

On routers with more than one physical Ethernet port, the Ethernet instances refer to the different physical Ethernet ports. These routers can be configured for either **HUB** mode or **Port Isolate** mode.

In HUB mode all the Ethernet ports are linked together and behave like an Ethernet hub or switch. This means that the router will respond to all of its Ethernet IP addresses on all of its ports (as the hub/ switch behavior links the ports together).

In Port Isolate mode the router will only respond to its Ethernet 0 IP address on physical port **LAN 0,** its Ethernet 1 IP address on physical port **LAN 1**, etc. The router will not respond to its Ethernet 1 address on port **LAN 0** unless routing has been configured appropriately.

When configured for HUB mode it is important that no more than one of the router's Ethernet interfaces is connected to another hub or switch on the same physical network otherwise an Ethernet loop can occur. The default behavior is **HUB** rather than **Port Isolate**.

Port Isolate mode

If the router is running in Port Isolate mode, the following will be displayed, with an option to switch to Hub mode.

Hub Mode (factory default)

If the router is running in Hub mode, the following is displayed, with an option to switch to Port Isolate mode.

Ethernet Hub group

On routers with a built-in hub/switch, the Ethernet Hub Group parameter for each port is normally set to 0. This means that all ports belong to the same hub. If required however, the Hub Group parameter may be used to isolate specific ports to create separate hubs. For example, if Ethernet 0 and Ethernet1 have their Group parameter set to 0 whilst Ethernet 2 and Ethernet 3 have their Group parameter set to 1, the router will in effect be configured as two 2-port hubs instead of one 4-port hub. This means that traffic on physical ports **LAN 0** and **LAN 1** will not be visible to traffic on physical ports **LAN 2** and **LAN 3** (and vice versa). Group numbers can be 0-3 or use 255 for an interface to be in all groups. This parameter is not available on the web page when the router is configured for Port Isolate mode.

Metric

The connected metric of an interface. Changing this value will alter the metric of dynamic routes created automatically for this interface. The default metric of a connected interface is 1. By allowing the interface to have a higher value (lower priority), static routes can take preference to interface generated dynamic routes. For normal operation, leave this value unchanged.

MTU

The Maximum Transmit Unit for the specified interface. The default value is 0 meaning that the MTU will either be 1504 (for routers using a Kendin Ethernet device) or 1500 (for non-Kendin devices). The non-zero, values must be greater than 128 and not more than the default value. Values must also be multiples of 4 and the router will automatically adjust invalid values entered by the user. So, if the MTU is set to 1000, the largest IP packet that the router will send is 1000 bytes.

Enable auto-negotiation

Allows the router and the other Ethernet device it is connected to, to auto-negotiate the speed and duplex of the Ethernet connection.

Speed (currently 100Base-T)

Selects either of the **10Base-T**, **100Base-T**, or **Auto** modes. The currently selected mode is shown in brackets after the parameter name.
Note, enabling **Auto-negotiation** and manually setting the speed will only allow the selected speed to be negotiated.

Duplex

Selects either of **Full Duplex**, **Half Duplex** or **Auto** mode. Enabling **Auto-negotiation** and manually setting the Duplex will only allow the selected Duplex mode to be negotiated.

Max Rx rate

On models with multiple Ethernet interfaces, this parameter specifies a maximum data rate in Kbps that the router receives on this interface. This may be useful in applications where separate Ethernet interfaces are allocated to separate LANs and it is necessary to prioritize traffic from one LAN over another.

Max Tx rate

On models with multiple Ethernet interfaces, this parameter specifies a maximum data rate in kbps that the router will transmit on this interface. This may be useful in applications where separate Ethernet interfaces are allocated to separate LANs and it is necessary to prioritize traffic from one LAN over another.

TCP transmit buffer size

When set to a non-zero value, this parameter sets the TCP buffer size of transmitted packets in bytes. This is useful for slow / lossy connections such as satellite. Setting this buffer to a low value will prevent the amount of unacknowledged data from getting too high. If retransmits are required, a smaller TX buffer helps prevent retransmits flooding the connection.

Take this interface out of service after n seconds when the link is lost (such as cable removed or broken)

The length of time, in seconds, the router will wait after detecting that an Ethernet cable has been removed before routes that were using that interface are marked as out of service. If the parameter is set to 0, the feature is disabled such as routes using the interface will not be marked as out of service if the cable is removed.

Enable NAT on this interface

Selects whether IP Network Address Translation (NAT) or Network Address and Port Translation (NAPT) are used at the Ethernet interface. When the parameter is set to disabled, no NAT will take place. When this parameter is enabled, extra options described below will be displayed.

NAT and NAPT can have many uses but they are generally used to allow a number of private IP hosts (PCs for example) to connect to the Internet through a single shared public IP address. This has two main advantages, it saves on IP address space (the ISP only need assign you one IP address), and it isolates the private IP hosts from the Internet (effectively providing a simple firewall because unsolicited traffic from the Internet cannot be routed directly to the private IP hosts.

To use NAT or NAPT correctly in the example of connecting private hosts to the Internet, NAT or NAPT should be enabled on the router's WAN side interface and should be disabled on the router's LAN side interface.

IP address

When a private IP host sends a UDP or TCP packet to an Internet IP address, the router will change the source address of the packet from the private host IP to the router's public IP address before forwarding the packet onto the Internet host. Additionally it will create an entry in a **NAT table** containing the private IP source address, the private IP port number, the public IP destination address and the destination port number. Conversely, when the router receives a reply packet back from the public host, it checks the source IP, source port number and destination port number in the NAT table to determine which private host to forward the packet to. Before it forwards the packet back to the private host, it changes the destination IP address of the packet from its public IP address to the IP address of the private host.

IP address and Port

This mode behaves like NAT, but in addition to changing the source IP of the packet from the private host, it can also change the source port number. This is required if more than one private host attempts to connect using the same local port number to the same Internet host on the same remote port number. If such a scenario were to occur with NAT the router would be unable to determine which private host to route the returning packets to and the connection would fail.

Enable IPsec on this interface

Enables or disables IPSec security features for this Ethernet interface.

Use interface x,y for the source IP address of IPsec packets

By default, the source IP address for an IPsec Eroute is the IP address of the interface on which IPSec was enabled. By setting this parameter to either PPP or Ethernet and the relevant interface number, the source address used by IPSec matches that of the Ethernet or PPP interface specified.

Enable the firewall on this interface

Turns Firewall script processing **On** or **Off** for this interface.

Remote management access

The Remote access options parameter can be set to **No restrictions**, **Disable management**, **Disable return RST**, **Disable management an return RST**.

- When set to **No restrictions**, users on this interface can access the router's Telnet, FTP, and web services for the purpose of managing the router.

- When set to **Disable management**, users on this interface are prevented from managing the router via Telnet, FTP, or the web interface.

- For **Disable return RST**, whenever a router receives a TCP SYN packet for one of its own IP addresses with the destination port set to an unexpected value, such as a port that the router would normally expect to receive TCP traffic on, it will reply with a TCP RST packet. This is normal behavior. However, the nature of internet traffic is such that whenever an internet connection is established, TCYP SYN packets are to be expected. As the router's PPP inactivity timer is restarted each time the router transmits data (but not when it receives data), the standard response of the router to SYN packets such as transmitting an RST packet, will restart the inactivity timer and prevent the router from disconnecting the link even when there is no genuine traffic. This effect can be prevented by using the appropriate commands and options within the firewall script. However, on Digi 1000 series routers, or where you are not using a firewall, the same result can be achieved by selecting this option, such as when this option is selected the normal behavior of the router in responding to SYN packets with RST packets is disabled. The option will also prevent the router from responding to unsolicited UDP packets with the normal ICMP destination unreachable responses.

- The **Disable management & return RST** option prevents users from managing the router via the Telnet, FTP, and web interfaces and also disables the transmission of TCP RST packets as above.

Multihome additional consecutive addresses

Defines how many additional (consecutive) addresses the ethernet driver will own. For example, if the IP address of the interface was 10.3.20.40, and Multihome additional consecutive addresses was set to 3, the IP addresses 10.3.20.41, 10.3.20.42 and 10.3.20.43 would also belong to the Ethernet interface.

Enable IGMP on this interface

Enables or disables the Internet Group Management Protocol for this Ethernet interface.

Enable Bridge on this interface

Bridge mode only applies to models with built in Wi-Fi. If Wi-Fi is enabled, bridge mode must be enabled on the Eth 0. This creates an Ethernet bridge between the Wi-Fi access point and the physical Ethernet interface.

Generate Heartbeats on this interface

Enabling this option displays the parameters for Heartbeat packets. These are UDP packets which can contain status information about the router and can be used in conjunction with Remote Manager.

Send Heartbeat messages to IP address a.b.c.d every h hrs m mins s seconds

For this setting, **a.b.c.d** specifies the destination IP address for heartbeat packets and h, m and s specifies how often the router will transmit heartbeat packets to the specified destination in (**h**) Hours, (**m**) Minutes and (**s**) Seconds.

Use interface x,y for the source IP address

By default, heartbeat packets is sent with the source IP address of the interface on which they were generated. If the heartbeat is required to be sent via an IPSec tunnel, this parameter can be used to specify the source IP address of the heartbeat packet to ensure the source and destination match the eroute selectors.

Select the transmit interface using the routing table

When enabled, the UDP heartbeats chooses the best route from the routing table. If disabled the exit interface will be interface on which the heartbeat is configured.

Include IMSI information in the Heartbeat message

When enabled, the heartbeat includes the IMSI of the cellular module.

Include GPS information in the Heartbeat message

When enabled and the appropriate GPS hardware is installed, the heartbeat includes the GPS co-ordinates of the router.

Generate Ping packets on this interface

Enabling this option displays the parameters for enabling auto-pings to be transmitted from this interface. These pings can be monitored by the interface auto-pings were enabled on and in the event of no ping reply, the interface can be taken out of service for a specified amount of time, before allowing the interface to be used again. Another option is to enable auto-pings on this interface and let the firewall handle taking the interface out of service in the event of a failure. Both methods are explained in Application Notes on our Technical Support Documents web page.

Send n byte pings to IP host a.b.c.d every h hrs m mins s seconds

For this setting, **n** specifies the payload size of a ping packet when used with the auto ping feature. Leaving this parameter blank will use the default value. The address a.b.c.d specifies the destination IP address for auto-ping ICMP echo request. The values h, m and s specifies how often the router will transmit Auto-ping packets to the specified destination in (h) Hours, (m) Minutes and (s) Seconds.

Switch to sending pings to IP host a.b.c.d after n failures

For this setting, **a.b.c.d** specifies an alternative destination IP address for the auto-ping ICMP echo request to be sent to, should the main IP address specified in the parameter above fail to respond. This allows the router to double check there is a problem with the connection and not just with the remote device not responding. The value n specifies the number pings that need to fail before the 2nd IP address is checked. The extra IP address check is only enabled if this parameter is set to something other than 0.

Only send Pings when this Ethernet interface is "In Service"

If this parameter is enabled, ICMP echo requests will only be sent from this interface when it is in service. The default setting is disabled, ICMP echo requests are sent when the interface is in service and out of service.

Take this interface "Out of Service" after receiving no responses for s seconds

The length of time, in seconds, before a route will be designated as being out of service if there has been no response to ANY of the ICMP echo requests during that time period.

Keep this interface out of service for s seconds

The length of time, in seconds, for which any routes using this Ethernet interface will be held out of service after a ping failure is detected.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
n/a	n/a	ethvlan	n/a	Switch to Port Isolate Mode
n/a	n/a	ethhub	n/a	Switch to Hub Mode
eth	n	group	0-3,255	Ethernet Hub group
eth	n	metric	1-16	Metric
eth	n	mtu	64-1500	MTU
eth	n	auton	0,1	Enable auto-negotiation
eth	n	speed	0,10,100	Speed 0=Auto 10=10-BaseT 100=100-BaseT
eth	n	duplex	0,1,2	Duplex 0=Auto 1=Full 2=Half
eth	n	maxkbps	value in kbps	Max Rx rate
eth	n	maxtkbps	value in kbps	Max Tx rate
eth	n	tcptxbuf	value in bytes	TCP transmit buffer size
eth	n	linkdeact	0-86400	Take this interface out of service after n seconds when the link is lost
eth	n	do_nat	0,1,2	Enable NAT on this interface 0=Disabled 1=IP address 2=IP address and Port
eth	n	ipsec	0,1	Enable IPsec on this interface
eth	n	ipsecent	blank,ETH,PPP	Use interface x,y for the source IP address of IPsec packets x=Interface type
eth	n	ipsecadd	0-255	Use interface x,y for the source IP address of IPsec packets y=interface number
eth	n	firewall	0,1	Enable the firewall on this interface
eth	n	nocfg	0,1,2,3	Remote management access 0=No restrictions 1=Disable management 2=Disable return RST 3=Disable management and return RST

Entity	Instance	Parameter	Values	Equivalent Web Parameter
eth	n	mhome	0-255	Multihome additional consecutive addresses
eth	n	igmp	0,1	Enable IGMP on this interface
eth	n	bridge	0,1	Enable Bridge on this interface
eth	n	heartbeatip	IP address	Send Heartbeat messages to IP address a.b.c.d every h hrs m mins s seconds
eth	n	hrtbeatint	0-86400	Send Heartbeat messages to IP address a.b.c.d every h hrs m mins s seconds This CLI value is entered in seconds only.
eth	n	hbipent	blank,ETH,PPP	Use interface x,y for the source IP address x=Interface type
eth	n	hbipadd	0-255	Use interface x,y for the source IP address y=interface number
eth	n	hbroute	0,1	Select the transmit interface using the routing table
eth	n	hbimsi	0,1	Include IMSI information in the Heartbeat message

Ethernet QoS Parameters

The parameters on this page control the Quality of Service management facility. Each Ethernet interface has an associated QoS instance, where ETH 0 maps to QoS 5, ETH 1 maps to QoS 6 and so on. These QoS instances include ten QoS queues into which packets may be placed when using QoS. Each of these queues must be assigned a queue profile from the twelve available.

Enable QoS on this interface

This checkbox, when checked, reveals the following QoS configuration parameters:-

Link speed n Kbps

This setting should be set to the maximum data rate that this PPP link is capable of sustaining. This is used when calculating whether or not the data rate from a queue may exceed its minimum Kbps setting as determined by the profile assigned to it and send at a higher rate (up to the maximum Kbps setting).

Queue n

Below this column heading, is a list of ten queue instances. Each instance is associated with the profile and priority on the same row.

Profile n

This column contains the profile to be associated with the queue. There are twelve available, **0-11**, which are selected from the drop-down list boxes.

Priority

This column contains drop-down menu boxes which are used to assign a priority to the selected queue. The priorities available are **Very High**, **High**, **Medium**, **Low**, and **Very Low**.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
qos	n	linkkbps	Integer	Link speed n kbps
qos	n	q0prof	0-11	Queue 0 Profile
qos	n	q0prio	0-4 0=Very high 1=High 2=Medium 3=Low 4=Very Low	Queue 0 Priority
qos	n	q1prof	0-11	Queue 1 Profile
qos	n	q1prio	0-4	Queue 1 Priority
qos	n	q2prof	0-11	Queue 2 Profile
qos	n	q2prio	0-4	Queue 2 Priority
qos	n	q3prof	0-11	Queue 3 Profile
qos	n	q3prio	0-4	Queue 3 Priority
qos	n	q4prof	0-11	Queue 4 Profile
qos	n	q4prio	0-4	Queue 4 Priority
qos	n	q5prof	0-11	Queue 5 Profile
qos	n	q5prio	0-4	Queue 5 Priority
qos	n	q6prof	0-11	Queue 6 Profile
qos	n	q6prio	0-4	Queue 6 Priority
qos	n	q7prof	0-11	Queue 7 Profile
qos	n	q7prio	0-4	Queue 7 Priority
qos	n	q8prof	0-11	Queue 8 Profile
qos	n	q8prio	0-4	Queue 8 Priority
qos	n	q9prof	0-11	Queue 9 Profile
qos	n	q9prio	0-4	Queue 9 Priority

Ethernet VRRP Parameters

VRRP (Virtual Router Redundancy Protocol) allows multiple physical routers to appear as a single gateway for IP communications in order to provide back-up WAN communications in the event that the primary router in the group fails in some way. It works by allowing multiple routers to monitor data on the same IP address. One router is designated as the Master of the address and under normal circumstances it will route data as usual. However, the VRRP protocol allows the other routers in the VRRP group to monitor the Master and if, they detect that it is no longer operating, negotiate with each other to take over the role as owner. The protocol also facilitates the automatic re-prioritization of the original owner when it returns to operation.

Enable VRRP on this interface

Enables VRRP on this interface.

☑ Enable VRRP on this interface

VRRP Group ID: 0
VRRP Priority: 0
Send advertisements every 1 seconds when in MASTER mode
Switch to MASTER mode if no advertisements are received within 3 seconds
Delay VRRP startup by 0 seconds after the ethernet interface connects
Boost the priority by 0 for 0 seconds after switching to the MASTER state

VRRP Group ID

The VRRP group ID parameter identifies routers that are configured to operate within the same VRRP group. The default value is 0 which means that VRRP is disabled on this Ethernet interface. The value may be set to a number from **1** to **255** to enable VRRP and include this Ethernet port in the specified VRRP group.

VRRP Priority

The priority level of this Ethernet interface within the VRRP group from **0** to **255**. **255** is the highest priority and setting the priority to this value would designate this Ethernet interface as the initial Master within the group. The value selected for the VRRP priority should reflect the values selected for other routers within the VRRP group, such as no two routers in the group should be initialized with the same value.

Boost the priority by n for s seconds after switching to the MASTER state

Increases the VRRP priority by the specified amount for the specified amount of time when the router has become the VRRP group master. The reason for why you might want to do this is to provide some network stability if the original Master keeps going on and off line thus causing a lot of VRRP state switches.

Enable VRRP+ Probing

Enables VRRP+ probing on this Ethernet interface. VRRP with probing differs from standard VRRP in that it dynamically adjusts the VRRP priority of an interface and if necessary, changes the status of that interface from master to backup or vice-versa. It does this by probing an interface, either by sending an ICMP echo request (PING) or by attempting to open a TCP socket to the specified Probe IP address. Hence VRRP operation is enhanced to ensure that a secondary router can take over under a wider range of circumstances.

Send p probe to IP address a.b.c.d TCP port n

Configures VRRP+ to send a probe packet to desired IP address and TCP port. The TCP port is needed if the probe type is TCP. The routing code determines which interface should be used. This allows the router to test other interfaces and adjust the VRRP priority according to the status of that interface. For example, the user may wish to configure probing in such a way that the Digi router WAN interface is tested, and adjust the VRRP priority down if the WAN is not operational. Another example would be to probe the WAN interface of another VRRP router, and adjust the local VRRP priority up if that WAN interface is not operational. When configured to probe in this manner, it is necessary to configure a second Ethernet interface to be on the same subnet as the VRRP interface. This is because the VRRP interface cannot be used when it is in backup mode. The probes should be sent on this second interface. The second interface will have the other VRRP router as its gateway. The routing table should be configured to direct packets for the probe address to the desired interface.

every n seconds when in Backup state

The interval between successive probe attempts when the interface is in Backup state.

every n seconds when in Master state

The interval between successive probe attempts when the interface is in Master state.

Adjust priority n dir after x probe failures

Controls by how much and in which direction the VRRP priority is adjusted when the specified number of probes have failed.

Reset probe failure count after n probe successes

The number of consecutive successful probes that are required before the current failure count is reset to **0**.

Use interface x,y over which to send probe

Overrides the routing code and forces the probe packets to be sent out of a specific interface.

Get the source IP address from interface x,y

Enables probe packets having the source IP address from a specific interface, rather than the interface over which it is being transmitted.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
eth	n	vrrpid	0-255	VRRP Group ID
eth	n	vrrpprio	0-255	VRRP Priority
eth	n	vboostprio	0-255	Boost the priority by n for s seconds after switching to the MASTER state
eth	n	vboostsecs	Integer	Boost the priority by n for s seconds after switching to the MASTER state
eth	n	vprobemode	off, TCP, ICMP	Send p probe to IP address a.b.c.d TCP port n
eth	n	vprobeip	IP Address	Send p probe to IP address a.b.c.d TCP port n
eth	n	vprobeport	0-65535	Send p probe to IP address a.b.c.d TCP port n
eth	n	vprobebackint	0-32767	every n seconds when in Backup state
eth	n	vprobemastint	0-32767	every n seconds when in Master state
eth	n	vprobeadj	0-255	Adjust priority n dir after x probe failures
eth	n	vprobeadjup	0=down 1=up	Adjust priority n dir after x probe failures
eth	n	vprobefailcnt	0-255	Adjust priority n dir after x probe failures
eth	n	vprobesuccesscnt	0-255	Reset probe failure count after n probe successes
eth	n	vprobeent	Auto, ETH, PPP	Use interface x,y over which to send probe
eth	n	vprobeadd	Integer	Use interface x,y over which to send probe
eth	n	vprobeipent	Auto, ETH, PPP	Get the source IP address from interface x,y
eth	n	vprobeipadd	Integer	Get the source IP address from interface x,y

Logical Ethernet Interfaces

The logical Ethernet interfaces are virtual Ethernet interfaces. You can configure them as per the standard Ethernet interfaces except for the Speed and Duplex settings which require a physical interface.

Logical Ethernet interfaces assigns extra IP addresses to the router on the same or an alternate subnet using the same physical Ethernet connection.

Logical Ethernet interfaces is also used as bridging features (such as used in a Wi-Fi configuration) where it is desirable to not use a physical interface for the bridging.

MAC Filtering

Ethernet MAC filtering restricts which Ethernet devices can send packets to the router. If MAC filtering is enabled on an Ethernet interface, only Ethernet packets with a source MAC address that is configured in the MAC Filter table will be allowed. If the source MAC address is not in the MAC Filter table, the packet will dropped.

Enable MAC filtering on Ethernet interfaces

Enables MAC filtering on a specific Ethernet interface.

Enable MAC filtering on Ethernet interfaces	
Interface	**Enable**
ETH 0	☐
ETH 1	☐
ETH 2	☐
ETH 3	☐
ETH 4	☐
ETH 5	☐
ETH 6	☐
ETH 7	☐
ETH 8	☐
ETH 9	☐

MAC Address

The Ethernet source MAC address to allow. It is possible to allow a range of MAC addresses by configuring only the significant part of the MAC address. such as **00:04:2d** will allow all Ethernet packets with a source MAC address starting with **00:04:2d.**

MAC Address
No MAC addresses have been added
[   ]   Add

Apply

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
eth	n	macfilt	on, off	Enable MAC filtering on Ethernet interfaces
macfilt	n	mac	MAC address with no separators. Partial MAC address are allowed.	MAC Address

MAC Bridging

The Ethernet MAC bridge function creates an Ethernet bridge between two physically separate Ethernet networks. It is possible to allow bridging over DSL, W-Wan, ISDN and PSTN connections but note that the only restriction on the traffic sent across the link is done via MAC address filtering and that all Ethernet traffic will be bridged, no firewall restrictions are applied to this traffic.

Once the bridge has been configured, the MAC addresses to bridge need to be configured in the MAC bridge table.

Enable

Enables MAC bridging on the Ethernet interface.

Enable MAC bridging on Ethernet interfaces

Interface	Enable	Forward to IP Address	Port	Listen on Port
ETH 0	☐		0	0
ETH 1	☐		0	0
ETH 2	☐		0	0
ETH 3	☐		0	0
ETH 4	☐		0	0
ETH 5	☐		0	0
ETH 6	☐		0	0
ETH 7	☐		0	0
ETH 8	☐		0	0
ETH 9	☐		0	0

Forward to IP address

The IP address of the remote router to which the Ethernet packets will be bridged to.

Port

The TCP port that the remote router is listening on.

Listen on Port

The TCP port that the router will listen on for incoming bridged packet from the remote router.

MAC Address

The Ethernet destination MAC address of packets to be bridged. It is possible to allow a range of MAC addresses by configuring only the significant part of the MAC address. such as **00042d** will allow all Ethernet packets with a source MAC address starting with **00:04:2d**.

Mac Address
No MAC addresses have been added

[   ] [Add]

[Apply]

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
eth	n	srcbhost	IP Address	Forward to IP address
eth	n	srchport	0-65535	Port
eth	n	srcblistenport	0-65535	Listen on Port
bridgemac	n	mac	MAC address with no separators. Partial MAC address are allowed.	MAC Address

Spanning Tree Protocols

The Rapid Spanning Tree Protocol (RSTP) is a layer 2 protocol which ensures a loop free topology on a switched or bridged LAN whilst allowing redundant physical links between switches. When enabled, the TransPort device uses RSTP but this is backwards compatible with STP.

RSTP will not be enabled if the router is in **Port Isolate** mode. If an Ethernet interface is configured with a hub group, RSTP will be disabled on that interface.

Enable RSTP

Enables RSTP on the router.

Priority

The RSTP priority.

Group

The RSTP group that the router is in.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
stp	0	enable	on, off	Enable RSTP
stp	0	prio	0-65535	Priority
stp	0	group	-	Group
stp	0	debug	0, 1	Not available on the web interface.

Port status

To view the status of RSTP/STP on a router's Ethernet ports, the following commands can be used.

```
stp show
Port 0, Designated, Forwarding ctrl2:0x6
Port 1, Backup, Discarding ctrl2:0x1
Port 2, Backup, Discarding ctrl2:0x1
Port 3, Disabled, Discarding ctrl2:0x1
```

The port roles are:

Role	Description
Disabled	There is nothing physically connected to this Ethernet port.
Root	A forwarding port that has been elected for the spanning-tree topology, towards the root bridge.
Designated	A forwarding port for every LAN segment, away from the root bridge.
Alternate	An alternate path to the root bridge. This path is different than using the root port.
Backup	A backup/redundant path to a segment where another bridge port already connects.

The STP port states are:

State	Description
Disabled	The port is not functioning and cannot send or receive data.
Listening	The port is sending and receiving BPDUs and participates in the election process of the root bridge. Ethernet frames are discarded.
Learning	The port does not yet forward frames but it does learn source addresses from frames received and adds them to the MAC address table.
Forwarding	The port receiving and sending data, normal operation. STP still monitors incoming BPDUs that would indicate it should return to the blocking state to prevent a loop.
Locking	A port that would cause a switching loop, no user data is sent or received but it may go into forwarding mode if the other links in use were to fail and the spanning tree algorithm determines the port may transition to the forwarding state. BPDU data is still received in blocking state.

The RSTP port states are:

Role	Description
Learning	The port does not yet forward frames but it does learn source addresses from frames received and adds them to the MAC address table. The port processes BPDUs.
Forwarding	The port receiving and sending data, normal operation. STP still monitors incoming BPDUs that would indicate it should return to the blocking state to prevent a loop.
Discarding	A port that would cause a switching loop, no user data is sent or received but it may go into forwarding mode if the other links in use were to fail and the spanning tree algorithm determines the port may transition to the forwarding state. BPDU data is still received in blocking state.

Ethernet VLANs parameters

VLANs (Virtual LANs) facilitate splitting a single physical LAN into separate Virtual LANs. This is useful for security reasons, and also helps cut down on broadcast traffic on the LAN.

Enable VLAN support on Ethernet interfaces

This parameter enables VLAN support on the Ethernet interface.

Enable VLAN support on Ethernet interfaces	
Interface	Enable
ETH 0	☐
ETH 1	☐
ETH 2	☐
ETH 3	☐
ETH 4	☐
ETH 5	☐
ETH 6	☐
ETH 7	☐
ETH 8	☐
ETH 9	☐

VLAN ID

This parameter specifies the ID of the Virtual LAN. VLAN ID is used in the TCP header to identify the destination VLAN for the packet.

VLAN ID	Ethernet Interface	IP Address	Mask	Source IP Address	Source mask	
No VLAN configurations have been added						
	0 ⌄					Add

Reserve VLAN ID 0 for system usage

[Apply]

Ethernet Interface

The Ethernet port that tags the outgoing packets. Packets sent from this interface have VLAN tagging applied.

IP Address

The destination IP address. This parameter is optional. If configured, only packets destined for this IP address will have VLAN tagging applied.

Mask

The destination IP subnet mask. This parameter is optional. If configured, only packets destined for this IP subnet mask will have VLAN tagging applied.

Source IP Address

The source IP address. This parameter is optional. If configured, only packets from this IP address will have VLAN tagging applied.

Source Mask

The source IP subnet mask. This parameter is optional. If configured, only packets from this IP subnet mask will have VLAN tagging applied.

Ethernet VLANs CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
eth	n	vlan	on, off	Enable VLAN support on Ethernet interfaces
vlan	n	vlanid	0-4095	VLAN ID
vlan	n	ethctx	Integer	Ethernet Interface
vlan	n	ipaddr	IP Address	IP Address
vlan	n	mask	IP Mask	Mask
vlan	n	srcipaddr	IP Address	Source IP Address
vlan	n	srcmask	IP Mask	Source Mask

Configure Wi-Fi interfaces

The **Configuration > Network > Interfaces > Wi-Fi** section of the web interface that contains the configuration options required in order to configure and enable the Wi-Fi features.

Global Wi-Fi settings

Because of national restrictions on the channels available for use, the correct country should be selected from the drop down list to restrict the channels that are legal to use by the router. If required, a specific channel can be selected to over-ride the auto selection.

Country

Selecting a country from the drop down list restricts the channels that the router will use. See table for more info on licensed channels.

Network Mode

Select your chosen mode of operation from the drop down list. The options are:

- A

- B / G

This parameter is not available on all routers.

Channel

Selecting **Auto** allows the router to scan for a free channel within the range of legal channels for the selected country. It is possible to manually select a specific channel to use but care should be taken to ensure the selected channel is legal to use in the country.

Global Wi-Fi Settings CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
wifi	0	country	Country name	Country
wifi	0	chanmode	a / bg	Network Mode
wifi	0	channel	auto, 1-14	Channel

Below is a list of the countries that are currently supported:

Albania	Guatemala	Oman
Algeria	Honduras	Pakistan
Argentina	Hong Kong	Panama
Armenia	Hungary	Paraguay
Australia	Iceland	Peru
Austria	India	Philippines
Azerbaijan	Indonesia	Poland
Bahrain	Iran	Portugal
Belarus	Iraq	Puerto Rico
Belgium	Ireland	Qatar
Belize	Israel	Romania
Bolivia	Italy	Russia
Brazil	Jamaica	Saudi Arabia
Brunei	Japan	Singapore
Bulgaria	Jordan	Slovak Republic
Canada	Kazakhstan	Slovenia
Chile	Kenya	South Africa
China	North Korea	Spain
Colombia	South Korea	Sweden
Costa Rica	Kuwait	Switzerland
Croatia	Latvia	Syria
Cyprus	Lebanon	Taiwan
Czech Republic	Libya	Thailand
Denmark	Liechtenstein	Trinidad and Tobago
Dominican Republic	Lithuania	Tunisia
Ecuador	Luxembourg	Turkey
Egypt	Macau	U.A.E.
El Salvador	Macedonia	Ukraine
Estonia	Malaysia	United Kingdom
Faroe Islands	Mexico	United States
Finland	Monaco	Uruguay
France	Morocco	Uzbekistan
Georgia	Netherlands	Venezuela
Germany	New Zealand	Vietnam
Greece	Nicaragua	Yemen
	Norway	Zimbabwe

The following table lists the licensed channels that is used by the router when **Auto** is selected for the channel number:

Region	Channels
EMEA (excluding France)	1-13
France	10-13
Americas (excluding Mexico)	1-11
Mexico	1-8 Indoor, 9-11 outdoor
Israel	3-9
China	1-11
Japan	1-14

Note It is **illegal** to use restricted channels in certain countries.

Wi-Fi Hotspot

This section enables the configuration of the global parameters that are applicable if using any Wi-Fi node as a hotspot.

Enable Wi-Fi Hotspot on

Click the checkbox to enable Wi-Fi Hotspot support on a particular Wi-Fi node.

Splashscreen filename

Selects an ASP web file that will be presented to the client's internet browser when they connect for the first time.

Each client can connect for h hrs m mins

The amount of time that a Wi-Fi client can use the Wi-Fi hotspot before having to re-authenticate.

Hotspot Exceptions

It is possible to configure a number of web locations for which authentication is not required. These settings allow the splashscreen to access these locations in order to display them to the client when authenticating.

Wi-Fi Hotspot CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
wifinode	n	hotspot	on, off	Enable Wi-Fi Hotspot on
wifi	0	hotspot_fname	Filename	Splashscreen filename
wifi	0	hotspot_lifetime	Integer	Each client can connect for h hrs m mins.The CLI value is entered in seconds only.
hshosts	n	host	Hostname	Hotspot Exceptions

Wi-Fi Filtering

You can restrict access to the router via Wi-Fi. When the filtering is enabled, only MAC addresses configured in the table will be allowed to connect to the router.

Enable Wi-Fi filtering

Enable Wi-Fi filtering so that only clients who have their Wi-Fi MAC address configured in the MAC address table will be allowed to connect.

MAC Address

MAC addresses of Wi-Fi client that you wish to allow access to.

A valid MAC address has the format: **11:22:33:44:55:66**. When entering this parameter, omit the **:** separators. For example, **112233445566**.

Note Carefully review settings before applying changes. Incorrect settings can make the TransPort device inaccessible from the Wi-Fi network.

Wi-Fi Filtering CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
wifi	0	macfilter	on/off	Enable Wi-Fi filtering
wififilt	n	mac	MAC address with no separators, such as **112233445566**	MAC Address

Wi-Fi n parameters

When a Wi-Fi interface is configured to be an Access Point, an SSID must be configured for a Wi-Fi interface to operate.

In order to forward packets to and from a Wi-Fi interface, it must be bridged to a configured Ethernet interface. The Wi-Fi interface and Ethernet interface must be in the same Bridge instance.

If a DHCP server is required to run on the Wi-Fi interface, the DHCP server instance corresponding bridged Ethernet interface should be configured.

In some cases it may be necessary to bridge multiple Ethernet instances to a single Wi-Fi instance. If this is required, only one Ethernet instances is should be configured.

Enable this Wi-Fi interface

The Wi-Fi interface can be enabled or disabled.

Description

A descriptive name for the Wi-Fi interface to make it easier to identify.

SSID

When the Wi-Fi interface is configured to be an Access Point, this is the SSID that is advertised to the Wi-Fi clients to.

When the Wi-Fi interface is configured to be a Client, this is the SSID of the Access Point you wish to connect to.

Mode

The Wi-Fi interface can run in various modes. The options are:

- **Access Point**
- **Client**

Rogue Detection(Scan for unauthorised Access Points)

This Wi-Fi interface is a member of Bridge instance **n** and therefore bridged to the following interfaces.

When the Wi-Fi interface is configured to be an Access Point, in order to forward packets to and from the Wi-Fi interface it must be bridged with an Ethernet interface using a Bridge instance.

Interface

Interfaces that are currently members of the selected Bridge instance. Note that multiple Wi-Fi interfaces can be members of the same Bridge instance.

Link this Wi-Fi client interface with Ethernet n

When the Wi-Fi interface is configured to be a client, it must be bridged to a particular Ethernet interface.

This Wi-Fi rogue scanner will use Ethernet n

When the Wi-Fi interface is configured to be a rogue scanner, it uses the selected Ethernet interface.

Hide SSID

When enabled, the SSID is not included in the beacon messages transmitted by the Wi-Fi interface when in Access Point mode. This means that Wi-Fi clients will not be able to auto-detect the Access Point.

Isolation

When enabled, connected Wi-Fi clients is unable to communicate with other Wi-Fi clients or Ethernet hosts connected to this AP.

Wi-Fi CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
wifinode	0	enabled	on, off	Enable this Wi-Fi interface
wifinode	0	descr	String	Description
wifinode	0	ssid	String up to 32 characters	SSID
wifinode	0	mode	ap, client, rogue	Mode
wifinode	o	bridge_inst	0-3	This Wi-Fi interface is a member of Bridge instance n and therefore bridged to the following interfaces
eth	n	bridge_inst	0-3	Interface
eth	n	wificli	on, off	Link this Wi-Fi client interface with Ethernet n
eth	n	wificli_add	Integer	Link this Wi-Fi client interface with Ethernet n
wifinode	0	broadcastssid	on, off	Hide SSID
wifinode	0	isolation	on, off	Enable station isolation

Wi-Fi Security

This section is used to configure the security settings for the Wi-Fi interface.

If you are using multiple Wi-Fi interfaces at the same time, the interfaces need to use the same security settings (except for the pre-shared key (PSK)). The only alternative is that the Wi-Fi is used with no security.

Use the following security on this Wi-Fi interface

This parameter selects the security that is used on this Wi-Fi interface. The options are:

- **None**
- **WEP**
- **WPA-PSK**, also known as WPA Personal
- **WPA2-PSK**, also known as WPA2 Personal
- **WPA-RADIUS**, also known as WPA Enterprise
- **WPA2-RADIUS**, also known as WPA2 Enterprise

WEP Settings

The various WEP security settings for both Access Point and Client modes.

WEP Key size

The WEP key size to use.

WEP Key index

The WEP key index number. This needs to match the index selected on the connecting Wi-Fi clients or Access Points that this router wishes to connect to.

WEP Key / Confirm WEP Key

If the WEP key size is 64 bits, the key should be 5 characters long. If the WEP key size is 128 bits, the key should be 13 characters long.

WPA-PSK / WPA2-PSK

The various WPA-PSK / WPA2-PSK security settings for both Access Point and Client modes.

WPA Encryption

This parameter specifies the encryption algorithm to use. The options are:

- **TKIP**
- **AES (CCMP)**

WPA pre-shared key / Confirm WPA pre-shared key

The pre-shared key (PSK) to use. It must be between 8 and 63 characters long.

WPA-RADIUS / WPA2-RADIUS

The various WPA-RADIUS / WPA2- RADIUS security settings for both Access Point and Client modes.

The encryption algorithm to use. The options are:

- **TKIP**
- **AES (CCMP)**

The NAS ID of the RADIUS server.

The IP address of the RADIUS server

The password of the RADIUS server.

Wi-Fi Security CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
wifinode	0	security	none wep wpapsk wpa2psk wparadius wpa2radius	Use the following security on this Wi-Fi interface
wifinode	0	weptype	open, sharedkey	Not available on the WEB.
wifinode	0	wepkeylen	64, 128	WEP Key size
wifinode	0	wepkeyindex	1-4	WEP Key index
wifinode	0	wpatype	tkip, aes	WPA Encryption
wifinode	0	sharedkey	text	WEP Key/WPA pre-shared key
radcli	n*	nasid	String	RADIUS NAS ID
radcli	n*	server	IP Address	RADIUS Server IP Address
radcli	n*	password	String	RADIUS Server Password

* The Wi-Fi interfaces each use a fixed RADIUS client, such as,

- Wi-Fi 0 uses radcli 1
- Wi-Fi 1 uses radcli 2
- Wi-Fi 2 uses radcli 3 and so on.

The following table details the authentication and encryption algorithms and the CLI commands needed to configure them.

Network Authentication	Data Encryption	CLI Commands
Open	Disabled	wifinode 0 security none
Shared	Disabled	Not supported
Open	WEP	wifinode 0 security wep wifinode 0 weptype open wifinode 0 wepkeylen <64 | 128> wifinode 0 wepkeyindex <1..4> wifinode 0 sharedkey <5 or 13 char key>
Shared	WEP	wifinode 0 security wep wifinode 0 weptype sharedkey wifinode 0 wepkeylen <64 | 128> wifinode 0 wepkeyindex <1..4> wifinode 0 sharedkey <5 or 13 char key>
WPA	TKIP	wifinode 0 security wparadius wifinode 0 wpatype tkip wifinode 0 radiuscfg 1
WPA2	TKIP	wifinode 0 security wpa2radius wifinode 0 wpatype tkip wifinode 0 radiuscfg 1
WPA-PSK	TKIP	wifinode 0 security wpapsk wifinode 0 wpatype tkip wifinode 0 sharedkey <8..63 char key>
WPA2-PSK	TKIP	wifinode 0 security wpa2psk wifinode 0 wpatype tkip wifinode 0 sharedkey <8..63 char key>
WPA	AES	wifinode 0 security wparadius wifinode 0 wpatype aes wifinode 0 radiuscfg 1
WPA2	AES	wifinode 0 security wpa2radius wifinode 0 wpatype aes wifinode 0 radiuscfg 1

Network Authentication	Data Encryption	CLI Commands
WPA-PSK	AES	wifinode 0 security wpapsk wifinode 0 wpatype aes wifinode 0 sharedkey <8..63 char key>
WPA2-PSK	AES	wifinode 0 security wpa2psk wifinode 0 wpatype aes wifinode 0 sharedkey <8..63 char key>

Rogue Scan parameters

In Rogue Scan mode, the router performs a scan of the Wi-Fi channels and will report what Wi-Fi Access Points it detects. This feature can be used to detect unauthorised Access Points that might be trying to get unsuspecting Wi-Fi clients to connect them.

When an authorized Access Point is detected, an event log entry is created and an alarm (such as email, SMS, SNMP Trap) can be triggered.

It is possible to configure a list of the MAC addresses of the authorized Access Points that will not be reported when detected.

MAC Address

  The MAC address of an authorized Access Point.

Rogue Scan CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
macrogue	n	mac	MAC address with no separators such as 112233445566	MAC Address

Configure mobile interfaces

Wireless WAN functionality is only available on models that are fitted with a wireless WAN module, such as CDMA, GPRS, 3G, HSPA etc. This module is connected to one of the ASY ports (and USB controller on some models) and is controlled by the router using **AT** commands (in the same way as a modem). Any further references to W-WAN technologies such as CDMA, GPRS, 3G etc. will be referred to as GPRS, GSM, 3G or simply 'wireless' networks.

W-WAN modules provide always-on wireless data connectively over the GSM network at speeds of up to 7.2Mbps. This means that the router can be used in situations where no ISDN or xDSL service connection is available. In addition, wireless can be used to send or receive SMS alert messages (as an alternative to emails for issuing remote alert messages or for automating remote configuration of deployed routers).

Before attempting to connect to a wireless service, you need to set several parameters specific to your mobile network operator. It will be useful to have the following information to hand:

- The assigned APN (Access Point Name)
- PIN Number for your SIM card (if any)
- Username and password

Once the W-WAN router is correctly configured, check to see if it has obtained an IP address from the network by navigating to the Diagnostics-Status > PPP > PPP x page (where x is either 1 or 3 depending on the model) and checking the IP address parameter. (It should contain an IP address other than 0.0.0.0 or 1.2.3.4).

Additionally, check that the SIM is working correctly and also check the signal strength by navigating to the **Status > Mobile** page.
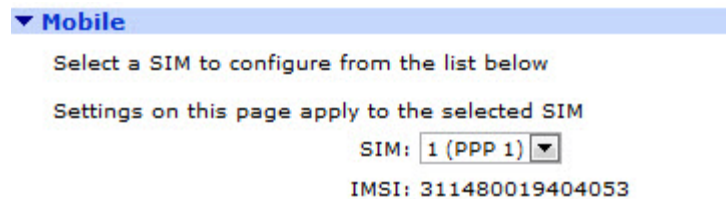
SIM

Select a SIM to configure. **SIM 1** specifies the SIM card fitted to the slot marked **SIM 1** in the router's SIM card slots. **SIM 2** specifies the SIM card fitted to the slot marked **SIM 2**.

Note When using a single SIM card, the default action is for the router to use **PPP 1** as the mobile interface. To configure dual SIMs for fail-over, go to **Configuration > Network > Interfaces > Mobile > SIM Selection** to launch the Dual SIM wizard.

Mobile Settings parameters

Select the service plan and connection settings used in connecting to the mobile network.

The **Configuration > Network > Interfaces > Mobile > Mobile Settings** menu options is divided in three sections.

Mobile Service Provider Settings

Here, you can set the following values:

Service Plan / APN

Enter the APN (Access Point Name) given by the service provider.

Use backup APN

Check this box to enable the backup APN option, then enter the backup APN in the text field.

APN

An alternative service APN for use in the event that the router cannot connect using the primary APN specified by the APN parameter. The router will only use this APN if the primary APN fails and the **Use backup APN** parameter is enabled.

Retry the main APN after n minutes

If the **Use backup APN** parameter is enabled, this parameter defines how long the router will use the backup APN before attempting to revert to the primary APN.

SIM PIN

Some SIM cards are locked with a Personal Identification Number (PIN) code to prevent misuse if they are lost or stolen. The GSM operator should be able to confirm if the SIM requires a PIN code. If you enter a PIN code in this field, the router will try to unlock the SIM before attempting to connect to the network.

Confirm SIM PIN

Enter the PIN again in this field to confirm it.

Username (Optional)

Some APNs require a username and password for the PPP connection. These are not always pre-defined such as any made-up username or password will suffice.

Password (Optional)

Enter the password for the PPP connection.

Confirm Password

Enter the password again in this field to confirm it.

Mobile service provider settings CLI commands SIM 1 (PPP 1)

Entity	Instance	Parameter	Values	Equivalent Web Parameter
modemcc	0	apn	Free text field	Service Plan / APN:
modemcc	0	usebuapn	on/off	Checkbox (Use Backup APN)
modemcc	0	buapn	Free text field	Use backup APN
modemcc	0	pin	SIM PIN number	SIM PIN:/Confirm SIM PIN
ppp	1	username	Free text field	Username:
ppp	1	password	Free text field	Password:/Confirm Password

Mobile service provider settings CLI commands SIM 2 (PPP 1)

Entity	Instance	Parameter	Values	Equivalent Web Parameter
modemcc	0	Apn_2	Free text field	Service Plan / APN:
modemcc	0	Usebuapn_2	on/off	Checkbox (Use Backup APN)
modemcc	0	Buapn_2	Free text field	Use backup APN
modemcc	0	Pin_2	SIM PIN number	SIM PIN:/Confirm SIM PIN
ppp	1	username	Free text field	Username:
ppp	1	password	Free text field	Password:/Confirm Password

Mobile Connection Settings

Re-establish connection when no data is received for a period of time.

This checkbox opens to show the following parameters:-

Inactivity Timeout: h hrs m mins s seconds

The amount of time the router will wait without receiving any PPP packets before disconnecting. An inactivity timeout reset with each received PPP packet.

Mobile Connection Settings CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	rxtimeout	OFF, ON	Re-establish connection when no data is received for a period of time.
ppp	1	rxtimeout	0-86400 (seconds)	Inactivity Timeout: h hrs m mins s seconds

Mobile Network Settings

Mobile Network Settings

☑ Enable NAT on this interface
    ◉ IP address   ○ IP address and Port

☑ Enable IPsec on this interface

    ☐ Keep Security Associations (SAs) when this Mobile interface is disconnected
Use interface | Default ▼ | 0   for the source IP address of IPsec packets

☐ Enable the firewall on this interface

Enable NAT on this interface

Enables or disables IP Network Address Translation (NAT) on the mobile interface.

This checkbox opens to show the following options:-

IP Address

Enables standard Network Address Translation (NAT).

IP address and Port

Enables Network Address and Port Translation (NAPT).

Enable IPsec on this interface

Enables or disables IPSec processing on the mobile interface. If enabled, packets sent or received on this interface must pass through the IPSec code before being transmitted. IPSec may drop the packet, pass it unchanged, or encrypt and encapsulate within an IPSec packet.

This checkbox opens to show the following parameters:-

Keep Security Associations (SAs) when this Mobile interface is disconnected

Configures the router to keep any existing IKE and IPsec associations should the link drop. This is usually applied on head-end routers with fixed IP addresses.

Use interface X, Y for the source IP address of IPsec packets

By default, the source IP address for an IPSec Eroute will be the IP address of the interface on which IPSec was enabled. By setting this parameter to either a PPP or Ethernet interface, the source IP address used by IPSec will match that of the Ethernet or PPP interface specified.

Enable the firewall on this interface

Enables or disables the Firewall script processing for the mobile interface.

Note   If the firewall is enabled on an interface and with the absence of any firewall rules, the default action is to block ALL traffic.

Mobile Network Settings CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	1	do_nat	1	Enable NAT on this interface IP Address
ppp	1	do_nat	2	Enable NAT on this interface IP Address and Port
ppp	1	ipsec	1	Enable IPsec on this interface
ppp	1	ipsec	2	Keep Security Associations (SAs) when this Mobile interface is disconnected
ppp	1	ipsecent	blank,ETH,PPP	Use interface X, Y for the source IP address of IPsec packets x=Interface type
ppp	1	ipsecadd	0-255	Use interface X, Y for the source IP address of IPsec packets y=interface number
ppp	1	firewall	OFF, ON	Enable the firewall on this interface

SIM Selection

This section allows you to launch the Dual SIM wizard for failing over from 1 SIM to another.

Click here to launch the Dual SIM wizard

Launches the Dual SIM wizard.

CDMA provisioning

CDMA provisioning is different from GSM since CDMA (in most cases) does not use a SIM card. The CDMA module provisioning process creates a CDMA data connection to the mobile carrier network. This authenticates the modem and retrieves account information which is written to flash memory on the CDMA module itself, not the router's configuration file. Mobile account information is stored on the CDMA module. Therefore, you cannot remove provisioning information from the CDMA module by performing a factory reset on your TransPort router.

If provisioning fails (the device does not obtain a phone number), contact the carrier and verify that the device has an active account. You will need to provide the MEID of the device which is available under **Management > Network Status > Interfaces > Mobile**. See *Quick Note 25, CDMA Provisioning on a Digi TransPort Router* for example configuration.

Provider

If the router was not supplied pre-provisioned, obtain the following details from the Service Provider:

- A 15-digit IMSI (International Mobile Subscriber Identity)
- An NAI (Network Access Identifier)
- An NAI password

Once these details have been obtained, it is possible to provision the CDMA module by inserting those details into the Automatic Provisioning section of this web page and clicking on the Start button.

Automatic provisioning

Sprint Vision uses Automatic provisioning (semi-automatic). In most cases, the TransPort router can be provisioned without entering any information into the configuration page. If for some reason the TransPort router is an older version using a module that does not support OMA DM, three fields of information must be entered into the Automatic configuration page. This information is provided by Sprint.

If required, enter the MSL/PTN/MSID parameters before clicking Start

MSL

The master subsidy lock (MSL) code. Get this code from the mobile operator.

PTN

The personal telephone number. Get this number from the mobile operator.

MSID

The mobile station identifier. Get this identifier from the mobile operator.

Automatic Provisioning CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
provision	0	string1	No data input required	MSL
provision	0	String2	No data input required	PTN
provision	0	String3	No data input required	MSID

Manual provisioning

Manual provisioning should only be attempted by experienced technical personnel who have obtained all the required information from the mobile operator. Technical personnel with previous provisioning experience should not require these parameters explaining.

MSL

The master subsidy lock (MSL) code. Get this code from the mobile operator.

MDN

The personal telephone number. Get this number from the mobile operator.

MIN/MSID

The mobile station identifier. Get this identifier from the mobile operator.

Manual provisioning CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
provision	0	String4	Free text field	MSL
provision	0	String5	Free text field	PTN
provision	0	String6	Free text field	MIN/MSID

Mobile IP settings

Mobile IP profile number

The Mobile IP profile number.

Network Access ID (NAI)

The Network Access ID.

MIP Home Address

The MIP Home Address.

Primary Home Agent

The Primary Home Agent.

Secondary Home Agent

The Secondary Home Agent.

HA shared secret: 0xn (Hex strings must start 0x)

The HA shared secret.

AAA shared secret: 0xn (Hex strings must start 0x)

The AAA shared secret.

HA SPI

The HA SPI.

AAA SPI

The AAA SPI.

Enable Reverse tunneling

Enables reverse tunneling, if required.

Mobile IP Settings CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
provision	0	String7	1	Mobile IP profile number:
provision	0	String8	Free text field	Network Access ID (NAI):
provision	0	String9	Free text field	MIP Home Address:
provision	0	String10	Free text field	Primary Home Agent:
provision	0	String11	Free text field	Secondary Home Agent:
provision	0	String12	Hex string	HA shared secret:0xn (Hex strings must start 0x)
provision	0	String13	Hex string	AAA shared secret: 0xn (Hex strings must start 0x)
provision	0	String14	Free text field	HA SPI:
provision	0	String15	Free text field	AAA SPI:
provision	0	String16	Free text field	Enable Reverse tunneling:

PRL update

The Preferred Roaming List is a list of bands and channels in order of preference which the CDMA module uses when it attempts to locate and connect to a cell system. If the router is having problems with CDMA reception, it would be beneficial to update the PRL information.

MSL

The master subsidy lock (MSL) code. Get this code this from the mobile operator.

PRL filename:

The name of preferred roaming list file. Get this file name from the mobile operator.

Note Except for older Sierra Wireless modules, PRL update on both the Verizon and Sprint networks is carried out over the air (OTA). Manual PRL update using a PRL file is not available. To initiate automatic over the air PRL update, click the Start button. Please note that PRL update is normally carried out as part of automatic provisioning on both Sprint and Verizon.

PRL update CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
provision	0	string1	Free text field	MSL
provision	0	string20	Free text field	PRL Filename

Advanced Mobile parameters

SIM PUK:

(Optional) If known, the SIM PUK code can be entered in these fields. If the router detects that a PUK is required due to a locked SIM, this number will be sent to the SIM. A SIM PIN must also be configured for the PUK parameter to take effect.

Confirm SIM PUK:

Enter the PUK code again in this field to confirm it.

Initialisation string <n>:

These parameters (**Initialisation string 1**, **Initialisation string 2**, **Initialisation string 3**) specify a number of command strings that are sent to the wireless module each time a wireless connection is attempted. These can be used to set non-standard wireless operating modes.

Each string is prefixed with the characters **AT** before being sent to the wireless module and they are sent to the wireless module in the order specified until an empty string is encountered. For example, Initialisation string 3 will not be sent unless Initialisation string 1 and Initialisation string 2 are both specified. Initialisation strings are not normally required for most applications as the router will normally be pre-configured for correct operation with most networks.

Hang-up string:

In a typical wireless application, the connection to the network is always on and under normal circumstances it is not necessary to hang-up the wireless module. Under certain circumstances however, the router may use the ATH command to try and disconnect the wireless module from the network, such as if an incorrect APN has been specified and the module is unable to attach to the network correctly.

This parameter specifies an alternative hang-up string that is sent to the wireless module when disconnecting a call. As with the Initialisation strings, it is not necessary to include the **AT** as this is inserted automatically by the router

Post Hang-up string:

Additional **AT** commands that are sent to the wireless module after it has been disconnected. As with the Initialisation strings, it is not necessary to include the **AT** as this is inserted automatically by the router.

Wait n seconds between hanging up and allowing another call

The length of time, in seconds, that the router will wait after hanging-up the wireless module before initiating another call attempt.

Wait n seconds between attachment attempts

The number of seconds between network attachment attempts, some networks require 60 seconds between attempts to attach to the wireless network.

Reset the module after n unsuccessful connection attempts

The router will normally make multiple attempts to connect to the wireless network in the event that the signal is lost. In some cases, this can result in a lock-up situation where the wireless network is unable to attach the wireless device due to the multiple attempts. This parameter specifies the number of attempts at connection that the router should make before power cycling the internal wireless module. Power cycling the wireless module forces it to re-register and reattach to the network. The default setting of 10 is the recommended value. Setting this parameter to 0 will prevent the router from power cycling the wireless module if it cannot obtain an IP address.

Reset the module after n unsuccessful status retrieval attempts

The router periodically collects status information from the internal wireless module. This information, which may be viewed on the **Management > Network Status > Interfaces > Mobile** web page, includes details of the signal strength and network attachment status. As a safeguard against problems communicating with the wireless module, the Status retries parameter may be used to specify the number of unsuccessful attempts to retrieve status information from the wireless module before power cycling it. The default setting of 30 is the recommended value. Setting this parameter to 0 will prevent the router from power cycling the wireless module if it cannot read the wireless status information.

Create a signal strength event every n minutes

Configures the router to write the signal strength to the Event Log every **n** minutes.

If registration is lost for 5 minutes

Controls whether the router will power cycle the wireless module after the network registration has been lost for 5 minutes. Setting this parameter to **Do not reset the module** will never recycle the wireless module, setting to **reset the module if GSM registration is lost** will power cycle the module after 5 minutes loss of GSM registration, and setting to **reset the module if GSM registration is lost** will power cycle the module after 5 minutes loss of GPRS, 3G or HSPA registration.

Preferred System:

Controls which mobile technology will be used as the preferred system (2G/3G).

- When set to **Auto**, the wireless module will choose the fastest technology available.

- When set to **GSM**, the wireless module will try GSM (GPRS/EDGE) technology first.

- When set to **WCDMA**, the wireless module will try WCDMA (UMTS/HSPA) technology first. For CDMA: Select CDMA for 2G (1xRTT) or EVDO for 3G.

Related CLI Commands-SIM Slot 1 (PPP 1)

Entity	Instance	Parameter	Values	Equivalent Web Parameter
modemcc	0	puk	sim puk code	SIM PUK/Confirm SIM PUK
modemcc	0	init_str	Free text field	Initialisation string 1
modemcc	0	init_str1	Free text field	Initialisation string 2
modemcc	0	init_str2	Free text field	Initialisation string 3
modemcc	0	hang_str	Free text field	Hang-up string:
modemcc	0	posthang_str	Free text field	Post Hang-up string:
modemcc	0	intercall_idle	0-2147483647	Wait n seconds between hanging up and allowing another call
modemcc	0	att_interval	0-2147483647	Wait n seconds between attachment attempts
modemcc	0	link_retries	0-2147483647	Reset the module after n unsuccessful connection attempts
modemcc	0	stat_retries	0-2147483647	Reset the module after n unsuccessful status retrieval attempts
modemcc	0	ss_interval	0-2147483647	Create a signal strength event every n minutes
modemcc	0	check_reg	0,1,2	If registration is lost for 5 minutes 0=do not reset the module 1=reset the module if the GSM registration is lost 2=reset the module if the GPRS registration is lost
modemcc	0	psys	0,1,2	Preferred System 0=Auto 1=GSM 2=WCDMA

Related CLI Commands-SIM Slot 2 (PPP 1)

Entity	Instance	Parameter	Values	Equivalent Web Parameter
modemcc	0	Puk_2	sim puk code	SIM PUK/Confirm SIM PUK
modemcc	0	init_str_2	Free text field	Initialisation string 1
modemcc	0	init_str1_2	Free text field	Initialisation string 2
modemcc	0	init_str2_2	Free text field	Initialisation string 3
modemcc	0	hang_str_2	Free text field	Hang-up string:
modemcc	0	posthang_str_2	Free text field	Post Hang-up string:
modemcc	0	intercall_idle_2	0-2147483647	Wait n seconds between hanging up and allowing another call
modemcc	0	att_interval_2	0-2147483647	Wait n seconds between attachment attempts
modemcc	0	link_retries_2	0-2147483647	Reset the module after n unsuccessful connection attempts
modemcc	0	stat_retries_2	0-2147483647	Reset the module after n unsuccessful status retrieval attempts
modemcc	0	ss_interval_2	0-2147483647	Create a signal strength event every n minutes
modemcc	0	check_reg_2	0,1,2	If registration is lost for 5 minutes 0=do not reset the module 1=reset the module if the GSM registration is lost 2=reset the module if the GPRS registration is lost
modemcc	0	Psys_	0,1,2	Preferred System 0=Auto 1=GSM 2=WCDMA

Advanced Mobile Network Settings parameters

Metric:

This parameter specifies the connected metric of the mobile interface. The default metric of a connected interface is 1. By allowing the interface to have a higher value (lower priority), static routes can take preference to interfaces. For normal operation, leave this value unchanged.

Generate Heartbeats on this interface

Heartbeat packets are UDP packets that contain status information about the router that may be used to locate a remote unit's current dynamic IP address.

This checkbox opens to show the following parameters:

Send Heartbeat messages to IP address a.b.c.d every h hrs m mins s secs

If these parameters are set to a non-zero value, the router will transmit heartbeat packets to the specified IP address/hostname at the specified interval.

Use interface x,y for the source IP address

Allows the selection of the source interface for the UDP heartbeats. For example, it may be required to send the heartbeat packets down a VPN tunnel. And in order to match the corresponding subnets of the VPN, it might require changing the source IP to match an inside Ethernet interface.

For normal operation, using the mobile interface as the source IP address, leave this value unchanged.

Select transmit interface using the routing table

When enabled, the UDP heartbeats chooses the best route from the routing table. If disabled the exit interface will be interface on which the heartbeat is configured.

Include IMSI information in the Heartbeat message

When enabled, the heartbeat includes the IMSI of the wireless module.

Include GPS information in the Heartbeat message

When enabled, the heartbeat includes the GPS co-ordinates of the router.

Generate Ping packets on this interface

This section relates to monitoring pings which can be sent from the mobile interface. For more details, refer to *Application Note 7, Wireless WAN problem Detection and Recovery*, available on www.digi.com.

```
☑ Generate Ping packets on this interface
   Send 0      byte pings to IP host                    every 0    hrs 0     mins 0     secs
   Send pings every 0    hrs 0     mins 0     secs if ping responses are not being received
   Switch to sending pings to IP host                  after 3      failures
   Ping responses are expected within 0     seconds
   ☐ Only send Pings when this interface is "In Service"
   ☐ New connections to resume with previous Ping interval
   Reset the link if no response is received within 0     seconds
   ☐ Use the ETH 0 IP address as the source IP address
   ☐ Defer sending pings if IP traffic is being received
```

This checkbox opens to show the following parameters:

Send n byte pings to IP host a.b.c.d every h hrs m mins s secs

If this parameter is set, the router will automatically generate a ping of n size to the IP host specified (IP address or hostname) at the interval specified. Deleting the IP host value disables the monitoring ping facility.

This parameter in conjunction with **Reset the link if no response is received within s seconds**, configures the router to use a back-up interface automatically should there be a problem with this interface.

Note   The n parameter specifies the PING size when using monitoring ping feature. The size indicates how large the ICMP packet should be excluding the size of the IP header.

Send pings every h hrs m mins s secs if ping responses are not being received

When set, the router uses this value as the interval to ping at when more than one ping request sent out the PPP interface is outstanding. This should be set to a shorter interval than the above ping request interval so that the router may more quickly react to a broken PPP link.

Switch to sending pings to IP host a.b.c.d after n failures

Allows a for more reliable problem detection before fail over occurs by testing connectivity to 2 IP addresses/hostnames. If an IP address or host name is entered and the n parameter has a value greater than **0**, when a ping failure is detected on the primary IP address, pings will be sent to this second IP address/hostname. This is to ensure that if the main IP address becomes unavailable for any reason and stops responding to ICMP requests, the router will check another IP address before starting fail over procedures.

Ping responses are expected within n seconds

When set to a non-zero value, the router waits for the interval specified for a response from a PING request before applying the **Send pings every h hrs m mins s secs if ping responses are not being received**. If this parameter is set to 0 (default), the time specified in the in **Send n byte pings to IP host a.b.c.d every h hrs m mins s secs** is allowed before applying the **Send pings every h hrs m mins s secs if ping responses are not being received**.

Only send Pings when this interface is "In Service"

When enabled, the interface sends ICMP echo requests only when it is in service. The default setting is off and ICMP echo requests are sent when the interface is in service and out of service.

New connections to resume with previous Ping interval

When enabled, this parameter controls the ping interval after deactivating and subsequently reactivating the mobile interface. It sets the ping interval to the same interval in use when the mobile link last disconnected.

Reset the link if no response is received within s seconds

An amount of time after which the device does not receive any ping response, the router terminates the mobile connection in an attempt to re-establish communications. Because by default the mobile link is always on, the router automatically attempts to re-establish a PPP connection that has been terminated.

Use the ETH 0 IP address as the source IP address

When enabled, the router uses the IP address of **ETH0** instead of the current IP address of the mobile interface as the source address for the auto PING packets.

Note This parameter is useful to send the monitoring pings down a VPN tunnel where the source IP address needs to match the LAN.

Defer sending pings if IP traffic is being received

When enabled, the timer configured in the **Send n byte pings to IP host a.b.c.d every h hrs m mins s secs** parameter is reset if IP data is sent across the mobile link.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	1	metric	0-256	Metric
ppp	1		OFF, ON	Generate Heartbeats on this interface
ppp	1	hrtbeatip	IP address	Send Heartbeat messages to IP address a.b.c.d every h hrs m mins s secs
ppp	1	hrtbeatint	0-2147483647 (seconds)	Send Heartbeat messages to IP address a.b.c.d every h hrs m mins s secs
ppp	1	hbipent	Default,PPP,Ethernet	Use interface x,y for the source IP address
ppp	1	hbipadd	number	Use interface x,y for the source IP address
ppp	1	hbroute	on/off	Select transmit interface using the routing table
ppp	1	hbimsi	on/off	Include IMSI information in the Heartbeat message
ppp	1	hbgps	on/off	Include GPS information in the Heartbeat message
ppp	1		OFF, ON	Generate Ping packets on this interface
ppp	1	pingsiz	number	Send n byte pings to IP host a.b.c.d every h hrs m mins s secs
ppp	1	pingip	IP addressd	Send n byte pings to IP host a.b.c.d every h hrs m mins s secs
ppp	1	pingint	0-2147483647 (seconds)	Send n byte pings to IP host a.b.c.d every h hrs m mins s secs
ppp	1	pingint2	0-2147483647 (seconds)	Send pings every h hrs m mins s secs if ping responses are not being received
ppp	1	pingip2	IP address	Switch to sending pings to IP host a.b.c.d after n failures
ppp	1	ip2count	number	Switch to sending pings to IP host a.b.c.d after n failures
ppp	1	pingresp	0-2147483647	Ping responses are expected within n seconds
ppp	1	pingis	on/off	Only send Pings when this interface is **In Service**
ppp	1	ping2cont	on/off	New connections to resume with previous Ping interval

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	1	pingdeact	0-2147483647	Reset the link if no response is received within s seconds
ppp	1	pingfreth0	on/off	Use the ETH 0 IP address as the source IP address
ppp	1	pingresetint	on/off	Defer sending pings if IP traffic is being received

SMS settings

You can configure the mobile routers to send and receive SMS messages. The sending of SMS messages could for example be in conjunction with sending alarms and received messages for configuration changes, or status requests.

Poll for incoming SMS messages

This checkbox opens to show the following parameter:-

Every n minutes

The interval, in minutes, that the router will wait in between checks for incoming SMS messages. Setting this interval to **0** turns off checking.

Enable command replies via SMS

Enables or disables replies to SMS commands.

Concatenate replies

Normally an SMS message is limited to 160 characters. However, the ETSI standard specifies a way to allow a number of SMS messages to be linked together by the sender (in this case the router). This enables the router to reply with long responses to SMS commands of longer than 160 characters. The reply comes back as a series of linked SMS messages which the phone reassembles and displays as one big message.

Note The routers cannot handle received concatenated SMS messages, it can only transmit concatenated SMS messages

Use this SMS message centre number n instead of the network default

This setting is optional. It is the number of the SMS message center (sometimes referred to as the Service Centre Address), used to relay SMS messages or alarms. This number must include the international dialing code, such as **44** for the UK, but not the **+** prefix or leading 0's, such as **44802000332**. SMS alarms are generated when the SMS trigger priority is greater than 0 and an event of this priority or higher occurs. SMS alarms may be configured using the **Configuration > Alarms > Event Settings > SMS** web page. If no number is specified, it is possible that the router operates using the default message centre for the GSM service to which you have subscribed.

SMS access level

The access level for SMS commands. The access level set here needs to match the level required by the command sent by SMS for the command to be accepted.

Use x as a command separator (default is CR)

The character to be used to separate multiple command lines when a remote SMS sender is controlling the router. The default separator is **<CR>.** As some SMS capable devices are not equipped with **<CR>** keys, an additional means of separating multiple lines is required.

Allow CLI commands from the following SMS numbers.

You may specify up to 10 numbers. Specifying ***** permits commands from any SMS number. Numbers are applied in the following input box. Click **Add** to submit.

Related CLI commands-SIM Slot 1 (PPP 1)

Entity	Instance	Parameter	Values	Equivalent Web Parameter
modemcc	0	sms_interval		Poll for incoming SMS messages:- Every n minutes
modemcc	0	sms_replies	on/off	Enable command replies via SMS
modemcc	0	sms_concat	Number 0=off 10=default when enabled	Concatenate replies
modemcc	0	sca	Free text field	Use this SMS message centre number n instead of the network default
modemcc	0	sms_access	0=Super (default) 1=High 2=Medium 3=Low 4=None 5=HighLow 6=HighMedium 7=CheckPar	SMS access level:
modemcc	0	sms_cmd_sep	Free text field	Use as a command separator (default is CR)
modemcc	0	sms_callerid	Mobile telephone number	Allow CLI commands from the following SMS numbers. (First SMS number)
modemcc	0	sms_callerid_1 to 9	Mobile telephone number	Allow CLI commands from the following SMS numbers. (additional SMS numbers 1 to 9)

Related CLI commands-SIM Slot 2 (PPP 1)

Entity	Instance	Parameter	Values	Equivalent Web Parameter
modemcc	0	sms_interval_2		Poll for incoming SMS messages:- Every n minutes
modemcc	0	sms_replies_2	on/off	Enable command replies via SMS
modemcc	0	sms_concat_2	Number 0=off 10=default when enabled	Concatenate replies
modemcc	0	Sca_2	Free text field	Use this SMS message centre number n instead of the network default
modemcc	0	sms_access_2	0=Super (default) 1=High 2=Medium 3=Low 4=None 5=HighLow 6=HighMedium 7=CheckPar	SMS access level:
modemcc	0	sms_cmd_sep	Free text field	Use as a command separator (default is CR)
modemcc	0	sms_callerid	Mobile telephone number	Allow CLI commands from the following SMS numbers. (First SMS number)
modemcc	0	sms_callerid_1 to 9	Mobile telephone number	Allow CLI commands from the following SMS numbers. (additional SMS numbers 1 to 9)

Configure DSL interfaces

Router models incorporating a DSL broadband interface includes a configuration page having the title shown above. By default, the configuration in this section is suitable for the majority of ADSL service providers in the UK. However, advanced users or users outside of the U.K. may wish or need to adjust some of the parameters.

Enable DSL

Enables or disables the use of DSL/ADSL functionality on the router.

Configure PVC

Select the required PVC instance from the drop-down selection box. Subsequent settings applies to the selected instance (see below).

PVC parameters

The PVC (Permanent virtual circuit) parameters are described here.

Enable this PVC

Check this box to enable PVC settings.

Encapsulation

The method of encapsulation to be used when transporting data over this APVC. The appropriate value can be selected from a drop list which includes the following options:

Option	Description
PPPoA VC-Mux	RFC 2364 VC-multiplexed PPP over AAL5
PPPoA LLC	RFC 2364 LLC encapsulated PPP over AAL5
PPPoE VC-Mux	RFC 2516 VC-multiplexed PPP over Ethernet
PPPoE LLC	RFC 2516 LLC encapsulated PPP over Ethernet
Bridged Ethernet VC-Mux	RFC 2684 VC-multiplexed bridged Ethernet
Bridged Ethernet LLC	RFC 2684 LLC encapsulated bridged Ethernet
Routed IP VC-Mux	RFC 1483 VC multiplexing routed IP over ATM
Routed IP LLC	RFC 1483 LLC encapsulated routed IP over ATM

To use PPPoA or PPPoE encapsulation, one of the available PPP instances must first be configured to use this APVC instance as its Layer 1 interface on the associated **Configuration > Interfaces > PPP > PPP n > Advanced page**.

VPI

The Virtual Path Identifier for this APVC in the range 0-255.

VCI

The Virtual Channel Identifier for this APVC in the range 0-65535.

Entity	Instance	Parameter	Values	Equivalent Web Parameter
apvc	0		0-255	VPI
apvc	0		0-65535	VCI

DSL Network Settings parameters

This DSL PVC is using PPP 1

The default interface for DSL. The default interface for DSL is PPP 1.

Description

A description for the DSL. This field is optional.

Username

The ADSL username.

Password

The password for the DSL account.

Confirm password

Enter the password for the DSL account again.

Enable NAT on this interface

Enables or disables IP Network Address Translation (NAT) or Network Address and Port Translation (NAPT) at the Ethernet interface. When the parameter is set to disabled, no NAT will take place. When this parameter is enabled, the extra options described below are displayed.

NAT and NAPT can have many uses, but they are generally used to allow a number of private IP hosts (PCs for example) to connect to the Internet through a single shared public IP address. This has two main advantages, it saves on IP address space (the ISP only need assign you one IP address), and it isolates the private IP hosts from the Internet, effectively providing a simple firewall because unsolicited traffic from the Internet cannot be routed directly to the private IP hosts.

To use NAT or NAPT correctly in the example of connecting private hosts to the Internet, NAT or NAPT should be enabled on the router's WAN side interface and should be disabled on the router's LAN side interface.

IP address

Enable standard Network Address Translation (NAT).

When a private IP host sends a UDP or TCP packet to an Internet IP address, the router changes the source address of the packet from the private host IP to the router's public IP address before forwarding the packet onto the Internet host. Additionally it will create an entry in a NAT table containing the private IP source address, the private IP port number, the public IP destination address and the destination port number. Conversely, when the router receives a reply packet back from the public host, it checks the source IP, source port number and destination port number in the NAT table to determine which private host to forward the packet to. Before it forwards the packet back to the private host, it changes the destination IP address of the packet from its public IP address to the IP address of the private host.

IP address and Port

Enable Network Address and Port Translation (NAPT).

This mode behaves like NAT but in addition to changing the source IP of the packet from the private host it can also change the source port number. This is required if more than one private host attempts to connect using the same local port number to the same Internet host on the same remote port number. If such a scenario were to occur with NAT the router would be unable to determine which private host to route the returning packets to and the connection would fail.

NAT Source IP address

If specified, and NAT mode is set to **NAT** or **NATP** for this interface, then the source address of packets being sent out this interface is changed to this address, rather than the interface address.

Enable IPsec on this interface

The IPSec parameter enables or disables IPSec processing on this interface. If this box is checked, packets sent or received on this interface must pass through the IPSec code before being transmitted. IPSec may drop the packet, pass it unchanged, or encrypt and encapsulate within an IPSec packet.

Keep Security Associations (SAs) when this Mobile interface is disconnected

Configures the router to keep any existing IKE and IPsec associations should the link drop. This is usually applied on head-end routers with fixed IP addresses.

Use interface X, Y for the source IP address of IPsec packets

By default, the source IP address for an IPSec Eroute is the IP address of the interface on which IPSec was enabled. By setting this parameter to either a PPP or Ethernet interface, the source IP address used by IPSec will match that of the Ethernet or PPP interface specified.

Enable the firewall on this interface

The Firewall parameter is used to turn Firewall script processing **On** or **Off** for this interface.

Note   If the firewall is enabled on an interface and with the absence of any firewall rules, the default action is to block ALL traffic. To configure the firewall, see the Firewall configuration on page 651 section.

Limit the data transmitted over this interface

On W-WAN networks (where charging is based on the amount of data transferred as opposed to time spent on-line), this parameter specifies a data limit after which the router will create an entry in the event log to indicate that this amount of data has been transferred. For example, if your monthly tariff includes up to 5Mb of data before you are charged an excess, you might set the Data limit warning level to **4000**. This would cause the router to place a warning entry in the event log once you had transferred 4Mb. This event could be used to trigger an email alert message, SNMP trap or SMS alert message.

Issue a warning event after

The maximum data to be transmitted before a warning entry is generated in the Event Log. You can select kilobytes, megabytes or gigabytes via the drop-down box.

Stop data from being transmitted after

The maximum amount of data that may be transferred before the router locks the interface and prevent further transfer. Along with the **Issue a warning event after** parameter, this setting is used on networks where the tariff is based on the amount of data transferred to help prevent excess charges being incurred. You can select kilobytes, megabytes or gigabytes via the drop-down box.

Reset the data limit on the x day of the month

If you wish to automatically unlock a locked interface at the start of a new billing period, set this parameter to the appropriate day of the month (from **1** to **28**). When this date is reached the router will unlock the interface and data transfer may resume. If the parameter is set to **0**, automatic unlocking will not occur and manual unlocking will be necessary (by clicking on the Clear Total Data Transferred button on the appropriate **Diagnostics-Statistics > PPP > PPP n** page. This parameter will also reset the statistics for the Data limit warning level (kb).

The factory default does not include any DSL settings and so when the router is first installed, the following message appears:

```
This DSL PVC is not assigned to any PPP interface.
Click here to jump to the PPP Mapping page.
```

When clicked, this link will redirect the browser to the
Configuration > Network > interfaces > Advanced > PPP Mappings page. From this page, select the desired PPP instance.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	1	description	Free text	Description
ppp	1	username	Free text	Username
ppp	1	password	Free text	Password
ppp	1	do_nat 1	ON	Enable NAT on this interface (IP Address)
ppp	1	do_nat 2	ON	Enable NAT on this interface (IP Address and port)
ppp	1	natip	IP Address	NAT Source IP Address
ppp	1	ipsec	ON/OFF	Enable IPSec on this interface
ppp	1	firewall	ON/OFF	Enable the firewall on this interface
ppp	1	dlwarnkb	Kbytes/ Mbytes/ GBytes	Issue a warning event after
ppp	1	dlstopkb	Kbytes/ Mbytes/ GBytes	Stop data from being transmitted after x Bytes data
ppp	1	dlrstday	1-28	Reset the data limit on the nth day of the month

PVC Traffic Shaping parameters

Service category

You can configure Each ATM PVC with a service category:

- UBR (unspecified bit rate, the default)
- VBR-nrt (variable bit rate, non-real-time)
- VBR-rt (variable bit rate, real-time)
- CBR (constant bit rate)
- Additional traffic parameters may be specified:
- PCR (peak cell rate in cells/sec)
- SCR (sustained cell rate in cells/sec)
- MBS (maximum burst size in cells)

The four service categories are characterized by the various traffic parameters as follows:

Service category	Traffic parameters
UBR	PCR, which may be zero for no limit
VBR-nrt	PCR, SCR, MBS
VBR-rt	PCR, SCR, MBS
CBR	PCR

This parameter specifies the maximum allowable rate at which cells can be transported along a connection in the ATM network. The PCR is the determining factor in how often cells are sent in relation to time in an effort to minimize jitter. PCR generally is coupled with the CDVT (Cell Delay Variation Tolerance), which indicates how much jitter is allowable.

Sustained cell rate (cells/sec)

A calculation of the average allowable, long-term cell transfer rate on a specific connection.

Maximum burst size (cells)

The maximum allowable burst size of cells that can be transmitted contiguously on a particular connection.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
apvc	0	servcat	UBR,VBR-ntr,VBR-rt,CBR	Service category
apvc	0	pcr	n	Peak cell rate (cells/sec)
apvc	0	scr	n	Sustained cell rate (cells/sec)
apvc	0	mbs	n	Maximum burst size (cells)

Advanced DSL parameters

Operational mode

The connection mode for the DSL link. The following options are available (default is Multi mode).

Values	Equivalent Web Parameter
Multi-mode	For Annex A models (such as PSTN / POTS) this option provides automatic selection between G.dmt, G.lite and ANSI (in the order listed). For Annex B models (such as ISDN) this option provides automatic selection between G.dmt (in the order listed)
ANSI	Annex A only-attempt to connect in ANSI T1.413 mode
G.dmt	Attempt to connect in ITU G.992.1 G.dmt mode
G.lite	Annex A only-attempt to connect in ITU G.992.2 G.lite mode
ADSL2	Connect using ADSL2
ADSL2+	Connect using ADSL2+

Load DSL firmware from flash file 'dspfw.bin' (if present)

Enables use of alternative +ADSL driver firmware and should only be enabled on the advice of the technical support team. This option also requires that an additional file be loaded onto the router.

Enable watchdog

This checkbox should only be enabled on the advice of the technical support team.

Manage this PVC using ATM OAM cells

Using Alarm indication signal (AIS) cells downstream and Remote defect indication (RDI) cells upstream, the router can detect faults between the connecting points of the VP/VC and suspend transfer of ATM cells until the VC fault condition is cleared.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
adsl	0	oper_mode	Multi,ANSI,G.dmt,G.lite,ADSL2, ADSL2+	Operational mode
adsl	0	usefwfile	ON/OFF	Load DSL firmware from flash file
adsl	0	watchdog	ON/OFF	Enable watchdog
apvc	0	oammanage	ON/OFF	Manage this PVC using ATM OAM cells

Additional CLI commands

The following command is not available from the web interface:

```
adsl 0 debug {0|1}
```

Where 0 is off and 1 causes debugging information to be sent to the CLI.

Configure GRE interfaces

Generic Routing Encapsulation (GRE) is a means of transporting IP packets from one device to another through an unencrypted point-to-point IP tunnel. Multiple tunnels may be configured to multiple devices. Below the GRE Interfaces sub menu, you will find the individual tunnel configuration.   When configured, a GRE tunnel is created between two devices.

Tunnel parameters

Description

A memorable name for this GRE instance, to make it easier to identify it.

IP address

The IP address of the virtual interface used by the tunnel. This parameter is used in conjunction with the mask parameter below. This parameter MUST be entered for the tunnel to work.

Mask

Use this parameter with the IP address parameter to clarify the subnet in use on the virtual interface. This would normally be a 30 bit mask as this is a point-to-point link (**255.255.255.252**).

Source IP Address

The two sub options here allows you to specify a source address either from a specified interface or by manually assigning an address. If you do not select either option the default address for the route the packet leaves the router through will be used (please note that if the interface through which the GRE packets exit does not have NATting turned on then the default router address will be used-by default this will be the Ethernet 0 address).

Use Interface:

The GRE tunnel source interface, which allows the tunnel end point to be a physical interface rather than a virtual IP address. This is for using GRE without IPSec. These parameters should not be used if the source address is used in the parameter below. Select from the drop down boxes the available interface type and number.

Use IP Address:

A virtual host IP address for the local end of the tunnel, configured for routing purposes. This IP address has no other use and needs no mask as it is a host address, such as **1.1.1.1**. This option is normally used in conjunction with IPSec. Do not use this parameter if the interface is selected as the source using the **Use Interface** options above.

Destination IP Address or Hostname

The FQDN or IP address of the remote end of the tunnel. This could also be the virtual host IP address for the remote end of the tunnel, configured for routing purposes. such as **2.2.2.2**.

Enable keepalives on this GRE tunnel

Select this checkbox to display the GRE keepalive parameters. Keepalives are needed so allow the router to determine whether the tunnel interface is receiving traffic correctly or not. If keepalives fail, the tunnel is marked as down.

Send a keepalive every s seconds

When configured to a non-zero value, keepalive packets is sent to the remote end of the tunnel and the response is monitored to detect if the tunnel is up or down. If the tunnel is detected as down, the routing table metric will be altered. Value is configured in seconds. If this value is set to zero then keepalives will not be used.

Bring this GRE tunnel down after no replies to n keepalives

The consecutive number of keepalive packets that need to fail before the tunnel is detected as being down.

Bring this GRE interface up to send keepalives

Whether or not the GRE keepalive packets will activate the tunnel. If set to **YES** and the tunnel drops the GRE keepalive packet will try to raise the tunnel again. If set to **NO** and the tunnel has been marked as down due to the GRE keepalives not being received, the router will only raise the tunnel if a packet (other than a GRE keepalive) needs to be routed.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
tun	n	descr	Free text field	Description
tun	n	IPaddr	Valid IP address	IP Address
tun	n	mask	Valid Subnet Mask	Mask
tun	n	source_ent	blank,ETH,PPP	Use interface x,y for the source IP address of GRE packets x=Interface type
tun	n	source_add	0-255	Use interface x,y for the source IP address of GRE packets y=interface number
tun	n	source	Valid IP address	Source IP address to use for GRE packets
tun	n	dest	Valid IP address	Destination IP address to use for GRE packets
tun	n	kadelay	Seconds	Send a keepalive every s seconds
tun	n	karetries	Number	Bring this GRE tunnel down after no replies to n keepalives
tun	n	kaactrq	On,off	Bring this GRE interface up to send keepalives

Advanced GRE parameters

Metric

The connected metric of an interface. The default metric of a connected interface is **1**. By allowing the interface to have a higher value (lower priority), static routes can take preference to interfaces. For normal operation, leave this value unchanged.

MTU

The maximum transmission unit. In this text box you can enter the greatest amount of data that can be transferred in one physical packet. The default value is **1400**.

Tunnel Key

This parameter is normally used with multi GRE (mGRE). The tunnel key adds an extra field to the GRE header where a key number can be applied. When used, incoming GRE packets must have a matching tunnel key number to be accepted by this tunnel. When the Tunnel key parameter is used the IP address parameter is not required.

Enable the firewall on this GRE tunnel

The Firewall parameter turns Firewall script processing **on** or **off** for this interface. If using the firewall for problem detection on a tunnel interface, the interface to put OOS will need to be specified, such as:

```
pass out break end on tun n from any to 100.100.100.29 port=4000 flags S!A inspect-state
oos ppp n 5
```

Enable GRE checksums

Selects whether to add GRE checksums to GRE packets when the router is terminating a GRE tunnel. Set this parameter to **off** to disable checksums, and to **on** to enables checksums.

Enable IGMP on this GRE tunnel

This IGMP parameter enables or disables the transmission and reception of IGMP packets on this interface. IGMP is used to advertise members of multicast groups. If IGMP is enabled, and a member of a multicast group is discovered on this interface, multicast packets for this group received on other interfaces will be sent out this interface.

Enable IP analysis:

When set to **on**, the un-encapsulated IP traffic is captured into the analyser trace.

Enable Tunnel analysis:

When set to **on**, the GRE encapsulated packets and keepalives is captured to the analyser trace.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
tun	n	metric	Numeric Metric value	Metric for the route associated with this interface
tun	n	MTU	MTU value	Maximum transmission unit size
tun	n	tunkey	Key number	Key number
tun	n	Firewall	on,off	Turn firewall on or off
tun	n	csum	on,off	Enable GRE checksums
tun	n	igmp	On, off	Enable IGMP packets
tun	n	ipanon	On, off	Enable IP analysis for traffic on this interface
tun	n	tunanon	On, off	Enable GRE tunnel analysis

Note **RIP Routing Parameters-CLI only:** Under the CLI commands for GRE Tunnels are parameters specifically relating to RIP. Please see the Interfaces > Ethernet / PPP / GRE parameters on page 373 section on RIP routing for configuration of these sub parameters.

Configure ISDN interfaces

The **Configuration > Network > Interfaces > ISDN** page has the following options:

- ISDN Answering
- ISDN Dialling
- LAPD

ISDN Answering parameters

This page allows you to configure the ISDN interface to receive incoming calls.

Load answering defaults button

Click this to button resets the default answering PPP interface (PPP 0) to the factory answering defaults.

Load answering defaults

Description

A memorable name for this PPP instance, to make it easier to identify it.

Only accept calls from calling numbers

ending with

Restricts the range of numbers from which ISDN will answer incoming calls, such as the ISDN interface will only answer a call if the trailing digits of the calling number match what is specified by this parameter. For example, if this parameter was set to **3**, incoming calls from **1234563** would be answered but calls from **1234567** would not.

with ISDN MSN ending with

If answering is disabled this parameter is not used.

Provides the filter for the ISDN Multiple Subscriber Numbering facility. It is blank by default but when set to an appropriate value on an answering interface, it will cause the router to answer incoming calls to only telephone numbers where the trailing digits match the value selected. For example, setting this parameter to **123** will prevent the router from answering any calls to numbers that do not end in **123**.

with ISDN sub-address ending with

If answering is disabled this parameter is not used.

Provides the filter for the ISDN sub-address facility. It is blank by default but when set to an appropriate value on an ISDN answering interface, it will cause the router to answer incoming calls only to ISDN numbers where the trailing digits match the Sub-address value. For example, setting the this parameter to 123 will prevent the router from answering any calls to numbers that do not end in 123.

Use the following local IP configuration

Local IP Address:

The IP address of the router's ISDN answering interface. Set this field to the desired local IP address.

Attempt to assign the following IP configuration to remote devices

Set this parameter if the remote system needs a supplied address. The interface makes an attempt to negotiate an IP address from the IP address pool. Generally, this parameter is enabled for incoming connections. This checkbox opens to show the following parameters.

Assign remote IP addresses from a.b.c.d to a.b.c.d

The range of IP addresses supplied to incoming callers. This parameter may require alteration if the default value **10.10.10.0** to **10.10.10.4** does not suit the remote network configuration.

Mask:

The IP netmask for the Remote network. This can be used to create a dynamic route to the remote network whenever the ISDN interface is active.

Primary DNS server:

The answering ISDN interface would normally supply its own PPP IP address to the peer for DNS requests. This parameter allows you to specify an alternative DNS IP address.

Secondary DNS server:

A secondary DNS server IP address to the peer for DNS requests, if required.

Enable NAT on this interface

Enables or disables IP Network Address Translation (NAT) on the answering ISDN interface.

This checkbox opens to show the following options:

IP Address

Enable standard Network Address Translation (NAT).

IP address and Port

Enable Network Address and Port Translation (NAPT).

Enable IPsec on this interface

Enables or disables IPSec processing on the ISDN interface. If enabled, packets sent or received on this interface must pass through the IPSec code before being transmitted. IPSec may drop the packet, pass it unchanged, or encrypt and encapsulate within an IPSec packet.

This checkbox opens to show the following parameters:

Keep Security Associations (SAs) when this ISDN interface is disconnected

Configures the router to keep any existing IKE and IPsec associations should the link drop. This is usually applied on head-end routers with fixed IP addresses.

Use interface X, Y for the source IP address of IPsec packets

By default, the source IP address for an IPSec Eroute is the IP address of the interface on which IPSec was enabled. By setting this parameter to either a PPP or Ethernet interface, the source IP address used by IPSec will match that of the Ethernet or PPP interface specified.

Enable the firewall on this interface

Enables or disables the Firewall script processing for the mobile interface.

Note If the firewall is enabled on an interface and with the absence of any firewall rules, the default action is to block ALL traffic. To configure the firewall, refer to the Firewall configuration on page 651 section.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	0	name	Free text field	Description:
ppp	0	cingnb	number	ending with
ppp	0	msn	number	with ISDN MSN ending with
ppp	0	sub	number	with ISDN sub-address ending with
ppp	0	ipaddr	IP address	Local IP Address:
ppp	0	mask	Network mask	Mask:
ppp	0	ipmin	IP address	Assign remote IP addresses from a.b.c.d to a.b.c.d
ppp	0	iprange	1-255	Assign remote IP addresses from a.b.c.d to a.b.c.d
ppp	0	dnsserver	IP address	Primary DNS server:
ppp	0	secdns	IP address	Secondary DNS server:
ppp	0	do_nat	1	Enable NAT on this interface IP Address:
ppp	0	do_nat	2	Enable NAT on this interface IP address and Port:
ppp	0	ipsec	1	Enable IPsec on this interface
ppp	0	ipsec	2	Keep Security Associations (SAs) when this ISDN interface is disconnected
ppp	0	ipsecent	Default,Ethernet,PPP	Use interface X, Y for the source IP address of IPsec packets
ppp	0	ipsecadd	number	Use interface X, Y for the source IP address of IPsec packets
ppp	0	firewall	on/off	Enable the firewall on this interface

Advanced ISDN parameters

These are the advanced settings for the ISDN interface.

Metric:

The connected metric of the mobile interface. The default metric of a connected interface is 1. By allowing the interface to have a higher value (lower priority), static routes can take preference to interfaces. For normal operation, leave this value unchanged.

Enable "Always On" mode of this interface

On

Configures the PPP instance so that if the router is disconnected, it tries to reconnect again after approximately 10 seconds or dictated by the **Configuration > Network > IP Routing/ Forwarding > IP Routing > When an "Always On" route becomes "In Service", wait n seconds before using it** parameter.

On and return to service immediately

This is similar to the above parameter. If you enable this parameter, the router will try and connect immediately and without delay.

Put this interface "Out of Service" when an always-on connection attempt fails

Usually, the always-on interfaces do not go out of service unless they have connected at least once. When this option is turned **On**, the interface goes out of service even if the first connection attempt fails.

Attempt to re-connect after n seconds

The length of time, in seconds, the router will wait after an **always-on** ISDN connection has been terminated before trying to re-establish the link.

If an inhibited PPP interface is connected, attempt to re-connect after n seconds

The value of this parameter takes precedence over **Configuration > Network > Interfaces > ISDN > ISDN Answering > Advanced > Wait n seconds after power-up before activating this interface** when some other PPP that is usually inhibited by this one is connected. This parameter typically reduces the connection retry rate when a lower priority PPP is connected.

Wait n seconds after power-up before activating this interface

If this parameter is not set to **0**, this is the initial delay after power up before the PPP is activated. After that, the usual always-on activation timers apply.

Control when this interface can connect using Time band n

The Time Band number to use for this ISDN instance (see Configure time bands on page 488).

Keep this interface up for at least n seconds

If you set this parameter to a non-zero value, ISDN will not close the connection for the specified period, even if the link is inactive.

Close this interface

After n seconds

The maximum time that this ISDN Interface may remain connected during any one session. After this time, the ISDN link is deactivated.

if it has been up for n minutes in a day

The maximum time that this ISDN interface may remain connected during any one day. After this time, the ISDN link is deactivated.

If the link has been idle for n seconds

The ISDN interface closes the connection if the link is inactive for the length of time specified by this parameter.

Alternative idle timer for static routes n seconds

An alternative Inactivity timeout for use in conjunction with the Use 2nd inactivity timeout when this route becomes available parameter on the **Configuration > Routing > Routing > Static Route n** pages. This timeout will only be used until the PPP next deactivates. After that, the normal timeout value is used.

If the link has been idle for s seconds

The router will deactivate this interface after the time specified in this text box if it detects that the link has not passed any traffic for that period.

Alternative idle timer for static routes s seconds

An alternative inactivity timeout for use in conjunction with the **Make PPP n interface use the alternative idle timeout when this route becomes available** parameter on the **Configuration > Network > IP Routing/Forwarding > Static Routes > Routes n > Advanced** web page. This timeout will only be used until the PPP instance next deactivates. After that the normal timeout value is used.

If the link has not received any packets for s seconds

The amount of time that the router waits without receiving any PPP packets before disconnecting. The timer is reset with each received PPP packet.

If the negotiation is not complete in s seconds

The maximum time (in seconds) allowed for the PPP negotiation to complete. If negotiations have not completed within this period, the interface is deactivated.

Generate an event after this interface has been up for m minutes

The number of minutes, if any, after which the router should create an event in the event log that states that the interface has been active for this period.

Limit the data transmitted over this interface

When checked, this checkbox enables the following parameters that control what data volume restrictions (if any) should be applied to this interface.

Issue a warning event after n units

The amount of traffic which causes a warning event to be generated in the event log stating that the specified amount of data has been transferred. The units are specified by a drop-down list, having the following options; **KBytes**, **MBytes**, **GBytes**. For example, if the monthly tariff includes up to 5MB of data before excess usage charges are levied, it would be useful to set this threshold to 4MB. This would cause the router to create a warning entry in the event log once 4MB of data had been transferred. This event could then be used to trigger an email alert, SNMP trap or SMS alert message.

Stop data from being transmitted after n units

The total amount of data that may be transmitted by this PPP instance before the link is blocked for further traffic, and the value in the drop-down list specifies the units which are kilobytes, megabytes, gigabytes.

Reset the data limit on the n day of the month

The value in this text box specifies the day of the month on which the data limit is reset to zero.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	metric	0-255	Metric
ppp	n	aodion	0-2 0=disabled 1=enabled 2=On and return to service immediately	Enable "Always On" mode of this interface, On, On and return to service immediately
ppp	n	immoos	ON, OFF	Put this interface "Out of Service" when an always-on connection attempt fails
ppp	n	aodi_dly	0-2147483647	Attempt to reconnect after s seconds
ppp	n	aodi_dly2	0-2147483647	If an inhibited PPP interface is connected, attempt to re-connect after s seconds
ppp	n	pwr_dly	0-2147483647	Wait s seconds after power-up before activating this interface
ppp	n	tband	0-4	Control when this interface can connect using Time Band n
ppp	n	minup	0-2147483647	Keep this interface up for at least s seconds
ppp	n	maxup	0-2147483647	Close this interface after s seconds
ppp	n	maxuptime	0-2147483647	if it has been up for m minutes in a day
ppp	n	timeout	0-2147483648	if the link has been idle for s seconds
ppp	n	timeout2	0-2147483648	Alternative idle timer for static routes s seconds
ppp	n	rxtimeout	0-2147483648	if the link has not received any packets for s seconds

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	maxneg	0-2147483648	if the negotiation is not complete in s seconds
ppp	n	uplogmins	0-2147483647	Generate an event after this interface has been up for m mins
ppp	n	dlwarnkb	0-2147483647	Issue a warning after n units
ppp	n	dlstopkb	0-2147483647	Stop data from being transmitted after n units
ppp	n	dlrstday	0-255	Reset the data limit on the n day of the month

ISDN dialing parameters

This section of the web interface appears when the router is fitted with an optional internal ISDN MODEM card. When first powered up, navigating to the **Configuration > Network > Interfaces > ISDN** page will show a message indicating that the MODEM card does not have a PPP instance associated with it. Follow the link on the page and select an unassigned PPP interface to the MODEM. When the browser is refreshed and the **Configuration > Network > Interfaces > ISDN** page redisplayed, it should show the parameters described below, along with a message at the top of the page indicating which PPP instance has been selected.

This ISDN interface is using PPP n

This message simply states which PPP instance has been assigned to the interface.

Description

A memorable name for the interface. This may be useful when referring to the interface, rather than having to remember the name and the function of the interface.

Dial out using numbers

The telephone numbers that should be used, in sequence, to make an outgoing connection.

Prefix n to the dial out number

The dialing prefix to use, if needed. This may be necessary when using a PABX.

Username

The username that should be used when using the PPP instance to connect to the remote peer. This will normally be provided by an ISP for use with a dial-in Internet access service.

Password

The password to use for authenticating the remote peer and is used in conjunction with the above username.

Confirm password

Type the password into this text box to enable the router to confirm that the password has been entered identically in both boxes.

Allow the remote device to assign a local IP address to this router

When this radio button is selected, the remote peer will assign this PPP interface an IP address.

Try to negotiate a.b.c.d as the local IP address for this router

If it would be useful, but not essential, to have a predefined IP address for the interface, the second radio button should be selected and the desired IP address entered into the text box to the right.

Use a.b.c.d as the local IP address for this router

If it is essential that the PPP interface has a specific IP address, this radio button should be selected and the IP address entered into the text box.

Use the following DNS servers if not negotiated

Primary DNS server

The IP address of the primary DNS server to use if a DNS server is not assigned as part of the PPP negotiation and connection process. It is fairly common practice for the DNS server to be assigned automatically by the ISP when making a connection.

Secondary DNS server

The IP address of the secondary DNS server to use if one is not automatically assigned by the remote peer.

Attempt to assign the following IP configuration to remote devices

When checked, this check box reveals the following four configuration parameters which control how the PPP instance assigns an IP address to a connecting remote peer. The primary and secondary DNS server addresses will also be sent to the remote peer

Assign remote IP addresses from a.b.c.d to a.b.c.d

The IP addresses in these text boxes define the pool of IP addresses to assign to remote peers during the IP protocol configuration phase of the PPP negotiation process.

Primary DNS server

The IP address of the primary DNS server that the remote peer should use when making DNS requests over the link.

Secondary DNS server

The IP address of the secondary DNS server that the remote peer should use when making DNS requests, should the primary server be unavailable.

Allow the PPP interface to answer incoming calls

When checked, this checkbox causes the PPP instance to answer an incoming call.

Only allow calling numbers ending with n

When set to answer calls, the value in this setting provides a filter for ISDN sub-addresses. This value is blank by default but when the PPP instance is set to answer calls, only numbers having trailing digits that match the sub-address value in this test will be answered. So for example, if this value is set to **123**, only calls from numbers with trailing digits that match this value will be answered; for example, **01942 605123**.

Enable NAT on this interface

Enables Network Address Translation to operate on this interface. This is the same as for other PPP interfaces.

IP address/IP address and Port

Whether IP address translation only should be applied or whether port number translation should also be applied to IP packets.

Enable IPsec on this interface

When checked, this checkbox causes the router to encrypt traffic on this interface using the IPsec protocol. The following two additional configuration parameters are revealed when this box is checked.

Keep Security Associations (SAs) when this ISDN interface is disconnected

When enabled, causes the router to maintain (such as not flush) the SA when the interface becomes disconnected. The normal behavior is to remove the SAs when the interface becomes disconnected.

Use interface x,y for the source IP address of IPsec packets

If it is required to use another interface (such as not the interface currently being configured) as the source address for IPsec packets, this may be achieved by selecting the desired interface from the drop-down list and typing the desired interface instance number into the adjacent text box.

Enable the firewall on this interface

When enabled, applies the firewall rules to traffic using this interface.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	name	Up to 25 characters	Description
ppp	n	phonenum	up to 25 digits	Dial out using numbers
ppp	n	ph2	"	"
ppp	n	ph3	"	"
ppp	n	ph4	"	"
ppp	n	prefix	0-9999999999	Prefix n to the dial out number
ppp	n	username	Up to 60 characters	Username
ppp	n	password	Up to 40 characters	Password
ppp	n	IPaddr	0.0.0.0	Allow the remote device to assign a local IP address to this router
ppp	n	IPaddr	Valid IP address a.b.c.d	Try to negotiate a.b.c.d as the local IP address for this router (in conjunction with l_addr)
ppp	n	l_addr	OFF,ON When ON, allows negotiation when OFF force use of specified IP address	Use a.b.c.d as the local IP address of this router
ppp	n	DNSserver	Valid IP address a.b.c.d	Use the following DNS servers if not negotiated Primary DNS server a.b.c.d

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	secDNS	Valid IP address a.b.c.d	Use the following DNS servers if not negotiated Secondary DNS server a.b.c.d
ppp	n	IPmin	Valid IP address a.b.c.d	Assign remote IP addresses from a.b.c.d to a.b.c.d
ppp	n	IPrange	0-255	Assign remote IP addresses from a.b.c.d to a.b.c.d
ppp	n	transDNS	Valid IP address a.b.c.d	Primary DNS server a.b.c.d
ppp	n	sectransDNS	Valid IP address a.b.c.d	Secondary DNS server a.b.c.d
ppp	n	ans	OFF,ON	Allow this PPP interface to answer incoming calls
ppp	n	cingnb	up to 25 digits	Only allow calling numbers ending with n
ppp	n	do_nat	0,1,2 0=Disabled 1=IP address 2=IP address and port	Enable NAT on this interface IP address/IP address and Port
ppp	n	nat_ip	Valid IP address a.b.c.d	NAT Source IP address a.b.c.d
ppp	n	ipsec	0=Disabled 1=Enabled 2=Enabled and Keep SAs	Enable IPsec on this interface/ Keep Security Associations when this ISDN interface is disconnected
ppp	n	firewall	OFF,ON	Enable the firewall on this interface

Advanced ISDN parameters

Metric

The route metric that should be applied to this interface. For details, see the PPP parameters on page 293 section.

Enable "Always On" mode of this interface

When enabled, causes the following two options to appear.

On/On and return to service immediately

These two radio buttons select whether the **always-on** functionality should simply be enabled or whether the additional facility to return the interface to the **In Service** state should be applied.

Put this interface "Out of Service" when an always-on connection attempt fails

Normally, always-on interfaces do not go out of service unless they have connected at least once. When checked, this checkbox causes the router to put the interface out of service even if the first connection attempt fails.

Attempt to re-connect after s seconds

Specifies the length of time in seconds that the router should wait after an always-on PPP connection has been terminated before trying to re-establish the link.

If an inhibited PPP interface is connected, attempt to re-connect after s seconds

The value in this setting takes precedence over the previous parameter when another PPP instance that is usually inhibited by this one is connected. This parameter typically reduces the connection retry rate when a lower priority PPP instance is connected.

Wait s seconds after power-up before activating this interface

The initial delay that the router applies before activating the PPP instance after power-up. After the initial power-up delay the normal always-on activation timers apply. If set to zero, no delay will be applied.

Control when this interface can connect using Time band n

These two controls, the check box and drop-down list, determine whether the Time Band function should be applied to this interface. Checking the checkbox enables the functionality and the desired time band instance is selected from the drop-down list. Time Band functionality is explained in Configure time bands on page 488.

Keep this interface up for at least s seconds

The minimum period that the PPP interface should remain available. This means that even if the link becomes inactive before this period expires, the connection will remain open.

Close this interface

After s seconds

The maximum time that the link remains active in any one session. After this time, the link will be deactivated.

If it has been up for m minutes in a day

The router deactivates the PPP instance after it has been active for the value specified in this text box.

If the link has been idle for s seconds

The router deactivates this interface after the time specified in this text box if it detects that the link has not passed any traffic for that period.

Alternative idle timer for static routes s seconds

An alternative inactivity timeout for use in conjunction with the **Make PPP n interface use the alternative idle timeout when this route becomes available** parameter on the **Configuration > Network > IP Routing/Forwarding > Static Routes > Routes n > Advanced** web page. This timeout is only used until the PPP instance next deactivates. After that the normal timeout value is used.

If the link has not received any packets for s seconds

The amount of time that the router will wait without receiving any PPP packets before disconnecting. The timer is reset with each received PPP packet.

If the negotiation is not complete in s seconds

The maximum time (in seconds) allowed for the PPP negotiation to complete. If negotiations have not completed within this period, the interface is deactivated.

Generate an event after this interface has been up for m minutes

The number of minutes (if any) after which the router should create an event in the event log that states that the interface has been active for this period.

Limit the data transmitted over this interface

When enabled, displays the following parameters that control any data volume restrictions that should be applied to this interface.

Issue a warning event after n units

The amount of traffic which causes a warning event to be generated in the event log stating that the specified amount of data has been transferred. The units are specified by a drop-down list, having the options kilobytes, megabytes, gigabytes. For example, if the monthly tariff includes up to 5MB of data before excess usage charges are levied, it would be useful to set this threshold to 4MB. This would cause the router to create a warning entry in the event log once 4MB of data had been transferred. This event could then be used to trigger an email alert, SNMP trap or SMS alert message.

Stop data from being transmitted after n units

The total amount of data that may be transmitted by this PPP instance before the link is blocked for further traffic, and the value in the drop-down list specifies the units which are **kilobytes**, **megabytes**, **gigabytes**.

Reset the data limit on the n day of the month

The day of the month on which the data limit is reset to zero.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	metric	0-255	Metric
ppp	n	aodion	0-2 0=disabled 1=enabled 2=On and return to service immediately	Enable "Always On" mode of this interface, On, On and return to service immediately
ppp	n	immoos	ON, OFF	Put this interface "Out of Service" when an always-on connection attempt fails
ppp	n	aodi_dly	0-2147483647	Attempt to reconnect after s seconds
ppp	n	aodi_dly2	0-2147483647	If an inhibited PPP interface is connected, attempt to re-connect after s seconds
ppp	n	pwr_dly	0-2147483647	Wait s seconds after power-up before activating this interface
ppp	n	tband	0-4	Control when this interface can connect using Time Band n
ppp	n	minup	0-2147483647	Keep this interface up for at least s seconds
ppp	n	maxup	0-2147483647	Close this interface after s seconds
ppp	n	maxuptime	0-2147483647	if it has been up for m minutes in a day
ppp	n	timeout	0-2147483648	if the link has been idle for s seconds
ppp	n	timeout2	0-2147483648	Alternative idle timer for static routes s seconds
ppp	n	rxtimeout	0-2147483648	if the link has not received any packets for s seconds
ppp	n	maxneg	0-2147483648	if the negotiation is not complete in s seconds
ppp	n	uplogmins	0-2147483647	Generate an event after this interface has been up for m mins
ppp	n	dlwarnkb	0-2147483647	Issue a warning after n units
ppp	n	dlstopkb	0-2147483647	Stop data from being transmitted after n units
ppp	n	dlrstday	0-255	Reset the data limit on the n day of the month

ISDN LAPD parameters

This page allows you to configure the ISDN LAPD interfaces. Link Access Protocol D (LAPD) is the protocol used for ISDN D-channel signaling and call setup.

LAPD 0 and LAPD 1 can be used as required for SAPI 16 traffic (such as X.25 over D-channel). LAPD 2 is normally reserved for ISDN call control.

Enable LAPD n

Disabling this parameter disables the LAPD instance. This may be necessary if you have an installation where two or more routers are connected to the same ISDN **S** bus. In this case, only one of the routers may be configured for D-channel X.25 on TEI1, SAPI16. On each of the other routers you must disable any LAPD instance for which the TEI is set to 1 in order to prevent it from responding to X.25 traffic on that TEI that is actually destined for another router.
When checked, this check box will also reveal the following configuration parameters.

Mode

When the DTE/DCE mode parameter is set to DTE, the router behaves as a DTE. This is the default value and should not be changed for normal operation across the ISDN network. If your application involves using two routers back-to-back, one of the routers should have the DTE mode value set to DCE.

N400 Counter

The standard LAPB/LAPD retry counter. The default value is 3 and it should not normally be necessary to change this.

RR Timer n msecs

The standard LAPB/LAPD Receiver Ready timer. The default value is **10,000ms** (10 seconds) and it should not normally be necessary to change this.

T1 Timer n msecs

The standard LAPB/LAPD timer. The default value is **1000** milliseconds (1 second) and it should not normally be necessary to change this.

T200 Timer n msecs

The standard LAPB/LAPD re-transmit timer, in milliseconds. The default value is **1000** milliseconds (1 second) and it should not normally be necessary to change this.

TEI

Each ISDN terminal device connected to your ISDN basic rate outlet must be assigned a unique Terminal Endpoint Identifier (TEI). In most cases, this is negotiated automatically. In some cases however, it may be necessary to assign a fixed TEI.

When TEI is set to 255, the TEI is negotiated with the ISDN network. To use a fixed TEI set the TEI parameter to the appropriate value as specified by your service provider.

D-channel X.25 Tx Window Size

The transmit window size when using D-channel X.25. The default is 7.

Tx Throughput

Used in conjunction with the **Rx Throughput** parameter to limit the maximum data throughput on a LAPD link in bits per second.

If this parameter is set to **0**, the router will transmit data across the LADP link as fast as possible whilst observing hardware or software flow control if enabled.

When set to a value greater than 0, the router will limit the rate at which data is transmitted over the LAPD link.

Note If multiple PAD or IP instances are sharing this LAPD instance, the maximum transmission rates of all instances will be limited.

Rx Throughput

Used in conjunction with the **Tx Throughput** parameter to limit the maximum data throughput on a LAPD link in bits per second.

If this parameter is set to 0, the router will transmit data across the LADP link as fast as possible whilst observing hardware or software flow control if enabled.

When set to a value greater than **0**, the router will limit the rate at which data can be received over the LAPD link when it detects that receive throughput exceeds the specified rate.

Note If multiple PAD or IP instances are sharing this LAPD instance, the maximum transmission rates of all instances will be limited.

Reactivate D-channel connection

When enabled, the router tries to reactivate a D-channel connection after disconnection by the network by transmitting SABME frames. If it is unable to reactivate the connection after retrying the number of times specified by the N400 counter, it will wait for 1 minute before repeating the retry sequence.

Enabling this parameter also deactivates the **Reactivate after n secs** parameter.

If this parameter is disabled, the router will not attempt to reactivate a D-channel link following deactivation by the network.

Reactivate after n secs

The number of seconds a deactivation has to be present before the LAPD instance will try to reactivate itself.

After X.25 PAD session is terminated

Determines whether the LAPD session is deactivated when an X.25 PAD session is terminated.

Deactivate the LAPD session

Enables automatic deactivation of a LAPD session when an X.25 PAD session is terminated.

Do not deactivate the LAPD session

Ensures the router does not deactivate the LAPD session when an X.25 PAD session is terminated.

Enable D64S Mode

D64S mode is a mode in which ISDN B-channel(s) may be used without the need to use any D channel protocol. It is sometimes referred to as nailed up ISDN. To enable this mode for this LAPD instance, Check the **D64S mode** parameter checkbox and ensure that the **TEI** parameter is set to **255**. This means that for any application that uses ISDN (such as. PPP) then it will use D64S mode.

First D64S B-channel

When using D64S mode there is no dialing protocol to negotiate which B-channel to use. This must therefore be specified using this parameter. Check the **B1** radio button to select channel **B1**. Check the **B2** radio button to select channel **B2** (if another channel is requested from an application then it will use the other unused B channel).

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
LAPD	n	enabled	off, on	Enable LAPD n
LAPD	n	dtemode	off, on	Mode
LAPD	n	n400	1-255	N400 Counter
LAPD	n	tnoact	1000-60000	RR Timer n msecs
LAPD	n	t1time	1-60000	T1 Timer n msecs
LAPD	n	t200	1-60000	T200 Timer n msecs
LAPD	n	tei	0-255	TEI
LAPD	n	window	1-7	D-channel X.25 Tx Window Size
LAPD	n	tthruput	0-1410065407	Tx Throughput
LAPD	n	rthruput	0-1410065407	Rx Throughput
LAPD	n	keepact	off, on	Reactivate D-channel connection
LAPD	n	reactsecs	0-2147483647	Reactivate after n secs
LAPD	n	nodeact	off	After X.25 PAD session is terminated: Deactivate the LAPD session
LAPD	n	nodeact	on	After X.25 PAD session is terminated: Do not deactivate the LAPD session
LAPD	n	d64smode	off, on	Enable D64S Mode
LAPD	n	d64schan	1, 2	First D64S B-channel: B1, B2

Answering ISDN calls

Digi routers can answer incoming B-channel ISDN calls with three main protocols: rate adaption protocols, LAPB, and PPP. Usually several instances of these protocols exist. This section explains how answering priorities work for the different protocols.

Protocol entities

The following protocol instances are capable of answering an incoming ISDN call:

Adapt

Adapt instances provide rate adaptation protocols such as V.120 or V.110.

LAPB

LAPB instances allow the router to answer incoming X.25 calls over ISDN. These instances can optionally connect the caller to a synchronous serial port, an asynchronous serial port bound to a PAD, or switch the call to another interface.

PPP

IP data tunneled over PPP instances allows remote access to the router's IP-based management features and also facilitates onward IP routing through any of the router's IP enabled interfaces.

The router automatically answers an incoming ISDN call if any of the following statements are true, subject to the entity's **MSN**, **Calling Number** and **Sub-address** parameters being set to their default values:

- An Adapt instance is bound to an asynchronous serial port (ASY) and the answer ring count (S0) for that serial port is set to 1
- A LAPB instance has its answering parameter set to On
- A PPP instance has its answering parameter set to On

If more than one of these protocols are configured to auto answer then the priority is as follows:

Adapt instances (normally V.120) will take priority over LAPB, which will take priority over PPP. If an Adapt instance is bound to an asynchronous serial port (ASY port) but the answer ring count (ATS0) is not set to 1 for that same serial port then Adapt entity will not answer automatically. If any other protocol entities (such as LAPB, PPP or another Adapt instance) are configured to answer then one of these protocol entities will answer the call. If no other protocol entities are configured to answer then a repeating RING message will be sent out of the serial port and the RS232 ring indicator control will be activated. If a terminal attached to the serial port sends ATA followed by carriage return then the ISDN call will be answered by the Adapt entity and any incoming data will be channeled out of the serial port and vice-versa.

Multiple Subscriber Numbers

An MSN (multiple subscriber number) is an alternative number provided by the telephone service provider which when dialed will also route through to your ISDN line. It is possible to purchase several MSNs for an ISDN line. This means that in effect one ISDN line can have several ISDN numbers.

Every entity in the router which is capable of answering an ISDN call (Adapt, LABP and PPP) has an MSN parameter.

A protocol entity's MSN parameter can be used to:

- Cause a protocol instance not to answer an incoming ISDN call (if the trailing digits of the ISDN number called do not match the entry in this field).

- Increase the answering priority of an instance (if more than one protocol instance is configured to answer and the trailing digits of the ISDN number called match the value of the MSN parameter for a particular protocol instance).

Example

Consider the following:

- An Adapt instance is bound to a serial port and **ATS0** for that serial port is set to **1**.

- PPP instance **0** has answering turned **On**.

- The ISDN line to which the router is connected has two numbers: the main number is **123456** and the MSN number is **123789**.

Normally, because ADAPT has a higher answering priority than PPP, the Adapt instance will answer when either of the numbers are called. However if the ISDN number dialed is **123456** and **456** is entered into the MSN parameter of PPP, PPP will answer instead. This will also have the effect of preventing PPP from answering if any other ISDN number (such as **123457**) has been called.

This means that whenever **123456** is called the PPP instance will answer, and whenever **123789** is called, the V120 instance will answer.

It is possible to connect multiple ISDN devices to the same ISDN line. MSNs can then be used to allow the different ISDN devices to be dialed individually (such as dial the main ISDN number), and get through to ISDN device one, dial the first MSN and get through to ISDN device number two, dial the second MSN, and get through to ISDN device number three, etc.).

Multiple PPP Instances

It is also possible to configure multiple instances of a particular entity to answer. For example, PPP instance, 0, 1 and 4 could be configured to answer. In this case, provided none of the PPP instances are busy, the PPP instance with the highest number will answer first. MSNs can also be used to ensure that a chosen PPP instance answers the call.

The multiple protocol entity answering instance rules are as follow:

Adapt

The lowest free Adapt instance with auto-answering enabled will answer first.

PPP

The lowest free PPP instance with answering on will answer first.

LAPB

The lowest free LAPB instance with answering on will answer first.

Configure ISDN to answer V.120 calls

V.120 is a protocol designed to provide high-speed point-to-point communication over ISDN. It provides rate adaptation and can optionally provide error control. Both the calling and called routers must be configured to use V.120 before data can be transferred. Similarly, if one router is configured to use the error control facility, the other must be configured in the same way.

Initial setup

Before using V.120 you must first bind one of the two available V.120 instances to the required ASY port using the **Configuration > Network > Interfaces > Serial > Protocol Bindings** page or by using the bind command from the command line, for example:

```
bind v120 0 asy 0
```

You should also select the appropriate method of flow control for the ASY port using the **Configuration > Network > Interfaces > Serial > Serial Port n** page or by using the **AT&K** command from the command line. Other ASY port options such as command echo, result code format, etc. should also be configured as necessary.

Initiating a V.120 call

Once the initial configuration is complete, V.120 calls may be initiated using the appropriate **ATD** command. For example:

```
atd01234567890
```

A successful connection will be indicated by a **CONNECT** result code being issued to the ASY port and the router will switch into on-line mode. In this mode, all data from the terminal attached to the bound ASY port will be passed transparently through the router across the ISDN network to the remote system. Similarly, all data from the remote system will be passed directly to the terminal attached to the bound ASY port.

If a V.120 call fails the router will issue the **NO ANSWER** or **NO CARRIER** result code to the ASY port and remain in command mode.

The ATD command may also be used to route a call to an ISDN sub-address by following the telephone number with the letter S and the required sub-address value. For example:

```
atd01234567890s003
```

In this case, the remote system will only answer the call if it has been configured to accept incoming calls on the specified sub-address.

Answering V.120 calls

To enable V.120 answering from the command interface, set register **S0** for the appropriate ASY port to a non-zero value. For example:

```
ats0=1
```

To ensure that you have set S0 for the correct ASY port, either enter it directly on that port or use the **AT\PORT** command to select the correct port first.

The actual value used for the parameter sets the number of rings the router will wait before answering.

Finally, you must ensure that there are no conflicts with other protocols configured to answer on other ASY ports. To do this, disable answering for the other ports/protocols or by using the MSN and/or Sub-address parameters to selectively answer calls to different telephone numbers using different protocols.

For example, if you have subscribed to the ISDN MSN facility, you may have been allocated say four telephone numbers ending in **4**, **5**, **6**, and **7**. You could then set the MSN parameter for the appropriate V.120 instance to **4** to configure V.120 to answer only incoming calls to the MSN number ending in 4.

If PPP answering is enabled, verify that you have **not** selected the same MSN and Sub-address values for PPP. If they are the same, V.120 will answer the call **only** if S0 is set to **1**. Otherwise, PPP will take priority and answer the call.

Configure PSTN interfaces

The the **Configuration > Network > Interfaces > PSTN** section of the web interface is displayed when the router is fitted with an optional internal PSTN MODEM card. When first powered up, navigating to the **Configuration > Network > Interfaces > PSTN** page shows a message indicating that the MODEM card does not have a PPP instance associated with it. Follow the link on the page and select an unassigned PPP interface to the MODEM. When the browser is refreshed and the **Configuration > Network > Interfaces > PSTN** page redisplayed, it should show the parameters described below, along with a message at the top of the page indicating which PPP instance has been selected.

This PSTN interface is using PPP n

Which PPP instance has been assigned to the interface.

Description

A memorable name for the PSTN interface. This may be useful when referring to the interface, rather than having to remember the name and the function of the interface.

Dial out using numbers

The telephone numbers that should be used, in sequence, to make an outgoing connection.

Prefix n to the dial out number

The dialing prefix to use, if needed. This may be necessary when using a PABX.

Username

The username that should be used when using the PPP instance to connect to the remote peer. This is normally provided by an ISP for use with a dial-in Internet access service.

Password

The password to use for authenticating the remote peer and is used in conjunction with the above username.

Confirm password

Type the password into this text box to enable the router to confirm that the password has been entered identically in both boxes.

Allow the remote device to assign a local IP address to this router

When this radio button is selected, the remote peer assigns this PPP interface an IP address.

Try to negotiate a.b.c.d as the local IP address for this router

If it is useful essential to have a predefined IP address for the interface, select the second radio button and enter the desired IP address into the text box to the right. This field is optional.

Use a.b.c.d as the local IP address for this router

If it is essential that the PPP interface has a specific IP address, select this radio button and the IP address entered into the text box.

Use the following DNS servers if not negotiated

Primary DNS server

The IP address of the primary DNS server to use if a DNS server is not assigned as part of the PPP negotiation and connection process. It is fairly common practice for the DNS server to be assigned automatically by the ISP when making a connection.

Secondary DNS server

The IP address of the secondary DNS server to use if one is not automatically assigned by the remote peer.

Attempt to assign the following IP configuration to remote devices

When enabled, reveals the following four configuration parameters which control how the PPP instance assigns an IP address to a connecting remote peer. The primary and secondary DNS server addresses are also sent to the remote peer

Assign remote IP addresses from a.b.c.d to a.b.c.d

The pool of IP addresses to assign to remote peers during the IP protocol configuration phase of the PPP negotiation process.

Primary DNS server

The IP address of the primary DNS server that the remote peer should use when making DNS requests over the link.

Secondary DNS server

The IP address of the secondary DNS server that the remote peer should use when making DNS requests, should the primary server be unavailable.

Allow the PPP interface to answer incoming calls

When enabled, causes the PPP instance to answer an incoming call.

Only allow calling numbers ending with n

When set to answer calls, the value in this text box provides a filter for ISDN sub-addresses. This value is blank by default but when the PPP instance is set to answer calls, only numbers having trailing digits that match the sub-address value in this test will be answered. So for example, if this value is set to 123, only calls from numbers with trailing digits that match this value will be answered. For example 01942 605123.

Enable NAT on this interface

When enabled, enables Network Address Translation to operate on this interface. This is the same as for other PPP interfaces.

IP address/IP address and Port

Select whether IP address translation only should be applied or whether port number translation should also be applied to IP packets.

Enable IPsec on this interface

When enabled, causes the router to encrypt traffic on this interface using the IPsec protocol. The following two additional configuration parameters are revealed when this box is checked.

Keep Security Associations (SAs) when this PSTN interface is disconnected

When enabled, causes the router to maintain (such as not flush) the SA when the interface becomes disconnected. The normal behavior is to remove the SAs when the interface becomes disconnected.

Use interface x,y for the source IP address of IPsec packets

If it is required to use another interface (such as not the interface currently being configured) as the source address for IPsec packets, this may be achieved by selecting the desired interface from the drop-down list and typing the desired interface instance number into the adjacent text box.

Enable the firewall on this interface

When enabled, applies the firewall rules to traffic using this interface.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	name	Up to 25 characters	Description
ppp	n	phonenum	up to 25 digits	Dial out using numbers
ppp	n	ph2	"	"
ppp	n	ph3	"	"
ppp	n	ph4	"	"
ppp	n	prefix	0-9999999999	Prefix n to the dial out number
ppp	n	username	Up to 60 characters	Username
ppp	n	password	Up to 40 characters	Password
ppp	n	IPaddr	0.0.0.0	Allow the remote device to assign a local IP address to this router
ppp	n	IPaddr	Valid IP address a.b.c.d	Try to negotiate a.b.c.d as the local IP address for this router (in conjunction with l_addr)
ppp	n	l_addr	OFF,ON When ON, allows negotiation when OFF force use of specified IP address	Use a.b.c.d as the local IP address of this router
ppp	n	DNSserver	Valid IP address a.b.c.d	Use the following DNS servers if not negotiated Primary DNS server a.b.c.d

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	secDNS	Valid IP address a.b.c.d	Use the following DNS servers if not negotiated Secondary DNS server a.b.c.d
ppp	n	IPmin	Valid IP address a.b.c.d	Assign remote IP addresses from a.b.c.d to a.b.c.d
ppp	n	IPrange	0-255	Assign remote IP addresses from a.b.c.d to a.b.c.d
ppp	n	transDNS	Valid IP address a.b.c.d	Primary DNS server a.b.c.d
ppp	n	sectransDNS	Valid IP address a.b.c.d	Secondary DNS server a.b.c.d
ppp	n	ans	OFF,ON	Allow this PPP interface to answer incoming calls
ppp	n	cingnb	up to 25 digits	Only allow calling numbers ending with n
ppp	n	do_nat	0,1,2 0=Disabled 1=IP address 2=IP address and port	Enable NAT on this interface IP address/IP address and Port
ppp	n	nat_ip	Valid IP address a.b.c.d	NAT Source IP address a.b.c.d
ppp	n	ipsec	0=Disabled 1=Enabled 2=Enabled and Keep SAs	Enable IPsec on this interface/ Keep Security Associations when this PSTN interface is disconnected
ppp	n	firewall	OFF,ON	Enable the firewall on this interface

Advanced PSTN parameters

Metric

The route metric that should be applied to this interface. See PPP parameters on page 293 for more detail.

Enable "Always On" mode of this interface

When enabled, causes the following two options to appear.

On/On and return to service immediately

Select whether the always-on functionality should simply be enabled or whether the additional facility to return the interface to the In Service state should be applied.

Put this interface "Out of Service" when an always-on connection attempt fails

Normally, always-on interfaces do not go out of service unless they have connected at least once. When checked, this checkbox causes the router to put the interface out of service even if the first connection attempt fails.

Attempt to re-connect after s seconds

The length of time in seconds that the router should wait after an always-on PPP connection has been terminated before trying to re-establish the link.

If an inhibited PPP interface is connected, attempt to re-connect after s seconds

The value in this text box takes precedence over the previous parameter when another PPP instance that is usually inhibited by this one is connected. This parameter would typically be used to reduce the connection retry rate when a lower priority PPP instance is connected.

Wait s seconds after power-up before activating this interface

The initial delay that the router applies before activating the PPP instance after power-up. After the initial power-up delay the normal always-on activation timers apply. If set to zero, no delay will be applied.

Control when this interface can connect using Time band n

These two controls, the check box and drop-down list, determine whether the Time Band function should be applied to this interface. Checking the checkbox enables the functionality and the desired time band instance is selected from the drop-down list. Time Band functionality is explained in the Configure time bands on page 488 section.

Keep this interface up for at least s seconds

The minimum period that the PPP interface should remain available. This means that even if the link becomes inactive before this period expires, the connection remains open.

Close this interface

After s seconds

The maximum time that the link remains active in any one session. After this time, the link is deactivated.

If it has been up for m minutes in a day

The router deactivates the PPP instance after it has been active for the value specified in this text box.

If the link has been idle for s seconds

The router deactivates this interface after the time specified in this text box if it detects that the link has not passed any traffic for that period.

Alternative idle timer for static routes s seconds

An alternative inactivity timeout for use in conjunction with the Make PPP n interface use the alternative idle timeout when this route becomes available parameter on the **Configuration > Network > IP Routing/Forwarding > Static Routes > Routes n > Advanced** web page. This timeout will only be used until the PPP instance next deactivates. After that the normal timeout value is used.

If the link has not received any packets for s seconds

The amount of time that the router will wait without receiving any PPP packets before disconnecting. The timer is reset with each received PPP packet.

If the negotiation is not complete in s seconds

The maximum time, in seconds, allowed for the PPP negotiation to complete. If negotiations have not completed within this period, the interface is deactivated.

Generate an event after this interface has been up for m minutes

The number of minutes, if any, after which the router should create an event in the event log that states that the interface has been active for this period.

Limit the data transmitted over this interface

When enabled, displays the following parameters that control what data volume restrictions (if any) should be applied to this interface.

Issue a warning event after n units

The amount of traffic which causes a warning event to be generated in the event log stating that the specified amount of data has been transferred. The units are specified by a drop-down list, with the options of kilobytes, megabytes, gigabytes. For example, if the monthly tariff includes up to 5MB of data before excess usage charges are levied, it would be useful to set this threshold to 4MB. This would cause the router to create a warning entry in the event log once 4MB of data had been transferred. This event could then be used to trigger an email alert, SNMP trap or SMS alert message.

Stop data from being transmitted after n units

The total amount of data that may be transmitted by this PPP instance before the link is blocked for further traffic, and the value in the drop-down list specifies the units, which are **kilobytes**, **megabytes**, and **gigabytes**.

Reset the data limit on the n day of the month

The day of the month on which the data limit is reset to zero.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	metric	0-255	Metric
ppp	n	aodion	0-2 0=disabled 1=enabled 2=On and return to service immediately	Enable "Always On" mode of this interface, On, On and return to service immediately
ppp	n	immoos	ON, OFF	Put this interface "Out of Service" when an always-on connection attempt fails
ppp	n	aodi_dly	0-2147483647	Attempt to reconnect after s seconds
ppp	n	aodi_dly2	0-2147483647	If an inhibited PPP interface is connected, attempt to re-connect after s seconds
ppp	n	pwr_dly	0-2147483647	Wait s seconds after power-up before activating this interface
ppp	n	tband	0-4	Control when this interface can connect using Time Band n
ppp	n	minup	0-2147483647	Keep this interface up for at least s seconds
ppp	n	maxup	0-2147483647	Close this interface after s seconds
ppp	n	maxuptime	0-2147483647	if it has been up for m minutes in a day
ppp	n	timeout	0-2147483648	if the link has been idle for s seconds
ppp	n	timeout2	0-2147483648	Alternative idle timer for static routes s seconds
ppp	n	rxtimeout	0-2147483648	if the link has not received any packets for s seconds
ppp	n	maxneg	0-2147483648	if the negotiation is not complete in s seconds
ppp	n	uplogmins	0-2147483647	Generate an event after this interface has been up for m mins
ppp	n	dlwarnkb	0-2147483647	Issue a warning after n units

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	dlstopkb	0-2147483647	Stop data from being transmitted after n units
ppp	n	dlrstday	0-255	Reset the data limit on the n day of the month

Configure DialServ interfaces

The Dialserv option module mimics a telephone exchange in that it supplies the required voltages on the line, generates a **RING** signal and has off-hook detection circuitry. It can be used to provide similar functionality to dialing into an ISP using an analogue MODEM. The card also contains an analogue MODEM to handle data on the line.

Use PPP/Protocol Switch

These radio buttons select whether the DialServ card uses a PPP instance or the protocol switch functionality to control traffic on the interface. If PPP is selected, the web page expands to reveal the standard PPP configuration settings. If Protocol Switch is selected, only the four settings described immediately below are visible.

Max time to RING line s seconds

The maximum number of seconds that the **RING** signal should be generated for.

RING frequency n Hz

The DialServ module generates a **RING** signal. The frequency of the **RING** is selected from this drop-down list. The available options are:

- **20Hz**
- **25Hz**
- **30Hz**
- **40Hz**
- **50Hz**

Initialisation string 1

The text string in this text box contains any required MODEM initialization commands.

Initialisation string 2

The text string in this text box contain initialization commands that will be issued to the MODEM after the first initialization string.

DialServ Network Settings parameters

The DialServ card may be configured to use PPP as the protocol to connect to the remote peer and as such should be assigned a free PPP instance to use as part of the configuration. If no PPP instance has been assigned and the module has been configured to use PPP, a link to the PPP mappings page and message appear.

If a PPP instance has been assigned, the following configuration options appear:

This DialServ interface is using PPP n

Which PPP instance (n) is being used by the DialServ card.

Description

A short string that describes the interface and is used as a convenience when referring to the interface.

Dial out using numbers

The telephone numbers that should be used, in sequence, to make an outgoing connection. These can be used to provide a dialback facility.

Prefix n to the dial out number

The dialing prefix to use, if needed. This may be necessary when using a PABX.

Username

The username that should be used when using the PPP instance to connect to the remote peer.

Password

The password to use for authenticating the remote peer and is used in conjunction with the above username.

Confirm Password

Type the password into this text box to enable the router to confirm that the password has been entered identically in both boxes.

Allow the remote device to assign a local IP address to this router

When this radio button is selected, the remote peer will assign this PPP interface an IP address.

Try to negotiate a.b.c.d as the local IP address for this router

If it would be useful, but not essential, to have a predefined IP address for the interface, the second radio button should be selected and the desired IP address entered into the text box to the right.

Use a.b.c.d as the local IP address for this router

If it is essential that the PPP interface has a specific IP address, this radio button should be selected and the IP address entered into the text box.

Use the following DNS servers if not negotiated

Primary DNS server

The IP address of the primary DNS server to use if a DNS server is not assigned as part of the PPP negotiation and connection process. It is fairly common practice for the DNS server to be assigned automatically by the ISP when making a connection.

Secondary DNS server

The IP address of the secondary DNS server to use if one is not automatically assigned by the remote peer.

Attempt to assign the following IP configuration to remote devices

When enabled, displays the following four configuration parameters that control how the PPP instance assigns an IP address to a connecting remote peer. The primary and secondary DNS server addresses will also be sent to the remote peer

Assign remote IP addresses from a.b.c.d to a.b.c.d

The IP addresses in these text boxes define the pool of IP addresses to assign to remote peers during the IP protocol configuration phase of the PPP negotiation process.

Primary DNS server

The IP address of the primary DNS server the remote peer should use when making DNS requests over the link.

Secondary DNS server

The IP address of the secondary DNS server that the remote peer should use when making DNS requests, should the primary server be unavailable.

Allow the PPP interface to answer incoming calls

When enabled, causes the PPP instance to answer an incoming call.

Only allow calling numbers ending with n

When the router is set to answer calls, this setting provides a filter for ISDN sub-addresses. This value is blank by default but when the PPP instance is set to answer calls, only numbers having trailing digits that match the sub-address value in this test will be answered. For example, if this value is set to **123**, only calls from numbers with trailing digits that match this value will be answered; for example, **01942 605123**.

Enable NAT on this interface

When enabled, enables Network Address Translation to operate on this interface. This is the same as for other PPP interfaces.

IP address/IP address and Port

Select whether IP address translation only should be applied or whether port number translation should also be applied to IP packets.

Enable IPsec on this interface

When enabled, causes the router to encrypt traffic on this interface using the IPsec protocol. The following two additional configuration parameters are revealed when this box is checked.

Keep Security Associations (SAs) when this PSTN interface is disconnected

When enabled, causes the router to maintain (such as not flush) the SA when the interface becomes disconnected. The normal behavior is to remove the SAs when the interface becomes disconnected.

Use interface x,y for the source IP address of IPsec packets

If it is required to use another interface (such as not the interface currently being configured) as the source address for IPsec packets, this may be achieved by selecting the desired interface from the drop-down list and typing the desired interface instance number into the adjacent text box.

Enable the firewall on this interface

When enabled, applies the firewall rules to traffic using this interface.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	name	Up to 25 characters	Description
ppp	n	phonenum	up to 25 digits	Dial out using numbers
ppp	n	ph2	"	Dial out using numbers
ppp	n	ph3	"	Dial out using numbers
ppp	n	ph4	"	Dial out using numbers
ppp	n	prefix	0-9999999999	Prefix
ppp	n	username	Up to 60 characters	Username
ppp	n	password	Up to 40 characters	Password
ppp	n	IPaddr	0.0.0.0	Allow the remote device to assign a local IP address to this router
ppp	n	IPaddr	Valid IP address a.b.c.d	Try to negotiate a.b.c.d as the local IP address for this router (in conjunction with l_addr)
ppp	n	l_addr	OFF,ON When ON, allows negotiation when OFF force use of specified IP address	Use a.b.c.d as the local IP address for this router (not negotiable)
ppp	n	DNSserver	Valid IP address a.b.c.d	Primary DNS server
ppp	n	secDNS	Valid IP address a.b.c.d	Secondary DNS server
ppp	n	IPmin	Valid IP address a.b.c.d	Assign remote IP addresses from a.b.c.d to a.b.c.d
ppp	n	IPrange	0-255	Assign remote IP addresses from a.b.c.d to a.b.c.d
ppp	n	transDNS	Valid IP address a.b.c.d	Primary DNS server a.b.c.d

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	sectransDNS	Valid IP address a.b.c.d	Secondary DNS server a.b.c.d
ppp	n	ans	OFF,ON	Allow this PPP interface to answer incoming calls
ppp	n	do_nat	0,1,2 0=Disabled 1=IP address 2=IP address and port	Enable NAT on this interface IP address/IP address and Port
ppp	n	natip	Valid IP address a.b.c.d	NAT Source IP address a.b.c.d
ppp	n	ipsec	0=Disabled 1=Enabled 2=Enabled and Keep SAs	Enable IPsec on this interface/ Keep Security Associations when this DialServ interface is disconnected
ppp	n	firewall	OFF,ON	Enable the firewall on this interface

Advanced DialServ parameters

Metric

The route metric that should be applied to this interface. For more information, see the PPP parameters on page 293 sections.

Enable "Always On" mode of this interface

When enabled, the following two options are displayed:

On/On and return to service immediately

Select whether the always-on functionality should simply be enabled or whether the additional facility to return the interface to the In Service state should be applied.

Put this interface "Out of Service" when an always-on connection attempt fails.

Normally, always-on interfaces do not go out of service unless they have connected at least once. When checked, this checkbox causes the router to put the interface out of service even if the first connection attempt fails.

Attempt to re-connect after s seconds

The length of time, in seconds, the router should wait after an "always-on" PPP connection has been terminated before trying to re-establish the link.

If an inhibited PPP interface is connected, attempt to re-connect after s seconds

This setting takes precedence over the previous parameter when another PPP instance that is usually inhibited by this one is connected. This parameter would typically be used to reduce the connection retry rate when a lower priority PPP instance is connected.

Wait s seconds after power-up before activating this interface

The initial delay that the router will apply before activating the PPP instance after power-up. After the initial power-up delay the normal always-on activation timers apply. If set to zero, no delay will be applied.

Control when this interface can connect using Time band n

These two controls, the check box and drop-down list, determine whether the Time Band function should be applied to this interface. Checking the checkbox enables the functionality and the desired time band instance is selected from the drop-down list. Time Band functionality is explained in the Configure time bands on page 488 section of this manual.

Keep this interface up for at least s seconds

The minimum period that the PPP interface should remain available. This means that even if the link becomes inactive before this period expires, the connection will remain open.

Close this interface

after s seconds

The maximum time that the link will remain active in any one session. After this time, the link will be deactivated.

If it has been up for m minutes in a day

The router deactivates the PPP instance after it has been active for the value specified in this text box.

If the link has been idle for s seconds

The router deactivates this interface after the time specified in this text box if it detects that the link has not passed any traffic for that period.

Alternative idle timer for static routes s seconds

An alternative inactivity timeout for use in conjunction with the **Make PPP n interface use the alternative idle timeout when this route becomes available** parameter on the **Configuration > Network > IP Routing/Forwarding > Static Routes > Routes n > Advanced** web page. This timeout will only be used until the PPP instance next deactivates. After that the normal timeout value is used.

If the link has not received any packets for s seconds

The amount of time that the router will wait without receiving any PPP packets before disconnecting. The timer is reset with each received PPP packet.

If the negotiation is not complete in s seconds

The maximum time, in seconds, allowed for the PPP negotiation to complete. If negotiations have not completed within this period, the interface is deactivated.

Generate an event after this interface has been up for m minutes

The number of minutes, if any, after which the router should create an event in the event log that states that the interface has been active for this period.

Limit the data transmitted over this interface

When enabled, displays the following parameters that control what data volume restrictions, if any, should be applied to this interface:

Issue a warning event after n units

The amount of traffic that will cause a warning event to be generated in the event log stating that the specified amount of data has been transferred. The units are specified by a drop-down list, having the following options; **KBytes**, **MBytes**, **GBytes**. For example, if the monthly tariff includes up to 5MB of data before excess usage charges are levied, it would be useful to set this threshold to 4MB. This would cause the router to create a warning entry in the event log once 4MB of data had been transferred. This event could then be used to trigger an email alert, SNMP trap or SMS alert message.

Stop data from being transmitted after n units

The total amount of data that may be transmitted by this PPP instance before the link is blocked for further traffic, and the value in the drop-down list specifies the units which are; **KBytes**, **MBytes**, **GBytes**.

Reset the data limit on the n day of the month

The day of the month on which the data limit is reset to zero.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	metric	0-255	Metric
ppp	n	aodion	0-2 0=disabled 1=enabled 2=On and return to service immediately	Enable "Always On" mode of this interface, On, On and return to service immediately
ppp	n	immoos	ON, OFF	Put this interface "Out of Service" when an always-on connection attempt fails
ppp	n	aodi_dly	0-2147483647	Attempt to reconnect after s seconds
ppp	n	aodi_dly2	0-2147483647	If an inhibited PPP interface is connected, attempt to re-connect after s seconds
ppp	n	pwr_dly	0-2147483647	Wait s seconds after power-up before activating this interface
ppp	n	tband	0-4	Control when this interface can connect using Time Band n
ppp	n	minup	0-2147483647	Keep this interface up for at least s seconds
ppp	n	maxup	0-2147483648	Close this interface after s seconds
ppp	n	maxuptime	0-2147483647	if it has been up for m minutes in a day
ppp	n	timeout	0-2147483648	if the link has been idle for s seconds
ppp	n	timeout2	0-2147483648	Alternative idle timer for static routes s seconds
ppp	n	rxtimeout	0-2147483648	if the link has not received any packets for s seconds
ppp	n	maxneg	0-2147483648	if the negotiation is not complete in s seconds
ppp	n	uplogmins	0-2147483647	Generate an event after this interface has been up for m mins
ppp	n	dlwarnkb	0-2147483647	Issue a warning after n units

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	dlstopkb	0-2147483647	Stop data from being transmitted after n units
ppp	n	dlrstday	0-255	Reset the data limit on the n day of the month

Configure serial interfaces

Digi routers support a variety of serial interfaces, either inbuilt or as optional add-on modules. Each asynchronous serial (ASY) port may be configured to operate at different speed, data format etc. These parameters may be changed using the web interface or from the command line using AT commands and S registers.
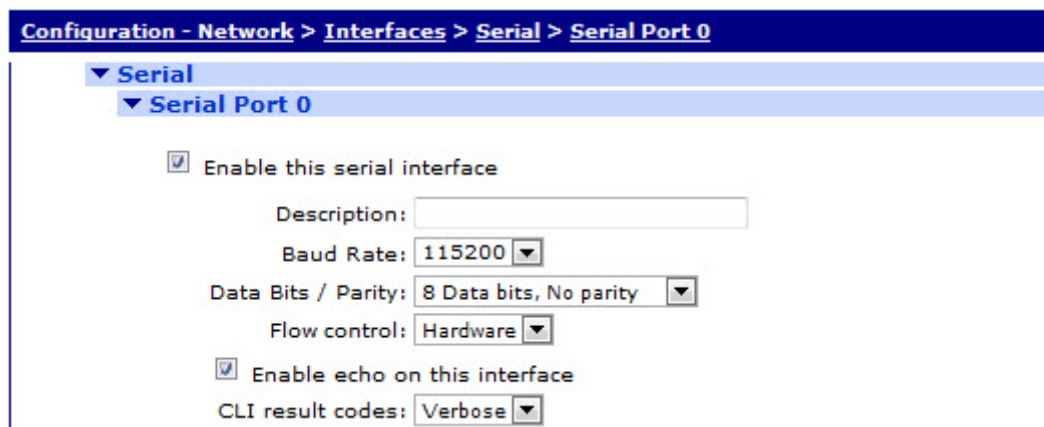
The **Configuration > Network > Interfaces > Serial** menu item opens out when clicked, to show the list of supported serial interfaces.

Note On models fitted with W-WAN modules, one of the interfaces (and its associated web page) will be dedicated to the W-WAN module. The title will reflect this. Similarly, on models fitted with an analogue MODEM, one of the interfaces will be entitled PSTN port.

This section describes the basic configuration of a serial port.

Enable this serial interface

When disabled, this is the only item that appears in the section. Enabling this setting displays additional configuration parameters.

Description

A description for the interface. For example, if the serial interface is connected to a card payment device, the description could read **Till 1** or similar appropriate text.

Baud Rate

The required baud rate for the associated serial port.

Data Bits / Parity

The required data format for the interface. 8 data bits, no parity is a very common configuration.

Note When the serial port is not in 8-bit parity mode (such as it is in either 8-bit no parity, or 7-bit with parity), the router will continually check for parity when receiving AT commands and adjust and match accordingly.

Flow Control

The router supports software flow control using **XON/XOFF** characters and hardware flow control using the RS232 **RTS** and **CTS** signals. Use this drop-down list to select **Software**, **Hardware** or a combination of **Both**. To disable flow control, select the **None** option.

Enable echo on this interface

When enabled, enables command echo when using the command line interpreter. Disable this setting if the attached terminal provides local echo.

CLI result codes

The required level of verbosity for command result codes. The available options are:

- **Verbose**
- **Numeric**
- **None**

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
asy	n/a	descr	Free text-description of interface	Description
S31=n	n/a	n/a	Where n= 3=115200 4=57600 5=38400 6=19200 7=9600 8=4800	Baud rate
S23=n	n/a	n/a	Where n= 0=None 1=Odd 2=Even 5=8 Data Odd 6=8 Data Even Default 0	Data Bits / Parity
&Kn	n/a	n/a	Where n = 0=None 1=Hardware 2=Software 3=Both	Flow Control
&En	n/a	n/a	Where n = 0=No echo 1=echo	Enable echo on this interface
&Vn	n/a	n/a	Where n = 0=numeric 1=verbose	CLI result codes

Advanced Serial Port parameters

The configuration parameters in this section are changed less frequently than those in the basic section and so are given a separate page in order to reduce screen clutter.

Answer V.120 calls after n rings (0 = Don't answer)

Controls the answering of incoming V.120 calls. When set to zero, V.120 answering is disabled, otherwise V.120 answering is enabled on this interface. Enter the number of rings to wait before answering the call into this text box. This is equivalent to setting the value of the **S0** register for the associated serial port.

DCD

Selects how the Data Carrier Detect (**DCD**) signal is controlled. The available options are:

- **Auto**: Configures the router so that it will only assert the **DCD** line when an ISDN connection has been established; this is equivalent to **AT&C1**.

- **On**: Configures the router such that the **DCD** line is always asserted when the router is powered-up; this is equivalent to **AT&C0**.

- **Off**: Configures the router such that the **DCD** line is normally asserted but is de-asserted for the time period specified by the **S10** register after a call is disconnected; this is equivalent to **AT&C2**.

- **Pulse Low**

DTR Control

This drop-down selection box controls how the router responds to the **DTR** signal. The available options are:

- **None:** Configures the router to ignore the **DTR** signal; this is equivalent to **AT&D0**.

- **Drop call**: Configures the router to disconnect the current call and return to AT command mode when the **DTR** signal from the attached terminal (DTE) is de-asserted; this is equivalent to **AT&D1**.

- **Drop line and call**: Configures the router to disconnect the current call, drop the line and return to AT command mode when the **DTR** signal is de-asserted; this is equivalent to **AT&D2**.

- **Drop call on transition**

- **Drop line and call on transition**

DTR de-bounce time s x 20 milliseconds

The length of time (in multiples of 20ms) for which the DTR signal must be de-asserted before the router acts on any options that are set to trigger on loss of this signal. Enter the desired multiple into the text box. Increasing this value makes the router less sensitive to "bouncing" of the DTR signal. Conversely, decreasing this value makes the router more sensitive. The default of **100ms** (5 times 20ms) is a reasonable value.

Escape Character

The character used in the escape sequence. The default is the **+** symbol (ASCII value **43**, **0x2b**). Changing this value has the same effect as changing the **S2** register.

Escape Delay s x 20 milliseconds

The required minimum length of the pause (in multiples of 20ms) in the escape sequence. The default is **50 x 20ms,** which means that the escape sequence becomes **+++**, a pause of 1 second and then **AT,** to drop back to AT command mode. If a delay of some other value is required, enter it in the text box.

Forwarding Timeout s x 10 milliseconds

The length of time that the router will wait for more data after receiving at least one octet of data through the serial port and transmitting it onwards. This timer is reset each time more data is received. The router will forward data onwards when either the forwarding timer expires or the input buffer becomes full. This parameter applies to ADAPT, TCPDIAL, TCPPERM and PANS.

Break Transmit Escape Character c

The character used in the escape sequence. The **-** symbol (ASCII value **45**, **0x2d**) is a recommended value. Changing this value has the same effect as changing the S3 register. To use the break sequence, type **-** 3 times, with a 1-second pause either side of the 3 **-** characters. When the Async port detects the following sequence:

```
<guard time 1 sec>---<guard time 1 sec>
```

Instead of outputting the three minus characters (they are removed from the output stream), a **BREAK** condition is placed on the Async transmitter for 1 second.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
S0=n	n/a	n/a	Where n= 0-255	Answer V.120 call after n rings
&Cn	n/a	n/a	Where n = 0=On 1=Auto 2=Off 3=Pulse low	DCD
&Dn	n/a	n/a	Where n = 0=None 1=Drop line 2=Drop line & call 5=Drop call on transition 6=Drop line & call on transition	DTR
S45=n	n/a	n/a	Where n= 0-255	DTR de-bounce
S2=n	n/a	n/a	Where n= ASCII value	Escape Character
S12=n	n/a	n/a	Where n= 0-255	Escape delay
S15=n	n/a	n/a	Where n= 0-255	Forwarding Timeout
S3=n	n/a	n/a	Where n= ASCII value	Break Transmit Escape Character

Profiles

> ▶ **Advanced**
>
> Each serial port can have two profiles which can be configured differently.
> You can configure which profile is used at power-up.
>
> Use profile `0 ▼` at power-up
> `Load Config from Profile` `0 ▼`
> `Apply & Save Changes to Profile` `0 ▼`
>
> `Apply`

Each serial port can have two profiles which can be configured differently. Which profile is in force when the router powers-up is selected here.

Power-up profile n

Select **0** from the drop-down selection box to choose profile **0** to be active when the router powers-up. Select **1** from the selection box to make profile **1** the active profile.

Load Profile n

Select **0** from the drop-down selection box and click the button to load profile **0**.

Save Profile

Select **0** from the drop-down selection box and click the button to save profile **0** after making any changes.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
&Yn			Where n = 0,1	Power-up profile n
&Zn			Where n = 0,1	Load Profile n
&Wn			Where n = 0,1	Save Profile n

Sync parameters

The most common form of serial communications these days is asynchronous. Synchronous serial communications links are still in use, and Digi routers can support these. HDLC is a synchronous protocol that is still in use and can be used with Digi routers. This section describes how to configure the synchronous communications interfaces. To enable synchronous mode, a protocol such as LAPB must be configured to use a synchronous port as its lower layer interface. On certain models, an informational message will appear on the web page which states that jumper settings may need to be changed in order to support synchronous serial operation.

Note The number of synchronous serial ports available varies depending on the model and any optional modules fitted.

Description

A description of the interface, should one be required.

Clock source Internal / External

Select between internal or external clock sources for the interface.

Mode

The specific serial protocol to use. Which buttons appear depend upon the capabilities of the interface. The options available are; **V.35**, **EIA530**, **RS232**, **EIA530A**, **RS449**, and **X.21**.

Invert RX clock

When enabled, causes the router to invert the voltage level of the receive clock signal.

Invert TX clock

When enabled, causes the router to invert the voltage level of the transmit clock signal.

Encoding NRZ / NRZI

Select between non-return to zero (NRZ) and non-return to zero (inverted) (NRZI) signal encodings.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
sy	0	descr	Text description of interface	Description
sy	0	clksrc	int,ext	Clock source
sy	0	rxclkinv	OFF,ON	Invert RX clock
sy	0	txclkinv	OFF,ON	Invert TX clock
sy	0	encode	nrz,nrzi	Encoding

Rate Adaption parameters

The router supports two rate adaptation protocol (Adapt) instances. Each instance enables the selection and configuration of the protocol to be used for rate adaptation over an ISDN B channel. The supported protocols are; V.110, V.120 and X.75. Depending on which protocol is selected, there may be an associated LAPB instance (distinct from the two general purpose LAPB instances), as for example, when V.120 is used in error-corrected (multi-frame) mode. Clicking the triangle at the left of the blue bar opens up the two instances described below.

This page displays the configuration parameters directly relevant to the rate adaptation protocol only, LAPB configuration pages are to be found here in the **Configuration > Network > Legacy Protocols > X.25 > LAPB** page. When configuring LAPB parameters, be aware that LAPB 2 is used for adapt 0 and LAPB 3 is used for adapt 1.

Attempt to redial the connection n times if rate adaption has not been negotiated

If an ISDN connection is established, but rate adaption is not negotiated, the value in this text box specifies how many times the router should drop the connection and redial it.

Drop the connection if it is idle for h hrs m mins s secs

The time to wait before dropping the connection if the connection becomes idle.

Leased line mode

When enabled, allows the router to attempt to maintain the connection automatically once it has been established.

Enable TCP rate adaption

When enabled, enables use of rate adaptation when using a TCP connection rather than an ISDN line. When enabled, the following controls become enabled:

Connect to IP Address a.b.c.d Port n

When using a TCP connection, these text entry boxes allow the user to specify the IP address and port number that the protocol should use.

Listen on Port

The port number that the router is listening on when in socket mode.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
adapt	0,1	dial_retries	0-255	Attempt to redial the connection n times
adapt	0,1	tinact	0-86400	Drop the connection if it is idle for h hrs m mins s secs
adapt	0,1	leased_line	OFF,ON	Leased line mode
adapt	0,1	sockmode	0,1 0=disable 1=enable	Enable TCP rate adaption
adapt	0,1	ip_addr	valid IP address a.b.c.d	Connect to IP Address a.b.c.d Port n
adapt	0,1	ip_port	valid TCP port number	Connect to IP Address a.b.c.d Port n
adapt	0,1	lip_port	valid TCP port number	Listen on Port n

Command Mappings parameters

The router supports a number of command aliases which specify strings to be substituted for commands entered at the command line. The table on this page contains two text entry boxes and an **Add** button. Up to 23 command mappings may be specified. An example may make this clear. Suppose, a user coming from a Unix™ background feels more comfortable typing **ls** rather than the native **dir** command in order to list the files in a directory. To achieve this aliasing, enter **ls** into the **From** column in the table, **dir** into the **To** column and then click the **Add** button.

From

The substitute text.

To

The command that should be substituted.

Add

Click this button to add the command mapping.

Delete

When the mapping has been added, a **Delete** button is enabled in the right-hand column. Clicking this button removes the binding from the table.

Note If either string contains spaces, the entire string must be enclosed within double quotation marks. When substituting a command, upper case characters are considered the same as the corresponding lower case characters.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
cmd	n	cmdmapi	Replacement command	From
cmd	n	cmdmapo	Command to be substituted	To

Protocol Bindings parameters

Digi routers are soft configurable to allow different protocols to be used on different interfaces. The process of selecting which protocol will be used on a particular interface is referred to as binding. So, for example Serial (ASY) port 0 may be used for an ISDN B channel X.25 connection in which case PAD 0 would be bound to Serial 0 (assuming that PAD 0 is the required PAD). (To complete this example, it would also be necessary to associate the PAD with a LAPB instance using the appropriate page). Protocols are bound to serial interfaces using a table with a drop-down list box for selecting the protocol and a drop-down list for selecting the serial port.

By default, if no specific protocol has been bound to a serial interface, a PPP instance will automatically be associated with that port. This means that PPP is treated as the default protocol associated with the serial ports.

Protocol

Select the desired protocol from this drop-down list.

Bound to

Select the desired serial port from this drop-down list.

Add

Click this button to add the binding.

Delete

When a binding has been added, it appears in the table and a **Delete** button is enabled in the right-hand column. Click this button to remove the binding. Note that the binding does not come into force until the **Apply** button at the bottom of the page has been clicked.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
bind	n	prot1	Valid protocol, such as PAD 0	Protocol
bind	n	id1	Valid serial port such as ASY 5	Bound to

To display a list of the current bindings enter the command:

`bind ?`

Command line examples:

`bind pad 0 asy 0`

`binds PAD 0 to serial port 0.`

`bind v120 0 asy 3`

`binds V.120 instance 0 to asynchronous serial port 3.`

To access the Internet using PPP via a terminal connected to serial interface **2**, enter the command:

bind ppp 1 asy 2

Currently it is only possible to bind a TANS instance to an ADAPT instance using the bind command. The format of the command is:

`bind adapt <instance> tans <instance>`

TRANSIP Serial Ports parameters

TransIP is a way of using virtual serial ports for serial connections over an IP socket, in effect multiplying the number of concurrent serial connections to a router. TransIP can be configured to actively connect on a TCP socket (such as make outgoing connections). The message at the top of this page states which serial interface is being used for the TransIP connection.

```
▼ TRANSIP Serial Ports
    ▼ Transip 0
        This TransIP is using Serial port 11
                          Listen on port: 0
        Connect to IP Address or Hostname: [            ]  Port  0
                 Send TCP Keep-Alives every: 0        seconds
        ☐ Enable Stay Connected mode
        ☐ Disable command echo
                            Escape char: 0
                           Escape delay: 0        milliseconds


        [ Apply ]
```

Listen on port n

The TCP port number that the router should listen on.

Connect to IP Address or Hostname a.b.c.d Port n

The IP address or hostname text entry box should contain a valid IP address or the hostname which the router should use to make the outgoing TransIP connection.
If this parameter is set (such as non-zero), the number defined the TCP port number to use when making TCP socket connections. When set to **0**, TransIP is listening only on the port defined above.

Send TCP Keep-Alives every s seconds

The amount of time, in seconds, a connection stays open without any traffic being passed.

Enable Stay Connected mode

When enabled, causes the router to refrain from clearing the TCP socket at the end of a transaction, data call or data session (depending on what the TansIP serial port was bound to and what protocol it was using). Leaving this checkbox unchecked allows the router to clear the socket. For example, if the TransIP port is bound to a TPAD and the box is unchecked, the TransIP TCP socket will be cleared at the end of the TPAD transaction.

Disable command echo

When enabled, command echo for the TransIP port is disabled. When unchecked, all commands issued are echoed back to the TransIP TCP socket.

Escape char c

The ASCII character used as the escape character which is by default **+**. Entering this escape character three times followed by a pause of at least the **Escape delay** parameter below and then an **AT** command will cause the router to switch back to command mode from online mode. This is equivalent to the **S2** register setting.

Escape delay s milliseconds

The delay required between entering the escape sequence (default **+++**) and the **AT** command for the router to drop back into command mode. This is equivalent to the **S12** register setting.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
transip	n	port	Valid port number 0-65535	Listen on port
transip	n	host	Valid IP address a.b.c.d or hostname	Connect to IPaddress a.b.c.d or Hostname
transip	n	remport	Valid port number 0-65535	Port
transip	n	keepact	0-255	Send TCP Keep-Alives every s seconds
transip	n	staycon	ON,OFF	Enable Stay Connected mode
transip	n	cmd_echo_off	ON,OFF	Disable command echo
transip	n	escchar	Valid ASCII character	Escape char c
transip	n	esctime	0-255	Escape delay s milliseconds

RealPort parameters

Digi devices use the patented RealPort COM/TTY port redirection for Microsoft Windows.

RealPort software provides a virtual connection to serial devices, no matter where they reside on the network. The software is installed directly on the host PC and allows applications to talk to devices across a network as though the devices were directly attached to the host. Actually, the devices are connected to a Digi device somewhere on the network. RealPort is unique among COM port re-directors because it is the only implementation that allows multiple connections to multiple ports over a single TCP/IP connection. Other implementations require a separate TCP/IP connection for each serial port. Unique features also include full hardware and software flow control, as well as tunable latency and throughput. Access to RealPort services can be enabled or disabled.

Encrypted RealPort

Digi devices also support RealPort software with encryption. Encrypted RealPort offers a secure Ethernet connection between the COM or TTY port and a device server or terminal server.

Encryption prevents internal and external snooping of data across the network by encapsulating the TCP/IP packets in a Secure Sockets Layer (SSL) connection and encrypting the data using Advanced Encryption Standard (AES), one of the latest, most efficient security algorithms. Access to Encrypted RealPort services can be enabled or disabled. Digi's RealPort with encryption driver has earned Microsoft's Windows Hardware Quality Lab (WHQL) certification. Drivers are available for a wide range of operating systems, including Microsoft Windows Server 2003, Windows XP, Windows 2000, Windows NT, Windows 98, Windows ME; SCO Open Server; Linux; AIX; Sun Solaris SPARC; Intel; and HP-UX. It is ideal for financial, retail/point-of-sale, government or any application requiring enhanced security to protect sensitive information.

Enable RealPort

Enables RealPort on the router.

Listen on port

The TCP port on which the router will listen for RealPort connections.

Maximum number of sockets

The maximum number of RealPort connections that the router will support.

Enable encrypted RealPort

Selecting this option enables encrypted RealPort on the router.

Encryption mode to listen on port

The TCP port on which the router will listen for encrypted RealPort connections.

Maximum number of encryption sockets

The maximum number of encrypted RealPort connections that the router will support.

Enable Device Initiated RealPort

Selecting this option enables router to make a RealPort connection to a host PC.

Connect to host a.b.c.d Port n

The IP address or hostname and TCP port that the router should use when making a device initiated connection.

Allow s seconds between connection attempts

The interval, in seconds, between device initiated connection attempts.

Send TCP Keep-Alives every s seconds

The interval at which TCP Keep-Alives are sent over the RealPort connection. A value of **0** means that Keep-Alives are not sent.

Send RealPort Keep-Alives every s seconds

The interval at which RealPort Keep-Alives are sent over the RealPort connection. A value of **0** means that Keep-Alives are not sent.

Enable exclusive mode

Enables exclusive mode. Exclusive mode allows a single connection from any one RealPort client ID to be connected only. If this setting is enabled and a subsequent connection occurs that has the same source IP as an existing connection, the old existing connection is forcibly reset under the assumption that it is stale.

Enable authentication

Enables RealPort authentication.

Authentication secret

Configures the RealPort authentication secret.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
rport	0	enabled	OFF,ON	Enable RealPort
rport	0	ipport	0-65535	Listen on port
rport	0	maxnbsocks	0-255	Maximum number of sockets
rport	0	encryption	OFF,ON	Enable encrypted RealPort
rport	0	encport	0-65535	Encryption mode to listen on port
rport	0	maxnbencsocks	0-255	Maximum number of encryption sockets
rport	0	initiate	OFF,ON	Enable Device Initiated RealPort
rport	0	IPaddr	Valid IP address a.b.c.d	Connect to host a.b.c.d Port n
rport	0	initiateport	0-65535	Connect to host a.b.c.d Port n
rport	0	initiatebackoff	0-255	Allow s seconds between connection attempts
rport	0	tcpkeepalives	0-255	Send TCP Keep-Alives every s seconds
rport	0	rportkeepalives	0-255	Send RealPort Keep-Alives every s seconds
rport	0	exclusive	OFF,ON	Enable exclusive mode
rport	0	auth	OFF,ON	Enable authentication
rport	0	secret	Up to 30 characters	Authentication secret

MultiTX parameters

The **MultiTX** page is for enabling and setting the MultiTX parameters. This page supports sending serial data to multiple (up to 5) TCP or UDP destinations. When enabled, the configured ASY port is opened and serial data from the port is sent to all configured destinations.

Enable Multitx

When enabled, displays the MultiTX settings in the GUI and enables the MultiTX function on the router.

Serial Port

The serial interface to use. Data received on this serial will be forwarded to all configured remote hosts.

Protocol

Whether TCP or UDP will be used as the transport method.

Socket Inactivity Timeout

If there is no data transmitted for the specified number of seconds, the socket will be closed. **0**=no timeout.

Send Socket ID

When enabled, the text entered into the **Socket ID** field is transmitted to the remote host when the socket connects.

Reopen Closed Socket

Enables an always-on mode. If the socket is closed for any reason, the router attempts to reconnect to the remote host.

Socket ID

Used in conjunction with **Send Socket ID**. The text entered is transmitted when the socket connects. **\r** can be used for **CR**. **\n** can be used for **NL**. **Hex** can be specified by using **\xhh** where hh is replaced with the hex code, such as **\x04** will define binary character **04**.

Send serial data only when the match string is present

When enabled, the match string function is enabled.

Match String

When enabled, serial data is forwarded to remote hosts only when the **Match String** text is present.

Strip match string before sending

When enabled, the text in the **Match String** field is removed before the data is forwarded to the remote host.

Remote host

Up to five remote hosts can be specified in these fields.

Host

Enter the hostname or IP address of the remote host in this field.

Port

Enter the TCP or UDP port number that the remote host is listening on.

Add

Click this button to add the remote host.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
multitx	0	enabled	OFF,ON	Enable MultiTX
multitx	0	srcport	OFF,ON (default: OFF)	Serial Port
multitx	0	prot1	OFF,ON (default: OFF)	protocol
multitx	0	send_sockid	0-255 (default: 0)	Send Socket ID
multitx	0	keepopen	OFF,ON	Reopen Closed Socket
multitx	0	sockid		Socket ID
multitx	0	fwd_match	0-65535	Send serial data only when the match string is present
multitx	0	matchstring	0-255	Match String
multitx	0	Strip_match	OFF,ON	Strip match string before sending

Configure Advanced interfaces settings

The **Configuration > Network > Interfaces > Advanced** menu has the following sub-menu options:

- External Modems
- PPP Mappings
- PPP *n*

Point-to-Point Protocol (PPP) is a standard protocol for transporting data from point to multipoint networks (such as IP) across point-to-point links (such as a serial or ISDN connection). This functionality is essential for dial-up Internet access.

As data is transferred across IP networks in synchronous format, the router supports asynchronous to synchronous PPP conversion. This allows asynchronous terminals connected to the routers to communicate with remote synchronous PPP devices. Normally, this is carried out using a single ISDN B-channel so that data can be transferred at speeds up to 64kbps. This is known as ASYNC to SYNC PPP operation and is supported as standard by most terminal adapters. To use ASYNC to SYNC PPP operation all that is necessary is to ensure that the PPP protocol is bound to the ASY port to which the terminal or PC is connected. (see **Configuration > Network > Interfaces > Serial**).

Note In order to use ASYNC to SYNC PPP the attached terminal must also support PPP (Windows dial-up networking supports PPP).

In addition to ASYNC to SYNC operation (where the router only converts the PPP from one form to another) the router can initiate its own PPP sessions. This is used for example when:

The router is configured as a router to connect an Ethernet network to the Internet via ISDN or W-WAN.

The router is answering an incoming ISDN call with PPP either for remote management or remote access to the Ethernet network to which the router is connected.

The router is accessed locally through the serial port for configuration purposes by setting up a Windows Dial-Up-Networking connection to the phone number **123**.

Note With the exception of MLPPP the parameters in this section are only relevant when the router is generating the PPP, such as they are NOT relevant for ASYNC to SYNC PPP operation.

The router also supports Multi-link PPP (MLPPP). MLPPP uses both ISDN B-channels simultaneously (and two PPP instances), to provide data transfer speeds up to 128Kbps for applications such as email or establishing a point-to-point connection between two routers.

External Modems parameters

The External Modems page contains external modem parameters. External modem support added to GPRS builds. It is now possible to have a GPRS build that can also make outgoing PPP connections via an external modem. It is also possible to answer incoming calls via an external modem.

The PPP **use_modem** field has been altered so the value indicates which modem type should be used. Value **1** indicates that GPRS modem should be used. Value **2** indicates that external modem should be used. It is now also possible, by including enough modem call control instances, to do multilink PPP over multiple external modems.

ASY Port

The physical ASY port for the external modem.

W-WAN mode

Enables W-WAN mode.

Initialization string n

These parameters (**Initialisation string 1**, **Initialisation string 2**, **Initialisation string 3**) allow you to specify a number of command strings that are sent to the wireless module each time a wireless connection is attempted. These can be used to set non-standard wireless operating modes.

Each string is prefixed with the characters **AT** before being sent to the wireless module and they are sent to the wireless module in the order specified until an empty string is encountered. For example, **Initialisation string 3** will not be sent unless **Initialisation string 1** and **Initialisation string 2** are both specified. Initialization strings are not normally required for most applications as the router will normally be pre-configured for correct operation with most networks.

Hang-up string

In a typical wireless application the connection to the network is **always on** and under normal circumstances it is not necessary to hang-up the wireless module. Under certain circumstances however, the router may use the **ATH** command to try and disconnect the wireless module from the network, such as if an incorrect APN has been specified and the module is unable to attach to the network correctly.

This parameter allows you to specify an alternative hang-up string that is sent to the wireless module when disconnecting a call. As with the Initialization strings, it is not necessary to include the **AT** as this is inserted automatically by the router.

Post hang-up string

Additional **AT** commands that are sent to the wireless module after it has been disconnected. As with the Initialization strings, it is not necessary to include the **AT** as this is inserted automatically by the router.

Listening init string

The listening initialization string parameter for external modems.

Listening init interval (secs)

The listening init string is sent at intervals specified by a listening init interval parameter.

Maximum RING count before answering incoming call

The count of the maximum number of rings before answering incoming call can be set in this field. The default value is **0**.

Minimum RING count before answering incoming call

The count of the minimum number of rings before answering incoming call can be set in this field. The default value is **0**.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
modemcc	n	asyport	0-255 (Default: 255)	
modemcc	n	init_str	Free text field	Initialisation string 1
modemcc	n	init_str1	Free text field	Initialisation string 2
modemcc	n	init_str2	Free text field	Initialisation string 3
modemcc	n	hang_str	Free text field	Hang-up string
modemcc	n	posthang_str	Free text field	Post Hang-up string
modemcc	0	linit_str	Free text field	Listening init string
modemcc	0	linit_int	0-2147483647	Listening init interval (secs)

PPP Mappings parameters

The PPP Mappings page contains two columns of as many interfaces as are supported by the router (this varies between models). Each row in the column contains a drop-down list box that allows the user to select what function should be associated with each PPP instance. The PPP instance number is the left-most column. So, for example, to assign a W-WAN interface to PPP instance 3, select **Mobile SIM1 or SIM2** from the drop-down box to the right of instance 3. If a W-WAN interface is fitted to the router, this is the default mapping.

Multilink PPP parameters

As mentioned above, the routers may support multilink PPP. This section describes the configuration of MLPP functionality.

The PPP interface must be configured with **Always On** mode enabled and an AODI NUA.

Desired local ACCM c

The Asynchronous Control Character Map (ACCM). The default value of **0x00000000** should work in most cases. Changing this value is for advanced users only.

Desired remote ACCM c

The ACCM for the remote peer. As above, the default value of **0xffffffff** should work in most cases and should only be changed if it is known that other characters should be used.

Username

The username used for logging on to the remote system.

Password

The password used for authentication with the remote system when using MLPP. This password is used for both B-channel PPP connections.

Confirm password

When changing the password, type the new password into this text box. The router checks that both fields are the same before changing the value.

Enable remote CHAP authentication

When enabled, causes the router to authenticate itself with the remote system using CHAP. If this parameter is set, the connection will fail if authentication fails. Generally, this checkbox should be left unchecked.

Enable short sequence numbers

When enabled, enables the use of 12-bit data packet sequence numbers, rather than the more usual 16-bit data packet sequence numbers.

Bring up the second ISDN B-channel

Never

When selected, causes the router not to activate the second B-channel.

When the data rate is greater than n bytes/sec for s seconds

When selected, the two associated text boxes become enabled and allow the user to enter the desired data rate (default **2000** bytes/second) that will trigger activation of the second B-channel and the period for which the data rate exceeds that value, before the channel is activated.

Drop the second ISDN B-channel

When the connection is terminated

When selected, the second B-channel is only deactivated when the connection is terminated.

When the data rate is less than n bytes/sec for s seconds

When selected, the above two text boxes are enabled. The value in the left-hand one specifies the data rate below which the traffic must fall before the secondary B-channel will be deactivated. The second box contains the time in seconds for which the data rate must be below threshold before the second B-channel is deactivated.

Note The following parameters are for use with **Always On Dynamic ISDN**.

Bring up the first ISDN B-channel

When the data rate is greater than n bytes/sec for s seconds

When **Always On** mode is enabled, these two settings specify the data rate and duration for which the data rate must be sustained before the B-channel is activated.

Drop the first ISDN B-channel

When the data rate is less than n bytes/sec for s seconds

When **Always On** mode is enabled, these two settings specify the data rate below the traffic must fall and the duration for which it is below the threshold before the B-channel is deactivated.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
mlppp	0	l_accm	0x00000000-0xFFFFFFFF	Desired local ACCM
mlppp	0	r_accm	0x00000000-0xFFFFFFFF	Desired remote ACCM
mlppp	0	username	Valid username	username
mlppp	0	password	Valid password	password
mlppp	0	epassword	Encrypted password	None-this parameter is not configurable
mlppp	0	r_chap	ON, OFF	Enable remote CHAP authentication
mlppp	0	l_shortseq	ON, OFF Default OFF	Enable short sequence numbers
mlppp	0	up_rate	0-2147483648 Default 2000	When the data rate is greater than n bytes/sec
mlppp	0	up_delay	0-2147483648 Default 10	for s seconds
mlppp	0	down_rate	0-2147483648 Default 1000	When data rate is less than n bytes/sec
mlppp	0	down_delay	0-2147483648 Default 10	for s seconds
mlppp	0	dup_rate	0-2147483648 Default 500	When data rate is greater than n bytes/sec
mlppp	0	dup_delay	0-2147483648 Default 5	for s seconds
mlppp	0	ddown_rate	0-2147483648 Default 500	When data rate is less than n bytes/sec
mlppp	0	ddown_delay	0-2147483648 Default 5	for s seconds

PPP parameters

This section contains those parameters which may need to be adjusted when setting up a PPP connection, but in general can be left at their default values.

Load answering defaults

Clicking this button causes the router to read the default PPP answering default parameters from a default configuration stored in memory.

Load dialing defaults

Clicking this button causes the router to read the PPP dialing parameters from a default configuration stored in memory.

Description

A description of the PPP instance that may make it easier to refer to. For example, the PPP instance used to connect to an ISP may be named MyISP.

This PPP interface will use

If the PPP mappings have been set up previously using the PPP mappings page, this box will contain the name of the protocol that has been assigned to this PPP instance. If the mapping has not been set up previously and if no default mappings apply, the value for this setting should be **Not Assigned**. Select the required the required physical interface from the drop-down selection box.

Dial out using numbers

To allow the router to automatically make outgoing calls, the ISDN number must be specified. The four text boxes allow four telephone numbers to be entered. The first one is required, the others are optional and will be used in rotation. These numbers may be the number of the Internet Service Provider (ISP) or another router.

Prefix n to the dial out number

When making outgoing PPP calls, the value specified in this text box is inserted before the actual number being called. This may be required if a PABX system is in use which requires a prefix to be used in order to get an outside line. For example, when using AODI or BACP, the remote peer may provide a number to be used for raising an additional B-channel to increase the bandwidth. However, such a number will not normally include the digits needed to connect to an outside line via a PABX.

Username

The username to be used for MLPPP login.

Password

The password to be used for MLPPP login. This password is used for both B-channel PPP connections.

Confirm password

Type the password in this text box to confirm that the password has been correctly typed in.

Note The following three radio buttons control how the IP address for the router is assigned.

Allow the remote device to assign a local IP address to this router

When this radio button is selected, the remote peer will assign this PPP interface an IP address.

Try to negotiate a.b.c.d as the local IP address for this router

If it would be useful, but not essential, to have a predefined IP address for the interface, the second radio button should be selected and the desired IP address entered into the text box to the right.

Use a.b.c.d as the local IP address for this router

If it is essential that the PPP interface has a specific IP address, this radio button should be selected and the IP address entered into the text box.

Use mask a.b.c.d for this interface

The default value in this text box will normally work, and should only be changed if it is known that the default is not appropriate. Since PPP is a peer-to-peer protocol, this value is appropriate in most situations.

○ Allow the remote device to assign a local IP address to this router
○ Try to negotiate to use 1.2.3.4   as the local IP address for this router
◉ Use 1.2.3.4   as the local IP address for this router (i.e. not negotiable)
Use mask 255.255.255.255   for this interface

Use the following DNS servers if not negotiated

Primary DNS server

The IP address of the primary DNS server to use if a DNS server is not assigned as part of the PPP negotiation and connection process. It is fairly common practice for the DNS server to be assigned automatically by the ISP when making a connection.

Secondary DNS server

The IP address of the secondary DNS server to use if one is not automatically assigned by the remote peer.

DNS Port

```
Use the following DNS servers if not negotiated
            Primary DNS server: [            ]
          Secondary DNS server: [            ]
                     DNS Port: [53]
```

Attempt to assign the following IP configuration to remote devices

When enabled, displays following four configuration parameters, which control how the PPP instance assigns an IP address to a connecting remote peer. The primary and secondary DNS server addresses will also be sent to the remote peer

Assign remote IP addresses from a.b.c.d to a.b.c.d

The IP addresses in these text boxes define the pool of IP addresses to assign to remote peers during the IP protocol configuration phase of the PPP negotiation process.

Primary DNS server

The IP address of the primary DNS server that the remote peer should use when making DNS requests over the link.

Secondary DNS server

The IP address of the secondary DNS server that the remote peer should use when making DNS requests, should the primary server be unavailable.

```
☑ Attempt to assign the following IP configuration to remote devices
  Assign remote IP addresses from [10.10.10.0]    to [10.10.10.4]
            Primary DNS server: [            ]
          Secondary DNS server: [            ]
```

Request packet data connection

Allow the PPP interface to answer incoming calls

When enabled, causes the PPP instance to answer an incoming call.

Only allow calling numbers ending with n

When set to answer calls, this setting provides a filter for ISDN sub-addresses. This value is blank by default but when the PPP instance is set to answer calls, only numbers having trailing digits that match the sub-address value in this test will be answered. So for example, if this value is set to **123**, only calls from numbers with trailing digits that match this value will be answered, for example, **01942 605123**.

Close the PPP connection after s seconds

The maximum time that the link will remain active in any one session. After this time, the link will be deactivated.

if it has been up for m minutes in a day

The router deactivates the PPP instance after it has been active for the value specified in this text box.

if it has been idle for h hrs m mins s secs

The router deactivates the PPP instance after the time specified in these text boxes if it detects that the link has not seen traffic.

Alternative idle timer for static routes s seconds

An alternative inactivity timeout for use in conjunction with the **Make PPP n interface use the alternative idle timeout when this route becomes available** parameter on the **Configuration > Network > IP Routing/Forwarding > Static Routes > Routes n > Advanced** web page. This timeout will only be used until the PPP instance next deactivates. After that the normal timeout value is used.

If the link has not received any packets for s seconds

The amount of time the router waits without receiving any PPP packets before disconnecting. The timer is reset with each received PPP packet.

if the negotiation is not complete in s seconds

The maximum time, in seconds, allowed for the PPP negotiation to complete. If negotiations have not completed within this period, the interface is deactivated.

Enable NAT on this interface

When enabled, causes the router to apply Network Address Translation (NAT) to IP packets on this interface. When enabled, the following additional parameters appear:

IP address/IP address and Port

These radio buttons select whether IP address translation only should be applied or whether port number translation should also be applied to IP packets.

NAT Source IP address a.b.c.d

The IP address of the interface that should be used as the source address in IP packets crossing the NAT interface.

Enable IPsec on this interface

When enabled, causes the router to use the IPsec protocol to secure the connection.

When enabled, the following additional parameters are displayed:

Keep Security Associations (SAs) when this PSTN interface is disconnected

When enabled, causes the router to maintain (such as not flush) the SA when the interface becomes disconnected. The normal behavior is to remove the SAs when the interface becomes disconnected.

Use interface x,y for the source IP address of IPsec packets

If it is required to use another interface (such as not the interface currently being configured) as the source address for IPsec packets, this may be achieved by selecting the desired interface from the drop-down list and typing the desired interface instance number into the adjacent text box.

Enable the firewall on this interface

Enabling this checkbox causes the router to apply the firewall settings to traffic using this interface. When debugging connections issues it is often helpful to ensure that this checkbox is NOT checked, as incorrect firewall rules will prevent a connection from passing network traffic. If the connection works when the firewall is turned off but fails when turned on, a good place to start checking parameters would be in the firewall settings page, **Configuration > Security > Firewall**.

Remote management access

The Remote access options parameter can be set to **No restrictions**, **Disable management**, **Disable return RST**, **Disable management and return RST**.

• When set to **No restrictions**, users on this interface can access the router's Telnet, FTP, and web services for the purpose of managing the router.

• When set to **Disable management**, users on this interface are prevented from managing the router via Telnet, FTP, or the web interface.

• For **Disable return RST**, whenever a router receives a TCP SYN packet for one of its own IP addresses with the destination port set to an unexpected value, such as a port that the router would normally expect to receive TCP traffic on, it will reply with a TCP RST packet. This is normal behavior. However, the nature of internet traffic is such that whenever an internet connection is established, TCYP SYN packets are to be expected. As the router's PPP inactivity timer is restarted each time the router transmits data (but not when it receives data), the standard response of the router to SYN packets, such as transmitting an RST packet, will restart the inactivity timer and prevent the router from disconnecting the link even when there is no genuine traffic. This effect can be prevented by using the appropriate commands and options within the firewall script. However, on Digi 1000 series routers, or where you are not using a firewall, the same result can be achieved by selecting this option, such as when this option is selected the normal behavior of the router in responding to SYN packets with RST packets is disabled. The option will also prevent the router from responding to unsolicited UDP packets with the normal ICMP destination unreachable responses.

• The **Disable management an return RST** option prevents users from managing the router via the Telnet, FTP, and web interfaces and also disables the transmission of TCP RST packets as above.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	name	Free text field	Description
ppp	n	l1iface	The layer 1 interface, such as Async Port, PPTP, W-WAN	This PPP interface will use
ppp	n	l1nb	Layer 1 Interface number Default: 0	This PPP interface will use value
ppp	n	l2face	The lower layer interface, such as. LAPB, LAPD, XOT	This PPP interface will use
ppp	n	l2nb	Lower layer interface number. Default: 0	
ppp	n	aodinua		
ppp	n	phonenum	up to 25 digits	Dial out using numbers
ppp	n	ph2	up to 25 digits	Dial out using numbers
ppp	n	ph3	up to 25 digits	Dial out using numbers
ppp	n	ph4	up to 25 digits	Dial out using numbers
ppp	n	prefix	0-9999999999	Prefix n to the dial out number
ppp	n	username	Valid username	Username
ppp	n	password	Valid password	Password
ppp	n	epassword	The encrypted password	None-this parameter is not configurable
ppp	n	r_addr	Default 0.0.0.0 set automatically	Allow the remote device to assign a local IP address to this router
ppp	n	IPaddr	Valid IP address a.b.c.d	Try to negotiate a.b.c.d as the local IP address for this router
ppp	n	l_addr	Valid IP address Default 1.2.3.4	Use a.b.c.d as the local IP address for this router

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	mask	Valid IP address Default 255.255.255.255	use mask a.b.c.d for this interface
ppp	n	DNSserver	Valid IP address	Primary DNS server
ppp	n	secDNS	Valid IP address	Secondary DNS server
ppp	n	DNSport	Valid IP address Default 53	DNS Port
ppp	n	IPmin	Valid IP address Default 10.10.10.10	Assign remote IP addresses from a.b.c.d to a.b.c.d
ppp	n	IPrange	0-255 Default 5	Assign remote IP addresses from a.b.c.d to a.b.c.d Note that these are not directly equivalent. This address is obtained by adding the range value to the minimum.
ppp	n	transDNS	Valid IP address	Primary DNS server
ppp	n	sectransDNS	Valid IP address	Secondary DNS server
ppp	n	cingnb	up to 25 digits	Only allow numbers ending with n
ppp	n	msn	up to 9 digits	with ISDN MSN ending with n
ppp	n	sub	up to 17 digits	with ISDN sub-address ending with n
		cli		
ppp	n	maxup	0-2147483648	Close the PPP connection after s seconds
ppp	n	maxuptime	0-2147483647	if it has been up for m minutes in a day
ppp	n	timeout	Default 300s (5 minutes)	if it has been idle for h, m, s
ppp	n	timeout2	0-2147483648	Alternative idle timer for static routes s seconds
ppp	n	rxtimeout	0-2147483648	if the link has not received any packets for s seconds
ppp	n	maxneg	0-2147483648	if the negotiation is not complete in s seconds
ppp	n	do_nat	0,1 0=Off 1=On	Enable NAT on this interface

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	natip	Valid IP address a.b.c.d	NAT Source IP address a.b.c.d
ppp	n	ipsec	0,1 0=Off 1=On	Enable IPsec on this interface
ppp	n			Keep Security Associations (SAs) when this PPP interface is disconnected
ppp	n	ipsecent	Default PPP Ethernet	Use interface x,y for the source address of IPsec packets
ppp	n	ipsecadd	Valid interface number	Use interface x,y for the source address of IPsec packets
ppp	n	firewall	OFF, ON	Enable the firewall on this interface
ppp	n	qos	OFF, ON	Enable QoS on this interface
ppp	n	use_modem		
ppp	n	cdma_backoff	0,1 Default: 1	
ppp	n	ndis	OFF, ON	
ppp		nocfg	0,1,2,3	Remote management access 0=No restrictions 1=Disable management 2=Disable return RST 3=Disable management and return RST
ppp	n	igmp	OFF, ON	Enable IGMP
ppp	n	ifspeed	64000 bps	None. CLI command only. The **ppp** command allows configuring the interface speed for reporting in SNMP.
ppp	n	norxrst	OFF, ON	

Mobile PPP parameters

Mobile telephone modules fitted into the router use PPP to connect to the network and send and receive traffic. This section describes parameters relevant to setting up a mobile telephone module.

Use SIM Any, SIM1, SIM2

These radio buttons are used to select which of the SIM cards fitted should be used by the module.

Detach W-WAN if the link fails

When enabled, causes the router to issue the command to detach the mobile telephone module from the wireless network if it detects that the link has failed. Link failure is detected by a PPP ping response timer or by a firewall request.

Detach W-WAN between connection attempts

Controls whether the module stays attached to the network if multiple connection attempts are required to establish a connection. This functionality may be useful if the connection to the mobile telephone network is not very reliable. Connecting to the mobile telephone network to send and receive data is a two-stage process. The first stage is where the module signals its wish to join the network and is accepted by the local cell. The second stage involves negotiating the link parameters and transferring data. Sometimes it may be necessary to cleanly detach from the network in order to start the process from the ground up.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	gprs_sim	0-2 0=Any 1=SIM1 2=SIM2	Use SIM, Any, SIM 1, SIM 2
ppp	n	detach_on_fail	OFF,ON	Detach W-WAN if the link fails
ppp	n	detach	OFF,ON	Detach W-WAN between connection attempts

Advanced PPP parameters

This section contains PPP configuration parameters that do not normally need changing from the defaults and are therefore placed in a separate section to reduce clutter on the web pages.

Metric

The connected metric of the interface. The default metric of a connected interface is 1. By allowing the interface to have a higher value (lower priority), static routes can take precedence over interfaces. For normal operation, leave this setting unchanged.

Allow this PP interface to settle for s x 100 milliseconds

On wireless links, it is possible that the initial packets sent to the interface by the TCP layer may be dropped by the network if they are sent too quickly after PPP negotiation has completed. This setting defines the delay in notification sent to the TCP layer that PPP negotiation has completed.

> Metric: 1
>
> Allow this PPP interface to settle for 0 x 100 milliseconds after the connection has come up

Enable "Always On" mode of this interface

If the **Always on** option is available on the interface, enabling this setting reveals the following two radio buttons. When this functionality is enabled, the router will automatically try to reconnect after about 10 seconds if the link becomes disconnected. This parameter should be enabled when using AODI or W-WAN.

On

Default action, the interface will always try and raise this PPP link.

On and return to service immediately

These two radio buttons enable the **Always on** functionality and additionally the facility to return to the in-service state after a disconnect event.

Put this interface "Out of Service" when an always-on connection attempt fails

Normally, always-on interfaces will not go out of service unless they have connected at least once. When checked, this checkbox causes the router to put the interface out of service even if the first connection attempt fails.

Attempt to re-connect after s seconds

The length of time, in seconds, the router should wait after an **Always on** PPP connection has been terminated before trying to re-establish the link.

If a PPP interface that would be inhibited by this PPP is connected, attempt reconnection after s seconds

The value in this setting takes precedence over the previous parameter when another PPP instance that is usually inhibited by this one is connected. This parameter would typically be used to reduce the connection retry rate when a lower priority PPP instance is connected.

Wait s seconds after power-up before activating this interface

The initial delay the router applies before activating the PPP instance after power-up. After the initial power-up delay the normal always-on activation timers apply. If set to zero, no delay will be applied.

Keep this interface up for at least s seconds

The minimum period that the PPP interface should remain available. This means that even if the link becomes inactive before this period expires, the connection will remain open.

Enable Multilink PPP on this interface

When enabled, enables the multilink PPP capability of the router. (See above for configuration details).

Click here to assign a timeband to this interface

Clicking this link redirects the browser to the timeband configuration page **Configuration > Network > Timebands**.

Add a route to a.b.c.d if the peer's IP address is not negotiated

Normally, the IP address for a device connecting to a remote peer is assigned by the remote peer. If this is not the case then the router will need a route to the remote peer. This setting is set to the IP address of the remote peer so that it can be added to the routing table.

Forward IP broadcasts over this interface if the interface is on the same IP network as an Ethernet interface

When enabled, causes the router to route broadcast packets to and from Ethernet interfaces. This will only occur if the PPP instance has issued an address which is part of the Ethernet interface network.

Send LCP echo request packet to the remote peer

When enabled, displays the configuration parameters that cause the router to send Link Control Protocol (LCP) packets to the remote peer at specified intervals. This feature can be useful for keeping a link active (W-WAN, for example).

Send LCP echo requests every s seconds

The value in this text box sets the interval at which to send the packets. When set to **0**, transmission of LCP packets is disabled.

Disconnect the link after n failed echo requests

The number of consecutive failed echo requests allowed before the router terminates the link. When set to **0**, this functionality is disabled, such as the router will not terminate the link if the LCP echo requests do not elicit a response from the remote.

Generate Heartbeats on this interface

When enabled, displays the configuration options controlling how the router sends heartbeat packets. Generating a valid configuration enables the router to send heartbeat packets to the specified destination. Heartbeat packets are UDP packets that contain various items of information about the router and which may include status information that may be used to locate its current dynamic IP address. Heartbeats may also contain GPS position information and mobile telephone module information.

Send Heartbeat messages to IP address a.b.c.d every h hrs, m minutes, s secs

The left-hand text box contains the IP address of the destination for the heartbeat packets. The remaining text boxes specify the desired interval between sending heartbeat packets.

Use interface x,y for the source IP address

Select of the source interface for the UDP heartbeats. Selecting an Ethernet source allows the packets to follow the routing table instead of being sent out from the PPP interface on which they are set.

Select transmit interface using the routing table

When enabled, causes the router to choose the best route from the routing table. If unchecked, the exit interface will be the interface on which the heartbeat is configured.

Include IMSI information in the Heartbeat message

When enabled, causes the router to include the IMSI of the wireless MODEM module in the heartbeat packet.

Include GPS information in the Heartbeat message

When enabled, causes the router to include the GPS co-ordinates in the heartbeat packet.

Generate Ping packets on this interface

When enabled, this checkbox causes the router to reveal the configuration parameters that enable the sending of ICMP echo request (ping) packets. This feature can be used as part of a backup interface strategy.

Send n byte pings to IP host a.b.c.d every h hrs, m mins, s secs

Controls how the ICMP echo requests are generated. The value in the left-hand text box specifies the number of data bytes in the echo request. Typical values are **32** or **64** octets. The IP host text box specifies the IP address of the host to which the ping packets are sent. The remaining parameters specify how often the ping should be sent.

Send pings every h hrs, m mins, s seconds if ping responses are not being received

These three text boxes specify the interval at which to send pings when more than one ping request is outstanding. When left at the default of zero this function is disabled.

Switch to sending pings to IP host a.b.c.d after n failures

These parameters allow for more reliable problem detection before failover occurs. If the value in the first text box is a valid IP address, and the value in the second text box is greater than zero, when a ping failure is detected on the primary host address, this secondary host is tried. This is to ensure that should the primary host become unavailable for any reason and stops responding to the ICMP echo requests, the router will check an alternative IP address before initiating the failover procedure. The value in the second text box is the number of pings that should be allowed to fail before checking the secondary IP address.

Ping responses are expected within s seconds

When the value in this text box is set to a non-zero value, the router will wait for that specified interval for a response from a ping request before applying the timeout specified in the **Send pings every … if ping responses are not being received setting** above. If the value is set to **0** (the default) then the router applies the timeout without modification.

Only send Pings when this interface is "In Service"

When enabled, causes the router to only send ICMP requests when the PPP instance is in service. The default setting is unchecked which means that ICMP requests are sent when the interface is in service and out of service.

New connections to resume with previous Ping interval

When enabled, causes the router to use the ping interval that was in force when the PPP interface last disconnected.

Reset the link if no response is received within s seconds

The period for which the router should wait before terminating the PPP connection if no response to the auto-pings has been received. This behavior is useful in the attempt to re-establish communications, since the router will automatically attempt to restart an always-on link that has been terminated. This function is primarily used where IP traffic is being carried over a W-WAN link and where the associated PPP instance has been configured into the always-on mode.

Use ETH 0 IP address as the source IP address

When enabled, causes the router to use the IP address of interface **ETH 0** as the source address for ICMP echo requests instead of the current IP address of the PPP interface.

Defer sending pings if IP traffic is being received

One of the uses for sending ICMP echo requests is as a keepalive mechanism. When this checkbox is enabled, the router defers sending the ping packets out if IP traffic is being received, since in this case, separate keepalives are not needed.

Limit the data transmitted over this interface

Some service providers impose a (usually monthly) limit on the amount of data sent over a link and levy additional charges if the limit is exceeded. This is fairly common practice for W-WAN links. When checked, this checkbox causes the router to stop sending data on the interface when the preset data limit has been exceeded. The interface is unlocked manually by clicking the **Clear Total Data Transferred** button on the **Management > Network Status > Interfaces > Advanced > PPP > PPP n** page. Alternatively, it may be reset automatically on a certain day of the month.

Issue a warning event after n Kbytes/Mbytes/GBytes

The value in this text box is the amount of traffic which will cause a warning event to be generated in the event log stating that the specified amount of data has been transferred. The units are specified by a drop-down list, having the following options; **KBytes**, **MBytes**, **GBytes**. For example, if the monthly tariff includes up to 5MB of data before excess usage charges are levied, it would be useful to set this threshold to **4MB**. This would cause the router to create a warning entry in the event log once 4MB of data had been transferred. This event could then be used to trigger an email alert, SNMP trap or SMS alert message.

Stop data from being transmitted after n Kbytes/Mbytes/GBytes

The value in this text box specifies the total amount of data that may be transmitted by this PPP instance before the link is blocked for further traffic, and the value in the drop-down list specifies the units which are; **KBytes**, **MBytes**, **GBytes**.

Reset the data limit on the n day of the month

The day of the month on which the data limit is reset to zero.

When the link disconnects, indicate that the connection failed if no IP packets were received

Reset this interface if n packets are transmitted and the connection has been up for at least s seconds

The values in these text boxes control the circumstances under which the link may be reset. If the number of packets text box has a value greater than zero, the router will reset the link if that many IP packets have been transmitted but none have been received, and the link has been active for at least the value specified in the second text box.

Reboot the router after n consecutive resets

If the value in this text box is non-zero, the router will reboot if the PPP link has been reset the specified number of times as a consequence of the value **n packets** (described above) being exceeded.

Reboot the router after n consecutive connection failures

If the value in this text box is non-zero, the router will reboot if it fails to establish a connection over this PPP instance after the specified number of consecutive attempts.

Use RADIUS for authentication when acting as a server

Use RADIUS instance

Allow this PPP interface to attempt to connect n times before allowing other PPP interfaces inhibited by this interface to connect

The number of connection attempts this PPP instance is allowed to make before other PPP instances that are inhibited by this instance may make connection attempts.

If this PPP interface gets disconnected, allow it to attempt to reconnect n times before allowing other PPP interfaces inhibited by this interface to connect

On W-WAN routers, this setting specifies the number of times that a PPP instance which was connected and is then disconnected, is allowed to attempt to reconnect before other PPP instances that were inhibited by this PPP instance will be allowed to connect.

Inhibit this PPP interface if the following PPP instances n are Active | Active and not out of service | Not out of service | Connected and not out of service

Inhibition of this PPP interface may be controlled by the state of other PPP instances. This behavior is controlled by the options in this drop-down menu box.

If this PPP interface is inhibited and data needs to be sent

The options in this drop-down selection box control the behavior of the router in the situation where the PPP instance is in its inhibited state but there is data waiting to be sent over the interface. The options are:

Do not bring up interface

Leaves the situation as it is with the interface remaining inhibited.

Bring up interface and use normal idle period

Removes the inhibit state from the interface and uses the normal idle time associated with it to control when it deactivates.

Bring up interface and use idle period of s seconds

Causes the interface to become activated but rather than using the idle timer associated with the interface, specify the idle timeout.

Allow this PPP interface to attempt to connect 0 times before allowing other PPP interfaces inihibited by this interface to connect

If this PPP interface gets disconnected, allow it to attempt to reconnect 0 times before allowing other PPP interface inhibited by this interface to connect

Inhibit this PPP interface if the following PPP instances [ ] are [Active ▼]

If this PPP interface is inhibited and data needs to be sent [do not bring up interface ▼]
- do not bring up interface
- bring up interface and use normal idle period
- bring up interface and use idle period of

☑ Inhib... nnected but operational

☑ Attem... ...erface

Inhibit other PPP interface if this PPP interface is disconnected but operational

When enabled, enables this PPP instance to inhibit other PPP instances if it is operational but not currently active.

Attempt to negotiate DEFLATE compression on this interface

When enabled, causes the router to compress the data transferred over this link. When unchecked, compression is disabled. The effectiveness of data compression varies with the type of data but a typical ratio achieved for a mix of data such as web pages, spreadsheets, databases, text files and (uncompressed) image files would be between 2:1 and 3:1. Using compression has the effect of increasing the effective throughput. Using compression may offer cost savings on a network where charges are based upon the amount of data transferred (such as W-WAN networks). If the data is already compressed (such as **.zip** files or JPEG images) then the compression algorithm will detect this and send the data without attempting further compression.

☑ Inhibit other PPP interface if this PPP interface is disconnected but operational

☑ Attempt to negotiate DEFLATE compression on this interface

Attempt to negotiate MPPE encryption on this interface

When enabled, causes the router to attempt to negotiate Microsoft Point-to-Point Encryption (MPPE) with the remote peer. If the remote peer is unable to negotiate MPPE, negotiations will fail. When negotiated, the PPP instance will encrypt the PPP frames as per the MPPE specification.

MPPE key size

The values in this drop-down list select the length (in bits) of the encryption key. The options are:

- **Auto**

- **40 bits**

- **56 bits**

- **128 bits**

Auto indicates that the router will accept whatever the remote suggests. For the other values, the remote must accept and request the key size specified, else the PPP negotiations will fail.

Enable MPPE stateless mode

When this checkbox is checked, the router negotiates stateless mode in which the session key is changed after the transmission of each packet. Stateless mode may be useful for lossy links.

Note MPPE does not provide authentication, only encryption. This is because the encryption keys are determined by the PPP engines themselves on start-up.

Use PPP m for processing CHAP

TCP transmit buffer size n bytes

When the value in this text box is set to a non-zero value, the router uses the value to set the size of the TCP buffer for transmitted packets. This is useful for slow and/or lossy connections such as satellite links. Setting this buffer to a low value will prevent the amount of unacknowledged data from getting too high. If retransmits are required, a smaller TX buffer helps prevent retransmits flooding the connection.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	metric	0-255	Metric
ppp	n	settledly	0-200	Allow this PPP interface to settle for s seconds after the connection has come up
ppp	n	aodion	0-2 0=disabled 1=enabled 2=On and return to service immediately	Enable "Always On" mode of this interface, On, On and return to service immediately
ppp	n	autoassert	0,1, 3 0=no autoassert 1=autoassert with route up delay 2=autoassert with no route up delay	
ppp	n	immoos	ON, OFF	Put this interface "Out of Service" when an always-on connection attempt fails
ppp	n	rdoosdly	ON, OFF	remote disconnect
ppp	n	aodi_dly	0-2147483647	Attempt to reconnect after s seconds
ppp	n	aodi_dly2	0-2147483647	If a PPP interface that would be inhibited by this PPP is connected, attempt to re-connect after s seconds
ppp	n	pwr_dly	0-2147483647	Wait s seconds after power-up before activating this interface
ppp	n	minup	0-2147483647	Keep this interface up for at least s seconds
ppp	n	multi	OFF, ON	Enable Multilink PPP on this interface
ppp	n	netip	Valid IP address a.b.c.d	Add a route to a.b.c.d if the peer's IP address is not negotiated
ppp	n	rbcast	OFF, ON	Forward IP broadcasts over this interface if this interface is on the same IP network as an Ethernet interface
ppp	n		OFF, ON	Send LCP echo request packet to the remote peer

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	echo	0-2147483648	Send LCP echo requests every s seconds
ppp	n	echodropcnt	0-2147483648	Disconnect the link after n failed echo requests
ppp	n			Generate Heartbeats on this interface
ppp	n	hrtbeatip	Valid IP address a.b.c.d	Send Heartbeat messages to IP address a.b.c.d every h hrs, m mins, s secs
ppp	n	hrtbeatint	0-2147483648	Send Heartbeat messages to IP address a.b.c.d every h hrs, m mins, s secs
ppp	n	hbipent	Blank, PPP, ETH Blank is default	Use interface x,y for the source IP address
ppp	n	hbipadd	Valid interface number 0-2147483648	Use interface x,y for the source IP address
ppp	n	hbiproute	OFF, ON	Select transmit interface using the routing table
ppp	n	hbimsi	OFF, ON	Include IMSI information in the Heartbeat message
ppp	n	hbgps	OFF, ON	Include GPS information in the Heartbeat message
ppp	n		OFF, ON	Generate Ping packets on this interface
ppp	n	pingsiz	0-2147483648	Send n byte pings to IP host a.b.c.d every h hrs, m mins, s secs
ppp	n	pingip	Valid IP address a.b.c.d	Send n byte ping to IP host a.b.c.d every h hrs, m mins, s secs
ppp	n	pingint	0-2147483648	Send n byte ping to IP host a.b.c.d every h hrs, m mins, s secs
ppp	n	pingint2	0-2147483648	Send pings every h hrs, m mins, s seconds if ping responses are not being received
ppp	n	pingip2	Valid IP address a.b.c.d	Switch to sending pings to IP host a.b.c.d after n failures
ppp	n	ip2count	0-2147483648	Switch to sending pings to IP host a.b.c.d after n failures
ppp	n	pingresp	0-2147483648	Ping responses are expected within s seconds

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	pingis	OFF, ON	Only send Pings when this interface is "In Service"
ppp	n	ping2cont	OFF, ON	New connections to resume with previous Ping interval
ppp	n	pingdeact	0-2147483648	Reset the link if no response is received within s seconds
ppp	n	pingfreth0	OFF, ON	Use ETH 0 IP address as the source IP address
ppp	n	pingresetint	OFF, ON	Defer sending pings if IP traffic is being received
ppp	n		OFF, ON	Limit the data transmitted over this interface
ppp	n	dlwarnkb	0-2147483647	Issue a warning event after n XBytes
ppp	n	dlstopkb	0-2147483647	Stop Data from being transmitted after n XBytes
ppp	n	dlrstday	0-255	Reset the data limit on the n day of the month
ppp	n			When the link disconnects, indicate that the connection failed if no IP packets were received
ppp	n	sscnt	0-2147483648	Reset this interface if n packets are transmitted and the connection has been up for at least s seconds
ppp	n	sssecs	0-2147483648	Reset this interface if n packets are transmitted and the connection has been up for at least s seconds
ppp	n	lscnt	0-2147483648	Reboot the router after n consecutive resets
ppp	n	rebootfails	0-2147483648	Reboot the router after n consecutive connection failures
ppp	n	radius	OFF, ON	Use RADIUS for authentication when acting as a server
ppp	n	radiuscfg		Use RADIUS instance
ppp	n	acttries	0-255	Allow this PPP interface to attempt to connect n times before allowing other PPP interfaces inhibited by this interface to connect

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	pdacttries	0-255	If this PPP interface gets disconnected, allow it to attempt to reconnect n times before allowing other PPP interfaces inhibited by this interface to connect
ppp	n	inhibitno	0-2147483648	Inhibit this PPP interface if the following PPP instances n are Active, Active and not out of service, not out of service, Connected and not out of service
ppp	n	inhmode	0-3	Inhibit this PPP interface if the following PPP instances n are Active, Active and not out of service, not out of service, Connected and not out of service
ppp	n	actmode	OFF,ON	Inhibit other PPP interface if this PPP is interface is disconnected but operational
ppp	n	trafficto	0-2147483648	If this PPP interface is inhibited and data needs to be sent do not bring up the interface, bring up interface and use normal idle period, bring up interface and use idle period of s seconds
ppp	n	deflate	0,1 0=Off 1=On	Attempt to negotiate DEFLATE compression on this interface
ppp	n	mppe	OFF, ON	Attempt to negotiate MPPE encryption on this interface
ppp	n	mppebits	0, 40, 56, 128 0=Auto	MPPE key size
ppp	n	mppeless	OFF, ON	Enable MPPE stateless mode
ppp	n	other_local_PPP_mode	OFF, ON	Use PPP for processing CHAP
ppp	n	other_local_PPP_inst		Use PPP n for processing CHAP
ppp	n	tcptxbuf	0-2147483648	TCP transmit buffer size n bytes
ppp	n	pppdebug	OFF, On	
ppp	n	norxrst	OFF, ON	
ppp	n	noremaddr	OFF, ON	

PPP Negotiation parameters

When PPP starts up, the devices at both ends of the link negotiate the link parameters, in order to find a common subset that both devices can use. The negotiation may be summarized by saying that both ends send negotiation packets with the following message:

these are the values that I wish to use and these are the values that I wish you to use.

Restrict the negotiation time to s seconds

The maximum time allowed for a PPP negotiation to complete. If negotiations have not completed in this time, the PPP instance is disconnected.

Desired local ACCM

The local Asynchronous Control Character Map which has the default value **0x00000000**. Changing this value is for advanced users.

Desired remote ACCM

The remote ACCM which has the default value **0xffffffff**. As above, the default will work in nearly all circumstances and should be changed only where really necessary.

Desired local MRU n bytes

The desired local Maximum Receive Unit (MRU), the default value of **1500** octets will work fine in most cases.

Desired remote MRU n bytes

The value in this text box is the desired MRU for the remote end of the link. The default value of **1500** octets will be fine in most cases.

Request local ACFC

When enabled, causes the router to request Address Control Field Compression (ACFC). When negotiated, the address/control fields are removed from the start of the PPP header.

Request remote ACFC

When checked, this checkbox causes the router to ask the remote device to request ACFC.

Request local PAP authentication

When enabled, causes the router to use the Password Authentication Protocol (PAP) before allowing a connection to be made. Generally, this parameter is enabled for incoming connections and disabled for outgoing connections.

Request remote PAP authentication

When enabled, causes the router to authenticate itself with the remote device using PAP. If this parameter is set, the connection will fail if authentication is not successful. Generally, this parameter is disabled.

Request local CHAP authentication

When enabled, causes the router to use the Challenge Handshake Authentication Protocol (CHAP) for local authentication. As with PAP, this parameter is generally enabled for incoming connections and disabled for outgoing connections.

Request remote CHAP authentication

As with PAP above, this checkbox controls whether or not the router should authenticate itself with the remote device using CHAP. The connection will fail if authentication fails. Generally, this parameter is enabled for outgoing connection and disabled for inbound connections.

Request local (VJ) compression

When enabled, causes the router to request the use of Van Jacobson compression which compresses TCP/IP headers to about 3 octets, rather than the standard 40 octets. This is generally only used to improve efficiency on slow links.

Request remote (VJ) compression

When enabled, causes the router to send a negotiation packet that requests that the remote device requests VJ compression.

Request local PFC

When enabled, causes the router to request Protocol Field Compression (PFC) which compresses PPP protocol fields from 2 octets to 1 octet.

Request remote PFC

When enabled, causes the router to ask the remote device to request Protocol Field Compression.

Request BACP

When enabled, the router will use the Bandwidth Allocation Control Protocol (BACP) to determine the ISDN number to dial for the seconds or third multi-link connection.

Request callback

When enabled, requests a callback when it dials into a remote device. The answering PPP instance of the remote router must also be configured with the telephone number of the calling router and a suitable username, password combination.

Allow remote end to request callback

Controls whether or not the router will respond to incoming callback requests. The options are:

- Off

- Desired

- Required.

Allow this unit to authenticate using

CHAP-MD5

Selecting enabled from the drop-down menu allows the router to authenticate logins using the CHAP MD-5 algorithm.

MS-CHAP

Selecting enabled from the drop-down menu allows the router to authenticate logins using Microsoft's proprietary MS-CHAP algorithm.

MS-CHAPv2

Selecting enabled from the drop-down menu allows the router to authenticate logins using version 2 of Microsoft's proprietary MS-CHAP algorithm.

Allow a remote unit to authenticate using

CHAP-MD5

When enabled, allows the router to authenticate with a remote unit using the CHAP-MD5 algorithm.

MS-CHAP

When enabled, allows the router to authenticate with a remote unit using Microsoft's MS-CHAP algorithm.

MS-CHAPv2

When enabled, allows the router to authenticate with a remote unit using version 2 of Microsoft's MS-CHAP algorithm.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	maxneg	0-2147483648	Restrict the negotiation time to s seconds
ppp	n		OFF, ON	Disconnect if the remote request an IP address
ppp	n	l_accm	0x00000000-0xFFFFFFFF Default 0x00000000	Desired local ACCM
ppp	n	r_accm	0x00000000-0xFFFFFFFF Default 0xFFFFFFFF	Desired remote ACCM
ppp	n	l_mru	0-n Default 1500	Desired local MRU
ppp	n	r_mru	0-n Default 1500	Desired remote MRU
ppp	n	l_acfc	OFF, ON	Request local ACFC
ppp	n	r_acfc	OFF, ON	Request remote ACFC
ppp	n	l_pap	OFF, ON	Request local PAP authentication
ppp	n	r_pap	OFF, ON	Request remote PAP authentication
ppp	n	l_chap	OFF, ON	Request local CHAP authentication
ppp	n	r_chap	OFF, ON	Request remote CHAP authentication
ppp	n	l_comp	OFF, ON	Request local (VJ) compression
ppp	n	r_comp	OFF, ON	Request remote (VJ) compression
ppp	n	l_pfc	OFF, ON	Request local PFC
ppp	n	r_pfc	OFF, ON	Remote PFC
ppp	n	l_bacp	OFF, ON	Request BACP
ppp	n	l_callb	OFF, ON	Request callback
ppp	n	r_callb	0-2 0=Off 1=Desired 2=Required	Allow remote end to request callback

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	l_md5	0-2 0=Disabled 1=Enabled 2=Preferred	Allow this unit to authenticate using CHAP-MD5
ppp	n	r_md5	0,1 0=Off 1=On	Allow remote unit to authenticate using CHAP-MD5
ppp	n	l_ms1	0,1 0=Disabled 1=Enabled 2=Preferred	Allow this unit to authenticate using MS-CHAP
ppp	n	r_ms1	0,1 0=On 1=Off	Allow remote unit to authenticate using MS-CHAP
ppp	n	l_ms2	0-2 0=Disabled 1=Enabled 2=Preferred	Allow this unit to authenticate using MS-CHAPv2
ppp	n	r_ms2	0,1 0=Off 1=On	Allow remote unit to authenticate using MS-CHAPv2
ppp	n	lcn	0-4096	LCN
ppp	n	lcnup	1=up, 0=down	LCN direction
ppp	n	defpak	16,32,64,128,256,512 or 1024	Default X.25 packet size
ppp	n	cingnua	text (valid NUA)	Use NUA
ppp	n	ipmode	0=XOT, 1=raw TCP	Use TPAD over interface
ppp	n	baklcn	1-4095	(Backup) LCN
ppp	n	baklcnup	1=up, 0=down	(Backup) LCN direction
ppp	n	bakl2iface	lapb, lapd, tcp, ssl, vxn	Use backup interface
ppp	n	bakl2nb	0-255	Use backup interface
ppp	n	bakcingnua		
ppp	n	baknum		

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	dmnr_reg		
ppp	n	dmnrtun_add		

PPP QoS parameters

The parameters on this page control the Quality of Service management facility. Each PPP instance has an associated QoS instance, where **PPP 0** maps to **QoS 0**, **PPP 1** maps to **QoS 1**, and so on. These QoS instances include ten QoS queues into which packets may be placed when using QoS. Each of these queues must be assigned a queue profile from the twelve available.

To configure the PPP QoS parameters, set the following values:

Enable QoS on this interface

When enabled, displays the following QoS configuration parameters:-

- **Link speed n Kbps**: The value in this text entry box should be set to the maximum data rate that this PPP link is capable of sustaining. This is used when calculating whether or not the data rate from a queue may exceed its minimum Kbps setting as determined by the profile assigned to it and send at a higher rate, up to the maximum Kbps setting.

- **Queue n**: Below this column heading, is a list of ten queue instances. Each instance is associated with the profile and priority on the same row.

- **Profile n**: This column contains the profile to be associated with the queue. There are twelve available, **0-11**, selected from the drop-down list boxes.

- **Priority**: This column contains drop-down menu boxes which are used to assign a priority to the selected queue. The priorities available are: **Very High**, **High**, **Medium**, **Low**, and **Very Low**.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
qos	n	linkkbps	0-	Link speed n kbps
qos	n	q0prof	0-11	Queue 0 Profile
qos	n	q0prio	0-4 0=Very high 1=High 2=Medium 3=Low 4=Very Low	Queue 0 Priority
qos	n	q1prof	0-11	Queue 1 Profile
qos	n	q1prio	0-4	Queue 1 Priority
qos	n	q2prof	0-11	Queue 2 Profile
qos	n	q2prio	0-4	Queue 2 Priority
qos	n	q3prof	0-11	Queue 3 Profile
qos	n	q3prio	0-4	Queue 3 Priority
qos	n	q4prof	0-11	Queue 4 Profile
qos	n	q4prio	0-4	Queue 4 Priority
qos	n	q5prof	0-11	Queue 5 Profile
qos	n	q5prio	0-4	Queue 5 Priority
qos	n	q6prof	0-11	Queue 6 Profile
qos	n	q6prio	0-4	Queue 6 Priority
qos	n	q7prof	0-11	Queue 7 Profile
qos	n	q7prio	0-4	Queue 7 Priority
qos	n	q8prof	0-11	Queue 8 Profile
qos	n	q8prio	0-4	Queue 8 Priority
qos	n	q9prof	0-11	Queue 9 Profile
qos	n	q9prio	0-4	Queue 9 Priority

PPP Sub-Configs parameters

PPP Sub-Configs is an alternative to using an entire PPP instance if only a few parameters are different to those in an existing PPP instance. Using PPP Sub-Configs, you can define up to 50 sub-configs and saves them on system memory.

To configure the PPP Sub-Configs parameters, set the following values:

Nb

The instance number for a sub-config.

Description

The name to easily identify the sub-config.

Username

The username that is used when authenticating with the remote system and is usually only required for outgoing PPP calls.

Password

The password for authentication with the remote system.

Confirm

When changing the password, enter it into this text box also to allow the router to check for simple typing errors.

Dialout Number

The ISDN number to make outgoing calls. This must be a valid number in order to allow the router to make outgoing calls. This number could be the number of the Internet Service Provider (ISP) or another router.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
pppcfg	1-50	name	Up to 25 characters	Description
pppcfg	1-50	username	Valid username up to 60 characters	Username
pppcfg	1-50	password	Valid password up to 40 characters	Password
pppcfg	1-50	phonenum	Up to 25 digits	Dialout Number

Configure PPP over Ethernet

PPP over Ethernet (PPPoE) is a means of establishing a PPP connection over the top of an Ethernet connection. The implementation provided is compliant with RFC 2516, "A Method for Transmitting PPP Over Ethernet". A typical application would be to allow non-PPPoE enabled devices to access Internet services where the connection to the Internet is provided by an ADSL bridge device.

Using the web page(s)

There is no dedicated web page for configuring the router to use PPPoE; rather there are a number of parameters that appear on other web pages that must be used in conjunction with each other to establish a PPPoE connection over the appropriate Ethernet interface.

In particular, the following configuration pages and parameters are important.

On the appropriate **Configuration > Network > Interfaces > Advanced > PPP n-n** pages, you should configure the following parameters on the **Configuration > Network > Interfaces > Advanced > PPP n-n > PPP n** pages:

As a minimum requirement the **Username** and **Password** parameters should be initialized.

The **This PPP interface will use x,y** defines the physical Ethernet interface over which the PPPoE session will operate. In most cases this is **PPPoE 0** (for **Ethernet 0**). The fact that you have selected **PPPoE 0** as the physical interface for operation with PPP automatically enables PPPoE mode. If another Ethernet instance is used, **Eth 1** for example, this will need to be specified as **PPPoE 1** to ensure the correct MAC address is used, this is in the format **0** or blank for **port 0**, **1** for **port 1**, **2** for **port 2** etc.

If necessary, continue to the page **Configuration > Network > Interfaces > Advanced > PPP n-n > PPP n > Advanced** and set the **Enable "Always On" mode of this interface** parameter to **On** to configure the router so that it will attempt to renegotiate the PPP link should it go down for any reason.

PPP negotiation

The **advanced PPP options** on this page should be initialized as required by your ISP.

In addition:

- **Desired Local MRU** and **Desired Remote MRU** should be set to "**1492**".
- **Request Local ACFC** and **Request Remote ACFC** should be set to "No".
- **Request Local PFC** and **Request Remote PFC** should be set to "No".
- **Desired Local ACCM** and **Desired Remote ACCM** should be set to "0xffffffff".

Using text commands

There are no specific PPPoE commands available to the user via the text command interface. The appropriate **ppp** CLI commands should be used to set the required options.

Configure DHCP servers

This section covers configuring DHCP servers from the web interface and command line. It covers the following topics:

- About DHCP servers on page 325
- DHCP Server parameters for Ethernet n on page 326
- Advanced DHCP parameters on page 329
- Advanced DHCP options on page 330
- Logical Ethernet interfaces on page 331
- DHCP options on page 332
- Static lease reservations on page 333

About DHCP servers

Digi routers incorporate one or more Dynamic Host Configuration Protocol (DHCP) servers, one for each Ethernet port. DHCP is a standard Internet protocol that allows a DHCP server to dynamically distribute IP addressing and configuration information to network clients.

The **Configuration > Network > DHCP server** pages in the web interface include a web page for configuring each of the DHCP servers. Additionally, there is a separate page for mapping MAC addresses to fixed IP addresses.

DHCP Server parameters for Ethernet n

Enable DHCP Server

When enabled, displays the following parameters:

IP Addresses a.b.c.d to a.b.c.d

There are six text boxes in this part of the page; three rows of two. The values in these specify the starting and ending addresses for the range of IP addresses that will be handed out by the DHCP server. Each of the three rows can be used to specify a different IP address pool, all pools should be within the same subnet. When the minimum IP address text box is clear, the DHCP service will be disabled. In other words, in order to enable the DHCP service, there must be at least one minimum IP address and a range.

Using the CLI, this is specified slightly differently, a starting address and a range are specified instead.

Mask

The subnet mask used to on the network to which the router is connected.

Gateway

A gateway is required in order to route data to IP addresses that are not on the local subnet. The value in this text box specifies the IP address of the gateway (which is usually the IP address of the router itself as configured by the IP address of the Ethernet interface associated with this DHCP instance). Alternatively, this may be set to the IP address of another router on the LAN.

DNS Server

The IP address of the primary DNS server to be used by clients on the LAN. This will usually be the IP address of the route itself. Alternatively, this may be set to the IP address of an alternative DNS server on the LAN.

Secondary DNS Server

The IP address of a secondary DNS server (if available) to be used by DHCP clients on the LAN.

Domain Name

The domain name that will be returned to clients.

Lease Duration d days h hrs m mins

How long a DHCP client can use the assigned IP address before it must renew its configuration with the DHCP server. When configuring this value using the command line interface be aware that this parameter is specified in minutes. The three boxes here are for convenience when using long lease durations.

Wait for s milliseconds before sending DHCP offer reply

When the checkbox box is enabled, the router will use the value in the text box as the delay to use prior to sending out the **DHCP_OFFER** message. Enabling this functionality and setting the delay to a non-zero value will allow other DHCP servers on the network to respond first.

Only send offers to Wi-Fi clients

When enabled, causes the router to only send DHCP offers to Wi-Fi clients. This is useful if the router is being used as an access point and there is a separate DHCP server on the Ethernet LAN.

DHCP Relay

Forward DHCP requests to a.b.c.d

The values in these two text boxes specify the IP addresses of the two supported DHCP relay agents. If the DHCP server is on a different subnet, specifying the IP address of the server in this text box will cause the router to forward DHCP requests to the IP address specified. The DHCP server must be within 4 hops.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
dhcp	n	IPmin	Valid IP address a.b.c.d	IP Addresses a.b.c.d
dhcp	n	IPrange	0-2147483647 Default 20	to a.b.c.d
dhcp	n	IPmin2	Valid IP address a.b.c.d	IP Addresses a.b.c.d
dhcp	n	IPrange2	0-2147483647 Default 0	to a.b.c.d
dhcp	n	IPmin3	Valid IP address a.b.c.d	IP Addresses a.b.c.d
dhcp	n	IPrange3	0-2147483647 Default 0	to a.b.c.d
dhcp	n	mask	Valid IP address a.b.c.d	Mask
dhcp	n	gateway	Valid IP address a.b.c.d	Gateway
dhcp	n	DNS	Valid IP address a.b.c.d	DNS Server
dhcp	n	DNS2	Valid IP address a.b.c.d	Secondary DNS Server
dhcp	n	domain	Up to 64 characters	Domain Name
dhcp	n	lease	0-2147483648 minutes Default 20160 minutes (14 days)	Lease Duration d days, h hrs, m mins
dhcp	n	respdelms	0-2147483647	Wait for s milliseconds before sending DHCP offer reply
dhcp	n	wifionly	OFF,ON	Only send offers to Wi-Fi clients
dhcp	n	fwdip	Valid IP address a.b.c.d	Forward DHCP requests to a.b.c.d
dhcp	n	fwdip2	Valid IP address a.b.c.d	Forward DHCP requests to a.b.c.d

Advanced DHCP parameters

Next Bootstrap Server a.b.c.d

The IP address of a secondary configuration server. This server does not have to be on the same logical subnet as the client.

Server Hostname

The name of a host that the DHCP client can make contact with in order to download a boot file.

Boot file

The name of the boot file the client can download from the host specified in the **Server Hostname** text box.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
dhcp	n	nxtsvr	Valid IP address a.b.c.d	Next Bootstrap Server
dhcp	n	sname	Up to 64 characters	Server Hostname
dhcp	n	file	Up to 64 characters	Boot file

Advanced DHCP options

NetBIOS Name Server a.b.c.d

The IP address of the primary WINS server address.

Secondary NetBIOS Name Server a.b.c.d

The IP address of the secondary WINS server address.

TFTP Server Address a.b.c.d

The IP address of a TFTP server. This is mainly used for boot images.

FTP Server Address a.b.c.d (for WYSE Terminals)

The IP address of an FTP server and is a custom option for use with WYSE terminals.

FTP Root Dir (for WYSE Terminals)

The root directory for FTP transfers. This is also a custom option for use with WYSE terminals.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
dhcp	n	NBNS	Valid IP address a.b.c.d	NetBIOS Name Server a.b.c.d
dhcp	n	NBNS2	Valid IP address a.b.c.d	Secondary NetBIOS Name Server a.b.c.d
dhcp	n	tftp	Valid IP address a.b.c.d	TFTP Server Address a.b.c.d
dhcp	n	ftp	Valid IP address a.b.c.d	FTP Server Address a.b.c.d
dhcp	n	ftproot	Up to 64 characters	FTP Root Dir

Logical Ethernet interfaces

The web pages in this section are simply a duplicate of the previously described Ethernet interface, pages but they apply to logical, rather than physical Ethernet interfaces.
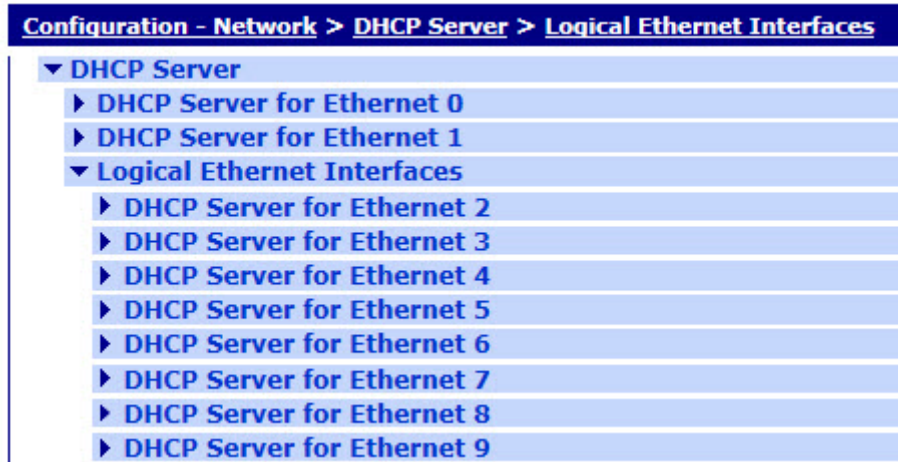
DHCP options

The **DHCP Options** pages allow custom (or non-standard) DHCP options to be configured and sent to the DHCP client when requesting an IP address and other DHCP parameters. This is useful for devices such as IP telephones that use specific strings. On the web page, these (up to ten) options are configured using a table.

The table contains the following fields:

Option

The DHCP option number.

Data type

The data type for the option and can be any one of the following; **1**, **2**, or **4** byte value, IPv4 address, text string or hexadecimal data.

Value

The actual data that will be sent in the DHCP option message.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
dhcpopt	n	optnb	0-2147483647 Default 0	Option
dhcpopt	n	type	i1=1 byte value i2=2 byte value i4=4 byte value ipv4=IPv4 address string=string hex=hexadecimal	Data type
dhcpopt	n	value	Up to 127 octets	Value

For example, to set the option number to **9** for the LPR Server, the command is:

```
dhcpopt 0 optnb 9
```

Static lease reservations

The **Static Lease Reservations** page controls the configuration of MAC address to IP address mappings and is used to assign a specific IP address to a particular Ethernet MAC address. This is particularly useful for mobile applications, such as W-WAN where a particular item of mobile equipment should be issued with the same IP address regardless of when it was last connected to the network. Up to ten MAC to IP address reservations may be specified.

Note It is important to ensure that the IP addresses specified here DO NOT fall within the IP address ranges specified in the DHCP server page.

IP Address a.b.c.d

The IP address to be assigned.

MAC Address aa.bb.cc.dd.ee.ff

The MAC address which is to be given the above IP address. As is usual with the configuration tables, clicking the **Add** button adds the entry to the table, and clicking the **Delete** button removes an existing entry from the table.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
mac2ip	n	IPaddr	Valid IP address a.b.c.d	IP Address a.b.c.d
mac2ip	n	mac	Valid MAC address aa.bb.cc.dd.ee.ff	MAC Address aa.bb.cc.dd.ee.ff

Two separate commands are required to set up a mapping, these are:

```
mac2ip <instance> mac <MAC address>
mac2ip <instance> IPaddr <IP address>
```

where **<instance>** can be **0-9**.

Configure network services

This section covers configuring network services from the web interface and command line.

Network Services page

The **Network Services** web page collects together a number of services that are provided by the router into one section to enable the user to quickly enable or disable these services without having to navigate to multiple sections of the menu. Detailed configuration is performed within the specific section.

Network Services parameters

Enable Network Management Protocol (SNMP)

Enables and disables remote management of the router using SNMP. This checkbox does not actually directly control the SNMP functionality, but enables or disables the remaining SNMP controls on this page.

Note Simply clicking on this checkbox may not be sufficient to allow this service to start working. Depending upon the version selected below, additional configuration may be required.

To perform detailed configuration, including setting up command filters, users and SNMP traps, go to **Configuration > Remote Management > SNMP**.

Enable SNMP v1

When this checkbox is checked, the router uses SNMP version 1.

UDP Port n

The standard UDP port that is used by this service is **161** which is used as the default. If a different port is required, enter the port number into the text entry box.

Enable SNMP v2c

When enabled, the router uses SNMP version 2c.

Enable SNMP v3

When enabled, the router uses SNMP version 3.

Enable Simple Network Timer Server (SNTP)

When enabled, the router acts as a Simple Network Time Protocol (SNTP) time server.

Source

This drop-down selection menu selects the source used to supply time data for the SNTP server. The usual options are:

- Internal real time clock (RTC) device

- A GPS module (if supported)

- An NTP client (if supported).

Enable Secure Shell Server (SSH / SFTP)

The simplest way to check the status or configuration of the router or to upload new firmware is to use the CLI over a directly connected ASY port or via a telnet session. Both of these options have security implications. If a user wishes to gain access to the command line interface of the router but using a more secure protocol, then selecting this checkbox will enable a secure shell to start. This option also enables support for SFTP for secure file transfers.

Enable Telnet Server

Selects between a simple telnet server or telnet over SSL. When this option is selected, the simple, insecure version of telnet is enabled.

Enable Telnet over SSL

If security is an issue, then selecting this option with the radio button disables the simple version and enables telnet over the secure socket layer (SSL) protocol.

Enable Web Server (HTTP)

Much of the configuration of the router can be performed using the web interface as described here. However, HTTP is an insecure protocol. For security reasons, this service can be disabled by deselecting this radio button and hence, enabling the following secure web server. If security is not such an issue, selecting this option allows the simpler and slightly more convenient web server to be used.

Enable Secure Web Server (HTTPS)

Select this radio button to disable the insecure HTTP protocol and enable the HTTPS service.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
snmp	n	v1enable	0,1 0=Off 1=On	Enable SNMP v1
snmp	n	port	Default 161	UDP Port n
snmp	n	v2cenable	0,1 0=Off 1=On	Enable SNMP v2c
snmp	n	v3enable	0,1 0=Off 1=On	Enable SNMP v3
sntp	0	srvr_mode	ON,OFF	Enable Simple Network Time Server (SNTP)
sntp	0	time_src	0=RTC 1=GPS 2=NTP Client	Source
sockopt	n	ssh_server_ena	ON, OFF	Enable Secure Shell Server
sockopt	n	telnets	ON, OFF	Enable Telnet over SSL
sockopt	n	https	ON, OFF	Enable Secure Web Server

Configure DNS servers and Dynamic DNS

This section describes configuring DNS servers and Dynamic DNS from the web interface and command line. It covers the following topics:

- Configure DNS Servers on page 338
- Configure Dynamic DNS on page 344

Configure DNS Servers

The DNS server selection parameters give the ability to specify a DNS server based on the DNS query. For example, DNS lookups for internal servers can be directed to an internal DNS server and all other DNS requests can be sent direct to an external DNS server managed by the ISP.

DNS Server n parameters

For DNS requests matching pattern, send the request to

The hostname pattern to match for the specified DNS server. This parameter needs a wildcard to prefix the domain name. For example, to match DNS queries for all digi.com servers, enter ***.digi.com**. When using this feature, it is recommended that the last DNS server selection hostname pattern is set to ***** to match all other DNS lookups. This ensures that all the DNS lookup configuration is kept together for ease of troubleshooting. If this is not done, the lookups will use the DNS server configured on the interface of the default route.

DNS Server a.b.c.d

The IP address of the DNS server to use when a DNS request matches the hostname pattern.

Secondary DNS Server a.b.c.d

In the event of the primary DNS server not being available, the IP address in this text box specifies the destination for DNS queries matching the hostname pattern.

Route using

Routing table / Interface x,y

The two radio buttons associated with this text control whether the router should look up the route to the DNS server by using the routing table or should send the DNS query out of a specific interface. When the Interface radio button is selected, the drop-down box and interface instance text box are enabled. The options available for the interface are PPP and Ethernet. The adjacent text box should be filled in with the number of a valid instance of the interface, such as **Ethernet 3**. (Different router models support different numbers of interfaces).

Use source IP Address of

Sending interface / Interface x,y

The two radio buttons control whether the DNS query should go out having the source address of the sending interface or a different interface. This will be required for routing if the route to the DNS server is via an IPsec tunnel, to ensure the local and remote subnet selectors match.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
dnssel	n	pattern	***.domain.com**	For DNS requests matching pattern, send the request to
dnssel	n	svr	Valid IP address	DNS Server a.b.c.d
dnssel	n	secsvr	Valid IP address	Secondary DNS Server a.b.c.d
dnssel	n	ent	PPP,Ethernet	Interface x,y
dnssel	n	add	Valid interface number	Interface x,y
dnssel	n	ipent	PPP,Ethernet	Interface x,y
dnssel	n	ipadd	Valid interface number	Interface x,y

DNS Server Update parameters

Dynamic DNS is supported in accordance with RFC2136 and RFC2485. This allows routers to update specified DNS servers with their IP addresses when they first connect to the Internet and at regular intervals thereafter. The parameters in this section control how the router updates a specified DNS server with its IP address when it first connects to the Internet and at regular intervals thereafter.

This is not to be confused with the popular dynamic DNS service **dyndns.com**; there is a separate page for configuring the router to work with **dyndns.com**. See Configure Dynamic DNS on

Send an update to DNS Server a.b.c.d for

The IP address in this text box specifies the DNS server that should be sent the updated information. The server must support **DNS Update messages**. Dynamic DNS is generally offered as a subscription-based service by ISPs, but for a large number of deployed routers, it may be more appropriate to set up a dedicated DNS server locally.

Name

The member of the DNS zone to update. This name is used in conjunction with the zone parameter (below) to uniquely identify the router. So, for example, if the router has a name of **epos33**, the full address of the router will be **epos33.mycompany.com**.

Zone

The DNS zone to update. When using Dynamic DNS, it will be necessary to have domain name (this may be purchased from an appropriate vendor). This domain name, such as **mycompany.com** is what should be entered into the zone field.

When the default route changes

Interface x,y becomes active

The two radio buttons determine when the update is sent, such as when the default route changes or when the specified interface becomes active. The drop-down list offers the options of PPP or Ethernet and the text box is used to enter the instance number for the specified interface.

Also send an update every h hrs, m mins, s secs

The interval at which the router will issue update messages to the DNS server.

The DNS server should delete all previous records

When enabled, causes the DNS server to delete all records of previous addresses served to the router.

DNS Server Username

The username that has been allocated by the Dynamic DNS service provider.

DNS Server Password

The password that has been allocated by the Dynamic DNS service provider.

Password is Base64 encoded

Some Dynamic DNS servers issue passwords that are Base64 encoded, such as Linux Base servers. If this is the case, check this check box to switch on the Base64 decoding of the password before transmission. The password is not actually transmitted as part of the message but is used to create a signature that is appended to the message. If the password is issued as a hexadecimal string and not straight text, the password in the password text box must be given the prefix **0x**.

Confirm DNS Server Password

The password should be entered into this text box to confirm it.

Local time offset from GMT

Auto detect

These two radio buttons control whether the offset of the local time from GMT should be auto-detected or specified. This feature is required since a GMT timestamp must be included as part of the authentication message. When set to auto-detect the router will automatically apply the correction. When auto detect is not selected, the correct offset should be selected from the drop-down list.

Required Time Accuracy

The permitted variance between the router's time and that of the DNS server. If the time difference exceeds this limit, the DNS update will fail.

Allow DNS clients to cache this entry for s seconds

How long a router that resolved the address is allowed to cache that address.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
dnsupd	0	server	Valid IP address a.b.c.d	Send an update to DNS Server a.b.c.d
dnsupd	0	name	up to 20 characters	Name
dnsupd	0	zone	up to 64 characters	Zone
dnsupd	0	ifent	PPP,ETH	when interface x,y becomes active
dnsupd	0	ifadd	Valid instance number	when interface x,y becomes active
dnsupd	0	upd_int	0 – 2147483648 (seconds)	Also send an update every h hrs, m mins s secs
dnsupd	0	delprevrr	OFF,ON	The DNS server should delete all previous records
dnsupd	0	username	Valid username (up to 20 characters)	DNS Server Username
dnsupd	0	password	Valid password (up to100 characters)	DNS Server Password
dnsupd	0	b64pwd	OFF,ON	Password is Base64 encoded
dnsupd	0	autozone	OFF,ON	Local time offset from GMT auto detect
dnsupd	0	tzone	–2147483648 - 2147483647 (hours)	Local time offset from GMT n
dnsupd	0	fudge	0 – 2157483648 (seconds)	Required Time Accuracy s seconds
dnsupd	0	ttl	0 – 2157483648 (seconds)	Allow DNS clients to cache this entry for s seconds

Configure Dynamic DNS

The Dynamic DNS client (DynDNS) updates DNS hostnames with the current IP address of a particular interface. Dynamic DNS operates under the specification supplied by **DynDNS** (go to http://dyn.com), referred to in the web interface as **Dynamic DNS**.

When an interface connects, the client checks the current IP address of that interface. If the IP address differs from that obtained from the previous connection, the Dynamic DNS service is contacted, and the hostnames specified in the **Hostname** parameters are updated with the new address.

Dynamic DNS parameters

Service Provider

Selects the Dynamic DNS service provider. Dynamic TransPort routers support the Dynamic DNS services **Dynamic DNS** (at **dyn.com**) **No-IP** (at **noip.com)**. TransPort routers may be compatible with other Dynamic DNS services, which can be selected by setting the **Service Provider** setting to **Other**. For more information about Dynamic DNS services, including other service providers, see this article:

https://en.wikipedia.org/wiki/Dynamic_DNS

Host and Domain Name(s)

Up to five host/domain names that are to be updated using the service.

Destination port

The IP port to use as the destination port. The default value is 0 which causes the router to use the default port number which is port **80**.

DynDNS User Name

The username to use when updating the hostnames. This will have been supplied by the service provider.

DynDNS Password

The password to use when updating the hostnames. This will have been supplied by the service provider.

Confirm DynDNS Password

Enter the password into this text box to confirm it.

DynDNS DDNS System

The value selected from this drop-down list is used to identify the dynamic DNS system containing the hostnames to be updated. The available options are:

- **Dynamic DNS**
- **Static DNS**
- **Custom DNS**

When default route/interface x,y becomes active, send DDNS update

The radio buttons select whether or not the router should use the default interface or the interface specified from the drop-down list. If the specified interface option is selected, the required interface is selected from the drop-down list and the interface instance is entered into the adjacent text box. If the default interface is selected, the client will keep track of and use the current default route.

Use Wildcards

Selects whether or not wildcard matching on the hostname will be performed. The options are:

- **Disable wildcards**
- **Enable wildcards**
- **No change to service settings**

When enabled, the Dynamic DNS service will match DNS requests of the form ***.hostname** where ***** matches any text. For example, if Hostname1 was set to **site.dyndns.com** and wildcard matching was enabled, than **www.site.dyndns.com** would resolve to the interface address.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
dyndns	0	hostname1	Up to 40 characters	Host and Domain Name(s)
dyndns	0	hostname2	Up to 40 characters	Host and Domain Name(s)
dyndns	0	hostname3	Up to 40 characters	Host and Domain Name(s)
dyndns	0	hostname4	Up to 40 characters	Host and Domain Name(s)
dyndns	0	hostname5	Up to 40 characters	Host and Domain Name(s)
dyndns	0	port	0 - 65535	Destination port #
dyndns	0	username	Up to 20 characters	DynDNS User Name
dyndns	0	password	Up to 25 characters	DynDNS Password
dyndns	0	system	Blank, statdns, custom	DynDNS DDNS System
dyndns	0	ifent	Blank,ETH,PPP	When default route/interface x,y becomes active, send DDNS update
dyndns	0	ifadd	0 -2147483647	When default route/interface x,y becomes active, send DDNS update
dyndns	0	wildcard	0,1,2 0=Disable wildcards 1=Enable wildcards 2=No change to service settings	Use Wildcards

Advanced Dynamic DNS parameters

The parameters in this section do not normally need changing from their defaults.

Note Before configuring dynamic DNS or any of these parameters, it is recommended that you view the information and resources available at the website http://dyn.com.

Update interval d days

The number of days between dynamic DNS updates.

Supply the IP address in the update

When enabled (the default), causes the router to supply the IP address as part of the dynamic DNS update. When unchecked, the IP address is not supplied and the DYNDNS server attempts to determine the correct IP address by other means (IP source address in update packet). This mode would normally only be used if the router is behind a NAT router.

Only send update when this router is the VRRP master

When enabled, causes the router to not send DDNS updates unless at least one Ethernet interface is a VRRP master.

Enable debug

When enabled, enables debug tracing of the dynamic DNS transactions.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
dyndns	0	updateint	0 -255	Update interval d days
dyndns	0	noip	OFF,ON	Supply the IP address in the update
dyndns	0	ifvrrpmaster	OFF,ON	Only send update when this router is the VRRP master
dyndns	0	debug	OFF,ON	Enable debug

Configure IP routing and forwarding

This section covers configuring IP routing and forwarding from the web interface and command line. It covers the following topics:

View the TransPort routing table

To view the Digi TransPort routing table from the web interface, navigate to **Management > Network Status > IP Routing Table**.

From the command line, use the command:

```
route print
```

Supported routes

TransPort routers support three main types of routes:

- Dynamic routes
- Static routes
- Default routes

Dynamic routes

Dynamic routes are created automatically when an interface is configured or connected.

For example configuring an **Ethernet 0** interface with an IP address of **192.168.1.1** and mask of **255.255.255.0** will cause a dynamic route to be created automatically.

Thus any packet with destination IP address in the range **192.168.1.0** to **192.168.1.255** will automatically be routed through to the **Ethernet 0** interface.

Static routes

To add static routes, configure a route in **Configuration > Network > IP Routing/ Forwarding > Static Routes > Routes 0 – 9 > Route n**, where **n** is an instance number.

The minimum configuration settings required to add a static route are:

- **IP Address**
- **Mask**
- **Interface**
- **Interface number**

If a static route is pointing at an Ethernet interface then optionally a gateway IP address can be added. If a gateway IP address is not added then the gateway IP address configured for the Ethernet interface itself will be used automatically.

Default routes

To add default routes, configure a route in **Configuration > Network > IP Routing/ Forwarding > Static Routes > Default Route n,** where n is an instance number.

Default routes will match packets with any destination IP address (when in service).

If a default route is configured, packets with destination IP addresses that do not match any of the dynamic or static routes will be sent out the interface specified in the first **in service** default route.

Routing modes

The TransPort has two routing modes available, these are:

- **TransPort routing mode**: This is the original routing method and may be seen on existing installations.
- **CIDR routing mode:** Now enabled by default on new TransPort routers.

The CLI command to switch between the two modes is:

```
ip 0 cidr [off|on]
```

TransPort routing mode

When you enable the TransPort routing mode, CIDR routing is disabled.

When the TransPort receives an IP packet to route, the routing table is used to decide through which interface to send the packet.

Usually the destination IP address of the IP packet is compared with the IP Address and Mask of each entry in the routing table in index order, regardless of the order in the routing table or length of mask.

There may be more than one match, and in this case, the index number of the route is taken into account. The index number is simply the route number in the config. That is, Static Route 0 or 1 is index **0** or **1**.

Static routes are checked first, then dynamic routes, then default routes.

CLI command: `ip 0 cidr off`

CIDR routing mode

When the TransPort receives an IP packet to route, the routing table is used to decide through which interface to send the packet.

Usually the destination IP address of the IP packet is compared with the IP Address and Mask of each entry in the routing table.

There may be more than one match and in this case the most specific route is used to route the packet. Such as, a matching **/24** route is used before a matching **/16** route.

If multiple routes match the destination and have the same prefix length, the index number of the routes in the routing table is used to determine the route.

CLI command: `ip 0 cidr on`

Route metrics

Route Metric settings can be set to override the order in which the routes are searched.

Routes with lower metric numbers will always be used in preference to routes with higher metric numbers even if the routes with higher metric numbers appear first in the routing table.

Route metrics can be configured by means of the following route parameters:

- **Connected Metric**
- **Disconnected Metric**

Route metrics can be altered automatically according to various circumstances. This allows for automatic backup connection paths.

Routes and interfaces can be put out of service.

Whenever an interface is out of service (OOS), any route pointing at the interface will also be out of service.

Whenever a route is out of service, the metric value will be set to **16** in TransPort routing mode and **17** in CIDR mode.

IP Routing parameters

Enable CIDR routing

When enabled, the following six text boxes are displayed:

Connected Interfaces

The CIDR metric that the router should apply to connected interfaces.

Static Routes

The CIDR metric that the router should use for static routes. The default is **1**.

eBGP Routes

The CIDR metric that the router should use for eBGP routes. The default is **20**.

OSPF Routes

The CIDR metric that the router should use for OSPF routes. The default is **110**.

RIP Routes

The CIDR metric that the router should use for RIP routing. The default is **120**.

iBGP Routes

The CIDR metric that the router should use for iBGP routes. The default is **200**.

Maximum static route metric

The maximum value for the routing metric. The default is **16**.

Route directed IP broadcasts

When checked, this checkbox causes the router to route directed broadcasts. The default state for this parameter is **Off**. A directed broadcast is an IP packet with a destination address that is a valid broadcast address for a subnet but does not originate from that subnet. Directed IP broadcasts are used to send a broadcast from one interface to the subnet of another.

Wait s seconds before using an alternative route

The value in this text box specifies the latency to apply before passing traffic on an alternative route in the current route becomes unavailable.

If an interface is configured for "dial on demand" and fails to connect,

Mark a static route as "Out Of Service" for s seconds

The value in this text box specifies the default time that a route should be marked as out of service if the interface it uses fails to establish a connection.

When an "Always On" route becomes "In Service", wait s seconds before using it

The value in this text box specifies the delay that the router should apply to a route before passing traffic on it once it has come into service.

Related CLI commands
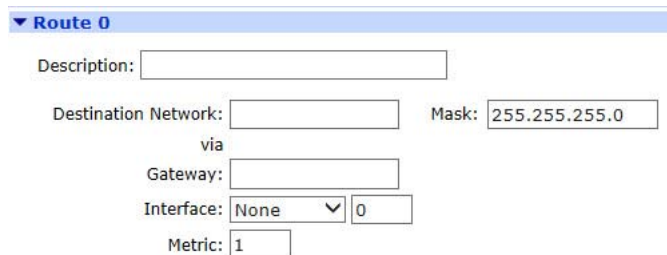
Entity	Instance	Parameter	Values	Equivalent Web Parameter
ip	0	cidr	on,off	Enable CIDR routing
ip	0	admin_connected	0-2147483647	Connected Interfaces
ip	0	admin_static	0-2147483647	Static Routes
ip	0	admin_ebgp	0-2147483647	eBGP Routes
ip	0	admin_ospf	0-2147483647	OSPF Routes
ip	0	admin_rip	0-2147483647	RIP Routes
ip	0	admin_ibgp	0-2147483647	iBGP Routes
ip	0	inf_metric	0-2147483647	Maximum static route metric
ip	0	route_dbcast	0-255	Route directed IP broadcasts
ip	0	route_dly	0-2147483647	Wait s seconds before using an alternative route
ip	0	route_dwn	0-2147483647	If an interface is configured for "dial on demand" and fails to connect, Mark a static route as **Out Of Service** for **s** seconds
ip	0	routeup_dly	0-2147483647	When an **Always On** route becomes **In Service**, wait **s** seconds before using it

Static routes

The static routing web pages and command line parameters described below control the static routing table used by the router. These allow the setting up of static IP routes for particular IP subnets, networks or addresses.

Route n parameters

Each of the static route instances has its own configuration page. These are described below.

Description

A memorable name for the route to be assigned.

Destination Network a.b.c.d

The IP address of the destination subnet, network or IP address for the route. If the router receives a packet with a destination IP address that matches the Destination Network/Mask combination it will route the packet through the interface specified below.

Mask a.b.c.d

The network mask that is used in conjunction with the above destination network address to specify the.

Gateway a.b.c.d

Used to override the default gateway IP address configured for the Ethernet interfaces. Packets matching the route will use the gateway address specified in the route rather than the address specified on the Ethernet interface configuration page. This parameter does **not** apply to routes using PPP interfaces.

Interface x,y

The interface used to route the packets is selected from the drop-down list and the interface instance number is entered into the adjacent text box. The available options are:

- **None**
- **PPP**
- **Ethernet**
- **Tunnel**

Use PPP sub-configuration

If PPP sub-configurations are defined, this text will appear in normal highlighting (such as not disabled out) and text box will accept the number for the desired sub-configuration to use on this route. This parameter will not appear on those models that do not support PPP sub-configurations.

Metric n

The routing metric to use when the interface is connected. This should have a value between **1** and **16** and is used to select which route should be used when the subnet for a packet matches more than one of the IP route entries.

Each route can be assigned a **connected metric** and a **disconnected metric**. The connected metric parameter specifies the metric for a route whose interface is active. The disconnected metric specifies the metric for a route whose interface is inactive. Normally both values should be the same but in some advanced routing scenarios necessary to use different values.

If a particular route fails, it automatically has its metric set to **16**, which means that it is temporarily deemed as being out of service. The default out of service period is set by the IP route out of service parameter. Note however, that this default period may be overwritten in certain situations such as when a firewall stateful inspection rule specifies a different period. When a route is out of service, any alternative routes (with matching subnets) will be used first.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
route	n	descr	Up to 20 characters	Description
route	n	IPaddr	Valid IP address a.b.c.d	Destination Network a.b.c.d
route	n	mask	Valid netmask a.b.c.d	Mask a.b.c.d
route	n	gateway	Valid IP address a.b.c.d	Gateway
route	n	ll_ent	Blank,PPP,ETH,TUN	Interface x,y
route	n	ll_add	0-2147483647	Interface x,y
route	n	upmetric	0-2147483647	Metric

Advanced Static Route parameters

Use metric n when the interface is not active

The routing metric to use when the interface is not active.

```
Use metric 1     when the interface is not active

☑ Use this route only if the source IP address of the packet matches
    IP Address: [            ]
          Mask: [            ]

☑ Include this route in RIP advertisements

☑ Make PPP 0      interface use the alternative idle timeout when this route becomes available

Wait for  0      seconds after power up before allowing this route to activate the interface
```

Use this route only if the source IP address of the packet matches

When enabled, the following two parameters are enabled.

IP Address a.b.c.d

If necessary, these IP Address and Mask parameters may be used to further qualify the way in which the router routes packets. If the values in this text box and the following Mask parameter are set, the source address of the packet being routed must match these parameters before the packet will be routed through the specified interface.

Mask a.b.c.d

The netmask that is used in conjunction with the IP address as explained above.

Include this route in RIP advertisements

When enabled, the router includes this static route to be included in RIP advertisements.

Make PPP n interface use the alternative idle timeout when this route becomes available

When enabled, this check box, in conjunction with the PPP interface instance number in the text box, cause the router to use the alternative inactivity timeout specified for that interface when this route comes back into service. This feature is useful when it is preferable to close down a backup route quickly when a primary route comes back into service.

Wait for s seconds after power up before allowing this route to activate the interface

The delay the router should wait after power-up before packets matching this route will initiate a connection of the interface configured in the route. It is typically used on W-WAN routers that have ISDN backup to prevent unnecessary ISDN connections from being made while a W-WAN connection is first being established.

Mark this route as "Out of Service" in the interface fails to connect after n consecutive attempts

Normally, if an interface is requested to connect by a route and fails to connect, the route metric is set to 16 for the period of time specified by the Mark a static route as **Out Of Service for s seconds** parameter on the **Configuration > Network > IP Routing/Forwarding > IP Routing** page. If the value in this text box is non-zero, the route metric will not be set to **16** until the number of connection attempts specified by this parameter have been made.

If the interface is configured for "dial on demand"

Mark this route as "Out Of Service" if the interface fails to connect after 0 consecutive attempts

If the interface fails to connect, try again in 0 seconds

☐ Deactivate the interface after it successfully connects

Do not allow this interface to be activated by this route for 10 seconds after last activation attempt

If the interface fails to connect, try again in s seconds

If an interface is requested to connect by this route (due to IP traffic being present) and it fails to connect, the route will be marked as out of service but the router will continue to attempt to connect at the interval specified by the value in this text box. If the interface does connect, the router will clear the out of service status for the route.

Deactivate the interface after it successfully connects

When enabled, the router deactivates an interface once a successful activation attempt has been made. This is used in conjunction with the above retry parameter. If the above retry parameter is not set, this checkbox is disabled.

Do not allow this interface to be activated by this route for s seconds after the last activation attempt

The delay to wait before re-initiating a connection after it has dropped whilst still required.

Only queue one packet whilst waiting for the interface to connect

When enabled, the router enqueues only one packet while waiting for the interface to connect. When unchecked, the router will enqueue two packets.

☑ Only queue one packet whilst waiting for the interface to connect

When this route becomes available, deactivate the following interfaces

None ⌄ 0   after 0   seconds
None ⌄ 0   after 0   seconds

When this route becomes unavailable, deactivate the following interfaces

None ⌄ 0   after 0   seconds
None ⌄ 0   after 0   seconds

When this route becomes available, deactivate the following interfaces x,y x,y

The interfaces specified by the values in these two pairs of drop-down list and text boxes are deactivated when this route becomes available again after being out of service. This feature is typically used to deactivate backup interfaces when the primary interface becomes available after being out of service. Select the required interface from the drop-down list and enter the interface instance number into the text box as usual.

When this route becomes unavailable, remove the "Out of Service" state on x,y

This drop-down list and text box are used to specify the interface (available options are None, PPP, Ethernet and Tunnel) and instance that should be taken out of the **Out of Service** state when the interface that this route is configured to use is deactivated.

Keep this route in service for s seconds after OOS state is cleared

When enabled, the following text box is enabled (such as it is no longer disabled), allowing a value to be entered. The value specifies the period that the interface specified above will remain in service even though it is actually unable to pass traffic immediately. This is behavior useful in situations where a PPP interface is activating and traffic should not try the next interface until this one has been allowed a certain amount of time to come up. When this timer expires, if the interface is unable to pass traffic, it will be marked **Out of Service** and the next interface will be tried.

☑ Keep this route in service for `0` seconds after OOS state is cleared

Assign this route to recovery group: `0`

Assign this route to recovery group n

Assigns the route to a recovery group. This means that if all the routes in a particular recovery group go out of service, the out of service status is cleared for all routes in that group. If one route in a group comes back into service, all routes with a lower priority (metric) also have their out of service status cleared.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
route	n	metric	0-2147483647	Use metric n when the interface is not active
route	n	srcip	Valid IP address a.b.c.d	IP Address a.b.c.d
route	n	srcmask	Valid netmask a.b.c.d	Mask a.b.c.d
route	n	inrip	on,off	Include this route in RIP advertisements
route	n	doinact2	on,off	Make PPP n interface use the alternative idle timeout when this route becomes available
route	n	inact2add	0-2147483647	Make PPP n interface use the alternative idle timeout when this route becomes available
route	n	pwr_dly	0-255	Wait for s seconds after power up before allowing this route to activate the interface

Entity	Instance	Parameter	Values	Equivalent Web Parameter
route	n	actooslim	0-2147483647	Mark this route as **Out Of Service** if the interface fails to connect after n consecutive attempts
route	n	chkoos_int	0-2147483647	If the interface fails to connect, try again in s seconds
route	n	chkoos_deact	0-255	Deactivate the interface after it successfully connects
route	n	dial_int	0-255 Default 10	Do not allow this interface to be activated by this route for s seconds after the last activation attempt
route	n	q1	on,off	Only queue one packet whilst waiting for the interface to connect
route	n	deact_ent	Blank,PPP	When this route becomes available, deactivate the following interfaces x,y
route	n	deact_add	0-2147483647	When this route becomes available, deactivate the following interfaces x,y
route	n	deact_ent2	Blank,PPP	When this route becomes available, deactivate the following interfaces x,y
route	n	deact_add2	0-2147483647	When this route becomes available, deactivate the following interfaces x,y
route	n	unoos_secs	0-2147483647	Keep this route in service for s seconds after OOS state is cleared
route	n	rgroup	0-255	Assign this route to recovery group n

Default Route n parameters

The following web pages and associated command line commands are used to set up default IP routes that route non-local IP addresses not specified in a static route. The parameters are identical to those on the static route pages with the exception that there are no IP address or Mask parameters.

Description

Assigns a convenient and memorable description for the route.

Default route via:

Gateway a.b.c.d

Used to override the default gateway IP address configured for the Ethernet interfaces. Packets matching the route will use the gateway address specified in the route rather than the address specified on the Ethernet interface configuration page. This parameter does NOT apply to routes using PPP interfaces.

Interface x,y

The interface used to route the packets is selected from the drop-down list and the interface instance number is entered into the adjacent text box. The available options are:

- **None**
- **PPP**
- **Ethernet**
- **Tunnel**

Metric n

The routing metric to use when the interface is connected. This should have a value between **1** and **16** and is used to select which route should be used when the subnet for a packet matches more than one of the IP route entries.

Each route may be assigned a **connected metric** and a **disconnected metric**. The connected metric parameter is used to specify the metric for a route whose interface is active. The disconnected metric is used to specify the metric for a route whose interface is inactive. Normally both values should be the same but in some advanced routing scenarios necessary to use different values.

If a particular route fails, it will automatically have its metric set to **16** which means that it is temporarily deemed as being out of service. The default out of service period is set by the IP route out of service parameter. Note that this default period may be overwritten in certain situations such as when a firewall stateful inspection rule specifies a different period. When a route is out of service, any alternative routes (with matching subnets) will be used first.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
def_route	n	descr	Up to 20 characters	Description
def_route	n	gateway	Valid IP address a.b.c.d	Gateway a.b.c.d
def_route	n	ll_ent	Blank,PPP,ETH,TUN	Interface x,y
def_route	n	ll_add	0-2147483647	Interface x,y
def_route	n	upmetric	1-16	Metric

Advanced Default route

Use metric n when the interface is not active

The routing metric to use when the interface is not active.

Use this route only if the source IP address of the packet matches

When enabled, the following two parameters are enabled:

IP address a.b.c.d

If necessary, these **IP Address** and **Mask** parameters can be used to further qualify the way in which the router routes packets. If the values in this text box and the following Mask parameter are set, the source address of the packet being routed must match these parameters before the packet will be routed through the specified interface.

Mask a.b.c.d

The netmask that is used in conjunction with the IP address as explained above.

Include this route in RIP advertisements

When enabled, the router includes this static route to be included in RIP advertisements.

Make PPP x interface use the alternative idle timeout when this route becomes available

When enabled, this check box, in conjunction with the PPP interface instance number in the text box, cause the router to use the alternative inactivity timeout specified for that interface when this route comes back into service. This feature is useful when it is preferable to close down a backup route quickly when a primary route comes back into service.

Wait for s seconds after power up before allowing this route to activate the interface

The delay that the router should wait after power-up before packets matching this route will initiate a connection of the interface configured in the route. It is typically used on W-WAN routers that have ISDN backup in order to prevent unnecessary ISDN connections from being made whilst a W-WAN connection is first being established.

If the interface is configured for "dial on demand"

Mark this route as "Out Of Service" if the interface fails to connect after n consecutive attempts

Normally, if an interface is requested to connect by a route and fails to connect, the route metric is set to 16 for the period of time specified by the Mark a static route as Out Of Service for s seconds parameter on the **Configuration > Network > IP Routing/Forwarding > IP Routing** page. If the value in this text box is non-zero, the route metric will not be set to 16 until the number of connection attempts specified by this parameter have been made.

If the interface fails to connect, try again in s seconds

If an interface is requested to connect by this route (due to IP traffic being present) and it fails to connect, the route will be marked as out of service but the router will continue to attempt to
connect at the interval specified by the value in this text box. If the interface does connect, the router will clear the out of service status for the route.

Deactivate the interface after it successfully connects

When enabled, the router deactivates an interface once a successful activation attempt has been made. This is used in conjunction with the above retry parameter. If the above retry parameter is not set, this checkbox is disabled.

Do not allow this interface to be activated by this route for s seconds after the last activation attempt

The delay to wait before re-initiating a connection after it has dropped while still required.

Only queue one packet whilst waiting for the interface to connect

When enabled, the router enqueues only one packet while waiting for the interface to connect. When unchecked, the router enqueues two packets.

When this route becomes available, deactivate the following interfaces x,y x,y

The interfaces specified by the values in these two pairs of drop-down list and text boxes will be deactivated when this route becomes available again after being out of service. This feature is typically used to deactivate backup interfaces when the primary interface becomes available after being out of service. Select the required interface from the drop-down list and enter the interface instance number into the text box as usual.

When this route becomes unavailable, remove the "Out Of Service" state on x,y

This drop-down list and text box are used to specify the interface (available options are **None**, **PPP**, **Ethernet**, and **Tunnel**) and instance that should be taken out of the **Out of Service** state when the interface that this route is configured to use is deactivated.

Keep this route in service for s seconds after OOS state is cleared

When enabled, the following text box is enabled (such as it is no longer disabled out), allowing a value to be entered. The value specifies the period that the interface specified above will remain in service even though it is actually unable to pass traffic immediately. This is behavior useful in situations where a PPP interface is activating and traffic should not try the next interface until this one has been allowed a certain amount of time to come up. When this timer expires, if the interface is unable to pass traffic, it will be marked Out of Service and the next interface will be tried.

Assign this route to recovery group n

Used to assign the route to a recovery group. This means that if all the routes in a particular recovery group go out of service, the out of service status is cleared for all routes in that group. If one route in a group comes back into service, all routes with a lower priority (metric) also have their out of service status cleared.

Related CLI commands
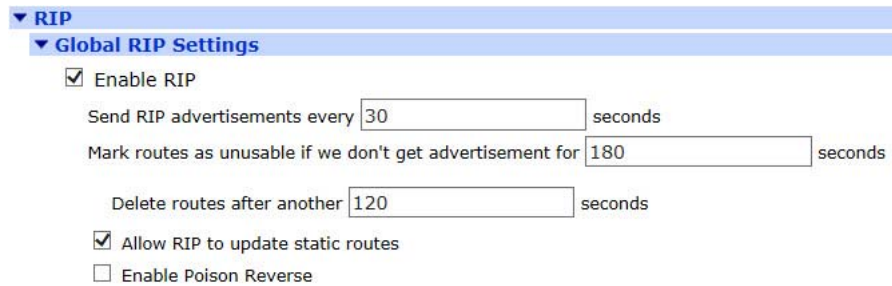
Entity	Instance	Parameter	Values	Equivalent Web Parameter
def_route	n	metric	0-2147483647	Use metric n when the interface is not active
def_route	n	srcip	Valid IP address a.b.c.d	IP Address a.b.c.d
def_route	n	srcmask	Valid netmask a.b.c.d	Mask a.b.c.d
def_route	n	inrip	on,off	Include this route in RIP advertisements
def_route	n	doinact2	on,off	Make PPP n interface use the alternative idle timeout when this route becomes available
def_route	n	inact2add	0-2147483647	Make PPP n interface use the alternative idle timeout when this route becomes available
def_route	n	pwr_dly	0-255	Wait for s seconds after power up before allowing this route to activate the interface
def_route	n	actooslim	0-2147483647	Mark this route as "Out Of Service" if the interface fails to connect after n consecutive attempts
def_route	n	chkoos_int	0-2147483647	If the interface fails to connect, try again in s seconds
def_route	n	chkoos_deact	0-2147483647	Deactivate the interface after it successfully connects
def_route	n	dial_int	0-255 Default 10	Do not allow this interface to be activated by this route for s seconds after the last activation attempt
def_route	n	q1	on,off	Only queue one packet whilst waiting for the interface to connect
def_route	n	deact_ent	Blank,PPP	When this route becomes available, deactivate the following interfaces x,y
def_route	n	deact_add	0-2147483647	When this route becomes available, deactivate the following interfaces x,y

Entity	Instance	Parameter	Values	Equivalent Web Parameter
def_route	n	deact_ent2	Blank,PPP	When this route becomes available, deactivate the following interfaces x,y
def_route	n	deact_add2	0-2147483647	When this route becomes available, deactivate the following interfaces x,y
def_route	n	unoos_secs	0-2147483647	Keep this route in service for s seconds after OOS state is cleared
def_route	n	rgroup	0-255	Assign this route to recovery group n

RIP parameters

The web pages and command line commands described in this section control the configuration of the routing Information Protocol (RIP) functionality of the router.

Global RIP Settings

Enable RIP

When enabled, enables the RIP functionality.

Send RIP advertisements every s seconds

The interval between sending RIP packets. These packets contain the current routes held by the router (such as any active PPP routes), static routes and the default route. A value of 0 disables sending.

Mark routes as unusable if we don't get advertisements for s seconds

The time for which an updated metric will apply when a RIP update is received. If no updates are received within this period, the usual metric will take over.

Delete routes after another s seconds

The length of time that the router will continue to advertise this route when a RIP update timeout occurs and the route metric is **16**. This behavior is designed to help propagate the dead route to other routers. The router will no longer use a metric advertised by a RIP update if the route has been set out of service locally.

Allow RIP to update static routes

When enabled, allows an incoming, matching RIP update to change the metric of the static route. This happens when the update matches a configured static route.

Enable Poison Reverse

When enabled, enables poison reverse, to notify when a neighboring router is unavailable.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
rip	n	enable	on,off	Enable RIP
rip	n	interval	0-2147483647	Send RIP advertisement every s seconds
rip	n	ripto	0-2147483647	Mark routes as unusable if we don't get advertisement for s seconds
rip	n	riplingerto	0-2147483647	Delete routes after another s seconds
rip	n	updatestatic	on,off	Allow RIP to update static routes
rip	n	poisonreverse	on,off	Enable Poison Reverse

Access Lists parameters

The router has the ability to modify route metrics based upon received RIP responses. Static routes and default routes will have their metric modified if the route fits within one of the routes found within the RIP packet. For Ethernet routes, the gateway for the route will be set to the source address of the RIP packet. The route modifications will be enforced for **180 seconds**, unless another RIP response is received within that time.

RIP packets must have a source address that is included in the RIP access list.

Adding permitted IP addresses to the access list is controlled using a table with the single parameter described below.

IP Address a.b.c.d

The IP address to be added to the list of IP addresses that RIP packets must come from if they are to modify route metrics. Up to ten IP addresses may be added. The **Add** and **Delete** buttons work in the usual way for configuration tables.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
riprx	0-9	IPaddr	Valid IP address a.b.c.d	IP Address a.b.c.d

Authentication Keys parameters

RIP authentication keys are used with the plain password and MD5 RIP authentication methods.

Key k

The RIP authentication key. Enter a string of up to 16 characters long. A current key will not be displayed.

Confirm Key

Re-enter the new authentication key into this text box to allow the router to check that the two are identical.

Key ID (MD5 only)

The ID for the authentication key. The ID is inserted into the RIP packet when using RIP v2 MD5 authentication and is used to look up the correct key for received packets. The valid range is **0-255**.

Valid from now/dd,mm,yy

These two radio buttons select, between having the validity period for the key starting immediately of allowing a start date to be defined. The starting date is specified using a drop down list to select the start day, a drop-down list to select the start month and a text box to enter the start year. Selecting the **Disable** option from the day and **None** from the month means that this key should not be used. The year can be specified as either two or four digits, such as **11** or **2011**.

Expires Never/dd,mm,yy

These two radio buttons select between defining the end date using the drop-down lists and text box or by setting the expiration to **Never**. The key end day is selected from the first drop down list. Selecting **Disable** means that the key should not be used. The end month is selected from the second drop-down list. Selecting **None** means that the key should not be used. The year is entered into the text box and can be in two- or four-digit format.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ripauth	0-9	key	Up to 16 characters	Key k
ripauth	0-9	keyid	0-255	Key ID
ripauth	0-9	sday	0-31	Valid from d,m,y
ripauth	0-9	smon	0-12	Valid from d,m,y
ripauth	0-9	syear	0-65535	Valid from d,m,y
ripauth	0-9	eday	0-31	Expires d,m,y
ripauth	0-9	emon	0-12	Expires d,m,y
ripauth	0-9	eyear	0-65535	Expires d,m,y

Interfaces > Ethernet / PPP / GRE parameters

The configuration in these three sub-menus is identical.

Send RIP advertisements on this interface

Check this box to enable RIP and to reveal further configuration parameters below.

Use RIP

RIP version level. Select from the values **V1**, **V2** and **V1 Compat** (version 1-compatible). When RIP version is set to **V1** or **V2**, the router will transmit RIP version 1 or 2 packets respectively (version 2 packets are sent to the all routers multicast address **224.0.0.9**). When RIP Version is set to **V1 Compat**, the router will transmit RIP version 2 packets to the subnet broadcast address. This allows **V1** capable routers to act upon these packets.

Send RIP advertisements as

- **Broadcasts**: RIP packets are by default sent out on a broadcast basis or to a multi-cast address. Do not change this parameter unless you intend to alter this behavior.

- **Multicasts** (Only visible when **V2** is selected in the **Use RIP** option above): This is automatically selected for sending to the default RIP v2 multicast address **224.0.0.9**.

- **<BLANK BOX>**: This parameter may be used to force RIP packets to be sent to a specified IP or multicast address. It is particularly useful if you need to route the packets via a VPN tunnel. By default Broadcasts/multicasts are selected, depending on your RIP version.

Use Authentication:

Selects the authentication method for RIP packets. Only one option is enabled multiple selections are not possible.

None

When set to **Off**, the interface sends and receives packets without any authentication.

Access list

When set to **Access List**, the interface sends RIP packets without any authentication. When receiving packets, the interface checks the sender's IP address against the list entered on the **Configuration > Network > IP Routing / Forwarding > RIP > Global RIP settings > Access Lists** page, and if the IP address is present in the list, the packet is allowed through.

Plain password

When set to **Plain password (V1+V2)**, the interface uses the first valid key it finds (set on the **Configuration > Network > IP Routing / Forwarding > RIP > Global RIP settings > Authentication Keys > Authentication Key n pages**), and use the plain text RIP authentication method before sending the packet out. If no valid key can be found, the interface will not send any RIP packets. When receiving a RIP packet, a valid plain text key must be present in the packet before it will be accepted. This method can be used with both RIP V1 and RIP V2.

MD5

When set to **MD5 (V2 only)**, the interface uses the first valid key it finds (set on the **Configuration > Network > IP Routing / Forwarding > RIP > Global RIP settings > Authentication Keys > Authentication Key n** pages), and uses the MD5 authentication algorithm before sending the packet out. If no valid key can be found, the interface will not send any RIP packets. Received RIP packets must be authenticated using the MD5 authentication algorithm before they will be accepted. This method can be used with RIP V2.

Only send RIP advertisements when this interface is in service

Select this parameter for RIP advertisements only to be sent when the interface is in the UP state in the routing table.

Use Triggered RIP on this interface

Enables triggered RIP (RFC2091). When triggered RIP is enabled, RIP timers are disabled.

Include this interface in Rip advertisements

Select to cause the subnet configured on this interface to not be advertised by RIP.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
tun/ ppp	n	rip	0,1	Enable RIP=1 Disable RIP=0
tun/ ppp	n	ripip	Valid IP address a.b.c.d	Unicast RIP update address
tun/ ppp	n	ripauth	0-3	0=None 1=Access List 2=Plain Password 3=MD5 v2 only
tun/ ppp	n	ripis	on,off	Turn on to send updates only when in service
tun/ ppp	n	inrip	on,off	Include interface subnet in RIP advertisements
tun/ ppp	n	triggeredrip	on,off	Enable RIP RFC2091

OSPF parameters

Open Shortest Path First (OSPF) is an Interior Gateway Protocol (IGP) developed for IP networks based on the shortest path first or link-state algorithm.

The router uses link-state algorithms to send routing information to all nodes in a network by calculating the shortest path to each node based on a topography of the network constructed by each node. Each router sends that portion of the routing table that describes the state of its own links and the complete routing structure (network topography).

The advantage of the shortest path first algorithms is that they result in smaller, more frequent update everywhere. They converge quickly, thus preventing such problems as routing loops and Count-to-Infinity (where routers continuously increment the hop count to a particular network). This makes for a stable network.

To use OSPF on the router, a valid configuration file must exist in the router's filing system.

Enable OSPF

When enabled, displays the following parameters:

OSPF Configuration Filename

The file that contains the configuration data for OSPF is selected from this drop-down list. The file should have a **.conf** extension.

Load Config file

When this button is clicked, the router attempts to load the file specified in the file selection list box into the edit window below the button. The text in the window can be edited as required.

Save Config File

When this button is clicked, the text in the edit window will be saved to the filename specified in the drop-down list above. These three controls allow loading, editing, an saving an OSPF configuration file.

Restart OSPF after configuration file is saved

When enabled, restarts the OSPF functions once the edited configuration file has been saved.

Restart OSPF if a fatal error occurs

When enabled, restarts OSPF functioning after a delay of 5 seconds if a fatal error occurs.

OSPF Tracing

In common with some of the other functionality of the router, OSPF supports some debug functionality. The amount of information in the debug traces is controlled from this drop-down list. The available levels are **Off**, **Low**, **Med**, and **High**. Selecting **Off** disables debug tracing.

Ignore MTU indications

All OSPF routers must have the same Maximum Transmitted Unit (MTU) and this value is advertised in the OSPF packets. When checked, the router ignores received packets that have a MTU that differs from that of the router itself.

Use Interface IPsec source IP

When enabled, OSPF functions use the source IP address of the interface specified in **Configuration > Network > Interfaces > Advanced > PPP n: Use interface x,y for the source IP address of IPsec packets on the interface being used**. When unchecked, OSPF uses the source IP address of the interface being used for its source address.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ospf	0	Enable	on,off	Enable OSPF
ospf	0	conffile		OSPF Configuration Filename
ospf	0	new_cfg_rest	on,off	Restart OSPF after a configuration file is saved
ospf	0	fatal_rest	on,off	Restart OSPF if a fatal error occurs
ospf	0	debug	0-3 0=Off 1=Low 2=Med 3=High	OSPF Tracing
ospf	0	ignore_mtu	on,off	Ignore MTU indications
ospf	0	useipsecent	on,off	Use Interface IPsec source IP

BGP parameters

The Border Gateway Protocol (BGP) routing protocol is supported by TransPort routers. This page contains the configuration parameters used to control the behavior of BGP. Most of the configuration is controlled by a configuration file (raw text) named bgp.cnf. This file would normally be created in a text editor on a computer and loaded onto the router. The router contains a simple editor that can be used to modify the file. The configuration parameters described here mainly define what action is to be taken when errors occur, and specify the configuration file to be used.

Enable BGP

When enabled, enables BGP routing.

BGP Configuration Filename

The configuration file to use is selected from this drop-down list. The default filename is **bgp.cnf**. An error message will be displayed if the specified file cannot be found.

Load Config file

Click this button to load the file specified from the drop-down list. The contents of the file will be visible in the edit window which appears below the button.

Save Config File

If the edit functions are used to modify the file, it can be saved back to the filing system by clicking this button.

Restart BGP after configuration file is saved

When enabled, the router restarts routing using BGP after the file has been saved using the above **Save** button.

Restart BGP if a fatal error occurs

When enabled, the router restarts routing using BGP if a fatal error occurs.

Advertise non-connected networks

When enabled, BGP advertises networks that exist in the BGP configuration file but that are not actually a connected network or interface.

BGP Tracing

As with OSPF, the level of debug tracing information is selected from this drop-down list. The available levels are; **Off**, **Low**, **Med**, and **High**.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
bgp	0	enable	on,off	Enable BGP
bgp	0	conffile		BGP Configuration Filename
bgp	0	new_cfg_rest	on,off	Restart BGP after configuration file is saved
bgp	0	fatal_rest	on,off	Restart BGP if a fatal error occurs
bgp	0	allow_non_nets	on,off Default ON	Advertise non-connected networks
bgp	0	debug	0-3	BGP Tracing

IP Port Forwarding / Static NAT Mappings parameters

The router supports Network Address Translation (NAT) and Network Address and Port Translation (NAPT). NAT or NAPT may be enabled on a particular interface such as a PPP instance. When operating with NAT enabled, this interface has a single externally visible IP address. When sending IP packets, the local IP addresses (for example on a local area network) are replaced by the single IP address of the interface. The router keeps track of the local IP addresses and port numbers so that if a matching reply packet is received, it is directed to the correct local IP address. With only one externally visible IP address, NAT effectively prevents external computers from addressing specific local hosts, thus providing a very basic level of "firewall" security.

Static NAT mappings allow received packets destined for particular ports to be directed to specific local IP addresses. For example, to have a server, running on a local network, externally accessible, a static NAT mapping would be set up using the local IP address of the server and the port number used to access the required service.

Configuring IP port forwarding and static NAT mapping is done by entering the following configuration values into a table and using the Add button to add them into the NAT configuration for the router.

External Min Port

The lowest port number to be redirected.

External Max Port

The highest port number to be redirected.

Forward to Internal IP Address a.b.c.d

The IP address to which packets containing the specified destination port number are to be redirected.

Forward to Internal Port

The IP port number to which packets containing the specified port number are to be redirected. When set to **0**, no port remapping occurs and the original port number is used. The NAT mode parameter of the appropriate interface must be set to **NAPT** rather than **NAT** or **OFF** for this parameter to take effect.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
nat	0-29	minport	0-65535	External Min Port
nat	0-29	maxport	0-65535	External Max Port
nat	0-29	IPaddr	Valid IP address a.b.c.d	Forward to Internal IP Address a.b.c.d
nat	0-29	mapport	0-65535	Forward to Internal Port

Command format

`Nat <entry> <parameter> <value>`

Example commands

To set the IP address for entry 0 in the table to 10.1.2.10 enter the command:

`nat 0 IPaddr 10.1.2.10`

Multicast Routes parameters

Digi TransPort routers support multicast routes, allowing them to route packets to multicast group addresses. Up to 20 different static multicast routes may be configured.

Static multicast routes must be used in conjunction with the IGMP parameter on the outbound interface. For example, after configuring a static multicast route for multicast traffic via PPP 1, the IGMP parameter in **Configuration > Network > Interfaces > IGMP** must be set to **On**. Multicast routing is configured using a table with the following parameters.

Multicast Address a.b.c.d

This parameter is used in conjunction with the **Mask** parameter below, to specify the destination multicast group address for packets that will match this route. So, if a router receives a packet with a destination multicast group address that matches the specified **Multicast Address/Mask** combination, it will route that packet through the interface specified by the Interface parameters below.

Mask a.b.c.d

The address mask that is used in conjunction with the **Multicast Address** parameter as described above.

Interface x,y

These two parameters in the drop-down list and adjacent text box specify the interface and interface instance used to route packets matching the **Multicast Address/Mask** combination. The options available in the drop-down list are; **PPP**, **Ethernet**, **Tunnel**.

Enable multicast source path checking

Enables multicast source path checking.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
mcast	0-19	IPaddr	Valid IP address a.b.c.d	Multicast Address a.b.c.d
mcast	0-19	mask	Valid IP address a.b.c.d	Mask a.b.c.d
mcast	0-19	ll_ent	PPP,ETH,TUN	Interface x,y
mcast	0-19	ll_add	Valid interface number 0-2147483647	Interface x,y

Virtual Routing and Forwarding (VRF)

Virtual Routing and Forwarding (VRF) is an IP technology that allows multiple instances of a routing table to coexist on the same router at the same time. Because the routing instances are independent, the same or overlapping IP addresses can be used without conflict. VRF is also used to refer to a routing table instance that can exist in one or multiple instances per each VPN on a Provider Edge (PE) router.

VRF-Lite (Multi-VRF)

VRF-Lite is an application based on VRF that extends the concept of VRF to the Customer Edge (CE) router on the customer's premises. It supports multiple, overlapping, independent routing and forwarding tables per customer.

Any routing protocol supported by normal VRF can be used in a VRF-Lite CE implementation. The CE supports traffic separation between customer networks. As there is no MPLS functionality on the CE, no label exchange happens between the CE and PE.

Information Model Objects (IMOs)

- Virtual Routing Forwarding (VRF) Entity (IVrf)
- Equivalent Routing Entry (IRoutingEntries)
- Virtual Routing Entry (IVrfEntry)
- Multi Protocol BGP Entity (IMpBgp)
- Equivalent Cross Virtual Routing Entry (ICrossVrf)
- Cross Virtual Routing Entry (ICrossVrfRoutingEntry)

Virtual Routing Forwarding (VRF) Entity

The Virtual Routing Forwarding (VRF) Entity **<XREF>** object describes the routing and address resolution protocols' independent forwarding component of a MPLS-BGP based VPN router. It is bound by its Logical Sons attribute to all the Network layer IP Interface objects among which it is routing IP packets.

Attribute name	Attribute description	Scheme	Polling interval
Virtual Routing Table	Array of Equivalent Routing Entries	IPCore	Configuration
Exported Route Targets	Array of route target identifiers	IPCore	Configuration
Imported Route Targets	Array of route target identifiers	IPCore	Configuration
Address Families	List of the address families (IPv4, IPv6, or both)	IPCore	Configuration
Route Distinguisher	Route distinguisher	IPCore	Configuration
ARP Entity	Address resolution entity (ARP entity)	IPCore	Configuration
Name	VRF name	IPCore	Configuration
Logical Sons	Array of all IP interfaces among which this VRF entity is routing IP packets	IPCore	N/A
Description	Description of the VRF	IPCore	Configuration
Import Route-map	Name of the VRF import route map used to import IP prefixes into the VRF	IPCore	Configuration
Export Route-map	Name of the VRF export route map used to export IP prefixes from the VRF	IPCore	Configuration

Equivalent Routing Entry

The Equivalent Routing Entry and Virtual Routing Entry objects describe a routing table's entries. Each is an array of Virtual Routing Entries sharing a single IP Subnetwork destination.

Attribute name	Attribute description	Scheme	Polling interval
Routing Entries	Array of Virtual Routing Entries sharing a single destination	IPCore	Configuration

Virtual Routing Entry

Attribute name	Attribute description	Scheme	Polling interval
Next Hop BGP Address	Next hop Border Gateway Protocol (BGP) IP address	IPCore	Configuration
Incoming and Outgoing Inner Label	Incoming and outgoing inner MPLS label	IPCore	Configuration
Outer Label	Outer MPLS label	IPCore	Configuration
Destination IP Subnet	Final destination IP subnet	IPCore	Configuration
Next Hop IP Address	Next hop IP address	IPCore	Configuration
Type	Route entry type (Null, Other, Invalid, Direct, Indirect, Static)	IPCore	Configuration
Routing Protocol Type	Routing protocol type (Null, Other, Local, Network Managed, ICMP, EGP, GGP, Hello, RIP, IS-IS, ES-IS, Cisco IGRP, BBN, SPF, IGP, OSPF, BGP, EIGRP)	IPCore	Configuration
Outgoing Interface Name	Outgoing IP interface name	IPCore	Configuration

Multi Protocol BGP Entity

The Multi Protocol BGP Entity object describes the Border Gateway Protocol (BGP) component of a MPLS-BGP based VPN router. It is bound by its Logical Sons attribute to all Virtual Routing Forwarding (VRF) Entity objects among which it is routing IP packets.

Attribute name	Attribute description	Scheme	Polling interval
BGP Identifier	Border Gateway Protocol (BGP) identifier	IPCore	Configuration
Local Autonomous System	Local peer autonomous system	IPCore	Configuration
Cross Virtual Routing Table	Array of Equivalent Cross Virtual Routing Entry	IPCore	Configuration
BGP Neighbors	Array of BGP neighbor entries	IPCore	Configuration
Logical Sons	Array of all VRF Entity objects among which this Multi Protocol BGP Entity is routing IP packets	IPCore	Configuration

Equivalent Cross Virtual Routing Entry

The Equivalent Cross Virtual Routing Entry and Cross Virtual Routing Entry objects describe the first dimension of a cross virtual routing table, as an array of Cross Virtual Routing Entry objects sharing a single Virtual Routing Forwarding (VRF) Entity destination.

Attribute name	Attribute description	Scheme	Polling interval
Virtual Routing Entries	Array of Cross Virtual Routing Entry objects sharing a single destination	IPCore	Configuration
Exported Route Targets	Virtual Routing Entity (VRF) name	IPCore	Configuration

Cross Virtual Routing Entry

Attribute name	Attribute description	Scheme	Polling interval
Outgoing Virtual Routing Entity Identifier	Outgoing virtual routing entity Object Identifier (OID)	IPCore	Configuration
Incoming and Outgoing Virtual Routing Tags	Incoming and outgoing virtual routing tags	IPCore	Configuration
Destination IP Subnet	Final destination IP subnet	IPCore	Configuration
Next Hop IP Address Type	List of the address families (IPv4, IPv6, or both)	IPCore	Configuration
Type	Route entry type (Null, Other, Invalid, Direct, Indirect, Static)	IPCore	Configuration
Routing Protocol Type	Routing protocol type (Null, Other, Local, Network Managed, ICMP, EGP, GGP, Hello, RIP, IS-IS, ES-IS, Cisco IGRP, BBN, SPF IGP, OSPF, BGP, EIGRP)	IPCore	Configuration
Outgoing Interface Name	Address resolution entity (ARP entity)	IPCore	Configuration

Configuring VRFs

To configure one or more VRFs, perform these steps:

Step	Command	Purpose
1	Switch# configure terminal	Enters global configuration mode.
2	Switch(config)# ip routing	Enables IP routing.
3	Switch(config)# ip vrf *vrf-name*	Names the VRF and enters VRF configuration mode.
4	Switch(config-vrf)# rd *route-distinguisher*	Creates a VRF table by specifying a route distinguisher. Enter either an AS number and an arbitrary number (**xxx:y**) or an IP address and arbitrary number (**A.B.C.D.y**).
5	Switch(config-vrf)# route-target {export|import|both} *route-target-ext-community*	Creates a list of import, export, or import and export route target communities for the specified VRF. Enter either an AS number and an arbitrary number (**xxx:y**) or an IP address and arbitrary number (**A.B.C.D.y**). **Note:** This command is effective only if BGP is running.
6	Switch(config-vrf)# import map *route-map*	(Optional) Associates a route map with the VRF.
7	Switch(config-vrf)# interface *interface-id*	Enters interface configuration mode and specifies the Layer 3 interface to associate with the VRF. The interface can be a routed port or SVI.
8	Switch(config-if)# ip vrf forwarding *vrf-name*	Associates the VRF with the Layer 3 interface.
9	Switch(config-if)# end	Returns to privileged EXEC mode.
10	Switch# show ip vrf [brief|detail|interfaces] [vrf-name](config-if)# ip vrf forwarding *vrf-name*	Verifies the configuration. Displays information about the configured VRFs.
11	Name of the VRF export route map used to export IP prefixes from the VRF	Saves your entries in the configuration file.

Configure Virtual Private Networking (VPN)

This section covers configuring Virtual Private Networking (VPN) from the web interface and command line. It covers the following topics:

- About Virtual Private Networks (VPNs) on page 389
- About Internet Protocol Security (IPSec) on page 389
- IPsec parameters on page 394
- PPTP parameters on page 445
- OpenVPN parameters on page 447

About Virtual Private Networks (VPNs)

This section provides background on IPSec and VPNs.

VPNs

Virtual Private Networks (VPNs) are used to securely connect two private networks together so that devices may connect from one network to the other network using secure channels. VPN uses IP Security (IPSec) technology to protect the transferring of data over the Internet. This section covers concepts and settings for configuring VPNs.

VPNs (Virtual Private Networks) are networks that use the IPSec protocols to provide one or more secure routes, or tunnels, between endpoints. Users are issued either a shared secret key or public/ private key pair that is associated with their identity. When a message is sent from one user to another, it is automatically signed with the user's key. The receiver uses the secret key or the sender's public key to decrypt the message. These keys are used during IKE exchanges along with other information to create session keys that only apply for the lifetime of that IKE exchange.

About Internet Protocol Security (IPSec)

An inherent problem with the TCP protocol used to carry data over the vast majority of LANs and the Internet is that it provides virtually no security features. This lack of security, and publicity about hackers and viruses, prevent many people from even considering using the Internet for any sensitive business application. IPSec provides a remedy for these weaknesses adding a comprehensive security layer to protect data carried over IP links.

IPSec (Internet Protocol Security) is a framework for a series of IETF standards designed to authenticate users and data, and to secure data by encrypting it during transit.

Benefits of IPSec

- IPSec is typically used to attain confidentiality, integrity, and authentication in the transport of data across inherently insecure channels.

- When properly configured, IPSec provides a highly secure virtual channel across cheap, globally available networks such as the Internet, or creates a "network within a network" for applications such as passing confidential information between two users across a private network.

Protocols defined within IPSec

The protocols defined within IPSec include:

- **IKE**: Internet Key Exchange protocol
- **ISAKMP**: Internet Security Association and Key Management Protocol
- **AH**: Authentication Header protocol
- **ESP**: Encapsulating Security Payload protocol
- **HMAC**: Hash Message Authentication Code
- **MD5**: Message Digest 5
- **SHA-1**: Security Hash Algorithm

Cryptographic (encryption) techniques include:

- **DES**: Data Encryption Standard
- **3DES**: Triple DES
- **AES**: Advanced Encryption Standard (also known as Rijndael)

Two key protocols within the framework are AH and ESP. AH is used to authenticate users, and ESP applies cryptographic protection. The combination of these techniques is designed to ensure the integrity and confidentiality of the data transmission. Put simply, IPSec is about ensuring that:

- Only authorized users can access a service.
- No one else can see what data passes between one point and another.

Modes of operation in IPSec

There are two modes of operation for IPSec, transport mode and tunnel mode.

- In transport mode, only the payload (such as the data content), of the message is encrypted.
- In tunnel mode, the payload and the header and routing information are all encrypted thereby by providing a higher degree of protection.

Data Encryption Methods in IPSec

There are several different algorithms available for use in securing data whilst in transit over IP links. Each encryption technique has its own strengths and weaknesses and this is really, a personal selection made with regard to the sensitivity of the data you are trying to protect. Some general statements may be made about the relative merits but users should satisfy themselves as to suitability for any particular purpose.

DES (64-bit key)

This well-known and established protocol has historically been used extensively in the banking and financial world. It is relatively "processor intensive", such as to run efficiently at high data rates a powerful processor is required. It is generally considered very difficult for casual hackers to attack but may be susceptible to determined attack by well-equipped and knowledgeable parties.

3-DES (192-bit key)

Again, this is a well-established and accepted protocol but as it involves encrypting the data three times using DES with a different key each time, it has a very high processor overhead. This also renders it almost impossible for casual hackers to attack and very difficult to break in any meaningful time frame, even for well-equipped and knowledgeable parties.

AES (128-bit key)

Also known as Rijndael encryption, AES is a standard adopted by many USA and European organizations for sensitive applications. It has a relatively low processor overhead compared to DES and it is therefore possible to encrypt at higher data rates. As with 3-DES, it is almost impossible for casual hackers to attack and is very difficult to break in any meaningful time frame, even for well-equipped and knowledgeable parties.

To put these into perspective, common encryption programs that are considered "secure" (such as PGP) and on-line credit authorization services (such as Web-based credit card ordering) generally use 128-bit encryption.

Note Data rates are the maximum that could be achieved but may be lower if other applications are running at the same time or small IP packet sizes are used.

X.509 Certificates

In the previous section, security between two points was achieved by using a "pre-shared secret" or password. Certificates provide this sort of mechanism but without the need to manually enter or distribute secret keys. This is a complex area but put simply a user's certificate acts a little like a passport providing proof that the user is who they say they are and enclosing details of how to use that certificate to decrypt data encoded with it. Passports however can be forged so there also needs to be proof that the passport has been properly issued and hasn't been changed since it was. On a paper passport this is achieved by covering the photograph with a coating that shows if it has been tampered with, embedding the user's name in code in a long string of numbers, etc. In the same way, for a Security Certificate to be genuine it has to be protected from alteration as well. Like a passport, you also have to trust that the issuer is authorized and competent to create the certificate.

Certificates use something called a "Public/Private Key Pair". This a complex area but the principle is that you can create an encryption key made up from two parts, one private (known only to the user), the other public (known to everyone). Messages encrypted with someone's public key can only be recovered by the person with the Public AND Private key but as encrypting the message to someone in the first place only requires that you know their public key, anyone who knows that can send them an encrypted message, so you can send a secure message to someone knowing only their publicly available key. You can also prove who you are by including in the message your "identity" whereupon they can look up the certified public key for that identity and send a message back that only you can understand. The important principles are:

- Your private key cannot be determined from your public key.
- You both need to be able to look up the other's certified ID.

Once you have established a two-way secure link, you can use it to establish some rules for further communication.

Before this gets any more complicated, let us assume Digi International is a competent authority to issue certificates, and examine how certificates are used.

Generally, the issuing and management of certificates will be provided as a managed service by Digi or its partners, but some general information is provided here for system administrators.

Certificates are held in non-volatile files on the router. Any private files are named **privxxxx.xxx** and cannot be copied, moved, renamed, uploaded or typed. This is to protect the contents. They can be overwritten by another file, or deleted.

Two file formats for certificates are supported:

- **PEM**: Privacy Enhanced MIME
- **DER**: Distinguished Encoding Rules

Certificate and key files should be in one of these two formats, and should have an extension of.**pem** or **.der** respectively.

Note   The equivalent filename extension for.pem files in Microsoft Windows is **.cer**. By renaming.**pem** certificate files to **.cer**, it is possible to view their makeup under Windows.

The router maintains two lists of certificate files.

- The first is a list of "Certificate Authorities" or CAs. Files in this list are used to validate public certificates sent by remote users. Public certificates must be signed by one of the certificates in the CA list before the router can validate them. Certificates with the filename **ca*.pem** and **ca*.der** are loaded into this list at start-up time. In the absence of any CA certificates, a public certificate cannot be validated.

- The second list is a list of public certificates that the router can use to obtain public keys for decrypting signatures sent during IKE exchanges. Certificates with a filename **cert*.pem** and **cert*.der** are loaded into this list when the router is powered on or rebooted. Certificates in this list will be used in cases where the remote router does not send a certificate during IKE exchanges. If the list does not contain a valid certificate communication with the remote unit cannot take place.

Both the host and remote units must have a copy of a file called **casar.pem**. This file is required to validate the certificates of the remote units.

In addition, the host unit should have copies of the files **cert02.pem** (which allows it to send this certificate to remote units) and **privrsa.pem**. Note that before it can send this certificate, the **Remote ID** parameter in the **Configuration > Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec n - n > IPsec n** page must be set to **host@Digi.co.uk**.

The remote unit must have copies of **cert01.pem** and **privrsa.pem**. In addition, any Eroutes that are going to use certificates for authentication should be configured as follows:

Our ID

Should be set to **info@Digi.co.uk**. This is the same as the subject **Altname** in certificate **cert01.pem**, which makes it possible for the router to locate the correct certificate to send to the host.

Authentication Method

Should be set to **RSA Signatures**. This indicates to IKE that RSA signatures (certificates) are to be used for authentication. When IKE receives a signature from a remote unit, it needs to be able to retrieve the correct public key so that it can decrypt the signature, and confirm that the signature is correct. The certificate must either be on the FLASH file system, or be provided by the remote unit as part of the IKE negotiation. The ID provided by the remote unit is used to find the correct certificate to use. If the correct certificate is found, the code then checks that it has been signed by one of the certificate authority certificates (**ca*.pem**) that exist on the unit. The code first checks the local certificates, and then the certificate provided by the remote (if any). IKE will send a certificate during negotiations if it is able to find one that has subject **AltName** that matches the ID being used. If not able to locate the certificate, then the remote must have local access to the file so that the public key can be retrieved.

A typical setup may be that the host unit has a copy of all certificates. This means that the remote units only require the private key, and the certificate authority certificate. This eases administration as any changes to certificates need only be made on the host. Because they do not have a copy of their certificate, remote units rely on the host having a copy of the certificate. An alternative is that the remote units all have a copy of the certificate, as well as the private key and certificate authority certificate, and the host only has its own certificate. This scenario requires that the remote unit send its certificate during negotiations. It can validate the certificate because it has the certificate authority certificate.

IPsec parameters

IPsec (Internet Protocol security) refers to a group of protocols and standards that may be used to protect data during transmission over the internet (which is inherently insecure). Various levels of support for IPsec can be provided on the router depending on the model. The web pages located under the **Configuration > Network > Virtual Private Networking (VPN) > IPsec** are used to set the various parameters and options that are available. You should note however that this is a complex area and you should have a good understanding of user authentication and data encryption techniques before you commence. For further information refer to the IPsec and VPNs section in this manual. Also check the Technical Notes section of the Digi International web site at www.digi.com for the latest IPsec application notes.

The first stage in establishing a secure link between two endpoints on an IP network is for those two points to securely exchange a little information about each other. This enables the endpoint responding to the request to decide whether it wishes to enter a secure dialogue with the endpoint requesting it. To achieve this, the two endpoints commonly identify themselves and verify the identity of the other party. They must do this in a secure manner so that the process cannot be listened in to by any third party. The IKE protocol is used to perform this checking and if everything matches up it creates a Security Association (SA) between the two endpoints, normally one for data being sent **to** the remote end and one for data being received **from** it.

Once this initial association exists the two devices can talk securely about and exchange information on what kind of security protocols they would like to use to establish a secure data link, such as what sort of encryption and/or authentication they can use and what sources/ destinations they will accept. When this second stage is complete (and provided that both systems have agreed what they will do), IPSec will have set up its own Security Associations which it uses to test incoming and outgoing data packets for eligibility and perform security operations on before passing them down or relaying them from the tunnel.

IPsec Tunnels > IPsec n parameters

Once the IKE parameters have been set-up, the next stage is to define the characteristics of the IPsec tunnels, or encrypted routes. This includes items such as what source and destination addresses will be connected by the tunnel and what type of encryption and authentication procedures will be applied to the packets being tunneled. For obvious reasons it is essential that parameters such as encryption and authentication are the same at each end of the tunnel. If they are not, then the two systems will not be able to agree on what set of rules or policy to adopt for the IPsec tunnel and communication cannot take place.

Description

This parameter allows you to enter a name for IPsec tunnel to make it easier to identify.

The IP address or hostname of the remote unit

The IP address or hostname of the remote IPsec peer that a VPN will be initiated to.

Use a.b.c.d as a backup unit

The IP address or hostname of a backup peer. If the router cannot open a connection to the primary peer, this configuration will be used. Please note that the backup peer device must have an identical IPsec tunnel configuration as the primary peer.

Use these settings for the local LAN

These define the local LAN subnet settings used on the IPsec tunnel.

IP Address

Use this IP address for the local LAN subnet. This is usually the IP address of the router's Ethernet interface or that of a specific device on the local subnet (such as a PC running a client or host application).

Mask

Use this IP mask for the local LAN subnet. The mask sets the range of IP addresses that will be allowed to use the IPsec tunnel.

Use interface x,y

Use the IP address and mask of the specified interface.

Use these settings for the remote LAN

These define the remote LAN subnet settings used on the IPsec tunnel.

IP Address

Use this IP address for the remote LAN subnet. This is usually the IP address of the peer's Ethernet interface or that of a specific device on the local subnet (such as a PC running a client or host application).

Mask

Use this IP mask for the remote LAN subnet. The mask sets the range of IP addresses that will be allowed to use the IPsec tunnel.

Remote Subnet ID

Normally used with L2TP/IPsec VPNs. When the router is in server mode and negotiating IPsec from behind a NAT box, this parameter should be configured to the ID sent by the remote Windows client (this is usually the computer name).

Use the following security on this tunnel

These settings define the security identities used on the IPsec tunnel.

Security type	Description
Preshared Keys	Requires that both IPsec peers share a secret key, or password, that can be matched by and verified by both peers.
	To configure the PSK, a user will need configuring that matches the inbound ID of the remote peer and the PSK is configured using the password parameter. This is done via **Configuration > Security > Users**. The **User** configuration serves a dual purpose, in that it may contain entries for normal login access (such as HTTP, FTP or Telnet), and entries for IPsec tunnels.
XAUTH Init Preshared Keys	Used when the remote peer is a Cisco device using XAUTH and PSK authentication.
RSA Signatures	Select this option when the IPsec authentication will use X.509 certificates.
XAUTH Init RSA	Used when the remote peer is a Cisco device using XAUTH and X.509 certificates for authentication.

Our ID

When Aggressive mode is **On**, this parameter is a string of up to 20 characters. It is sent to the remote peer to identify the initiator (such as the router). The variable **%s** can be used in this parameter which will cause the router's serial number to be sent. It can be prefixed with other text if required.

When certificates are being used, this parameter should be configured with the **Altname** field in a valid certificate held on the router.

Our ID type

Defines how the remote peer is to process the Our ID configuration.

ID type	Description
IKE ID	The Our ID parameter is a simple key ID (such as **vpnclient1**).
FQDN	The Our ID parameter is a Fully Qualified Domain Name (such as **vpnclient1.anycompany.com**)
User FQDN	The Our ID parameter is a Fully Qualified Domain Name with a user element (such as **joe.bloggs@anycompany.com**)
IPv4 Address	An IPv4 Address in dotted decimal notation.

Remote ID

When Aggressive mode is **On**, this parameter is a string of up to 20 characters, used to identify the remote peer. It should contain the same text as the Our ID parameter in the remote peer's configuration. When Aggressive mode is **Off**, this parameter must be the IP address of the remote peer.

RSA Key File

This parameter can be used to override the private key filename in the IKE configuration. It is only used when RSA Signatures (Certificates) are being used for the authentication stage of the IKE negotiation.

Use enc encryption on this tunnel

The ESP encryption protocol to use with this IPsec tunnel. The options are:

- **No** (None)
- **Null**
- **DES**
- **3DES**
- **AES (128 bit keys)**
- **AES (192 bit keys)**
- **AES (256 bit keys)**

If the dropdown options only display **None** and **Null**, the router requires encryption enabling. See your Digi sales contact regarding enabling encryption.

Use auth authentication on this tunnel

The ESP authentication algorithm to use with this IPsec tunnel. The options are:

- **No (None)**
- **MD5**
- **SHA1**

Use Diffie Hellman group

The Diffie Hellman (DH) group to use when negotiating new IPsec SAs. When used, the IPsec SA keys cannot be predicted from any of the previous keys generated. The options are **No PFS**, **1**, **2**, or **3**. The larger values result in stronger keys, but they take longer to generate.

Use IKE n to negotiate this tunnel

The IKE version to use to negotiate this IPsec tunnel.

Use IKE configuration

The IKE configuration instance to use with this Eroute when the router is configured as an Initiator.

Bring this tunnel up

Controls how the IPsec tunnel is brought up. The options are:

- **All the time**
- **Whenever a route to the destination is available**
- **On demand**

If the tunnel is down and a packet is ready to be sent

Defines the action that is performed when the IPsec tunnel is down and a packet needs to be sent. The options are:

- **Bring the tunnel up**
- **Drop the packet**
- **Send the packet without encryption and authentication**

Bring this tunnel down if it is idle for h hrs m mins s secs

Used when the IPsec tunnel is configured to come up on demand and defines how long the IPsec tunnel should remain up if there is no traffic is being sent on the tunnel.

Renew the tunnel after

Defines the constraints of when the IPsec tunnel SA has to be renewed.

h hrs m mins s secs

Renew the IPsec SA after the specified amount of time.

n units of traffic

Renew the IPsec SA after the specified amount of traffic has been passed over the tunnel.

The units can be Kbytes, Mbytes or Gbytes.

A value of **0** means that this parameter is not used, and SAs will expire and be renewed based time, rather than amount of traffic.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
eroute	n	descr	String	Description
eroute	n	peerip	IP address or hostname	The IP address or hostname of the remote unit.
eroute	n	bakpeerip	IP address or hostname	Use **n** as a backup unit.
eroute	n	locip	IP address	IP Address (for Local LAN)
eroute	n	locmsk	IP Mask	IP Mask (for Local LAN)
eroute	n	locipifent	blank, ETH, PPP	Use interface **x,y** x=Interface type
eroute	n	locipifadd	Integer	Use interface **x,y** **y**=interface number
eroute	n	remip	IP address	IP Address (for Remote LAN).
eroute	n	remmsk	IP Mask	IP Mask (for Remote LAN).
eroute	n	remnetid	String	Remote Subnet ID.
eroute	n	authmeth	Off, Preshared, xauthinitpre, rsa, xauthinitrsa	Use the following security on this tunnel.
eroute	n	ourid	String	Our ID.
eroute	n	ouridtype	0=IKE ID 1=FQDN 2=User FQDN 3=IPv4 Address	Our ID type.
eroute	n	peerid	String	Remote ID.
eroute	n	privkey	Filename	RSA Key File.

Entity	Instance	Parameter	Values	Equivalent Web Parameter
eroute	n	espenc	off, null, des, 3des, aes	Use enc encryption on this tunnel.
eroute	n	enckeybits	128, 192, 256	Use enc encryption on this tunnel.
eroute	n	espauth	off, md5, sha1	Use auth authentication on this tunnel.
eroute	n	dhgroup	0, 1, 2, 3	Use Diffie Hellman group.
eroute	n	ikever	1, 2	Use IKE n to negotiate this tunnel.
eroute	n	ikecfg	0, 1	Use IKE configuration.
eroute	n	autosa	0=On Demand 1=When a route to the destination is available 2=All the time	Bring this tunnel up.
eroute	n	nosa	drop, pass, try	If the tunnel is down and a packet is ready to be sent.
eroute	n	inact_to	Integer	Bring this tunnel down if it is idle for **h** hrs **m** mins **s** secs. This CLI value is entered in seconds only.
eroute	n	ltime	Integer	Renew the tunnel after **h** hrs **m** mins **s** secs. This CLI value is entered in seconds only.
eroute	n	lkbytes	Integer	Renew the tunnel after n units of traffic. This CLI value is entered in Kbytes only.

Tunnel Negotiation parameter

Enable IKE tracing

Enables the router to write IKE negotiation information in the analyser trace.

Negotiate a different IP address and Mask

The IPsec tunnel can be configured to negotiate a different local LAN IP address and mask. The firewall can then be used to translate the source addresses of the packets to a value that lies within the negotiated range. This is so that a packet can match more than one IPsec tunnel but will use a different source address (from the peer's perspective) depending on which IPsec tunnel gets used.

IP Address

The alternative IP address to negotiate.

Mask

The alternative IP mask to negotiate.

Negotiate a virtual IP address using MODECFG

Used when the remote peer is a Cisco device using MODECFG to assign a specific IP address to this router during SA setup negotiations. This is commonly seen in Remote Access (RA) type VPNs and EasyVPN solutions.

XAuth ID

Extended Authentication ID for use with Cisco XAUTH.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
eroute	n	debug	on, off	Enable IKE tracing
eroute	n	neglocip	IP Address	Negotiate a different IP address and Mask
eroute	n	neglocmsk	IP Mask	Negotiate a different IP address and Mask
eroute	n	vip	on, off	Negotiate a virtual IP address using MODECFG
eroute	n	xauthid	String	XAuth ID

Advanced parameters

IPsec mode

Selects the IPsec encapsulation type to use on the IPsec tunnel. In Tunnel mode, the entire IP packet (header and payload) is encrypted. In Transport mode, only the IP payload is encrypted.

Use algorithm AH authentication on this tunnel

The AH authentication algorithm to use with this IPsec tunnel. The options are:

- No (None)

- MD5

- SHA1

Use algorithm compression on this tunnel

The compression algorithm to use with this IPsec tunnel. The options are:

- No (None)

- DEFLATE

Delete SAs when this tunnel is down

When selected, all SAs associated with the IPsec tunnel are deleted when the tunnel goes out of service.

Delete SAs when router is not a VRRP master

When selected, at least one Ethernet interface must be set as VRRP Master before the router can create SAs. If the router switches away from VRRP Master state, the SAs will be deleted. When the router switches back to VRRP Master state, the SAs will be created automatically.

Go out of service if automatic establishment fails

The router will take the IPsec tunnel out of service if the automatic establishment fails rather than continually retrying.

Go out of service after n consecutive auto-negotiation failures

The router will take the IPsec tunnel out of service if the auto-negotiation fails for the specified consecutive number of times rather than continually retrying.

This tunnel can only use apn

When enabled, this parameter allows you to choose between using the main APN or the backup APN, as defined in the **Configuration > Network > Serial > W-WAN Port page**.

Link tunnel with interface with x,y

When enabled, this parameter can be set so that the IPsec tunnel will only match packets using the specified interface. When this parameter is enabled, the route will take outgoing packets going through this IPsec tunnel and recheck to see if the resultant packet also goes through a tunnel.

If the inner tunnel is an IPsec tunnel (such as needs IKE), you can get the inner IKE to use the correct source address (matching the outer tunnel selectors) by enabling the Use secondary IP address parameter and the inner IKE will use the IP address configured in the Secondary IP address parameter on the **Configuration > Network > Advanced Network Settings** page.

Inhibit this IPsec tunnel when IPsec tunnels n are up

A list of IPsec tunnels that can inhibit this IPsec tunnel from being used as long as they are up. If this IPsec tunnel has been allowed to come up, and the IPsec tunnel that inhibits it comes back up, this IPsec is taken down and any SAs that may have existed are removed. As soon as an inhibiting IPsec tunnel goes down, the router will check to see if the inhibited IPsec tunnel can now create SAs.

Inhibit this IPsec tunnel unless IPsec tunnel n is up

This IPsec tunnel will be inhibited unless specified IPsec tunnel is also up.

IKE negotiation source IP address is taken from the

Defines which IP address IKE uses as the source IP address during the negotiation.

Interface

Use the IP address of the interface over which the IKE packets will be transmitted.

Secondary IP address

Use the IP address configured in the Secondary IP address parameter on the **Configuration > Network > Advanced Network Settings** page.

Interface x,y

Use the IP address of the specified interface.

Tunnel this IPsec tunnel inside another IPsec tunnel

It is possible to tunnel packets from an IPsec tunnel within a second (or more) tunnel. When this parameter is enabled.

NAT-Traversal Keepalive timer s seconds

Sets the interval period, in seconds, that the router will use to send regular packets to a NAT device in order to prevent the NAT table entry from expiring.

Allow protocol IP protocol(s) in this tunnel

This restricts the type of IP packets that will be tunneled through the IPsec tunnel. The options are:

- **All**
- **TCP**
- **UDP**
- **GRE**

IP packets with ToS values n must use this tunnel

Packets with matching ToS fields will only be tunneled through this IPsec tunnel and no others. The usual traffic selector matching still takes place as normal. Packets that don't have matching ToS values will get tunneled as normal. Enter the ToS values as a comma separated list, such as **2,4**.

Only tunnel IP packets with

Restricts the IP packets that will be tunneled to those with matching TCP/UDP port numbers.

local TCP/UDP port n

Allow IP packets with matching source TCP/UDP ports to be tunneled.

remote TCP/UDP port n

Allow IP packets with matching destination TCP/UDP ports to be tunneled.

local TCP/UDP port in the range of n1 to n2

Allow IP packets with source TCP/UDP ports in the specified range to be tunneled. This is only available when IKEv2 is used.

remote TCP/UDP port in the range of n1 to n2

Allow IP packets with destination TCP/UDP ports in the specified range to be tunneled. This is only available when IKEv2 is used.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
eroute	n	mode	tunnel, transport	IPsec Mode.
eroute	n	ahauth	off, md5, sha1	Use a AH authentication on this tunnel.
eroute	n	ipcompalg	off, deflate	Use c compression on this tunnel.
eroute	n	oosdelsa	on, off	Delete SAs when this tunnel is down.
eroute	n	ifvrrpmaster	on, off	Delete SAs when router is not a VRRP master.
eroute	n	nosaoos	on, off	Go out of service if automatic establishment fails.
eroute	n	nosadeactcnt	Integer	Go out of service after **n** consecutive auto-negotiation failures.
eroute	n	check_apnbu	on, off	This tunnel can only use apn.
eroute	n	apnbu	0=Main APN 1=Backup APN	This tunnel can only use apn.
eroute	n	ifent	blank, ETH, PPP	Link tunnel with interface with x,y. x=Interface type
eroute	n	ifadd	Integer	Link tunnel with interface with x,y. y=Interface number
eroute	n	inhibitno	Comma separated list of Integers	Inhibit this IPsec tunnel when IPsec tunnels n are up.
eroute	n	requireno	Integer	Inhibit this IPsec tunnel unless IPsec tunnel n is up.
eroute	n	usesecip	on, off	IKE negotiation source IP address is taken from the Secondary IP Address.

Entity	Instance	Parameter	Values	Equivalent Web Parameter
eroute	n	ipent	blank, ETH, PPP	IKE negotiation source IP address is taken from the Interface x,y. x=Interface type
eroute	n	ipadd	Integer	IKE negotiation source IP address is taken from the Interface x,y. y=Interface number
eroute	n	intunnel	on, off	Tunnel this IPsec tunnel inside another IPsec tunnel.
eroute	n	natkaint	Integer	NAT-Traversal Keepalive timer s seconds.
eroute	n	proto	off, tcp, udp, gre	Allow protocol IP protocol(s) in this tunnel.
eroute	n	toslist	Comma separated list of Integers	IP packets with ToS values n must use this tunnel.
eroute	n	locport	0-65535	Only tunnel IP packets with local TCP/UDP port.
eroute	n	remport	0-65535	Only tunnel IP packets with remote TCP/UDP port.
eroute	n	locfirstport	0-65535	Only tunnel IP packets with local TCP/UDP port in the range of n1 to n2.
eroute	n	loclastport	0-65535	Only tunnel IP packets with local TCP/UDP port in the range of n1 to n2.
eroute	n	remfirstport	0-65535	Only tunnel IP packets with remote TCP/UDP port in the range of n1 to n2.
eroute	n	remlastport	0-65535	Only tunnel IP packets with remote TCP/UDP port in the range of n1 to n2.

Set up IPsec tunnels for multiple users

For small numbers of users it is usual to set up an individual eroute for each user. However, to ease configuration where large numbers of users are required, the ***** character can be used as a wildcard to match multiple user IDs. For example, setting the **Peer ID** parameter to **Digi*** would match all remote units having an **Our ID** parameter starting with **Digi**, such as **Digi01**, **Digi02**, etc.

Example

To set up multiple users in this way, first set up the **Our ID** parameter on the host unit to a suitable name, such as **Host1**. Then set the **Peer ID** parameter to **Remote*** for example. In addition, an entry would be made in the user table with **Remote*** for the Username and a suitable **Password** value, such as **mysecret**.

Each of the remote units that required access to the host would then have to be configured with an **Our ID** parameter of **Remote01**, **Remote02**, etc., and each would have to have an entry in their user table for **User Host1** along with its password, such as the pre-shared key.

Parameter	Host Router	Remote Router1	Remote Router2	Remote Router1
Peer ID	Remote*	Host1	Host1	Host1
Our ID	Host1	Remote01	Remote02	Remote03
Username	Remote*	Host1	Host1	Host1
Password	mysecret	mysecret	mysecret	mysecret

IPsec Default Action

Like a normal IP routing set-up, IPSec Tunnels have a default configuration that is applied if no specific tunnel can be found. This is useful when, for instance, you wish to have a number of remote users connect via a secure channel, for example, to access company financial information, but also still allow general remote access to other specific servers on your network or the Internet.

```
▼ IPsec Default Action
  When a packet is received which does not match any IPsec tunnel
    ⦿ Pass the packet
    ○ Drop the packet
  When a packet is to be transmitted which does not match any IPsec tunnel
    ⦿ Pass the packet
    ○ Drop the packet
```

When a packet is received which does not match any IPsec tunnel

How the router responds if a packet is received when there is no SA.

- If you select the **Drop the packet** option, only packets that match a specified IPsec tunnel are routed; all other data will be discarded. This has the effect of enforcing a secure connection to all devices behind the router.

- If you select the **Pass the packet** option, packets that match an IPsec tunnel are decrypted and authenticated (depending on the IPsec tunnel's configuration) but data that does not match will also be allowed to pass.

When a packet is to be transmitted which does not match any IPsec tunnel

How the router will respond if a packet is transmitted when there is no SA.

- If you select the **Drop the packet** option, then only packets that match a specified IPsec tunnel are routed, all other data is discarded.

- If you select the **Pass the packet** option, then data that matches an IPsec tunnel is encrypted and authenticated, depending on the IPsec tunnel configuration, but data that does not match will also be allowed to pass.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
def_eroute	0	nosain	drop, pass	When a packet is received which does not match any IPsec tunnel.
def_eroute	0	nosaout	drop, pass	When a packet is to be transmitted which does not match any IPsec tunnel.

IPsec Groups

This mode of operation can be used when the router is terminating tunnels to a large number of remote devices such as when being used as a VPN Concentrator. To keep the size of the configuration file in the router small and also to maintain ease of configuration, only the information that is used for all tunnels is stored on the router. All other information that is site specific is stored in a MySQL database. This means the number of sites that can be configured is limited only by the SQL database size and performance. This will be literally millions of sites, depending upon the operating system and hardware of the MySQL PC. The number of sites that can be connected to concurrently are much smaller and limited by the model of the router.

• The router with the IPsec Group/MySQL configuration is the VPN Concentrator.

• The remote sites will normally not require an IPsec group configuration as they will normally only need to connect to a single peer, the VPN Concentrator.

• The VPN Concentrator will normally need only a single IPsec group configured.

• The local and remote subnet parameters need to be set up wide enough to encompass all the local and remote networks.

• The VPN Concentrator can act as an initiator and/or a responder. In situations where there are more remote sites than the router can support concurrent sessions, it will normally be necessary for the VPN Concentrator and the remote sites to be both an initiator and a responder. This is so both the remote sites and the head-end can initiate the IPsec session when required.

• It is also important to configure the IPsec tunnels to time out on inactivity to free up sessions for other sites. In the case of the VPN Concentrator acting as an initiator, when it receives a packet that matches the main IPsec tunnel, if no Security Associations already exist, it looks up the required parameters in the database.

• The TransPort will then create a dynamic IP tunnel containing all the settings from the base IPsec tunnel and all the information retrieved from the database.

• At this point, IKE will create the tunnel (IPsec security associations) as normal.

• The dynamic IPsec tunnel will continue to exist until all the IPsec Security Associations have been removed.

• When the maximum supported (or licensed) number of tunnels has been reached by the router, the oldest Dynamic IPsec tunnels (those that have not been used for the longest period of time) and their associated IPsec Security Associations are dropped, to allow new inbound VPNs to connect.

Logic flow: creation of IPSec SAs

Logic flow for VPN Concentrator acting as initiator

The VPN Concentrator normally acts as an initiator when it receives an IP packet for routing with a source address matching the IPsec tunnel local subnet address & mask and a destination address matching the remote subnet address & mask, provided an IPsec SA does not already exist for this site.

1. If an IPsec group is configured to use the matching IPsec tunnel, the router uses a MySQL query to obtain the site specific information in order to create the SAs.

2. The VPN Concentrator creates a SELECT query using the destination IP address of the packet and the mask configured in the IPsec group configuration to determine the remote subnet address. This means that the remote subnet mask must be the same on all sites using the current IPsec group.

3. Once the site-specific information is retrieved, the router creates a dynamic IPsec Tunnel which is based upon the base IPSec tunnel configuration plus the site specific information from the MySQL database.

4. The router then uses the completed IPsec tunnel configuration and IKE to create the IPsec SAs.

5. For the pre-shared key, IKE uses the password returned from the MySQL database rather than doing a local look up in the user configuration.

6. Once created, the SAs are linked with the dynamic IPsec tunnel. Replacement SAs are created as the lifetimes start to get low and traffic is still flowing.

7. When all SAs to this remote router are removed, the dynamic IPsec tunnel is removed, so that IPsec tunnel can then be re-used to create tunnels to other remote sites.

8. When processing outgoing packets, dynamic IPsec Tunnels are searched before base IPsec tunnels. So, if a matching dynamic IPsec tunnel is found, it is used, and the base IPsec tunnel is only matched if no dynamic IPsec tunnel exists.

9. Once the dynamic IPsec tunnel is removed, further outgoing packets will match the base IPsec tunnel and the process is repeated.

Logic flow for VPN Concentrator acting as a responder to a session initiated from the remote site

1. When a remote site needs to create an IPsec SA with the VPN Concentrator it sends an IKE request to the VPN Concentrator.

2. The VPN Concentrator needs to be able to confirm that the remote device is authorized to create an IPsec tunnel. The remote site supplies its ID to the host during the IKE negotiations. The VPN Concentrator uses this ID in a search of the IPsec tunnels configured and dynamic IPsec tunnels to see if the supplied ID matches the configured Peer ID (peerid). If a match is found, the MYSQL database is queried to retrieve the information required to complete the negotiation (such as pre-shared key/password). If no matching base IPsec tunnel is found, the local user configuration is used to locate the password, and a normally configured IPsec tunnel must also exist.

3. Once the information is retrieved from the MySQL database, IKE negotiations continue, and the created IPsec SAs will be associated with the dynamic IPsec tunnel.

4. As long as the dynamic IPsec tunnel exists, it behaves just like a normal IPsec tunnel. such as SAs being replaced/removed as required.

5. If errors are received from the MySQL database, or not enough fields are returned, the dynamic IPsec tunnel is removed, and IKE negotiations in progress are terminated.

6. There are a limited number of dynamic IPsec tunnels. If the number of free dynamic IPsec tunnel is less than 10% of the total number of dynamic IPsec tunnel, the router periodically removes the oldest dynamic IPsec tunnel. This is done to ensure that there will always be some free dynamic IPsec tunnel available for incoming connections from remote routers. To view the current dynamic tunnels that exist using the WEB server, browse to **Management > Connections > Virtual Private Networking (VPN) > IPsec**. The table indicates the base IPsec tunnel and the **Remote Peer ID** in the status display, to help identify which remote sites are currently connected.

Preliminary IP Tunnel configuration

The IPsec tunnel configuration **Configuration > Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec n** differs from a normal configuration in the following ways:

- **Peer IP/hostname**: Because the peer IP address to each peer is unknown and is retrieved from the database, this field is left empty.

- **Bakpeerip** (CLI only): Because the peer IP address to each peer is unknown and is retrieved from the database, this field is left empty.

- **Peer ID**: When the host Digi is acting as a responder during IKE negotiations, the router uses the ID supplied by the remote to decide whether or not the MySQL database should be interrogated. So that the router can make this decision, the remote router must supply an ID that matches the peerid configured into the IPsec tunnel. Wildcard matching is supported which means that the peerid may contain ***** and **?** characters. If only one IPsec tunnel is configured, the peerid field may contain a *****, indicating that all remote IDs result in a MySQL look up.

- **Local subnet IP address / Local subnet mask**: Configured as usual.

- **Remote subnet IP address / Remote subnet mask**: These fields should be configured in such a way that packets to ALL remote sites fall within the configured subnet. such as if there are two sites with remote subnets **192.168.0.0/24**, and **192.168.1.0/24** respectively, a valid configuration for the host would be **192.168.0.0/23** so that packets to both remote sites match.

All other fields should be configured as usual. It is possible to set up other IPsec groups linked with other IPsec tunnels. This would be done if there is a second group of remote sites that have a different set of local and remote subnets, or perhaps different encryption requirements. The only real requirement is that this second group uses peer IDs that do not match up with those in use by the first IPsec group.

IPsec Group configuration

This configuration holds information relating to the MySQL database, and the names of the fields where the information is held. This configuration is also used to identify which IPsec tunnels are used to create dynamic IPsec tunnels.

Example MySQL schema

```
mysql> describe eroutes;
+-----------+-------------+------+-----+---------+-------+
| Field     | Type        | Null | Key | Default | Extra |
+-----------+-------------+------+-----+---------+-------+
| peerip    | varchar(20) | YES  |     | NULL    |       |
| bakpeerip | varchar(20) | YES  |     | NULL    |       |
| peerid    | varchar(20) | NO   | PRI |         |       |
| password  | varchar(20) | YES  |     | NULL    |       |
| ourid     | varchar(20) | YES  |     | NULL    |       |
| remip     | varchar(20) | YES  | UNI | NULL    |       |
| remmsk    | varchar(20) | YES  |     | NULL    |       |
+-----------+-------------+------+-----+---------+-------+
7 rows in set (0.01 sec)
```

Link this IPsec group with IPsec Tunnel

The base IPsec tunnel number. This parameter allows the router to see that an IPsec tunnel should use the group configuration to retrieve dynamic information from the database.

Remote mask to use for tunnels

Used in the SQL SELECT query in conjunction with the destination IP address of packets to be tunneled from the host to the remote peer to identify the correct record to select from the MySQL database.

MySQL Server IP Address or Hostname

The IP address or hostname of the MySQL Server.

MySQL Server Port

The port that the MySQL Server is listening on.

Username

The username to use when logging into the MySQL Server.

Password / Confirm Password

The password to use when logging into the MySQL Server.

Database name

The name of the database to connect to.

Database table

The name of the table when the remote site information is stored.

Remote subnet IP

The name of the field in the table where the 'remip' data is stored.

Remote subnet Mask

The name of the field in the table where the **remmsk** data is stored.

Peer IP Address

The name of the field in the table where the **peerip** data is stored.

Backup Peer IP Address

The name of the field in the table where the **bakpeerip** data is stored.

Peer ID

The name of the field in the table where the **peerid** data is stored.

Our ID

The name of the field in the table where the **ourid** data is stored.

Password

The name of the field in the table where the password to use in IKE negotiations is stored.

Note The default MySQL field names match the matching IPsec tunnel configuration parameter name. The default field name for the **password** field is **password**.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
egroup	n	eroute	Integer	Link this IPsec group with IPsec Tunnel
egroup	n	remmsk	IP Mask	Remote mask to use for tunnels
egroup	n	dbhost	IP Address or Hostname	MySQL Server IP Address or Hostname
egroup	n	dbport	0-65535	MySQL Server Port
egroup	n	dbuser	String	Username
egroup	n	dbpwd	String	Password / Confirm Password
egroup	n	dbname	String	Database name
egroup	n	dbtable	String	Database table
egroup	n	fremip	String	Remote subnet IP
egroup	n	fremmsk	String	Remote subnet Mask
egroup	n	fpeerip	String	Peer IP Address
egroup	n	fbakpeerip	IP Address	Backup Peer IP Address
egroup	n	fpeerid	String	Peer ID
egroup	n	fourid	String	Our ID
egroup	n	fpwd	String	Password

Use IPSec Egroups with an SQL database

When IPSec Egroups are used with a SQL database for dynamic Eroute configuration, there are CLI commands that will help with configuration and troubleshooting on the router.

Local Database commands

As well as using an external SQL database, the router can cache the SQL table entries it learns from the SQL server in RAM so if the SQL server goes offline for any reason, the database entries are still available to renew existing IPSec SAs.

To configure the caching options the command used is `sql 0 <parameter> <value>`.

The following parameters are available to configure the caching of database entries:

dbsrvmem <n>

This parameter is used to specify the amount of memory (RAM) the MySQL server cache should use. Where **<n>** is specified in multiples of 1k, such as **10Mb=10240**

To calculate the amount of memory to specify in this parameter:

- Note the size of the database file (**.csv**) that will be loaded into the router memory.

- Double this value and add **100Kb**, for example, if the csv file is **200Kb**, this would make a value of **500Kb** for the memory allocation. Use the command **sql 0 dbsrvmem 500**.

- Load the database file into memory and check the memory allocated and free using the **smem** command. This will show the memory allocated and left available. Increase the memory in the **dbsrvmem** command if required.

dbfile <name>

This is the name of the **.csv** file that the router will use to store the table definitions (1st line) and data records. This file is stored in flash and is used to populate the database stored in RAM on power up or when a new file matching this name has just been stored. The dbfile can be populated with records or be empty except for the definitions line. The dbfile stored in RAM will be populated from both the dbfile stored in flash and (if configured) via caching items learned from the main SQL server. The dbfile in flash can then be updated from the dbfile in RAM and saved.

dbname <name>

This is the name of the backup database in case the main database goes offline. This name needs to match the database name in use on the SQL server.

learn <off|on>

When enabled, the router will cache entries learned via the main SQL database in a file stored in RAM. This can be used as a backup in the event of the main SQL database going offline. To use learning mode, at least one column in the **.csv** dbfile must be marked as a unique key, with the **U** prefix.

For example, remip is marked as the unique key:

`peerip[IP],bakpeerid[IP],peerid[K20],password[20],ourid[20],remip[UKIP],remmsk[IP]`

Learning mode: saving entries

When learning mode is used, the dynamic backup database is stored in RAM. This database will be lost if the router is power-cycled. The database in RAM can be saved to flash to over-write the dbfile with the one in RAM that includes the learned entries or it can be saved to a new file.

To save the dbfile to flash from RAM, use the following command:

```
sqlsave 0 <filename>
```

Where *<filename>* is the name of the destination file.

For example, to save the learned database entries to a file called **backup.csv**:

```
sqlsave 0 backup.csv
```

If there are no learned entries, this command will not create a file. To view the number to learned entries, use the command **sql 0 ?**, and in the output, see the section headed **Learning info**:

```
Learning info.
items learned:0
matched retrievals:0
OK
```

Configure a TransPort to use a backup database

Once the router has been configured to run a SQL csv database locally, this backup csv database can be used in the event of the main SQL database going offline. The configuration parameters required are:

1. Configure the IP address of the SQL server to use.

```
egroup 0 dbhost "192.168.0.50"
```

2. Configure the IP address of the SQL server that will have a backup database. If a socket connection fails to this IP address, the router will use the backup IP address.

```
ipbu 0 IPaddr "192.168.0.50"
```

3. Configure the backup database IP address; that is, the loopback address of the router or an alternative SQL server, this example shows the loopback IP address of the router.

```
ipbu 0 BUIPaddr "127.0.0.1"
```

4. Set the amount of time in seconds that the connection to the main SQL server will be retried.

```
ipbu 0 retrysec 30
```

5. Set the router to use the backup IP address if the main database is unavailable.

```
ipbu 0 donext ON
```

For example, to configure and use a local backup database when the main SQL database at **192.168.0.50** is offline, the configuration may look similar to this:

```
egroup 0 dbhost "192.168.0.50"
sql 0 dbsrvmem 200
sql 0 dbfile "sardb.csv"
sql 0 dbname "sarvpns"
sql 0 learn ON
sqlsave 0 backup.csv
ipbu 0 IPaddr "192.168.0.50"
ipbu 0 BUIPaddr "127.0.0.1"
ipbu 0 retrysec 30
ipbu 0 donext ON
```

smem command: Display memory information

smem

Displays the amount of memory allocated, in use and available for use by the MySQL server on the router.

Transact SQL commands

To query a SQL database manually using transact SQL statements, the following commands can be used.

- To connect to the SQL server and database:

  sqlcon <host> <user> <pwd> <database>

  For example:

  sqlcon 192.168.0.50 sqluser sqlpass eroute-db

- To issue transact SQL statements:

  sqldo <"cmd">

  For example:

  sqldo "select * from site where subnet='10.110.100.0' limit 3"

- To limit the **sqldo** command to only act on specified fields, the following command can be used:

  sqlfields "<field1> <field2> <field3>"

  For example:

  sqlfields "remmsk password peerip"

  After issuing the **sqlfields** command, all further **sqldo** commands will apply to these fields only.

- When finished, to close the SQL server connection correctly:

  sqlclose

- If the database being queried is held locally on the router, these commands can be preceded with the SQL **debug** command to give extra feedback on any commands issued.

- To enable the SQL debug:

  sql 0 debug_opts 3

- To view the debug data via the ASY 0 port:

  debug 0

- To view the debug data via telnet:

  debug t

- To disable the SQL debug:

  sql 0 debug_opts 0

  debug off

Dead Peer Detection parameters

When Dead Peer Detection (DPD) is enabled on an IPsec tunnel, the router will send an IKE DPD request at regular intervals. If no response is received to the DPD request, the IPsec tunnel is considered as suspect and the requests are sent at a shorter interval until either the maximum number of outstanding requests allowed is reached or a response is received. If no response is received to the configured maximum requests, the IPSec tunnels are closed.

Note IKE DPD requests require that an IKE SA is present. If one is not present, the DPD request will fail.

To help ensure that an IKE SA exists with a lifetime at least as great as the IPsec lifetime, the router creates new IKE SAs whenever the IPsec SA lifetime exceeds the lifetime of an existing IKE SA and attempts to negotiate a lifetime for the IKE SA that is 60 seconds longer than the desired lifetime of the IPsec SA.

DPD can be enabled or disabled in each IKE configuration.

Mark the IPsec tunnel as suspect if there is no traffic for 60   seconds
Send a DPD request on a healthy link every 120   seconds
Send a DPD request on a suspect link every 5   seconds
Close the IPsec tunnels after no response for 3   DPD requests

Mark the IPsec tunnel as suspect if there is no traffic for n seconds

The period of time of inactivity on a tunnel before it is deemed to be suspect, such as if there is no activity on a healthy link for the time period defined, then the tunnel is them deemed to be suspect.

Send a DPD request on a healthy link every n seconds

The interval at which DPD requests are sent on an IPsec tunnel that is deemed to be healthy. A healthy link is one with traffic.

Send a DPD request on a suspect link every n seconds

The interval at which DPD requests are sent on an IPsec tunnel that is deemed to be suspect. A suspect link is one where there has been no traffic for a specified period of time.

Close the IPsec tunnels after no response for n DPD requests

The maximum number of DPD requests that will be sent without receiving a response before the IPsec tunnels are closed.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
dpd	0	inact	Integer	Mark the IPsec tunnel as suspect if there is no traffic for n seconds
dpd	0	okint	Integer	Send a DPD request on a healthy link every n seconds
dpd	0	failint	Integer	Send a DPD request on a suspect link every n seconds
dpd	0	maxfail	Integer	Close the IPsec tunnels after no response for n DPD requests

IKE parameters

The **Configuration > Network > Virtual Private Networking (VPN) > IPsec > IKE** folder opens to list configuration pages for **IKE 0** and **IKE 1** with a separate page for IKE Responder. The **IKE 0** instance can be used as an IKE initiator or as an IKE responder, while IKE 1 can only be used as an initiator. The **IKE 0** and **IKE 1** pages are used to set up the **IKE 0** and **IKE 1** initiator parameters as required. The **IKE Responder** page is used to set up the responder parameters for **IKE 0**.

IKE Debug parameters

Enable IKE Debug

Enables IKE debugging to be displayed on the debug port.

Debug Level

Sets the level of IKE debugging. The options are:

- **Low**

- **Medium**

- **High**

- **Very High**

Debug IP Address Filter

Used to filter out IKE packets with particular source or destination IP addresses. The format of this parameter is a comma-separated list of IP addresses. For example, to exclude the capture of IKE traffic from IP hosts **10.1.2.3** and **10.2.2.2**, enter **10.1.2.3,10.2.2.2** for this parameter.

Conversely, you may wish to only capture traffic to and from particular IP hosts. To do this, use a tilde (**~**) symbol before the list of IP addresses. For example, to only capture packets to and from IP host **192.168.47.1**, enter **~192.168.47.1** for this parameter.

Forward debug to port

When enabled, the IKE debug is sent to debug serial port.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ike	0	deblevel	0=Off 1=Low 2=Medium 3=High 4=Very High	Debug Level
ike	0	ipaddfilt	Comma-separated list of IP addresses	Debug IP Address Filter
ike	0	debug	on, off	Forward debug to port

IKE n parameters

Use the following settings for negotiation

The settings used during the IKE negotiation.

Encryption

The encryption algorithm used. The options are:

- **None**
- **DES**
- **3DES**
- **AES (128 bit keys)**
- **AES (192 bit keys)**
- **AES (256 bit keys)**

Authentication

The authentication algorithm used. The options are:

- **None**
- **MD5**
- **SHA1**

Mode

The negotiation mode. The options are:

- **Main**

- **Aggressive**

Historically, fixed IP addresses have been used in setting up IPSec tunnels. Today it is more common, particularly with Internet ISPs, to dynamically allocate the user a temporary IP address as part of the process of connecting to the Internet. In this case, the source IP address of the party trying to initiate the tunnel is variable and cannot be pre-configured.

In **Main** mode, such as non-aggressive, the source IP address must be known such as this mode can only be used over the Internet if the ISP provides a fixed IP address to the user or you are using X.509 certificates.

Aggressive mode was developed to allow the host to identify a remote unit (initiator) from an ID string rather than from its IP address. This means that it can be used over the Internet via an ISP that dynamically allocates IP addresses. It also has two other noticeable differences from main mode. Firstly, it uses fewer messages to complete the phase 1 exchange (3 compared to 5) and so will execute a little more quickly, particularly on networks with large turn-around delays such as GPRS. Secondly, as more information is sent unencrypted during the exchange, it is potentially less secure than a normal mode exchange.

Note Main mode can be used without knowing the remote unit's IP address when using certificates. This is because the ID of the remote unit (its public key) can be retrieved from the certificate file.

MODP Group for Phase 1

The key length used in the IKE Diffie-Hellman exchange to **768** bits (group 1) or **1024** bits (group 2). Normally this option is set to **group 1**; this is sufficient for normal use. For particularly sensitive applications, you can improve security by selecting **group 2** to enable a 1024 bit key length. Note, however, that this will slow down the process of generating the phase 1 session keys (typically from 1-2 seconds for group 1), to 4-5 seconds.

MODP Group for Phase 2

The minimum width of the numeric field used in the calculations for phase 2 of the security exchange. With **No PFS** (Perfect Forwarding Security) selected, the data transferred during phase 1 can be reused to generate the keys for the phase 2 SAs, hence speeding up connections. However, in doing this it is possible (though very unlikely), that if the phase 1 keys were compromised (such as discovered by a third party), the phase 2 keys might be more easily compromised. Enabling group **1** (**768**) or **2** (**1024**) or **3** (**1536**), IPSec MODP forces the key calculation for phase 2 to use new data that has no relationship to the phase 1 data and initiates a second Diffie-Hellman exchange. This provides an even greater level of security, but can take longer to complete.

Renegotiate after h hrs m mins s secs

How long the initial IKE Security Association stays in force. When this time expires, any attempt to send packets to the remote system results in IKE attempting to establish a new SA.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ike	n	encalg	des, 3des, aes	Encryption
ike	n	keybits	0, 128, 192, 256	Encryption (AES Key length)
ike	n	authalg	md5, sha1	Authentication
ike	n	aggressive	on, off	Mode
ike	n	ikegroup	1, 2, 5	MODP Group for Phase 1
ike	n	ipsecgroup	1, 2, 5	MODP Group for Phase 2
ike	n	ltime	1-28800	Renegotiate after h hrs m mins s secs This CLI value is entered in seconds only.

Advanced IKE parameters

Retransmit a frame if no response after n seconds

The amount of time, in seconds, that IKE will wait for a response from the remote unit before transmitting the negotiation frame.

Stop IKE negotiation after n retransmissions

The maximum number of times that IKE will retransmit a negotiation frame as part of the exchange before failing.

Stop IKE negotiation if no packet received for n seconds

The period of time, in seconds, after which the router will stop the IKE negotiation when no response to a negotiation packet has been received.

Enable Dead Peer Detection

Enables Dead Peer Detection. For more information, refer to the **Configuration > Network > IPsec > Dead Peer Detection (DPD)** page.

Enable NAT-Traversal

Enables support for NAT Traversal within IKE/IPsec. When one end of an IPsec tunnel is behind a NAT box, some form of NAT traversal may be required before the IPsec tunnel can pass packets. Turning NAT Traversal on enables the IKE protocol to discover whether or not one or both ends of a tunnel is behind a NAT box, and implements a standard NAT traversal protocol if NAT is not being performed. The version of NAT traversal supported is that described in the IETF draft document **draft-ietf-ipsec-nat-t-ike-03.txt**.

Send INITIAL-CONTACT notifications

Enables INITIAL-CONTACT notifications to be sent.

Retain phase 1 SA after failed phase 2 negotiation

Normally IKE functionality is to remove the phase 1 SA if the phase 2 negotiation fails. Enabling this parameter will cause the router to retain the existing phase 1 SA and retry the phase 2 again.

RSA private key file

The name of a X.509 certificate file holding the router's private part of the public/private key pair used in certificate exchanges. See X.509 Certificates on page 392 section for further explanation.

SA Removal Mode

Determines how IPsec and IKE SAs are removed.

- **Normal** operation will not delete the IKE SA when all the IPsec SAs that were created by it are removed and will not remove IPsec SAs when the IKE SA that was used to create them is deleted.

- R**emove IKE SA when last IPSec SA removed** deletes the IKE SA when all the IPsec SAs that it created to a particular peer are removed.

- **Remove IPSec SAs when IKE SA removed** deletes all IPSec SAs that have been created by the IKE SA that has been removed.

- **Both** removes IPSec SAs when their IKE SA is deleted, and deletes IKE SAs when their IPSec SAs are removed.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ike	n	retranint	0-255	Retransmit a frame if no response after n seconds
ike	n	retran	0-9	Stop IKE negotiation after n retransmissions
ike	n	inactto	0-255	Stop IKE negotiation if no packet received for n seconds
ike	n	dpd	on, off	Enable Dead Peer Detection
ike	n	natt	on, off	Enable NAT-Traversal
ike	n	initialcontact	on, off	Send INITIAL-CONTACT notifications
ike	n	keepph1	on, off	Retain phase 1 SA after failed phase 2 negotiation
ike	n	privrsakey	Filename	RSA private key file
ike	n	delmode	0=Normal 1=Remove IKE SA when last IPsec SA removed 2=Remove IPsec SAs when IKE SA remove 3=Both	SA Removal Mode
ike	n	openswan	on, off	None. This enables support for Openswan IKE implementations.

IKE Responder command

This page displays the various parameters for **IKE 0** when used in Responder mode.

Enable IKE Responder

Allows the router to respond to incoming IKE requests.

Accept IKE Requests with

Defines the settings that the router will accept during the negotiation

Encryption

The acceptable encryption algorithms.

Authentication

The acceptable authentication algorithms.

MODP Group between x and y

The acceptable range for MODP group.

Renegotiate after h hrs m mins s secs

How long the initial IKE Security Association will stay in force. When the IKE Security Association expires, any attempt to send packets to the remote system will result in IKE attempting to establish a new SA.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ike	0	noresp	on, off	Enable IKE Responder
ike	0	rencalgs	des, 3des, aes Multiple algorithms can specified in a comma-separated list	Encryption
ike	0	keybits	0, 128, 192, 256	Encryption (Minimum AES Key length)
ike	0	rauthalgs	md5, sha1 Multiple algorithms can specified in a comma separated list	Authentication
ike	0	rdhmingroup	1, 2, 5	MODP Group between x and y
ike	0	rdhmaxgroup	1, 2, 5	MODP Group between x and y
ike	0	ltime	1-28800	Renegotiate after h hrs m mins s secs This CLI value is entered in seconds only.

Advanced IKE Responder parameters

Stop IKE negotiation if no packet received for n seconds

The period of time in seconds after which the router will stop the IKE negotiation when no response to a negotiation packet has been received.

Enable NAT-Traversal

Enables support for NAT Traversal within IKE/IPsec. When one end of an IPsec tunnel is behind a NAT box, some form of NAT traversal may be required before the IPsec tunnel can pass packets. Turning NAT Traversal on enables the IKE protocol to discover whether or not one or both ends of a tunnel is behind a NAT box, and implements a standard NAT traversal protocol if NAT is not being performed. The version of NAT traversal supported is that described in the IETF draft **draft-ietf-ipsec-nat-t-ike-03.txt**.

Send INITIAL-CONTACT notifications

Enables **INITIAL-CONTACT** notifications to be sent.

Send RESPONDER-LIFETIME notifications

Enables **RESPONDER-LIFETIME** notifications sent to the initiator. If an initiator requests an IKE lifetime that is greater than the responder, a notification will be sent and the initiator should reduce its lifetime value accordingly.

Retain phase 1 SA after failed phase 2 negotiation

The name of a X.509 certificate file holding the router's private part of the public/private key pair used in certificate exchanges. See X.509 Certificates on page 392 for further explanation.

RSA private key file

The name of a X.509 certificate file holding the router's private part of the public/private key pair used in certificate exchanges. See X.509 Certificates on page 392 for further explanation.

SA Removal Mode

Determines how IPsec and IKE SAs are removed.

- **Normal** operation will not delete the IKE SA when all the IPsec SAs that were created by it are removed and will not remove IPsec SAs when the IKE SA that was used to create them is deleted.

- **Remove IKE SA when last IPSec SA removed** deletes the IKE SA when all the IPsec SAs that it created to a particular peer are removed.

- **Remove IPSec SAs when IKE SA removed** deletes all IPSec SAs that have been created by the IKE SA that has been removed.

- **Both** removes IPSec SAs when their IKE SA is deleted, and delete IKE SAs when their IPSec SAs are removed.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ike	0	inactto	0-255	Stop IKE negotiation if no packet received for n seconds
ike	0	natt	on, off	Enable NAT-Traversal
ike	0	initialcontact	on, off	Send **INITIAL-CONTACT** notifications
ike	0	respltime	on, off	Send **RESPONDER-LIFETIME** notifications
ike	0	keepph1	on, off	Retain phase 1 SA after failed phase 2 negotiation
ike	0	privrsakey	Filename	RSA private key file
ike	0	delmode	0=Normal 1=Remove IKE SA when last IPsec SA removed 2=Remove IPsec SAs when IKE SA remove 3=Both	SA Removal Mode

MODECFG Static NAT mappings parameters

MODECFG is an extra stage built into IKE negotiations that fits between IKE phase 1 and IKE phase 2. It performs operations such as extended authentication (XAUTH) and requesting an IP address from the host. This IP address becomes the source address to use when sending packets through the tunnel from the remote to the host. This mode of operation (receiving one IP address from the remote host) is called client mode. Another mode, network mode, allows the router to send packets with a range of source addresses through the tunnel.

If the router receives packets from a local interface that need to be routed through the tunnel, it performs address translation so the source address matches the assigned IP address before encrypting using the negotiated SA. Some state information is retained so that packets coming in the opposite direction with matching addresses/ports can have their destination address set to the source address of the original packet, in the same way as standard NAT.

If the remote end of the tunnel can access units connected to the local interface, the unit that has been assigned the virtual IP address needs to have some static NAT entries set up. When a packet is received through the tunnel, the router first looks up existing NAT entries, followed by static NAT entries to determine whether the destination address/port should be modified, and forwards the packet to the new address. If a static NAT mapping is found, the router creates a dynamic NAT entry that will be used for the duration of the connection. If no dynamic or stateful entry is found, the packet is directed to the local protocol handlers.

External Port	Forward to Internal IP Address	Forward to Internal Port	Range Port Count	
No mappings have been configured				
				Add

▼ MODECFG Static NAT mappings

Map the following port ranges
(you may configure up to 20 mappings):

External Port

The lowest destination port number to be matched if the packet is redirected.

Forward to Internal IP Address

An IP address to which packets containing the specified destination port number are redirected.

Forward to Internal Port

A port number to which packets containing the specified destination port number are redirected.

Port Range Count

The number of ports to be matched.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
tunsnat	n	minport	0-65535	External Port
tunsnat	n	maxport	0-65535	Port Range Count
tunsnat	n	ipaddr	IP Address	Forward to Internal IP Address
tunsnat	n	mapport	0-65535	Forward to Internal Port

IKEv2 parameters

When IKE Version 2 is supported, it is possible to specify whether the IKEv1 or IKEv2 protocol should be used to negotiate IKE SAs. By default, IKEv1 is used. Routers which have been upgraded to support IKEv2 will not require any changes to their configuration to continue working with IKEv1.

Use the following settings for negotiation

The settings used during the IKEv2 negotiation

Encryption

The encryption algorithm used. The options are:

- **None**
- **DES**
- **3DES**
- **AES (128 bit keys)**
- **AES (192 bit keys)**
- **AES (256 bit keys)**

Authentication

The authentication algorithm used. The options are:

- **None**
- **MD5**
- **SHA1**

PRF Algorithm

The PRF (Pseudo Random Function) algorithm used. The options are:

- **MD5**
- **SHA1**

MODP Group for Phase 1

Sets the key length used in the IKE Diffie-Hellman exchange to **768** bits (**group 1**) or **1024** bits (**group 2**). Normally, this option is set to **group 1** and this is sufficient for normal use. For particularly sensitive applications, you can improve security by selecting **group 2** to enable a 1024 bit key length. Note however that this will slow down the process of generating the phase 1 session keys (typically from 1-2 seconds for **group 1**), to 4-5 seconds.

Renegotiate after h hrs m mins s secs

How long the initial IKEv2 Security Association will stay in force. When it expires any attempt to send packets to the remote system will result in IKE attempting to establish a new SA.

Rekey after h hrs m mins s secs

When the time left until expiry for this SA reaches the value specified by this parameter, the IKEv2 SA will be renegotiated, such as a new IKEv2 SA is negotiated and the old SA is removed. Any IPSec child SAs that were created are retained and become children of the new SA.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ike2	n	iencalg	des, 3des, aes	Encryption
ike2	n	ienkeybits	128, 192, 256	Encryption (AES Key length)
ike2	n	iauthalg	md5, sha1	Authentication
ike2	n	iprfalg	md5, sha1	PRF Algorithm
ike2	n	idhgroup	1, 2, 5	MODP Group for Phase 1
ike2	n	ltime	1-28800	Renegotiate after h hrs m mins s secs This CLI value is entered in seconds only.
ike2	n	rekeyltime	1-28800	Rekey after h hrs m mins s secs This CLI value is entered in seconds only.

Advanced IKEv2 n parameters

Retransmit a frame if no response after n seconds

The amount of time in seconds that IKEv2 will wait for a response from the remote unit before transmitting the negotiation frame.

Stop IKE negotiation after n retransmissions

The maximum number of times that IKEv2 will retransmit a negotiation frame as part of the exchange before failing.

Stop IKE negotiation if no packet received for n seconds

The period of time, in seconds, after which the router will stop the IKE v2 negotiation when no response to a negotiation packet has been received.

Enable NAT-Traversal

Enables support for NAT Traversal within IKE/IPsec. When one end of an IPsec tunnel is behind a NAT box, some form of NAT traversal may be required before the IPsec tunnel can pass packets. Turning NAT Traversal on enables the IKE protocol to discover whether or not one or both ends of a tunnel is behind a NAT box, and implements a standard NAT traversal protocol if NAT is not being performed. The version of NAT traversal supported is that described in the IETF draft **draft-ietf-ipsec-nat-t-ike-03.txt**.

NAT traversal keep-alive interval n seconds

The interval, in seconds, in which the NAT Traversal keepalive packets are sent to a NAT device in order to prevent NAT table entry from expiring.

RSA private key file

The name of a X.509 certificate file holding the router's private part of the public/private key pair used in certificate exchanges. See X.509 Certificates on page 392 for further explanation.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ike2	n	retranint	0-255	Retransmit a frame if no response after n seconds
ike2	n	retran	0-9	Stop IKE negotiation after n retransmissions
ike2	n	inactto	0-255	Stop IKE negotiation if no packet received for n seconds
ike2	n	natt	on, off	Enable NAT-Traversal
ike2	n	natkaint	Integer	NAT traversal keep-alive interval n seconds
ike2	n	privrsakey	Filename	RSA private key file

IKEv2 Responder parameters

This page displays the various parameters for IKEv2 0 when used in Responder mode.

Enable IKEv2 Responder

Allows the router to respond to incoming IKE requests.

Accept IKEv2 Requests with

The settings that the router will accept during the negotiation

Encryption

The acceptable encryption algorithms.

Authentication

The acceptable authentication algorithms.

PRF Algorithm

The acceptable PRF (Pseudo Random Function) algorithms.

MODP Group between x and y

The acceptable range for MODP group.

Renegotiate after h hrs m mins s secs

How long the initial IKE Security Association will stay in force. When it expires any attempt to send packets to the remote system will result in IKE attempting to establish a new SA.

Rekey after h hrs m mins s secs

When the time left until expiry for this SA reaches the value specified by this parameter, the IKEv2 SA will be renegotiated, such as a new IKEv2 SA is negotiated and the old SA is removed. Any IPSec child SAs that were created are retained and become children of the new SA.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ike2	0	rencalgs	des, 3des, aes	Encryption
ike2	0	renckeybits	128, 192, 256	Encryption (Minimum AES key length)
ike2	0	rauthalgs	md5, sha1	Authentication
ike2	0	rprfalgs	md5, sha1	PRF Algorithm
ike2	0	rdhmingroup	1, 2, 5	MODP Group between x and y
ike2	0	rdhmaxgroup	1, 2, 5	MODP Group between x and y
ike2	0	ltime	1-28800	Renegotiate after h hrs m mins s secs This CLI value is entered in seconds only.
ike2	0	rekeyltime	1-28800	Rekey after h hrs m mins s secs This CLI value is entered in seconds only.

Advanced IKEv2 Responder parameters

Stop IKE negotiation if no packet received for n seconds

The period of time, in seconds, after which the router will stop the IKEv2 negotiation when no response to a negotiation packet has been received.

Enable NAT-Traversal

Enables support for NAT Traversal within IKE/IPsec. When one end of an IPsec tunnel is behind a NAT box, some form of NAT traversal may be required before the IPsec tunnel can pass packets. Turning NAT Traversal on enables the IKE protocol to discover whether or not one or both ends of a tunnel is behind a NAT box, and implements a standard NAT traversal protocol if NAT is not being performed.

The version of NAT traversal supported is that described in the IETF draft **draft-ietf-ipsec-nat-t-ike-03.txt**.

NAT traversal keep-alive interval n seconds

The interval, in seconds, in which the NAT Traversal keepalive packets are sent to a NAT device in order to prevent NAT table entry from expiring.

RSA private key file

The name of a X.509 certificate file holding the router's private part of the public/private key pair used in certificate exchanges. See X.509 Certificates on page 392 for further explanation.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ike2	0	inactto	0-255	Stop IKE negotiation if no packet received for n seconds
ike2	0	natt	on, off	Enable NAT-Traversal
ike2	0	natkaint	Integer	NAT traversal keep-alive interval n seconds
ike2	0	privrsakey	Filename	RSA private key file

L2TP parameters

The Layer 2 Tunneling Protocol (L2TP) provides a means for terminating a logical PPP connection on a device other than the one which terminates the physical connection. Typically, both the physical layer and logical layer PPP connections would be terminated on the same device, for example, a TransPort router.

With L2TP answering the call, the router terminates the layer 2 connection only and the PPP frames are passed in an L2TP tunnel to another device which terminates the PPP connection. This device is sometimes referred to as a Network Access Server (NAS).

L2TP n parameters

Act as a listener only

When enabled, the router **does not** actively attempt to establish an L2TP tunnel. In this mode, it will only use L2TP if the remote host requests it. When unchecked, the router will actively try to establish an L2TP connection with the remote host.

Enable Server mode

When enabled, the router acts as an L2TP server.

Initiate connections to a.b.c.d

The IP address of the remote host, such as the device that will terminate the L2TP connection.

Use a.b.c.d as a backup

It is possible to specify a backup remote L2TP host server using this parameter. The text box contains the IP address of the remote server to use.

Bring this tunnel up All the time/On demand

This parameter only applies to tunnels initiated from this router.

Bring this tunnel down if it is idle for h hrs, m mins, s secs

These radio buttons select whether or not the tunnel is permanently available or not. When set to On demand, the tunnel will not activate automatically but will wait until it is triggered by PPP. When set to On demand the values in the text boxes determine the timeout after which the L2TP tunnel will closed down after the last L2TP call on that tunnel.

L2TP Window Size

The L2TP window size is selected from this drop down list. Available values are from **1** to **7**.

Route UDP packets over interface x,y

These two text boxes specify the interface and its instance number that should be used for L2TP UDP sockets. Specifying these parameters allow the router to raise the interface should it be disconnected.

Source Port Normal/Variable

These radio buttons select the source port for the L2TP tunnel. When set to Normal the default port number of 1701 is used. When set to **Variable**, a random source port value will be used.

Name

The name that identifies the router during the negotiation phase when establishing an L2TP tunnel.

Authentication Off/Secret

The radio buttons select whether or not to use authentication. This is normally set to **Off** as most host systems require that IPsec be used over L2TP tunnels. If Authentication is set to **On**, authentication is enabled and the **Secret** parameter becomes relevant. The value in the text box contains a passphrase that is shared with the host and which will be used if the remote host requests authentication and Authentication is set to **Off** here.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
l2tp	n	listen	OFF,ON	Act as a listener only
l2tp	n	swap_io	OFF,ON	Enable server mode
l2tp	n	remhost	Valid IP address a.b.c.d	Initiate connections to a.b.c.d
l2tp	n	backremhost	Valid IP address a.b.c.d	Use a.b.c.d as a backup
l2tp	n	aot	OFF,ON	Bring this tunnel up All the time/On demand
l2tp	n	nocallto	0-4294967296	Bring this tunnel down if it is idle for h hrs, m mins, s secs
l2tp	n	window	1-7 Default=4	L2TP Window Size
l2tp	n	ll_ent	<blank>, PPP, ETH	Route UDP packets over interface x,y
l2tp	n	ll_add	0-2147483647	Route UDP packets over interface x,y
l2tp	n	rnd_srcport	OFF, ON	Source Port
l2tp	n	name	Up to 30 characters	Name
l2tp	n	auth	OFF,ON	Authentication Off/Secret
l2tp	n	secret	Up to 80 characters	Authentication Off/Secret

Advanced L2TP n parameters

Retransmit interval s milliseconds

The amount of time, in milliseconds, the router waits before retransmitting a **Start Control Connection Request (SCCRQ)** frame. The default value of **250ms** should be changed to a higher value (say **4000ms**) if L2TP is running over a GPRS link.

Retransmit count n

When using L2TP over GPRS or satellite networks, the first few packets are sometimes lost. Setting the retransmit count in the text box to a higher value than the default of **5** will increase reliability of the tunnel.

Layer 1 Interface Sync port n/ISDN

These radio buttons select the layer 1 (physical) interface to be used to terminate the L2TP connection. The available options are ISDN or one of the router's synchronous serial ports. When Sync port n is selected, the sync port number is selected from the drop-down list.

Allow this L2TP tunnel to answer incoming ISDN calls

When enabled, the L2TP entity answers incoming ISDN calls.

MSN

The filter for the ISDN Multiple Subscriber Numbering (MSN). It is blank by default but when the answering facility (above) is enabled, the router only answers ISDN calls where the trailing digits match this MSN value. For example, setting the MSN value to **123** prevents the router from answering calls from any calling number that does not end in **123**. This parameter is not used when answering is off.

Sub-address

The ISDN sub-address filter to use in conjunction with the ISDN answering function. When answering is set to **On** and there is a valid sub-address in this text box, the router only answers calls where the trailing digits of the calling sub-address match this sub-address. For example, setting the sub-address value to **123** prevents the router from answering calls where the sub-address does not end in **123**.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
l2tp	n	retxto	0-4294967296	Retransmit interval s milliseconds.
l2tp	n	retxcnt	0-4294967296	Retransmit count
l2tp	n	l1iface	0-255	Layer 1 Interface
l2tp	n	ans	OFF,ON	Allow this L2TP tunnel to answer incoming ISDN calls.
l2tp	n	msn	Up to 9 digits	MSN
l2tp	n	sub	Up to 17 digits	Sub-address

PPTP parameters

The Point-to-Point tunneling protocol (PPTP) is a common way of creating a VPN tunnel to a Microsoft Windows™ server.

PPTP works by ending a regular PPP session to the peer encapsulated by the Generic Routing Encapsulation (GRE) protocol. A second session on TCP port **1723** is used to initiate and manage the GRE session. PPTP connections are authenticated with Microsoft MSCHAP-v2 or EAP-TLS. VPN traffic is protected by MPPE encryption. PPTP does not work with GPRS/HSDPA mobile operators that assign a private IP address and then apply NAT to the traffic before it leaves their network. This because the server tries to build a tunnel back to the router on port **1723** but fails when the traffic is blocked by the mobile operator's firewall.

PPTP n parameters

Description

An identifier for the router.

Remote Host a.b.c.d

The IP address of the remote host, such as the device that will terminate the PPTP connection.

Use Interface x,y

The interface to be used for the PPTP tunnel is selected from this drop-down list, the text box next to it is for the interface instance. Specifying these parameters allow the router to raise the interface should it be disconnected. The interface options are:

- **Auto**
- **PPP**
- **Ethernet**

Accept incoming PPTP connections

When enabled, the router acts as a PPTP server and accepts incoming VPN connections.

Enable Server mode

When enabled, the router sends **call_out** call requests to the remote device. In the default state which is unchecked, the router sends a **call_in** request to the remote device.

Enable Socket mode

When enabled, enables the use of a Digi proprietary mode whereby PPP packets are sent via the PPTP control socket rather than in GRE packets.

Encrypt control data using SSL version n

When enabled, the router encrypts the control data using SSL. This is a Digi proprietary function and is not part of standard PPTP. The drop-down list allows the SSL version to be selected. The available options are:

- **Use default**
- **TLSv1 only**
- **SSLv2 only**

Enable PPTP debug

When enabled, enables debug tracing.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
pptp	0-9	name	Up to 30 characters	Description
pptp	0-9	remhost	Valid IP address a.b.c.d	Remote Host a.b.c.d
pptp	0-9	ll_ent	Blank, PPP, ETH Blank means Auto	Use Interface x,y
pptp	0-9	ll_add	0-4294967296	Use Interface x,y
pptp	0-9	listen	OFF,ON	Accept incoming PPTP connections
pptp	0-9	swap_io	OFF,ON	Enable Server mode
pptp	0-9	usesock	OFF,ON	Enable Socket mode
pptp	0-9	sslver	Blank,SSL,TLS1,SSL2 Blank is disabled (default) SSL means use default.	Encrypt control data using SSL version n
pptp	0-9	debug	OFF,ON	Enable PPTP debug

OpenVPN parameters

OpenVPN can be used for connecting to the router for secure management as well as access to services on the LAN side of the TransPort router, such as corporate messaging services, file servers and print servers for example.

OpenVPN is a full-featured SSL VPN which implements OSI layer 2 or 3 secure network extension using the industry standard SSL/TLS protocol, supports flexible client authentication methods based on certificates, smart cards, and/or username/password credentials, and allows user or group-specific access control policies using firewall rules applied to the VPN virtual interface. OpenVPN is not a web application proxy and does not operate through a web browser.
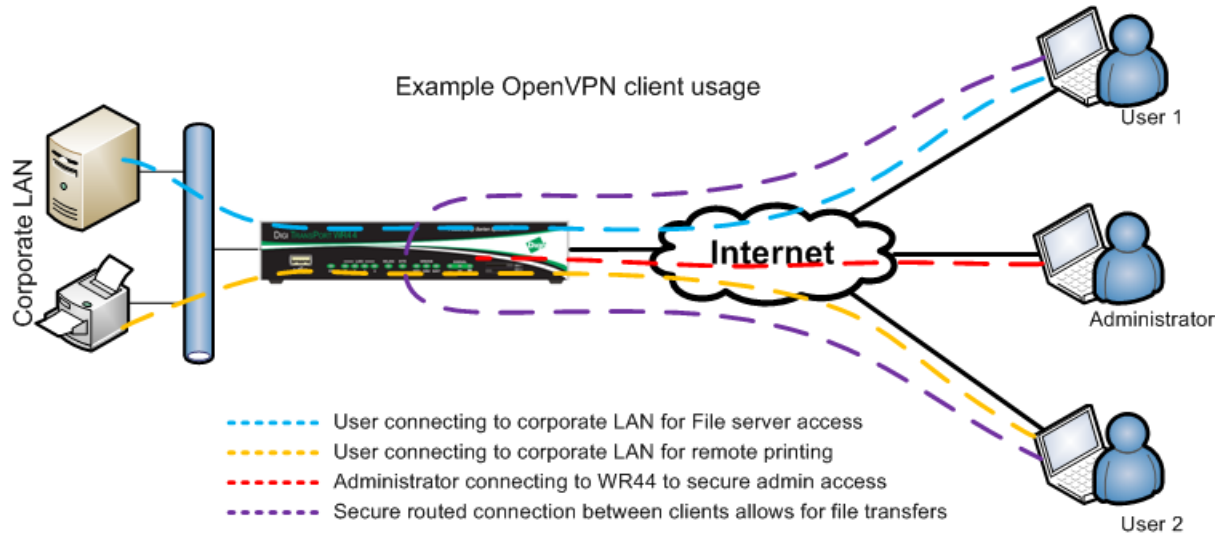
The Digi TransPort implementation of OpenVPN can be configured as an OpenVPN server, shown above, or as an OpenVPN client, connecting to an OpenVPN server.

On TransPort firmware, OpenVPN has been implemented as an interface. That means when an OpenVPN tunnel connects, an interface is added to the routing table. Static routes can be configured to point to an OpenVPN instance, and additionally, OpenVPN may learn routes from the tunnel peer and add these routes to the routing table for the duration of the OpenVPN tunnel. As each tunnel appears just like an interface, support for features like the firewall, NAT, IGMP, etc are the same as for other interfaces like PPP and ETH.

OpenVPN n parameters

Description

The text string is a friendly name to help identify this OpenVPN instance.

IP address a.b.c.d

This must be specified correctly. OpenVPN interfaces use a 30-bit mask. The first address is the network address, the second address is the server address, the third address is the client address, and the fourth address is the broadcast address. This address must be configured as the second IP address in the block of four. For example, the IP address **192.168.0.1**, if configured as a server, or **192.168.0.2**, if configured as a client.

Destination host a.b.c.d

Required only when the router is configured as an OpenVPN client. This is the IP address of the OpenVPN server.

Link socket interface x,y

If configured, OpenVPN sockets are only allowed to/from this interface and the routing table will be ignored. When set to **Auto**, the OpenVPN sockets use the routing table to identify the best interface to use.

Get link socket source address from this interface x,y

The values in these two text boxes define the interface (**Auto**, **PPP**, **ETH**) and the instance number of the interface to use as a source address for IP sockets when not using the interface that the socket was created on.

Even when this parameter is not configured, the IP address from the interface on which the socket was created will be used. The source address specified in this parameter will only be used if it will cause the traffic to match an Eroute and therefore be sent using IPsec or GRE.

MTU

Used to set the Maximum Transmit Unit for the OpenVPN instance, in bytes. The default setting is **1400**.

Metric

The connected metric, changing this value will alter the metric of dynamic routes created automatically for this interface.

NAT mode

Selects whether IP Network Address Translation (NAT) or Network Address and Port Translation (NAPT) are used at the Ethernet interface. When the parameter is set to disabled, no NAT will take place.

IP analysis

When enabled, the un-encapsulated IP traffic will be captured into the analyser trace.

Firewall

The Firewall parameter is used to turn Firewall script processing **On** or **Off** for this interface.

IGMP

This IGMP parameter is used to enable or disable the transmission and reception of IGMP packets on this interface. IGMP is used to advertise members of multicast groups. If IGMP is enabled, and a member of a multicast group is discovered on this interface, multicast packets for this group received on other interfaces will be sent out this interface.

Include in RIP advertisements

When enabled, the router includes this static route in RIP advertisements.

Automatically connect interface

If enabled, this OpenVPN instance will be considered as an Always On interface.

◉ Client Mode
    Connect to OpenVPN server: [_____]
    ☐ Automatically connect interface
    ☐ Obtain IP address from the OpenVPN server
    ☐ Obtain routes from the OpenVPN server
    ☐ Obtain DNS server IP address from the OpenVPN server
○ Server Mode
☐ Disconnect the tunnel if no IP traffic has been received for [0] hrs [0] mins [0] secs

☐ Enable NAT on this interface
☐ Enable Firewall on this interface

Server mode (listener)

Configures the OpenVPN instance to listen for inbound OpenVPN sockets.

Link socket port

The default port used by OpenVPN is **1194**. If a different or non-standard port number is used, specify it here.

Link socket protocol

OpenVPN can use TCP or UDP as the transport protocol. Select the required protocol here.

TLS auth password / Confirm TLS auth password

Allows the OpenVPN instance to use an extra level of security by having a TLS password configured.

Push IP address #1/#2/#3

When configured as an OpenVPN server, these parameters can be used to push subnets to the client that need to be routed via the OpenVPN server. Used in conjunction with the **Push Mask** parameter below.

Push mask #1/#2/#3

Used with the **Push IP address** parameter above to define subnets that should be routed via the OpenVPN server.

Push DNS server address #1/#2

When configured as an OpenVPN server, these parameters can be used to push DNS server settings to the OpenVPN client.

Pull interface IP address

When configured as an OpenVPN client, this option must be enabled for the router to obtain and use the local IP address supplied from the OpenVPN server.

Pull routes

When configured as an OpenVPN client, this option must be enabled for the router to use routes sent from the OpenVPN server.

Pull DNS server addresses

When configured as an OpenVPN client, this option must be enabled for the router to use DNS servers sent from the OpenVPN server.

Packet replay ID window

When set to a non-zero value, this enables sequence number replay detection. It indicates the number of packet IDs lower than the current highest ID to allow out of sequence.

Packet replay time window (seconds)

Set to a non-zero value to enable time tracking of incoming packets.

OpenVPN TX ping interval (seconds)

Interval between OpenVPN ping transmissions. These are required to detect the operational state of the VPN connection.

OpenVPN RX ping timeout (seconds)

The number of seconds, after which no OpenVPN ping has been received, the VPN will be marked as down.

Include IV

Enabling this option on includes an **IV** at the head of an encrypted packet. If one peer prepends this **IV** and the other isn't expecting it, packet decryption will fail.

Key negotiation timeout (seconds)

Maximum time, in seconds, to allow for a data channel key negotiation.

Key renegotiation interval (seconds)

Interval between key re-negotiations.

Key renegotiation bytes

If non-zero, a key renegotiation will take place after this many bytes have traveled through the data channel in either direction.

Key renegotiation packets

If non-zero, a key renegotiation will take place after this many packets have traveled through the data channel.

Inactivity timeout (seconds)

The tunnel is disconnected after the tunnel becomes inactive (that is, no IP traffic) for this many seconds. Note that the timer is only restarted with RX traffic, not TX traffic.

Data channel cipher

Sets the cipher used for data channel encryption/decryption. Select from the dropdown list.

Data channel digest

Sets the digest algorithm used for data channel authentication. Select from the dropdown list.

Debug

Enables output of OVPN related debug.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ovpn	n	descr	Up to 30 characters	Description
ovpn	n	IPaddr	Valid IP address a.b.c.d	IP address a.b.c.d
ovpn	n	dest	Valid IP address a.b.c.d	Destination host a.b.c.d
ovpn	n	ll_ent	<blank>, PPP, ETH	Link socket interface x,y x= interface type
ovpn	n	ll_add	0-2147483647	Link socket interface x,y y= interface number
ovpn	n	ip_ent	<blank>, PPP, ETH	Get link socket source address from this interface x,y x= interface type
ovpn	n	ip_add	0-2147483647	Get link socket source address from this interface x,y y= interface number
ovpn	n	mtu	0-2147483647	MTU
ovpn	n	metric	0-2147483647	Metric
ovpn	n	do_nat	0,1,2 0=Off 1=Address only 2= Address and port	NAT mode
ovpn	n	ipanon	OFF,ON	IP analysis
ovpn	n	firewall	OFF,ON	Firewall

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ovpn	n	igmp	OFF,ON	IGMP
ovpn	n	inrip	OFF,ON	Include in RIP advertisements
ovpn	n	autoup	OFF,ON	Automatically connect interface
ovpn	n	server	OFF,ON	Server mode (listener)
ovpn	n	port	0-65535	Link socket port
ovpn	n	proto	TCP,UDP	Link socket protocol
ovpn	n	tls_auth_key	Up to 30 characters	TLS auth password
ovpn	n	etls_auth_key		Enciphered version TLS auth password
ovpn	n	puship	Valid subnet a.b.c.d	Push IP address #1 a.b.c.d
ovpn	n	pushmask	Valid netmask a.b.c.d	Push mask #1 a.b.c.d
ovpn	n	puship2	Valid subnet a.b.c.d	Push IP address #2 a.b.c.d
ovpn	n	pushmask2	Valid netmask a.b.c.d	Push mask #2 a.b.c.d
ovpn	n	puship3	Valid subnet a.b.c.d	Push IP address #3 a.b.c.d
ovpn	n	pushmask3	Valid netmask a.b.c.d	Push mask #3 a.b.c.d
ovpn	n	pushdns	Valid IP address a.b.c.d	Push DNS server address #1 a.b.c.d
ovpn	n	pushdns2	Valid IP address a.b.c.d	Push DNS server address #2 a.b.c.d
ovpn	n	pullip	OFF,ON	Pull interface IP address
ovpn	n	pullroute	OFF,ON	Pull routes
ovpn	n	pulldns	OFF,ON	Pull DNS server addresses
ovpn	n	sreplay	0-2147483647	Packet replay ID window
ovpn	n	treplay	0-2147483647	Packet replay time window (seconds)
ovpn	n	pingint	0-2147483647	OpenVPN TX ping interval (seconds)
ovpn	n	pingto	0-2147483647	OpenVPN RX ping timeout (seconds)
ovpn	n	inciv	OFF,ON	Include IV

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ovpn	n	neg_timeout	0-2147483647	Key negotiation timeout (seconds)
ovpn	n	reneg_int	0-2147483647	Key renegotiation interval (seconds)
ovpn	n	reneg_bytes	0-2147483647	Key renegotiation bytes
ovpn	n	reneg_packets	0-2147483647	Key renegotiation packets
ovpn	n	inact_timeout	0-2147483647	Inactivity timeout (seconds)
ovpn	n	cipher	See cipher list below	Data channel cipher
ovpn	n	digest	See digest list below	Data channel digest
ovpn	n	debug	OFF,ON	Debug

Supported Cipher and Digest values for OpenVPN

Cipher values	Digest values
DES-EDE-CBC	md2WithRSAEncryption
AES128	ssl2-md5
DES	MD5
DES-CBC	sha1WithRSAEncryption
AES-128-CBC	ssl3-sha1
AES192	ssl3-md5
AES-192-CBC	SHA1
DES-EDE3-CBC	MD2
AES-256-CBC	RSA-MD2
AES-256	md5WithRSAEncryption
DES3	RSA-SHA1
	RSA-SHA1-2
	RSA-MD5

Configure Secure Sockets Layer (SSL)

This section covers configuring the Secure Sockets Layer (SSL) from the web interface and command line. It covers the following topics:

About the Secure Sockets Layer (SSL)

The secure socket layer (SSL) provides a secure transport mechanism is supported by Digi's TransPort routers.

Some sites require client side authentication when connecting to them. The router's SSL client handles the authentication for SSL connections using certificates signed by a Certificate Authority (CA). For more information regarding certificates and certificate requests, refer to the certificates page **Administration > X.509 Certificate Management > Certificate Authorities (CAs)**.

SSL Clients parameters

Configuring the SSL clients is performed on the **Configuration > Network > SSL** page. This page has a table with columns and parameters as follows:

SSL Client

This column is simply a list of the SSL client numbers supported by the router.

Client Certificate Filename

The name of the required certificate file is selected from those available on the router's filing system from this drop-down list.

Client Private Key Filename

The name of the file that contains the private key that matches the public key stored in the above parameter, is selected from this drop-down list.

Cipher List

The cipher list in this text box is a list of one or more cipher strings separated by colons. Commas or spaces are also accepted as separators but colons are normally used. The actual cipher string can take several different forms. It can consist of a single cipher suite such as RC4-SHA. It can represent a list of cipher suites containing a certain algorithm or cipher suites of a certain type. For example, **SHA1** represents all cipher suites using the SHA1 digest algorithm. Lists of cipher suites can be combined in a single cipher string using the **+** character. This forms the logical AND operation. For example, **SHA1+DES** represents all cipher suites containing SHA1 and DES algorithms. If left empty, the cipher list is not used. For more information see: www.openssl.org/docs/apps/ciphers.html.

Apply to Destination IP Address

Allows the configuration of multiple SSL destinations, each having a different certificate/key pair. When set, this parameter will lock the SSL client settings to a specific IP address. If this parameter is left blank, the configured SSL client settings will be used for any connection that requires SSL. As is usual with the tables on the configuration web pages, the relevant and appropriate parameters are selected and the **Add** button on the right-hand side is clicked to add the entry into the table. Once an entry has been added, it can be removed by clicking the **Delete** button in the right-hand column.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
sslcli	0-4	certfile	Up to 12 characters (DOS 8.3 format)	Client Certificate Filename
sslcli	0-4	keyfile	Up to 12 characters (DOS 8.3 format)	Client Private Key Filename
sslcli	0-4	cipherlist	Colon-separated list of ciphers	Cipher List
sslcli	0-4	IPaddr		Apply to Destination IP Address

SSL Server parameters

This page describes the parameters needed to configure the SSL server.

Server Certificate Filename

The file containing the server certificate is selected from this drop-down list.

Client Private Key Filename

The file containing the private key that matches the above certificate is selected from this drop-down list.

SSL Version

The version of the SSL protocol to use, is selected from this drop-down list. Selecting **Any** allows the use of any version. The available options are:

- **Any**
- **TLSv1 only**
- **SSLv2 only**

Cipher List

The list of ciphers is the same as described above for the client-side configuration table.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
sslsvr	0	certfile	Up to 12 characters (DOS 8.3 format)	Server Certificate Filename
sslsvr	0	keyfile	Up to 12 characters (DOS 8.3 format)	Server Private Key Filename
sslsvr	0	ver	Blank, TLS1, SSL2	SSL Version
sslsvr	0	cipherlist	Colon-separated list	Cipher List
sslsvr	0	debug	OFF, ON	n/a

Configure Secure Shell (SSH) server and client

This topic covers configuring the Secure Shell (SSH) server and client. It covers the following topics:

About the Secure Shell (SSH) server

The Secure Shell (SSH) server allows remote peers to access the router over a secure TCP connection using a suitable SSH client. The SSH server provides a Telnet-like interface and secure file transfer capability.

SSH uses a number of keys during a session. The host keys are used for authentication purposes. Keys unique to each SSH session are also generated and are used for encryption/authentication purposes.

The router supports SSH v1.5 and SSH v2. The host key file format differs for each version but there would normally only be one host key for each version. For this reason the router allows the user to configure two host key files. These keys may be changed from time to time, specifically if it suspected that the key has become compromised. Because the host keys need to be secure, it is highly recommended to store the files on the router's FLASH filing system using filenames prefixed with **priv** which makes it impossible to read the files using any of the normal methods (such as FTP). It is possible (using the **genkey** command) to create host keys in either format for use with SSH. Using this utility it is not necessary to have the host key files present on any other storage device (thus providing an additional level of security). For details on generating a private key file, see Generate an SSH private key from the web interface on page 468.

Unlike the Telnet server, you can configure the number of SSH server sockets that listen for new SSH connections.

Multiple SSH server instances can be configured, each instance can be configured to listen on a separate port number and can use different keys and encryption methods.

You can configure which authentication methods can be used in an SSH session and the preferred selection order. The router currently supports MD5, SHA1, MD5-96 and SHA1-96. If required, a public/private key pair can be used for authentication.

The router currently supports 3DES, 3DES-CBC and AES cipher methods.

DEFLATE compression is also supported. If DEFLATE compression is enabled and negotiated, SSH packets are first compressed before being encrypted, and delivered to the remote unit via the TCP socket.

Note The SSH server supports the SCP file copy protocol but does not support filename wildcards.

Configure Secure Shell (SSH) server parameters

Configuring SSH is performed on the **Configuration > Network > SSH Servers** page. Parameters are as follows:

Enable SSH Servers

When checked, this checkbox enables the SSH servers on the router.

SSH Server n parameters

The router supports eight individual SSH servers that are configured independently using the options described below.

Enable SSH Server

When enabled, enables the SSH server.

Use TCP port p

The TCP port number (default **22**) that the SSH server will use to listen for incoming connections. (Port **22** is the standard SSH port).

Allow up to n connections

The number of sockets listening for new SSH connections (default **1**).

Host Key 1 Filename

The filename of either an SSH V1 or V2 host key. It is highly recommended that the filename be prefixed with **priv** to ensure that the key cannot be easily accessed and compromised. This key may be generated using the facilities described in the Certificates section of this manual.

Host Key 2 Filename

The filename of either an SSH V1 or V2 key as above.

Note The maximum length for these filenames is **12 characters** and they must use the DOS 8.3 file naming convention.

Maximum login time s seconds

The maximum length of time, in seconds, a user can successfully complete the login procedure once the SSH socket has been opened. The socket is closed if the user has not completed a successful login within this period.

Maximum login attempts n

The maximum number of login attempts allowed in any one session before the SSH socket will be closed.

Use Deflate compression No/Yes, level n

The radio buttons select whether or not DEFLATE compression will be used. If compression is selected, the compression level is chosen from the drop-down list.

Enable Port Forwarding

When enabled, the router accepts traffic on ports other than **23**. This functionality is for use with SSH client applications, such as PuTTY, that have port forwarding capability. For example, one the SSH connection is active, traffic for the HTTP port **80** can be sent to the router securely.

Command Session IP Address a.b.c.d Port p

The values in these two text boxes are used to specify the host IP address and port number that the router will use to handle incoming requests for a command session from SSH clients. This is instead of the router's normal command interpreter. For example, if the values are IP address **127.0.0.1**, port **4000**, the SSH client will make a direct connection to **ASY 0** and the device attached to **ASY 0** will receive and process the commands from the SSH client.

Enable support for SSH v1.5

When enabled, the server negotiates SSH V1.5. The router must also have a SSH V1 key present and the filename entered into the SSG configuration.

Server key size

This option applies to V1 SSH. During initialization of an SSH session, the server sends its host key and a server key (which should be of a different size to the host key). The router generates this key automatically but the length of the server key is determined by this parameter. If when this value is set it is too similar to the length of the host key, the router will automatically adjust the selected value so that the key sizes are significantly different.

Enable support for SSH v2.0

When enabled, the server negotiates SSH V2. The router must also have a SSH V2 key present and the filename entered into the SSG configuration.

Actively start key exchange

This option applies to V2 SSH. Some SSH clients wait for the server to initiate the key exchange process when a new SSH session is started unless they have data to send to the server, in which case they will initiate the key exchange themselves. When checked, this checkbox causes the router to automatically initiate a key exchange without waiting for the client.

Rekey Never/After n units of data have been transferred

With SSH V2, it is possible to negotiate new encryption keys after the current ones have been used to encrypt a specified amount of data. The radio buttons select whether this feature should be used. If this feature is to be used the amount of data is entered into the text box and the applicable units (**Kbytes**, **Mbytes**, **Gbytes**) selected from the drop-down list.

Encryption Preferences

The following four configuration options allocate preferences to the encryption method that should be used to encrypt data on the link. A lower value indicates greater preference apart from zero which disables the option.

3DES

The preference level for the Triple-DES algorithm.

AES (128 bits)

The preference level for the 128-bit AES algorithm.

AES (192 bits)

The preference level for the AES algorithm using 192 bits.

AES (256 bits)

The the preference level for the AES algorithm using 256 bits.

Authentication Preferences

The following four configuration options allocate preferences to the authentication methods that should be used. As above, a value of **0** disables the particular authentication method, and lower values indicated greater preference than higher values. For example, if MAC SHA1-96 was the preferred method for authentication, this option would be given the value **1** and the other options given a value of **2** or greater. If all these parameters are set to the same value, the router automatically uses them in the following order:

- SHA1,
- SHA1-96
- MD5
- MD5-96

MAC MD5

The preference level for MAC MD5.

MAC MD5-96

The preference level for MAC MD5-96.

MAC SHA1

The preference level for MAC SHA1.

MAC SHA1-96

The preference level for MAC SHA1-96.

Enable Debug

The router supports logging and output of debugging information for situations where there are problems establishing a SSH connection. When enabled, this setting causes the router to trace and output information that should be helpful in diagnosing and resolving the problem.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ssh	0-7	port	0-65535	Use TCP port p
ssh	0-7	nb_listen	0-2147483647	Allow up to n connections
ssh	0-7	hostkey1	Up to 12 characters (8.3 format)	Host Key 1 Filename
ssh	0-7	hostkey2	Up to 12 characters (8.3 format)	Host Key 2 Filename
ssh	0-7	loginsecs	0-2147483647	Maximum login time **s** seconds
ssh	0-7	logintries	0-2147483647	Maximum login attempts **n**
ssh	0-7	comp	0=disabled	Use Deflate compression, level
ssh	0-7	fwd	0-2147483647	Enable port forwarding
ssh	0-7	cmdhost	Valid IP address a.b.c.d	Command session IP address a.b.c.d
ssh	0-7	cmdport	0-2147483647	Command session port p
ssh	0-7	svrkeybits	0-2147483647	Server key size
ssh	0-7	initkex	OFF,ON	Actively start key exchange
ssh	0-7	rekeybytes	0-2147483647 0=Do not rekey	Rekey After **n** units of data have been transferred
ssh	0-7	enc3descbc	0-2147483647 0=Disabled	3DES
ssh	0-7	encaes128cbc	0-2147483647	AES (128 bits)
ssh	0-7	encaes192cbc	0-2147483647	AES (192 bits)
ssh	0-7	encaes256cbc	0-2147483647	AES (256 bits)
ssh	0-7	macmd5	0-2147483647	MAC MD5
ssh	0-7	macmd596	0-2147483647	MAC MD5-96
ssh	0-7	macsha1	0-2147483647	MAC SHA1
ssh	0-7	macsha196	0-2147483647	MAC SHA1-96
ssh	0-7	debug	0,1 0=Off 1=On	Enable Debug

Configure Secure Shell (SSH) Client

SSH clients are configured on the **Configuration > Network > SSH Client** page.

SSH Client parameters

Maximum handshake time

The time, in seconds, to wait for the server to begin the banner exchange part of the protocol after the socket connects.

'known_hosts' Filename

The name of file to be used as the regular SSH client.

'identity' Filename

The name of file to be used as the regular SSH client.

'id_rsa' Filename

The name of an SSH V1 or V2 host key. There are two **id_rsa** files to allow the user to configure a SSHv1 private key into one field, and a SSHv2 private key into the other.

'_id rsa' Filename #2

The name of an SSH V1 or V2 host key.

Use Deflate compression No/Yes, level n

The radio buttons select whether or not DEFLATE compression will be used. If compression is selected, the compression level is chosen from the drop-down list.

Enable Public Key Authentication

When enabled, enables SSH public-key authentication to connect to OpenSSH.

Enable Password Authentication

When enabled, enables SSH password authentication to connect to OpenSSH.

Note No other authentication methods are supported.

Encryption Preferences

The following four configuration options allocate preferences to the encryption method that should be used to encrypt data on the link. A lower value indicates greater preference apart from zero which disables the option.

3DES

The preference level for the Triple-DES algorithm.

AES (128 bits)

The preference level for the 128-bit AES algorithm.

AES (192 bits)

The preference level for the AES algorithm using 192 bits.

AES (256 bits)

The preference level for the AES algorithm using 256 bits.

Authentication Preferences

The following four configuration options allocate preferences to the authentication methods that should be used. As above, a value of zero disables the particular authentication method and lower values indicated greater preference than higher values. So, for example if MAC SHA1-96 was the preferred method for authentication, this option would be given the value **1** and the other options given a value of **2** or greater. If all these parameters are set to the same value, the router automatically uses them in the following order: **SHA1**, **SHA1-96**, **MD5**, **MD5-96**.

MAC MD5

The preference level for MAC MD5.

MAC MD5-96

The preference level for MAC MD5-96.

MAC SHA1

The preference level for MAC SHA1.

MAC SHA1-96

The preference level for MAC SHA1-96.

Enable Server Keepalives

When enabled, enables server keepalives to use the same tcp connection for HTTP conversation instead of opening new one with each new request.

Enable Debug

The router supports logging and output of debugging information for situations where there are problems establishing a SSH connection. When enabled, this checkbox causes the router to trace and output information that should be helpful in diagnosing and resolving the problem.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
sshcli	0-7	conn_to	0-10 seconds	Time in seconds to wait for the server to begin the banner exchange part of the protocol after the socket connects.
sshcli	0-7	hostsfile	Up to 12 characters (8.3 format)	Key file to be used as the regular SSH client.
sshcli	0-7	idfile	Up to 12 characters (8.3 format)	Key file to be used as the regular SSH client.
sshcli	0-7	idrsafile	Up to 12 characters (8.3 format)	Name of either an SSH V1 or SSH V2 host key.
sshcli	0-7	idrsafile1	Up to 12 characters (8.3 format)	Name of either an SSH V1 or SSH V2 host key.
sshcli	0-7	comp	0=disabled	Use Deflate compression, level.
sshcli	0-7	pubkeyauth	0=disabled	Enables SSH public-key authentication to connect to OpenSSH.
sshcli	0-7	pwdauth	0=disabled	Enables SSH password authentication to connect to OpenSSH.
sshcli	0-7	enc3descbc	0-2147483647 0=Disabled	3DES.
sshcli	0-7	encaes128cbc	0-2147483647	AES (128 bits).
sshcli	0-7	encaes192cbc	0-2147483647	AES (192 bits).
sshcli	0-7	encaes256cbc	0-2147483647	AES (256 bits).
sshcli	0-7	macmd5	0-2147483647	MAC MD5.
sshcli	0-7	macmd596	0-2147483647	MAC MD5-96.
sshcli	0-7	macsha1	0-2147483647	MAC SHA1.
sshcli	0-7	macsha196	0-2147483647	MAC SHA1-96.
sshcli	0-7	svrlaliveint	0-2147483647	Interval in seconds to send the server a keepalive packet.

Entity	Instance	Parameter	Values	Equivalent Web Parameter
sshcli	0-7	svralivemax	number	Maximum number of keepalives to send without response before the connection is killed
sshcli	0-7	debug	0,1 0=Off 1=On	Enable Debug

SSH parameters

To fully configure SSH, a version1 SSH key and a version 2 SSH key need to be generated and the router configured to use them, described below.

Note SSH version 2 is more secure than version 1 and so is the recommended version to use. However, some SSH clients may only support version 1 keys and so the router supports both version 1 and version 2 SSH.

Generate an SSH private key from the web interface

1. Navigate to **Administration > X.509 Certificate Management > Key Generation** and select the size of the key file from the drop-down list. The larger the key file, the more secure it will be.

2. In the **Key** filename box, enter the name for the key file, or select from those already present using the drop-down selector. The filename should have a prefix of **priv** and a file extension of .**pem**, such as **privssh1.pem**. The 8.3 file name convention applies.

3. Check the checkbox marked Save in SSHv1 format in order to generate a version 1 SSH key. Click the **Generate** Key button to generate the private key file. The key file will be stored in the router's FLASH filing system.

4. To generate the second key, repeat steps 1 through 3. This time, however, make sure that the **Save in SSHv1** format checkbox is unchecked. Give this key file a different name to the version 1 file previously generated.

5. On the **Configuration > Network > SSH Server > SSH Server n** page, enter the filename generated in step 3 into the **Host Key 1 Filename** text box and the filename generated in step 4 into the **Host Key 2 Filename** text box.

6. Click the **Apply** button at the bottom of the page to apply changes. When the **Configuration successfully applied** message is displayed, click on the highlighted link to save the configuration.

Generate an SSH private key from the CLI

1. Generate the SSH V1 private key using the **genkey** command as follows:

    ```
    genkey <keybits> <filename> –ssh1
    ```

    where:

    <keybits>

    Is one of the following values; **384**, **512**, **768**, **1024**, **1536** or **2048**.

    <filename>

    Is the name for the file, such as **privssh1.pem**, as described for the web version of this procedure.

2. Generate the SSH V2 private key using the **genkey** command as in step 1, but this time, omit the **–ssh1** switch. For example:

    ```
    genkey 1024 privssh2.pem.
    ```

3. Set the first private key as the SSH Host key 1 using the following command:

    ```
    ssh 0 hostkey1 privssh1.pem
    ```

4. Set the second private key as SSH Host Key 2 using the following command:

    ```
    ssh 0 hostkey2 privssh2.pem
    ```

5. Save the configuration:

    ```
    config 0 save
    ```

SSH Authentication with a public/private key pair

Once SSH access has been configured and confirmed to be working, RSA key pair authentication can be added and used to replace password authentication.

This process will involve the use of PuTTYgen to create public and private keys. For full details on how to perform this procedure, see *Quick Note 010, SSH access using RSA key authentication* on www.digi.com.

Configure FTP Relay

This section covers configuring FTP relay agents from the web interface and command line interface. It includes the following topics:

- About FTP relay agents on page 471
- FTP Relay n parameters on page 472
- Advanced FTP Relay parameters on page 475

About FTP relay agents

FTP Relay agents allow any files to be transferred onto the router by a specified user, using the File Transfer Protocol (FTP). The files are temporarily stored in memory and then relayed to a specific FTP host. This is useful when the router is being used to collect data files from a locally attached device such as a webcam which must then be to a host system over a slower data connection such as W-WAN. In effect, the router acts as a temporary data buffer for the files.

The FTP Relay Agent can also be configured to email, as an attachment, any file it was unable to transfer to the FTP server. To do this, go to **Configuration > Alarms > SMTP Account** and set the **Email Template**, **To**, **From**, and **Subject** parameters as appropriate, and also configure the SMTP client.

FTP Relay n parameters

There are two FTP Relay Agents available, with a separate web page for each. For command line configuration, the instance number can be **0** or **1**.

Relay files for user locuser to FTP Server ftphost

The value in the left-hand text box is the name of the local user and should be one of the usernames assigned in the **Configuration > Security > Users** web page. This name is then used as the FTP login username when the local device needs to relay a file. The value in the right-hand text box is the name of the FTP host to which the files from the locally attached device are relayed.

Server Username

The username required to log in to the specified FTP host.

Server Password

The password to be used to log in to the host.

Confirm Server Password

The password should be retyped into this text box in order to confirm that it has been entered correctly, given that it is not echoed in clear text.

Remote directory

The full name of the directory on the FTP host to which the file is to be saved.

Rename file

When enabled, the router stores the uploaded files internally with a filename in the form **relnnnn,** where **nnnn** is a number that is incremented for each new file received. When the file is relayed to the FTP host the original filename is used. When unchecked, the file is stored internally using its original filename. This parameter should be set if it a file having a filename longer than **12** characters is to be uploaded. This is because the internal file system uses the 8.3 filename format, such as **autoexec.bat**.

Transfer Mode ASCII / Binary

These two radio buttons select between the two possible file transfer modes, binary data or ASCII data.

Transfer Command STORE / APPEND

These two radio buttons select between the two possible storage methods, either append to or replace existing file.

Attempt to connect to the FTP Server n times

The number of connection attempts that the router should make if the first attempt is not successful.

Wait s seconds between attempts

The interval, in seconds, the router should wait in between successive connections attempts.

Remain connected for s seconds after a file has been transferred

How long, in seconds, the router maintains the connection to the FTP host after transferring a file.

If unable to relay file Delete File / Retain file

These two radio buttons select the behavior with respect to storing the file if the router fails to connect to the FTP host (after retrying for the specified number of attempts). Select **Delete File** if the file should not be stored permanently. If the file is retained, manual intervention is required to recover it at a later stage.

Note If the file is not retained, it will be lost if the power is removed from the router.

Email the file before storing or deleting it

The configuration options following this checkbox are normally disabled (they should appear disabled in the browser). When this checkbox is enabled, the parameters are enabled and data can be entered into the text boxes.

Use Email Template File

The name of the template file that will be used to form the basis of any email messages generated by the FTP Relay Agent. This would normally be the standard **EVENT.EML** template provided with the router but alternative templates may be created if necessary (see Email Notification parameters on page 589).

To

The email address of the recipient of email messages generated by the FTP Relay Agent.

From

The email address of the router. In order for this to work, an email account must be in place with the Internet Service Provider.

Subject

A brief description of the content of the email.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
frelay	n	locuser	Up to 15 characters	Relay files for user **locuser**
frelay	n	ftphost	Up to 64 characters	to FTP Server **ftphost**
frelay	n	ftpuser	Up to 20 characters	Server Username
frelay	n	ftppwd	Up to 20 characters	Server Password
frelay	n	ftpdir	Up to 40 characters	Remote directory
frelay	n	norename	OFF,ON	Rename file
frelay	n	ascii	OFF,ON	Transfer Mode
frelay	n	appe	OFF,ON	Transfer Command
frelay	n	retries	0-2147483647	Attempt to connect to the FTP Server n times
frelay	n	retryint	0-2147483647	Wait s seconds between attempts
frelay	n	timeout	0-2147483647	Remain connected
frelay	n	savemode	OFF,ON	Delete/Retain file
frelay	n	smtp_temp	Up to 40 characters	Use Email Template File
frelay	n	smtp_to	Up to 100 characters	To
frelay	n	smtp_from	Up to 40 characters	From
frelay	n	smtp_subject	Up to 40 characters	Subject

Advanced FTP Relay parameters

Tx Buffer Size n bytes

The value in this text box specifies the size of the Tx socket buffer.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ftpcli	n	txbuf	0-2147483647	Tx Buffer Size

Configure IP passthrough

This topic covers configuring IP Passthrough from the web interface and command line. It covers the following topics:

- About IP passthrough on page 476
- IP Passthrough page configuration parameters on page 477
- Related CLI commands on page 478

About IP passthrough

IP passthrough is a useful feature if a host computer or server on the local area network needs to have access to it from the Internet with a public IP address. With IP passthrough configured, all IP traffic, not just TCP/UDP is forwarded back to the host computer. This feature can be useful for applications that do not function reliably through network address translation.

IP Passthrough page configuration parameters

In this configuration, the local PC shares the public IP addressing information with the WAN side of the router.

Enable IP Pass-through

Enables IP passthrough mode.

Ethernet interface

The Ethernet interface to which the local PC is connected.

PPP interface

The PPP interface that will share its WAN address with the local PC.

Mode

Selects the mode of operation for the passthrough functionality. The available options are **Normal/28 bit mask** and **Fixed IP Address/32 bit mask**. The default is **Normal/28 bit mask**. When **Fixed IP/32 bit mask** mode of operation is selected, the DHCP server provides a 32-bit subnet mask to the client and sets the address/subnet mask for the Ethernet interface to **192.168.1.1/32**.

Pinhole Configuration

The following parameters are checkboxes allowing specific protocols to be excluded from the IP passthrough feature. An excluded protocol terminates at the router instead of being forwarded to the local PC.

HTTP

When checked, this checkbox excludes HTTP from passthrough.

HTTPS

When checked, this checkbox excludes HTTPS from passthrough.

Telnet

When checked, this checkbox excludes Telnet from passthrough.

Telnet over SSL

When checked, this checkbox excludes SSL from passthrough.

SSH/SFTP

When checked, this checkbox excludes SSH/SFTP from passthrough.

SNMP

When checked, this checkbox excludes SNMP from passthrough.

GRE

When checked, this checkbox excludes GRE from passthrough.

Ping

When checked, this checkbox excludes the ICMP echo request from passthrough.

Other Ports

The list of TCP and UDP port numbers in this text box are added to the list of port numbers that are not forwarded to the local PC. Separate port numbers by commas.

Other Protocols

The list of protocol numbers in this text box are added to the list of port numbers that are not forwarded on to the local PC. Separate port numbers by commas.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
passthru	0	enabled	OFF,ON	Enable IP Pass-through
passthru	0	ethadd	0-2147483647	Ethernet interface
passthru	0	pppadd	0-2147483647	PPP interface
passthru	0	mode	0,1 0=Normal 1=32-bit mask	Mode
passthru	0	http	OFF,ON	HTTP
passthru	0	https	OFF,ON	HTTPS
passthru	0	telnet	OFF,ON	Telnet
passthru	0	telnets	OFF,ON	Telnet over SSL
passthru	0	ssh	OFF,ON	SSH/SFTP
passthru	0	snmp	OFF,ON	SNMP
passthru	0	gre	OFF,ON	GRE
passthru	0	ping	OFF,ON	Ping
passthru	0	ports	Comma-separated list of ports	Other Ports
passthru	0	protos	Comma-separated list of protocols	Other Protocols

Configure UDP echo

This section covers configuring UDP echo from the web interface or command line. It covers the following topics:

- About UDP echo on page 480
- UDP Echo n parameters on page 480
- Related CLI commands on page 481

About UDP echo

When enabled, the UDP echo client generates UDP packets that contain the router's serial number and ID and transmits them to the IP address specified by the configuration. When the remote router receives a UDP packet on a local port and UDP echo server is configured, it will echo the packet back to the sender. There may be more than one UDP echo instance available on the router. Instance 0 is used when specifying the local port to listen on.

UDP Echo n parameters

Depending on the router model, there may be instances of the UDP echo task supported by the router. Each has its own configuration web page, described below. For the command line configuration, valid instance numbers start at **0**.

Enable UDP Echo

This checkbox is disabled by default. When enabled, the configuration parameters associated with send UDP echo packets are displayed.

Send a UDP packet to IP address a.b.c.d port n every s seconds

The values in these three text boxes define the destination IP address for the UDP packets, the port number to which they should be sent and the sending interval. If the destination IP address is left blank, the router will not attempt to send any packets.

Use local port n

The local port the router should listen on for UDP packets. If any UDP packets are sent to this port, the router will send a copy back to the IP address and port they were sent from.

Route via Routing table / Interface x,y

These two radio buttons select whether the router should use its routing table to determine how to send the UDP packets or whether it should use the specified interface. If the specific interface is selected, the interface is selected from the drop-down list. The options available are PPP and Ethernet. The interface instance is specified in the adjacent text box.

Only send packet when the interface is "In Service"

When checked, and the router is using the specified interface, this checkbox will prevent the router from sending UDP packets if the interface is out of service.

Do not send any data with the UDP packet

When checked, this check box causes the router to send only a single null data byte. This is useful to minimize packet size when the interface has high data charges, such as W-WAN. When unchecked, the router sends packets containing the router's serial number and ID as text.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
udpecho	n	dstip	Valid hostname	Send a UDP packet to IP address a.b.c.d port n every s seconds
udpecho	n	dstport	0-65535	Send a UDP packet to IP address a.b.c.d port n every s seconds
udpecho	n	interval	0-2147483647	Send a UDP packet to IP address a.b.c.d port n every s seconds
udpecho	n	locport	0-65535	Use local port n
udpecho	n	userouting	OFF,ON	Route via Routing table
udpecho	n	ifent	PPP,ETH	Interface x,y
udpecho	n	ifadd	Valid interface instance 0-4294967296	Interface x,y
udpecho	n	onlyis	OFF,ON	Only send packet when the interface is **In Service**
udpecho	n	nodata	OFF,ON	Do not send any data with the UDP packet

Configure Quality of Service (QoS)

This section covers configuring the Quality of Service (QoS) from the web interface and command line. It covers the following topics:

- About Quality of Service (Qos) on page 483
- Configuring QoS in the web interface on page 484
- DSCP Mappings parameters on page 485
- Queue Profiles parameters on page 486

About Quality of Service (Qos)

The Quality of Service (QoS) functionality allows prioritizing different types of IP traffic. QoS is generally used to ensure that low priority applications do not use most of the available bandwidth to the detriment of those having a higher priority. For example, this might mean that EPOS transactions carried out over XOT will be prioritized over HTTP-type traffic used for Internet access. Without some form of QoS, all IP packets are treated as being equal, such as there is no discrimination between applications.

The IP packet **Type of Service (TOS)** field is used to indicate how a packet should be prioritized. Using the top 6 bits of the TOS field, a router that supports QoS will assign a Differentiated Services Code Point (DSCP) code to the packet. This may take place within the router when it receives the packet or another router closer to the packet source may have already assigned it. Based on the DSCP code, the router will assign the packet to a priority queue. There are currently four such queues for each PPP instance within the router. Each queue can be configured to behave a particular way so that packets in that queue are prioritized for routing according to predefined rules.

There are two principal ways in which priority may be implemented:

- A priority queue can be configured to allow packets to be routed at a specific data rate (providing that queues of a higher priority are not already using the available bandwidth)

- Weighted Random Early Dropping (WRED) of packets can be used as queues become busy, in an attempt to get the TCP socket generating the packets to back off its transmit timers. This prevents the queue overflow, which would result in all subsequent packets being dropped.

QoS is a complex subject and can have a significant impact on the performance of the router. For detailed background information on QoS, see the IETF document *RFC2472, Definition of the Differentiated Services Field*.

In Digi TransPort routers, the classification of incoming IP packets for the purposes of QoS takes place within the firewall. The firewall allows the system administrator to assign a DSCP code to a packet with any combination of source/destination IP address/port and protocol. Details of how this is done are given in the section on firewall scripts.

When the routing code within the router receives an incoming packet, it directs it to the interface applicable to that packet at that time (this is the case whether or not QoS is being applied). Just before the packet is sent to the interface, the QoS code intercepts the packet and assigns it to one of the available priority queues (currently 10 per PPP instance) based on its DSCP value.

Each priority queue has a profile assigned to it. This profile specifies parameters such as the minimum transmit rate to attempt, maximum queue length, and WRED parameters.

The packet is then processed by the queue management code, and either dropped or placed in the queue for later transmission.

Configuring QoS in the web interface

Several configuration are web pages associated with QoS functionality:

- The **Configuration > Network > QoS > DSCP Mappings** page contains parameters to configure DSCP operation.

- The **Configuration > Network > Queue Profiles** page contains parameters to manage the queue "profiles."

- Each **Configuration > Interfaces > Ethernet and Configuration > Interfaces > PPP** instance page contains a QoS sub-page which controls how QoS behaves on that particular interface.

When configuring QoS, be aware that the router supports ten queues, numbered from **0** to **9**, and that DSCP codes range from **0** to **64**.

DSCP Mappings parameters

The **Configuration > Network > QoS > DSCP Mappings** page contains parameters to configure DSCP operation. Each DSCP value must be mapped to a queue. These mappings are set up using this page.

Default

Selects the default queue. When this is changed, any DSCP codes that are set to use the default will have their queue number changed.

DSCP

A list of valid DSCP codes with an associated drop-down list box to the right.

Queue

Each of the DSCP codes in the left-hand column has a queue associated with it. To change the value from what is shown, select the desired value from the drop-down list.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
dscp	n	q	0-63 Default 4	Queue

Examples

- To display a DSCP mapping from the command line, type the following:

  `dscp <code> ?`

  Where **<code>** is a valid DSCP code from **0** to **63**, or **64** (see note below).

- To change the value of a parameter, use the following command:

  `dscp <code> q <value>`

  Where **<code>** is a valid DSCP code and <value> is from **0** to **9**.

- To set the default mapping value, enter the command:

  `dscp 64 q <value>`

  Where **<value>** is the default queue number required and has a value from **0** to **9**.

Note DSCP code **64** is not actually a valid code, but is used to set up the default priority.

Queue Profiles parameters

The **Configuration > Network > Queue Profiles** page contains parameters to manage the queue profiles. The queue profile determines how QoS queues with that profile assigned to them will behave. Up to 12 queue profiles can be defined using this page. These profiles can then be assigned to QoS queues as needed.

Queue

The queue number that relates to the queues defined in the DCSP mappings page.

Minimum kbps

The minimum data transfer rate in kilobits/second that the router will try to attain for the queue.

Maximum kbps

The maximum data transfer rate in kilobits/second that the router tries to attain for this queue. This means that if the router determines that bandwidth is available to send more packets from a queue that has reached its **Minimum kbps** setting, it sends more packets from that queue until the **Maximum kbps** setting is reached.

If the bandwidth on a queue should be restricted, setting the **Maximum kbps** value to the same as, or lower than the **Minimum kbps** value ensures that only the **Minimum kbps** setting is achieved.

Maximum Packet Queue Length

The maximum length of a queue in terms of the number of packets in the queue. Any packets received by the router that would cause the maximum length to be exceeded, are dropped.

WRED Minimum Threshold

The minimum queue length threshold for using the WRED algorithm to drop packets. Once the queue length exceeds this value, the WRED algorithm may cause packets to be dropped.

WRED Maximum Threshold

The maximum queue length threshold for using the WRED algorithm to drop packets. Once the queue length exceeds this value, the WRED algorithm causes all packets to be dropped.

WRED Maximum Drop Probability (%)

The maximum percentage probability used by the WRED algorithm to determine whether or not a packet should be dropped when the queue length is approaching the WRED maximum threshold value.

Note If the length of a queue is less than the **WRED Minimum Threshold** value, there is a zero-percent chance that a packet will be dropped. When the queue length is between the WRED minimum and maximum values, the percent probability of a packet being dropped increases linearly up to the WRED maximum drop probability.

WRED Queue Length Weight factor

A weighting factor used in the WRED algorithm when calculating the weighted queue length. The weighted queue length is based on the previous queue length and has a weighting factor that may be adjusted to provide different transmit characteristics. The actual formula used is:

```
new_length = (old_length * (1-1/2^n)) + (current_length * 1/2^n)
```

Small weighting factor values result in a weighted queue length that moves quickly and more closely matches the actual queue length. Larger weighting factor values result in a queue length that adjusts more slowly. If a weighted queue length moves too quickly (small weighting factor), it can result in dropped packets if the transmit rate rises quickly, but will also recover quickly after the transmit rate tails off. If a weighted queue length moves too slowly (large weighting factor), it allows a burst of traffic through without dropping packets, but may result in dropped packets for some time after the actual transmit rate drops off. Therefore, use care in selecting the weighting factor to suit the type of traffic using the queue.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
qprof	n	minkbps	0-2147483647	Minimum kbps
qprof	n	maxkbps	0-2147483647	Maximum kbps
qprof	n	qlen	0-2147483647	Maximum Packet Queue Length
qprof	n	minth	0-2147483647	WRED Minimum Threshold
qprof	n	maxth	0-2147483647	WRED Maximum Threshold
qprof	n	mprob	0-100	WRED Maximum Drop Probability (%)
qprof	n	wfact	0-2147483647	WRED Queue Length Weight factor

Examples

- To display a queue profile, enter the following command:

  ```
  gqprof <instance> ?
  ```

  Where **<instance>** is the number of the queue profile to be displayed.

- To change the value of a parameter, use the following command:

  ```
  qprof <instance> <parameter> <value>
  ```

- To set the maximum throughput for queue profile **5** to **10kbps**, enter the following command:

  ```
  qprof 5  maxkbps 10
  ```

Configure time bands

This section covers configuring time bands from the web interface or command line. It covers the following topics:

- About time bands on page 488
- Enable and disable time bands for a PPP instance on page 489
- Timeband page parameters on page 490
- Related CLI commands on page 491

About time bands

Digi TransPort routers support time bands. Time bands are used to determine periods of time during which PPP interfaces allowed or prevented from activating. For example, a router in an office could be configured so that the ADSL PPP interface is only raised on weekdays.

Time bands can only be applied to PPP instances.

Time bands are specified by a series of transition times. At each of these times, routing is either enabled or disabled. The default state for a time band is **On**, which means that PPP instances that are associated with unconfigured time bands will operate normally.

The router supports four time band configurations.

Whenever a time band transition occurs, an entry is made in the event log.

Enable and disable time bands for a PPP instance

On the **Configuration > Network > Timebands** page, enabling and disabling time bands for a particular PPP instance is controlled by the settings in a table having the following columns:

Interface

Lists the available PPP instances.

Enable

This column contains checkboxes; each checkbox controls whether or not time bands are enabled for the PPP instance in the left-hand column of the row. Check the checkbox to enable time bands for the associated PPP instance.

Timeband

Selects which of the four available time band instances should be associated with the PPP instance.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	tband	0-3	Timeband

The default state of this parameter is blank.

Timeband page parameters

The **Timeband** parameters pages configure one time band instance each. Configuration is controlled by a table, with the following parameters.

You can configure up to ten time band transitions.

Days

A set of checkboxes for selecting the days of the week to which the time band transitions apply. You can select days individually or in groups for convenience. To select all the days of the week, check the **All** checkbox. To select the weekend only, check the **Sat->Sun** checkbox. To select weekdays only, check the **Mon->Fri** checkbox.

Time

The transition time, specified in 24-hour format with a colon separator between hours and minutes.

State

The routing state, which can be **On** or **Off**. For convenience, this parameter toggles state for each new addition; if an **On** transition is configured, the default state for the next addition is **Off**. Clicking the **Add** button adds the entry into the table. Once an entry is added to the table, remove it by clicking the associated **Delete** button. To activate this time band instance, navigate to the associated **PPP Timeband** configuration page, and click the **Enable** checkbox, or enter the equivalent command line command.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
tband	0-3	days	ALL, MF, Mon, Tue, Wed, Thu, Fri, Sat, Sun	Days
tband	0-3	time	HH:MM	Time
tband	0-3	state	OFF, ON	State

Command format

```
tband <instance> <days#> <days>
tband <instance> <time#> <time>
tband <instance> <state#> <on|off>
```

To specify multiple days, separate the days with a comma, such as **Mon,Wed,Fri**. The abbreviation **MF** is used to specify Monday to Friday.

For example, to allow PPP routing only on weekdays between 9:00 a.m. and 5:30 p.m. enter these commands:

```
tband 0 days 0 mf
tband 0 time0 9
tband 0 state0 on
tband 0 days1 mf
tband 0 time1 5:30
tband 0 state1 off
```

Configure advanced network settings

This section covers configuring advanced network settings from the web interface and command line. It includes the following topics:

- About advanced network settings on page 492
- Advanced Network Settings descriptions on page 493

About advanced network settings

The basic network configuration settings cover most configurations and implementations, and in those cases, the settings should not require changes. The **Advanced Network Settings** are available for those instances where detailed settings for network features require changes.

Advanced Network Settings descriptions

The advanced network settings are on the **Configuration > Network > Advanced Network Settings** page.

First settings group

The first group of settings displayed are as follows:

Secondary IP Address a.b.c.d

An additional IP address to the router that is not associated with any particular interface. The router responds directly to incoming traffic for this address; it does not attempt to onward route any IP packets for this address.

When connected to a Serial interface using TCP

Advertise an MSS of n bytes

The maximum segment size used/advertised by an asynchronous serial port connected to TCP sockets.

Use a Rx Window size of n bytes

The Rx window size used/advertised by an asynchronous serial port connected to TCP sockets.

Default SSL version for outgoing connections

Selects which version of the SSL protocol to use in the **tcpdial** command. The options are:

- **Auto**, which allows the server to select the version.
- **TLSv1 only**
- **SSLv2 only**
- **SSLv3 only**

Some servers are configured to work with a particular version. Unless this version is specifically requested, the connection attempt will fail.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
cmd	n	sec_ip	Valid IP address	Secondary IP address a.b.c.d
sockopt	n	asymss	0-2147483648	When connected to a serial interface using TCP Advertise an MSS of n bytes
sockopt	n	asyrxwin	0-2147483648	Use a Rx Window size of n bytes
sockopt	n	sslver	0-3 0=Auto 1=TLSv1 2=SSLv2	Default SSL version for outgoing connections

Socket settings

Default source IP address interface x,y

The values in these two text boxes define the interface (**None**, **PPP**, **ETH**) and the instance number of the interface to use as a source address for IP when not using the interface that the socket was created on. The router creates general-purpose sockets automatically when the controlling application requests them, for example, when TPAD calls are made over IP or XOT. Normally, the source address used by the socket will be that of the outgoing interface, usually PPP. However, for some applications, such as when setting up a VPN, it may be necessary to specify that the socket uses a different source address such as that of the local Ethernet port. This parameter specifies the interface from which the source address should be derived.

Note Even when this parameter is not configured, the IP address from the interface on which the socket was created is used. The source address specified in this parameter is used only if it causes the traffic to match an Eroute and therefore be sent using IPsec or GRE.

Connect Timeout s seconds

The amount of time after which a TCP socket may remain idle before being closed. If the value is set to **0**, the socket may remain open indefinitely.

TCP socket inactivity timer s seconds

The maximum period of inactivity, in seconds, that can occur before and open TCP/IP socket is closed. The default value is **300** seconds (five minutes), and normally should not need to be changed.

TCP socket keep-alive s seconds

The amount of time, in seconds, between sending keep-alive messages over open TCP connections. The purpose of these messages is to prevent a connection from closing even when no data is being transmitted or received. The default value of this parameter is **0**, which disables keep-alive messages.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
sockopt	n	gp_ipent	0,PPP,ETH	Default source IP address interface **x,y**
sockopt	n	gp_ipadd	Valid interface number	Default source IP address interface **x,y**
sockopt	n	sock_connto	0-2147483648	Connect Timeout **s** seconds
sockopt	n	sock_inact	0-2147483648	TCP socket inactivity timer **s** seconds
sockopt	n	sock_keepact	0-2147483648	TCP socket keep-alive **s** seconds

XOT settings

Default source IP address interface x,y

The values in these two text boxes specify the interface (**None**, **PPP**, **ETH**) and instance number of that interface that IP address that XOT sockets should use instead of the interface that the socket was created on.

Note Even when this parameter is not configured, the IP address from the interface on which the socket was created will be used. The source address specified in this parameter will only be used if it will cause the traffic to match an Eroute and therefore be sent using IPsec or GRE.

NB of XOT listening sockets

The maximum number of XOT sockets available. This may be used to reduce the number of XOT sockets in order to free up more general-purpose sockets for other purposes. The default value of **0** enables the maximum number of XOT sockets available.

Maximum ACK time for XOT data

The maximum time allowance for a remote unit to acknowledge TCP data transmitted by a unit's socket. If this timer expires, the socket is aborted. The default value of **0** disables the timer.

Note There is no requirement for the remote unit to acknowledge received data immediately, therefore setting this parameter to too small a value is not recommended. Some stacks delay sending TCP ACKs in order that they can be incorporated with data sent by the application.

Do not deactivate outgoing XOT sockets when interface disconnects

When checked, this checkbox sets outgoing XOT sockets not to close when the interface they are using disconnects.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
sockopt	n	xot_ipent	Valid interface type, ETH, PPP	Default source IP address interface x,y
sockopt	n	xot_ipadd	Valid interface number	Default source IP address interface x,y
sockopt	n	xot_listens	0-2147483648	NB of XOT listening sockets
sockopt	n	xot_maxack	0-2147483648	Maximum ACK time for XOT data

Backup IP addresses

This page contains a table that is used to specify alternative IP addresses to use when the router fails when attempting to open a socket. These addresses are used only for socket connections that originate from the router and are typically used to provide back-up for XOT connections, TANS (TPAD answering) connections, or any application in which the router is making outgoing socket connections.

When a backup address is in use, the original IP address that failed to open is tested at intervals to check if it has become available again. Additionally, at the end of a session, the router remembers when an IP address has failed, and uses the backup address immediately for future connections. When the original IP address becomes available again, the router automatically detects this, and reverts to using that IP address.

The table has the following four column headings:

IP Address a.b.c.d

The original IP address to which the back-up address relates.

Backup IP address a.b.c.d

The backup address to try when the router fails to open a connection to the previous IP address.

Retry Time s (seconds)

The length of time, in seconds, the router waits between checks to see if a connection can be made to IP Address.

Try Next

When connection to the primary IP address has just failed, this text box determines whether a connection to the backup IP address should be attempted immediately or when the application next attempts to open a connection. When checked, the socket attempts to connect to the backup IP address immediately after the connection to the primary IP address failed and before reporting this failure to the calling application, such as TPAD. If the backup is successful, the application will not experience any kind of failure, even though the router has connected to the backup IP address. When unchecked, the socket reports the failure to connect back to the calling application immediately after the connection to the primary IP address has failed. The router does not try to connect to the backup IP address at this stage. The next time that the application attempts to connect to the same IP address, the router instead automatically connects to the backup IP address. Use the **Add** and **Delete** buttons to add and delete entries to and from the table.

Send "Backup IP" system messages to IP Address: a.b.c.d

The destination IP address to which system messages notifying of the unavailability of an IP address should be sent. This allows the router to send UDP messages to other routers to notify them that an IP address has become available/unavailable. Devices that receive the IP address available/unavailable messages search their own backup IP address tables for the IP addresses indicated, and tag those addresses as available/unavailable as appropriate.

Chaining backup IP addresses

It is possible to chain backup IP addresses by making multiple entries in the table.

For example, if the backup IP address for the original IP address appears as the IP address in the next row, along with a new backup IP address for that IP address. When the original IP address becomes unavailable, the router tries the backup IP address. If that IP address is unavailable, the router tries its backup IP address, and so on.

For example, if the original IP address is **192.168.0.1** with a backup IP address of **192.168.0.2**, setting the IP address in the next row to **192.168.0.2** with a backup IP address of **192.168.0.3** causes the router to try all these IP addresses in succession.

Note The time that it takes for a connection to an IP address to fail is determined by the **Connect timeout** parameter on the **Configuration > Network > Advanced Network Settings > Socket Settings** web page.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ipbu	n	IPaddr	Valid IP address a.b.c.d	IP Address a.b.c.d
ipbu	n	BUIPaddr	Valid IP address a.b.c.d	Backup IP Address a.b.c.d
ipbu	n	retrysec	0-2147483648	Retry Time **s** (seconds)
ipbu	n	donext	OFF,ON	Try Next
sarsys	0	dest	Valid IP address a.b.c.d	Send **Backup IP** system messages to IP address a.b.c.d

Configure legacy protocols

Older protocols that existed before TCP/IP became dominant are often referred to as legacy protocols. Examples of legacy protocols are X.25, SNA and LAPB.

Digi TransPort routers can connect to legacy networks such as X.25. They can also simulate a legacy network so that equipment that, in the past, would have connected to a legacy network, can connect to the Digi TransPort router instead. This means old equipment can be connected to modern networks such as HSUPA.

This section covers configuring legacy protocols from the web interface or command line. It covers the following topics:

- Configure Systems Network Architecture over IP (SNAIP) on page 500
- Configure TPAD parameters on page 509
- Configure X.25 parameters on page 521
- Configure MODBUS Gateway parameters on page 563
- Configure Protocol Switch software on page 567

Configure Systems Network Architecture over IP (SNAIP)

Digi TransPort routers can send Systems Network Architecture (SNA) traffic over TCP/IP, using the DLSw protocol, often called SNAIP. They can also can send HDLC traffic over TCP/IP.

About SNA

SNA uses Synchronous Data Link Control (SDLC), an unbalanced mode in which there is one master station and one or more secondary stations. Each secondary station owns a station address and can only respond when this address has just been polled by the master. A typical scenario is shown in the diagram below:
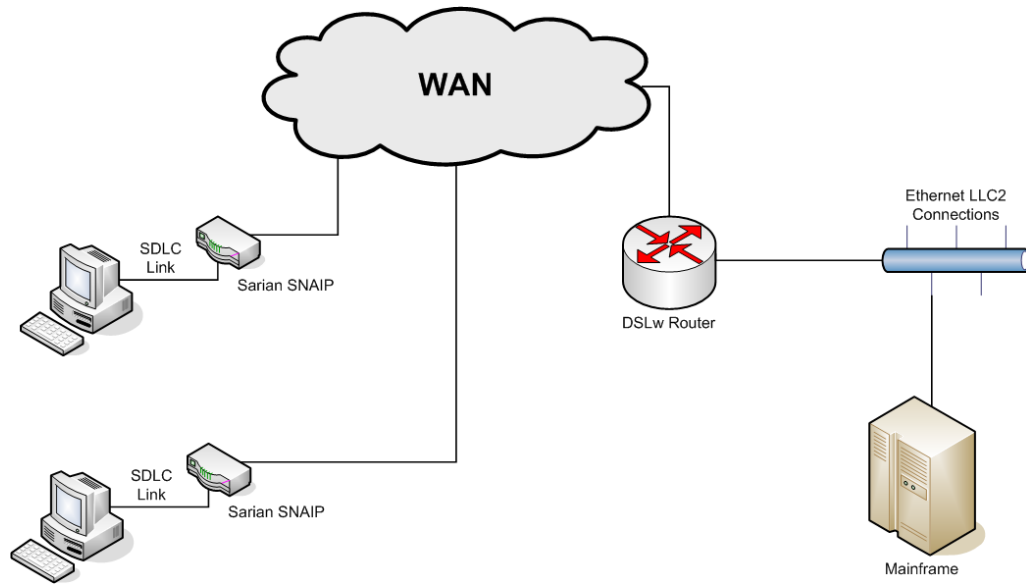
Configure SNAIP parameters

SNA is configured on **Configuration > Network > Legacy Protocols > SNAIP**. Parameters are as follows:

Description

A name for this SNAIP instance, to make it easier to identify.

Send SNAIP traffic over interface

The physical interface used for carrying SNAIP data. This can be set to either **ISDN**, **Serial Port**, or **SharedPort**.

- If **ISDN** is selected, SNAIP data is carried over the ISDN BRI physical interface.

- If **Serial Port** is selected, SNAIP data can be routed to either serial **Port 0** or serial **Port 1** (operating in synchronous mode). To configure **Port 0** or **Port 1** for synchronous operation go to **Configuration > Network > Interfaces > Serial > Serial Port x > Sync Port x**.

- If **Shared Port** is selected, the drop down list next to **Shared Port** specifies the SNAIP instance that has sync port configured. When sync port sharing is enabled only one SNAIP instance can currently own the sync port. Other SNAIP instances however can share this sync port in the event that there is more than one terminal residing on a multi-drop sync line. In this situation with multiple terminals, each terminal station will operate a DLSw state independently of all other stations.

The SNAIP parameter **Priority** is used to select the SNAIP instance to use when more than one is available; the highest number being given preference.

For example, consider that 4 SNAIP instances to all share sync port **0**. To do this, configure **SNAIP 0** in the usual way on **PORT 0**, then configure SNAIP instances **1**, **2**, and **3** to use **SharedPort** and Sync Port from **SNAIP 0**.

Use protocol

The protocol for the interface. Choose **LAPB**, **SNA** for SDLC or **RAW** for raw mode in which all L2 frames are transmitted and received. You can also choose **RAW_NOHDR** for raw mode with no DLSw headers.

Allow this unit to answer calls

This setting is only relevant when the interface is set to ISDN. If this parameter is set to **On**, the router answers incoming calls on the relevant LAPB session. To prevent the router from answering incoming calls on this LAPB session set the option to **Off**.

Only accept calls with MSN ending with

This setting is only relevant when the interface is set to ISDN. This is the filter for the ISDN Multiple Subscriber Numbering facility. By default, this setting is blank. When set to an appropriate value with answering calls parameter above enabled, the router to answer incoming calls only to ISDN numbers where the trailing digits of the called number match the MSN value. For example, setting the MSN parameter to **123** prevents the router from answering any calls to numbers that do not end in **123**.

Only accept calls with sub-address ending with

This setting is only relevant when the interface is set to ISDN. This is the filter for the ISDN sub-addressing facility. By default, this setting is blank. When set to an appropriate value, with answering calls parameter above enabled, the router answers incoming ISDN calls only where the trailing digits of the sub address called match the sub-address value. For example, setting the Sub-address to **123** prevents the router from answering any calls where the sub-address called does not end in **123**.

Assume station exists (Do not send TEST frames)

When this parameter is enabled, **TEST** frames are not transmitted and the **TEST** response is not expected. Instead, the router assumes the station exists and proceeds with the protocol as if the DLSw has received the **TEST** response.

Toggle DCD output each time the DLSw protocol enters the DISCONNECTED state

When this parameter is set to **On**, the **DCD** (Data Carrier Detect) output turns off briefly each time the DLSw protocol enters the **DISCONNECTED** state. Any attached equipment that needs to will see signals changing state.

Sync port should not send or receive data when WAN link is down

Causes the **Sync** port to be deaf and dumb (and have **DCD** low) while the connection with the WAN is down. This setting is supported to prevent terminals from assuming if L2 is up, the rest of the WAN link should be working, at which point the router could go into a management error state.

SNA parameters

Router to be Master on an unbalanced link

Enable this parameter if this router is to be the master in an unbalanced link, or set to **Off** if the router is to be a secondary station.

Polling Response Time

The poll time, in milliseconds, if the router is the master in an unbalanced link.

Polling Stations Addresses

This parameter is only applicable in SNA mode. Lists the station addresses on the data link as a comma-separated list of hex values, such as **c1,d1** for station addresses **0xc1** and **0xd1**.

SAPs

A list of SAP values which correspond to the station addresses.

DSAPs(blank=default)

The Destination SAP value, if left blank the SAP value above is used.

Send Null XID (XID with no Data)

When this parameter is set to **On**, a null XID SSP message will be sent when the router has just received or sent a **REACH ACK** SSP message.

Send XID with Data

A hex string to define binary data and defines an XID SSP message that would be sent in response to a **XIDFRAME** SSP message being received.

Tx Turn Around Time

The time, in milliseconds, between receiving a frame from an outstation and transmission back to the same station. If this parameter is set to **0**, this is disabled and the router can respond immediately. The minimum non-zero value is **10ms**.

Mode

Defines the mode in balanced links, such as HDLC. In unbalanced links such as SNA/SDLC, the mode is defined by being master or the station.

N400 counter

A standard LAPB retry counter. The default value is **3** and it should not normally be necessary to change this.

RR Timer

A standard LAPB/LAPD **Receiver Ready** timer. The default value is **10,000ms** (10 seconds) and it should not normally be necessary to change this.

T1 timer

A standard LAPB timer. The default value is **1000** milliseconds (1 second) and under normal circumstances, it should not be necessary to change it.

T200 timer

A standard LAPB re-transmit timer. The default value is **1000** milliseconds (1 second) and under normal circumstances, it should not be necessary to change it.

Window Size

The X.25 window size. The value range is from **1** to **7** with the default being **7**.

Disconnect link if there has been no activity for **x** seconds

The length of time, in seconds, before the link is disconnected if there has been no activity. If this parameter is **0** or not specified, then the inactivity timer is disabled. It is useful to set this to a short period of time, for example, 120 seconds, when an LAPB instance is being used over ISDN. This timer can be used as a backup hang-up timer, thus saving ISDN call charges. When LAPB is being used on a synchronous port, this parameter should normally be set to **0**.

SSP (WAN) parameters

Virtual MAC Address

Virtual MAC address. The host uses MAC addresses and SAP values as the addressing values to discriminate between circuits, in much the same way as an IP address & TCP port define an addressing point for a TCP socket. This is the MAC address that is reported as part of the DLSw protocol.

Virtual MAC Address of Peer

The Virtual MAC address of the peer.

IP address of the Peer DLSw unit

The IP address of the peer DLSw unit.

Listen on Port

The read IP port. The TCP socket SNAIP listens on.

Use Port **x** if this unit starts the DLSw protocol

The write IP port. This TCP socket will be opened by the router if it needs to start the DLSw protocol.

Use interface for source IP address

Setting this parameter to a **PPP** or **ETH** instance causes the source address used by this SNAIP instance to match that of the Ethernet or PPP interface specified.

Close TCP connection if it is idle for **x** secs

The maximum period of inactivity (in seconds) that may occur before an open TCP/ IP socket is closed. The default value is **300** seconds (5 minutes) and should not normally require altering.

DLSw Ver

The DLSw version to be used. Set to **0** (default) for version 1, set to **2** for version 2.

DLSw Role

When this parameter is set to **Active**, and the router is in SNA mode, this DLSw switch actively connects to the remote DLSw switch.

DLSw Window

The DLSw window size. The value range is from **10** to **100**. The default is **20**.

UDP Capable

Controls the UDP transmission of DLSw SSP packets. Reception is always enabled for version 2 support. If set to **OFF**, the state transitions occur just like DLSw version 1 but the router will indicate it is version 2-capable.

Use 1 socket

When this parameter is set to **On**, only one socket is used for both read and write data. This is useful if the router is behind a NAT box and incoming connections are not possible. This parameter can also be set to **Compatible**, in which mode both sockets are open to start with and then after a negotiation one of the sockets is dropped.

Include MAC Exclusivity Capability

On or **Off**. Set this parameter to **On** to include the MAC exclusivity value in the capabilities exchange message.

MAC Exclusivity Value

See above.

Ignore unsolicited response frames

When enabled, the router ignores unsolicited response frames.

Wait for Contact before progressing to CONNECT PENDING state

During the DLSw negotiation phase and when XID messages are being exchanged, this parameter controls which end sends the **CONTACT** message. Normally this would be off in which case this router would send the **CONTACT** message, but if this parameter is set, we would not send this message, but instead wait for it to be sent to us before progressing in the DLSw state machine.

Make immediate connection attempts before backing off

The number of successive connection attempts before backing off for the number of seconds (default **30**) defined in the **Backoff for x seconds...** parameter. This backoff might be necessary when a server is behind a firewalls that detects too many successive connection attempts in a certain time frame.

Backoff for **x** seconds before attempting to connect again

When backing off because of too many failed consecutive connection attempts, this parameter defines the time, in seconds, the router should remain idle before attempting another connection.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
snaip	x	l1iface	ISDN, Port, SharedPort	Send SNAIP traffic over interface.
snaip	x	l1nb	0–255 (Select LAPB, Port or SharePort instance)	Send SNAIP traffic over interface.
snaip	x	protocol	LAPB, SNA, RAW, RAW_NOHDR	Use the specified protocol.
snaip	x	ans	1=enabled, 0=disabled	Allow this unit to answer calls.
snaip	x	msn	text	Only accept calls with MSN ending with the specified text.
snaip	x	sub	text	Only accept calls with sub-address ending with the specified text.
snaip	x	autocontact	1=enabled, 0=disabled	Assume station exists. (Do not send TEST frames).
snaip	x	dcd_toggle	1=enabled, 0=disabled	Toggle DCD output each time the DLSw protocol enters the **DISCONNECTED** state.
snaip	x	l1oos	1=enabled, 0=disabled	Sync port should not send or receive data when WAN link is down.
snaip	x	master	1=enabled, 0=disabled	Router to be Master on an unbalanced link.
snaip	x	pollresp	0-2147483647	Polling Response Time.
snaip	x	stations	text	Polling Stations Addresses.
snaip	x	saps	text	SAPs.
snaip	x	dsaps	text	DSAPs(blank=default).
snaip	x	send_xid_null	1=enabled, 0=disabled	Send Null XID (XID with no Data).
snaip	x	xid_data	text	Send XID with Data.
snaip	x	turntxtim	0-2147483647	Tx Turn Around Time.
snaip	x	dtemode	1=DTE, 0=DCD	Mode.
snaip	x	n400	0-255	N400 counter.

Entity	Instance	Parameter	Values	Equivalent Web Parameter
snaip	x	tnoact	1000-60000	RR Timer.
snaip	x	t1time	1-60000	T1 timer.
snaip	x	t200	1-60000	T200 timer.
snaip	x	window	1-7	Window Size.
snaip	x	tinact	0-3000	Disconnect link if there has been no activity for x seconds.
snaip	x	vmac	Text (valid MAC address)	Virtual MAC Address.
snaip	x	peervmac	Text (valid MAC address)	Virtual MAC Address of Peer.
snaip	x	IPaddr	Text (valid IP address)	IP address of the Peer DLSw unit.
snaip	x	r_IPport	0-65535	Listen on Port.
snaip	x	w_IPport	0-65535	Use Port x if this unit starts the DLSw protocol.
snaip	X	srcipent	auto, eth, ppp	Use interface for source IP address.
snaip	x	srcipadd	0-255	Use interface for source IP address.
snaip	x	sock_inact	0-2147483647	Close TCP connection if it is idle for x secs.
snaip	x	ver	0-2	DLSw Ver.
snaip	x	passive	0= active, 1=passive	DLSw Role.
snaip	x	dlswwindow	1-100	DLSw Window.
snaip	x	udp_cap	1=enabled, 0=disabled	UDP Capable.
snaip	x	use1sock	On, Off, Compatible	Use 1 socket.
snaip	x	inc_mac_exc	1=enabled, 0=disabled	Include MAC Exclusivity Capability.
snaip	x	mac_exc_val	0-1	Mac Exclusivity Value.
snaip	x	iunsolresp	1=enabled, 0=disabled	Ignore unsolicited response frames.
snaip	x	waitforcontact	1=enabled, 0=disabled	Wait for Contact before progressing to **CONNECT PENDING** state.

Entity	Instance	Parameter	Values	Equivalent Web Parameter
snaip	x	con_attempts	0-2147483647	Make immediate connection attempts before backing off
snaip	x	con_boff_time	0-2147483647	Backoff for x seconds before attempting to connect again

Forcing SNAIP to use a specific instance

If several SNAIP instances share an ASY port, a switchover to a specific instance can be initiated by issuing **snasw x**, where **x** is the SNAIP instance number. This instance must be available to go online, or this command will fail.

To revert back and use the default instance, issue the **snadis x** command. Normal priorities are used to determine which SNAIP instance gets to use the SYNC port.

Configure TPAD parameters

About TPAD

TPAD is a simplified version of the X.25 PAD specification that is commonly used for carrying out credit-card clearance transactions. Digi routers support the use of TPAD over:

- ISDN B and D-channels
- TCP
- UDP
- SSL
- XoT

Automatic back-up between any two of these "layer 2 interfaces" or "transport protocols" is supported.

TPAD configuration pages parameters

TPAD parameters are configured on the **Configuration > Network > Legacy Protocols > TPAD** page and associated pages.

Use TPAD over interface

Selects whether the TPAD instance will use ISDN B-channel X.25, ISDN D-channel X.25, TCP, VXN or SSL as the transport protocol. For ISDN D-channel operation, select **LAPD**" option. For ISDN B-channel operation or operation through a synchronous port, select **LAPB**. In the case of LAPB and LAPD an interface number can also be specified. This parameter specifies which LAPB or LAPD instance to use for the relevant TPAD instance. Select **0** or **1** for LAPB. or **0** or **1** for LAPD. When using LAPB with ISDN, this parameter may be set to **255**, which means use any free LAPB instance. This is useful when more than 2 POS terminals are connected to the router and the acquirer does not support multiple Switched Virtual Circuits (SVCs) on a single B-Channel. A value of **254** uses an available LAPB instance, but will use the same ISDN B channel if two calls are attempted to the same ISDN number at the same time. (All services that the POS terminals may dial must support multiple SVCs if using the setting **254**.)

Use backup interface

Specifies a backup interface used automatically if the call to the primary interface fails. Note that the primary interface will be tried first for every new call attempt.

ISDN Settings parameters

Use number x to make outgoing ISDN calls

Used to specify an ISDN number. This is used in cases where no ISDN number is provided with the ATD command when making an outgoing call.

Use prefix x

A dialing code the router places in front of the telephone number that is issued by the terminal in the ATD command. For example, if the Prefix # was set to **0800** and the number specified by the terminal in the ATD command was **123456**, the actual number dialed by the router would be **0800123456**.

Remove prefix x from number in ATD command

A dialing prefix that is normally inserted by the terminal in the ATD command that is removed by the router before dialing takes place. For example, if the Prefix removal # was set to **0800** and the terminal issued an ATD command containing **0800123456** then the actual number dialed by the router would be **123456**.

Use suffix x

The Suffix # parameter may be set to contain additional numbers that are dialed after the number specified by B-channel ISDN #. For example, if B-channel ISDN # was set to **123456** and Suffix # was set to **789**, the actual number dialed would be **123456789**.

On the main interface Deactivate LAPB session x seconds after TPAD X.25 call has been cleared

Once a TPAD X.25 call has been cleared, the router will keep a LAPB instance active for the length of time set by this parameter. This is to allow further TPAD transactions to take place without having to make another ISDN call. The default value of 10 seconds should be acceptable for most applications. The value of **1** is a special value which means terminate layer 2 immediately the transaction is finished. (When the X.25 call is cleared.) If you select LAPD as the TPAD layer-2 interface, this value is automatically be set to **0** to disable layer-2 deactivation. You can override the **0** setting by entering a new value but note that most network service providers prefer that LAPD connections are not repeatedly deactivated.

On the backup interface Deactivate LAPB session x seconds after TPAD X.25 call has been cleared.

Equivalent to the deactivation timer above, but applies only to backup calls.

X.25 settings parameters

Default X.25 Packet Size

The default X.25 packet size for TPAD transactions.

Use NUA

The X.25 Network User Address for outgoing X.25 calls if no NUA is specified in the call string.

Use NUI

The X.25 Network User Identifier for outgoing X.25 calls if no NUI is specified in the call string.

LCN

The router supports up to eight logical X.25/TPAD channels. In practice, the operational limit is determined by the particular service to which you subscribe (usually 4). Each logical channel must be assigned a valid Logical Channel Number (LCN). The LCN parameter is the value of the first LCN that will be assigned for outgoing X.25 CALLs. The default is **1027**. For incoming calls, the router accepts the LCN specified by the caller.

LCN direction

Whether the X.25 LCN used for outgoing TPAD calls is incremented or decremented from the starting value when multiple TPAD instances share one layer 2 (LAPB or LAPD), connection. The default is **DOWN** and LCNs are decremented, such as if the first CALL uses **1024**, the next will use **1023**, etc. Setting the parameter to **UP** causes the LCN to be incremented from the start value.

On the backup interface

Use NUA

The LCN parameter is used to set the first LCN for the backup interface.

Use NUI

The X.25 Network User Identifier to be used for outgoing X.25 calls if no NUI is specified in the call string for the backup interface.

LCN

The first LCN for the backup interface.

LCN direction

Determines whether the LCN used for the backup X.25 interface is incremented or decremented from the starting value when multiple X.25 instances share a single layer 2 connection.

Report our NUA as **n** to the X.25 network

The NUA that the router will report to the X.25 network as its own NUA when making a call. It is also known as the calling NUA. Often the X.25 network will override this NUA.

Send X.25 RESTART packets

Sends X.25 RESTART packets.

Delay the X.25 RESTART packets by x milliseconds

The time, in milliseconds, to wait before sending the X.25 RESTART packets.

Call User Data

A text string that will be placed in the Call User Data field of an outgoing X.25 call request packet. Whether or not this information is required will depend on the X.25 host that you are connecting to. In most cases the information is not required.

X.25 calls

These setting control how transactions are sent to the host when TPAD is running in direct mode.

One per transaction

Only one transaction is allowed per call.

Allow consecutive transactions

Multiple transactions are allowed per X.25 call, but not until a response has been received from the host.

Allow concurrent transactions

Multiple transactions per X.25 call are allowed irrespective of whether a response has been received from the host.

Use ASCII character **x** as the delimiter character

The character used to separate a main NUA from a backup NUA, and a main NUI from a backup NUI in an ATD command. The default value is the ASCII **!** character (decimal 33).

Forward mode time **x** milliseconds

If not framed with STX and ETX characters, can still have data formatted after this period.

Create an event when reply from X.25 host matches

Used to generate a data trigger event (code 47) when the reply from the X.25 host contains the string specified in this parameter. You can configure the router to generate an email alert message when this event occurs. See file **LOGCODES.TXT** for a complete list of events.

XoT/TCP settings

Connect to remote IP address

When the router is configured for XOT or TCP socket mode, this parameter is used to specify the IP address of the host to which the TCP/XOT connection is made. The transport protocol must be set to TCP.

Port

When making a TCP socket connection (such as the transport protocol has been set to **TCP** not **XoT**), this parameter must be used to specify the TCP port number to use.

IP length header

When making a TCP socket connection (such as the transport protocol has been set to TCP), setting this parameter to **On** will pre-pend the data sent to the host with a 2-byte length header. The 2-byte length header is not included in the length calculation. When set to **8583 Ascii 4 byte**, the IP length header conforms to the ISO 8583 format. Setting this parameter to **On Inclusive** pre-pends a 2-byte length header, and the calculation of the length includes the 2 bytes of the length header.

TPAD Settings

Use Terminal ID (TID)

Inserts or replaces a Terminal ID in the APACS 30 string.

Replace TID provided by connected terminal with configured TID

When enabled, any Terminal ID provided by a connected terminal is replaced by the ID set in the **Use Terminal ID** field above.

The TID will be become inactive in n seconds.

The time, in seconds, before the Terminal ID is considered inactive. Local authorizations may be configured to occur on active TIDs (terminal Ids), so this parameter defines how long a time (without transactions) must pass for a TID to change from active to inactive.

Use TID xxxxxxxxx with incoming APACS 50 polling calls

The terminal ID to associate with this TPAD instance when answering an incoming APACS 50 polling call.

Use merchant Number

Inserts a merchant number into the APACS 30 string when the locally connected equipment does not transmit a merchant number.

Use Connect String

A string sent to the user's terminal when an outgoing TPAD call has been connected, instead of the normal ENQ character. For example, this might be used to make a TPAD connection look like a PAD connection by specifying **CON COM** as the connect string.

The polling character set is c

A string that specifies a character or set of characters to be treated as polling characters. The router responds to any of these characters using ACK. This parameter should normally be left blank.

Enable Message Numbering

When enabled, the router overrides the message numbering of the local equipment and substitute its own message numbering in the APACS 30 data. This is useful when the locally connected equipment does not automatically increment the APACS 30 message number.

Disable Direct Mode

Enabling this setting will prevent the router from automatically using Direct Mode (see below) when it receives an APACS 30 packet without any call set-up.

Boot to Direct Mode

Direct mode is a mode of operation whereby the router automatically routes APACS 30 packets to their destination without the terminal having to perform any call control. If this parameter is set to **Yes**, the next time the router is rebooted, it operates in direct mode. For direct mode to work you must set up the appropriate addressing information, such as Transport protocol, NUA, NUI, IP address etc. If this parameter is not enabled, the router still tries to use direct mode if it detects that it is required, due to the absence of call control information. This parameter can be used in certain cases when the router cannot automatically determine whether or not to use direct mode.

Use response code n in "unable to authorise" message

This parameter only applies when the router is operating in direct mode. In cases where the router is unable to send the APACS 30 packet to the remote host, it replies to the terminal with an unable to authorize message. By default, this message contains a response code **05**, which means declined. Entering a number for this parameter causes the router to use that number in place of the default response code. A value of **0** for this parameter prevents the router from replying.

Clearing time n milliseconds

The clearing time, in milliseconds, that an X.25 call is left open after receiving a response from the host. Each response from the host resets this timer.

Delay transmitting the APACS 30 string for x milliseconds after connecting to X.25 host

Setting this parameter causes the router to pause for the specified number of milliseconds in between successfully connecting to the remote X.25 host and transmitting the APACS 30 string.

Retransmit APACS 30 string if error detected

Enabling this setting causes the router to retransmit the APACS 30 string to the terminal if an error is detected, such as no ACK received from terminal.

STX/ETX removal

Enabling **Del STX&ETX** causes the router to strip off the **STX** and **ETX** characters that normally surround the APACS 30 string before sending it to the host. Enabling **Del STX only** causes the router to strip the **STX** character only.

Do not transmit ENQ characters

Under the TPAD protocol, the ENQ character is normally used to indicate that a call has connected and that the TPAD terminal may proceed with the transaction. Enabling this parameter will prevent the router from transmitting ENQ characters to the TPAD terminal when a connection is made.

Delay sending ENQ characters to TPAD terminal for x milliseconds when a call has been connected

Set s the delay, in milliseconds, from when the router first connects the call to when it transmits the ENQ to the terminal. By default, there is no delay.

Wait for **x** milliseconds for an ACK before retransmitting the data

The time the router waits for an ACK character to be received after sending data to the terminal. If an ACK character is not received within this time, the data is retransmitted. A value of **0** sets a delay of **1 second** (the default).

Transmit TPAD transactions directly in a Synchronous frame

If enabled, TPAD transactions are transmitted without any outer protocol, such as X.25, such as they are placed directly in a synchronous frame on ISDN. This sometimes referred to as HDLC by certain card acquirers.

Include LRC

The LRC (Longitudinal Redundancy Check) is a form of error checking that may be required by some TPAD terminals. When the Include LRC option is enabled the router will check the LRC sent by the terminal and if it indicates a problem has occurred NAK the message. If this parameter is enabled but no LRC is sent by the terminal, the transaction is not forwarded to the host.

Include LRC line

This parameter is normally disabled so that any LRCs received from a TPAD terminal will be removed before the transaction data is transmitted to the remote host. In most cases this is acceptable because the network will provide error correction and so the LRC is redundant. In some circumstances it may be necessary to enable this parameter so that the router transmits the LRC to the remote host along with the transaction data.

Force parity when sending data to the terminal

If enabled, the router always uses even parity when relaying data from a remote host to a locally connected TPAD terminal. To allow data to pass through without the parity being changed, disable this setting.

Strip parity when sending data to the host

Enabling this parameter causes the router to remove any parity before sending the data to the host.

Force parity when sending data to the host

If enabled, the router always uses EVEN parity when relaying data from the locally connected TPAD terminal to the remote host. To allow data to pass through without the parity being changed disable this setting.

Strip Trailing Spaces

If enabled, the TPAD instance looks at responses coming from the host and remove any trailing space characters from the end of the packet before relaying the data to the terminal. This may be necessary if the host system pads out responses with unnecessary spaces which can cause abnormal behavior in some terminals.

Acknowledge TPAD data packets

Causes the router to acknowledge TPAD data packets from the terminal. This parameter should normally be enabled. This parameter is only used if no polling characters (see above) are defined.

Convert leading STX character to SOH

If enabled, the router converts the leading STX character in a transaction to an SOH character.

Terminate TPAD call is EOT only

A TPAD call is normally terminated with a DLE EOT sequence. Some terminals only require the EOT character on its own. If this is the case then enable this parameter.

Clear TPAD call if there is no response to a TPAD transaction request for x seconds

The length of time, in seconds, the router waits for a response to a TPAD transaction request before clearing the TPAD call.

Generate an event when a TPAD transaction takes longer than x seconds

Setting this parameter to a non-zero value causes the router to generate an **Excessive Transaction Time** event (**code 56**) each time a TPAD transaction takes longer that the specified number of seconds. This could be used in conjunction with an appropriate Event Handler configuration to generate email alert messages or SNMP traps when TPAD transactions take longer than expected. See **Configuration > Alarms > Event Logcodes** for a complete list of events.

When the transaction time exceeds x milliseconds, increment the "SLA Exceptions" statistic

When the total transaction time exceeds the value (in ms) set in this parameter, the NB SLA exceptions statistic on the **Diagnostics - Statistics > TPAD** page is incremented. This statistic can be viewed on the CLI interface by entering the **at\mibs=tpad.n.stats** command, where **n** is the TPAD instance.

Clear the call x seconds after receiving a response

The time period for which the socket closing or the X.25 call clearing is delayed by after the TPAD session has finished. For example, if this parameter is set to **10,** then 10 seconds after the TPAD session is finished (**NO CARRIER** is seen on the ASY TPAD port) the network call (X25 or TCP socket) is cleared. The number **1** is a special value. If set to the number **1**, the call is cleared immediately, instead of after 1 second.

This parameter is for advanced users only. It enables TPAD transactions to be carried out using the V.120 protocol (**ATDV** command). The parameter is used in conjunction with the Polling Answering Service (PANS), and identifies which PANS instance is to be used for an outgoing V.120 call. For this to work, the PANS instance must be bound to a Rate Adaption instance.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
tpad	n	l2iface	lapb, lapd, tcp, ssl, vxn	Use TPAD over interface.
tpad	n	l2nb	0-255	Use TPAD over interface.
tpad	n	ipmode	0=XOT, 1=raw TCP	Use TPAD over interface.
tpad	n	bakl2iface	lapb, lapd, tcp, ssl, vxn	Use backup interface.
tpad	n	bakl2nb	0-255	Use backup interface.
tpad	n	bnumber	text (valid ISDN number)	Use number x to make outgoing ISDN calls.
tpad	n	prefix	text (numeric)	Use prefix x
tpad	n	prefix_rem	text (numeric)	Remove prefix x from number in ATD command.
tpad	n	suffix	text (numeric)	Use suffix x.
tpad	n	tl2deact	0-10000	On the main interface Deactivate LAPB session x seconds after TPAD X.25 call has been cleared.
tpad	n	baktl2deact	0-10000	On the backup interface Deactivate LAPB session x seconds after TPAD X.25 call has been cleared.
tpad	n	defpak	16,32,64,128,256,512,1024	Default X.25 Packet Size.
tpad	n	nua	text	Use NUA.
tpad	n	nui	text	Use NUI.
tpad	n	lcn	1-4095	LCN.
tpad	n	lcnup	1=up, 0=down	LCN direction.
tpad	n	baknua	text	(Backup) Use NUA.
tpad	n	baknui	numeric text	(Backup) Use NUI.
tpad	n	baklcn	1-4095	(Backup) LCN.
tpad	n	baklcnup	1=up, 0=down	(Backup) LCN direction

Entity	Instance	Parameter	Values	Equivalent Web Parameter
tpad	n	cingnua	numeric text	Report our NUA as n to the X.25 network.
tpad	n	cud	text	Call User Data.
tpad	n	samecall	0	One per transaction.
tpad	n	samecall	1	Allow consecutive transactions.
tpad	n	samecall	2	Allow concurrent transactions.
tpad	n	delimchar	32-127	Use ASCII character x as the delimiter character.
tpad	n	ftime	0-20000	Forward mode time x milliseconds.
tpad	n	trig_str	text	Create an event when reply from X.25 host matches.
tpad	n	IPaddr	IP address	Connect to remote IP address.
tpad	n	iphdr	0=Off 1=On 2=8583 Ascii 4 byte	IP length header.
tpad	n	termid	text	Use Terminal ID (TID).
tpad	n	dotermid	1=enabled, 0=disabled	Replace TID provided by connected terminal with configured TID.
tpad	n	tid	text	Use TID **xxxxxxxx** with incoming **APACS 50** polling calls.
tpad	n	merchnum	text	Use merchant Number.
tpad	n	useconstr	1=enabled, 0=disabled	Use Connect String.
tpad	n	constr	text	Use Connect String.
tpad	n	pollchars	text	The polling character set is c.
tpad	n	domsgnb	1=enabled, 0=disabled	Enable Message Numbering
tpad	n	disdir	1=enabled, 0=disabled	Disable Direct Mode.
tpad	n	bdir	1=enabled, 0=disabled	Boot to Direct Mode.
tpad	n	uaarc	0-99	Use response code n in **unable to authorise** message.
tpad	n	clear_dirtime	0-60000	Clearing time n milliseconds.
tpad	n	trandel	0-5000	Delay transmitting the APACS 30 string for x milliseconds after connecting to X.25 host.

Entity	Instance	Parameter	Values	Equivalent Web Parameter
tpad	n	teretran	1=enabled, 0=disabled	Retransmit APACS 30 string if error detected.
tpad	n	delstx	1=enabled, 0=disabled	**STX/ETX** removal.
tpad	n	no_enq	1=enabled, 0=disabled	Do not transmit **ENQ** characters.
tpad	n	tenqdel	0-5000	Delay sending **ENQ** characters to TPAD terminal for x milliseconds when a call has been connected.
tpad	n	tackdel	0-10000	Wait for x milliseconds for an **ACK** before retransmitting the data.
tpad	n	dsync	1=enabled, 0=disabled	Transmit TPAD transactions directly in a Synchronous frame.
tpad	n	inclrc	1=enabled, 0=disabled	Include LRC.
tpad	n	incllrc	1=enabled, 0=disabled	Include LRC line.
tpad	n	fpar	1=enabled, 0=disabled	Force parity when sending data to the terminal.
tpad	n	lrpar	1=enabled, 0=disabled	Strip parity when sending data to the host.
tpad	n	lfpar	1=enabled, 0=disabled	Force parity when sending data to the host.
tpad	n	strip_tspaces	1=enabled, 0=disabled	Strip Trailing Spaces.
tpad	n	ackdat	1=enabled, 0=disabled	Acknowledge TPAD data packets.
tpad	n	stx_2_soh	1=enabled, 0=disabled	Convert leading **STX** character to **SOH**.
tpad	n	eot_only	1=enabled, 0=disabled	Terminate TPAD call is EOT only.
tpad	n	tresp	0–1000	Clear TPAD call if there is no response to a TPAD transaction request for x seconds.
tpad	n	texcess	0–100	Generate an event when a TPAD transaction takes longer than x seconds
tpad	n	tsla	0–3000	When the transaction time exceeds x milliseconds, increment the SLA Exceptions statistic.
tpad	n	clear_time	0-2147483647	Clear the call x seconds after receiving a response
tpad	n	dialctx	0-255	If the terminal dial command specifies V.120 use PANS context x.

Configure X.25 parameters

The **Configuration > Network > Legacy Protocol > X.25** menu has the following sub-menu options:

- General
- LAPB
- NUI Mappings
- NUA / NUI Interface Mappings
- Calls Macros
- IP to X.25 Calls
- PADS n
- X.25 Settings
- IP Settings
- PADs
- X.25 PVCs

General X.25 parameters

This section contains some global X.25 settings.

When answering a X.25 call, use the addresses from CALL packet in the CALL CNF packet

If enabled, when answering a call, the called and calling addresses from the CALL packet are used in the X25 **CALL CNF** (call confirm packet) that the router sends to answer the call. This setting can be enabled on a per interface type basis, (LAPD, LAPB or XoT).

Reset XOT PVC if the router is the Initiator

If enabled, the router is responsible for resetting the links when an XOT PVC comes up. This parameter should only be set to **Off** when it is known that the responder will reset the links.

Reset XOT PVC if the router is the Responder

If set to **On**, the router is responsible for resetting the links on XOT PVC links when it is the responder. The default for this parameter is **Off**.

Include length of header in IP length header

For all X.25 calls that include an IP header length indication, such as IP Length Header is set to **On** a TPAD or PAD, etc, this parameter specifies whether the length indicated includes or excludes the length of the header itself. By default this setting is **Off**, in which case the length of the header is NOT included in the value.

For example, suppose there is one byte of data of value 67 to encode. Then, **00 01 67** is the encoding if this parameter is set to **Off** as the length (**00 01**) is **1**, because the length does not include the length of the header.

When set to **On,** the length of the IP header is included in the value, such as **00 03 67** is the encoding as the header bytes are included.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
X25gen	0	lapd_cnf_addr	1=enabled, 0=disabled	When answering a X.25 call, use the addresses from **CALL** packet in the **CALL CNF** packet. LAPD setting
X25gen	0	lapd_cnf_addr	1=enabled, 0=disabled	When answering a X.25 call, use the addresses from **CALL** packet in the **CALL CNF** packet LAPB setting
X25gen	0	xot_cnf_addr	1=enabled, 0=disabled	When answering a X.25 call, use the addresses from **CALL** packet in the **CALL CNF** packet XoT setting
X25gen	0	reset_xotpvc_ini	1=enabled, 0=disabled	Reset XOT PVC if the router is the Initiator
X25gen	0	reset_xotpvc_resp	1=enabled, 0=disabled	Reset XOT PVC if the router is the Responder
X25gen	0	en_incl_iphdr	1=enabled, 0=disabled	Include length of header in IP length header

X.25 LAPB parameters

LAPB (Link Access Procedure Balanced) is a standard subset of the High-Level Data Link Control (HDLC) protocol. It is a bit-oriented, synchronous, link-layer protocol that provides data framing, flow control and error detection and correction. LAPB is the link layer used by X.25 applications.

On Digi TransPort routers, LAPB can be used over ISDN or over a synchronous serial port.

Use: Serial port Port x (in Synchronous Mode)

To use the LAPB instance over a synchronous serial port enable this setting and select a serial port number. To configure settings of the synchronous port such as speed and clock source navigate to **Configuration > Network > Interfaces > Serial > Serial Port n > Sync Port n.**

Use: ISDN

Enable this setting to use LAPB over ISDN.

Mode DTE or DCE

Determines whether LAPB will behave as DTE (Data Terminal Equipment) or DCE (Data Circuit-terminating Equipment) in an X.25 protocol sense. Physical DTE vs. DCE wiring cannot be changed by configuration.

N400 Counter x

This is the standard LAPB retry counter. The default value is **3** and it should not normally need to be changed.

RR Timer x milliseconds

A standard LAPB Receiver Ready timer. The default value is **10,000 milliseconds** (**10 seconds**) and it should not normally be necessary to change this.

T1 Timer x milliseconds

A standard LAPB timer. The default value is **1000 milliseconds** (**1 second**) and under normal circumstances, it should not be necessary to change it.

T200 Timer x milliseconds

The standard LAPB re-transmit timer. The default value is **1000 milliseconds** (**1 second**) and under normal circumstances, it should not be necessary to change it.

X.25 Window Size

The X.25 window size. The value range is from **1** to **7** with the default being **7**.

Disconnect link if there has been no X.25 activity for x seconds

The length of time, in seconds, before the link is disconnected if there has been no X.25 activity. If this parameter is **0** or not specified, then the inactivity timer is disabled.

Disconnect link if there has been no activity for x seconds

The length of time, in seconds, before the link is disconnected if there has been no activity. If this parameter is zero or not specified, then the inactivity timer is disabled. It is useful to set this to a short period of time, for example, 120 seconds, when a LAPB instance is being used over ISDN for example with TPAD. Should the POS device fail to instruct TPAD to hang up then this timer can be used as a backup hang-up timer thus saving ISDN call charges. When LAPB is being used on a synchronous port, this parameter should normally be set to 0.

Send X.25 Restart packet on receipt of SABM frame

This parameter can be set to **No** or **Immediate**.

- When set to **Immediate**, the LAPB instance sends an X.25 restart packet immediately on receipt of an SABM (Set Asynchronous Balanced Mode) frame.

- If the parameter is set to **No**, no X.25 restart is sent.

ISDN Parameters

Allow this unit to answer calls

If enabled, this instance of LAPB answers incoming ISDN calls.

Only accept calls from calling number ending with

The filter for the ISDN Multiple Subscriber Numbering facility. It is blank by default. When set to an appropriate value with **Allow this unit to answer calls** enabled, the router answers incoming calls only to ISDN numbers where the trailing digits match the MSN value. For example, setting the MSN parameter to **123** prevents the router from answering any calls to numbers that do not end in **123**.

Only accept calls with sub-address ending with

The filter for the ISDN sub-addressing facility. It is blank by default but when set to an appropriate value, with **Allow this unit to answer calls** enabled, the router answers incoming ISDN calls only where the trailing digits of the sub address called match the Sub-address value. For example, setting the Sub-address to **123** prevents the router from answering any calls where the sub-address called does not end in **123**.

Keep ISDN LAPB link activated when user sends a DISC or X.25 PAD session terminated

When this parameter is enabled, the following setting is enabled:

Wait x milliseconds before attempting to establish the LAPB link after B-channel becoming active

This parameter sets the length of time (in milliseconds), that the LAPB instance will wait from an ISDN B-channel becoming active before attempting to establish a LAPB connection, such as the length of time for which the LAPB instance stays passive. The default is **0**, as most ISDN networks allow CPE devices to initiate a LAPB link. If your ISDN network does not permit CPE devices to initiate the LAPB link you should set this parameter to a value that allows the network sufficient time to establish the LAPB link.

Use as x a calling party number when making ISDN calls

This is Calling Line Identification. The router will only answer calls from numbers whose trailing digits match what is entered in this field. The line the router is connected to must have CLI enabled by the telecoms provider, and the calling number cannot be withheld.

Async Mux 0710 Parameters

For certain W-WAN modules LAPB is used to perform multiplexing of serial channels. If using LAPB for X.25 over ISDN or serial then these settings should be ignored. These settings should not be changed unless under the instruction of technical support.

Mux 0710 mode

If enabled, configures the LAPB instance to be used for multiplexing of serial channels instead of X.25.

Mux mode

Controls the multiplexing mode.

DLC

The data link channel number to use for this virtual ASY port.

ASY port

The physical ASY port over which to multiplex.

Virtual ASY port

The virtual ASY port number that this LAPB instance will multiplex over the physical port.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
lapb	n	l1iface	port, isdn (use "port" for sync port)	Use: Serial port Port x (in Synchronous Mode)
lapb	n	l1nb	0,1	Use: Serial port Port x (in Synchronous Mode) **0** for **Port 0**, **1** for **Port 1**
lapb	n	l1iface	port, isdn (use "isdn" for ISDN)	Use: ISDN
lapb	n	dtemode	DTE/DCE mode: 0=DTE 1=DCE	Mode DTE or DCE
lapb	n	N400	1-255	N400 Counter x
lapb	n	tnoact	1000-60000	RR Timer x milliseconds
lapb	n	t1time	1-60000	T1 Timer x milliseconds
lapb	n	t200	1-60000	T200 Timer x milliseconds
lapb	n	Window	1-7	X.25 Window Size
lapb	n	tinactx25	0-3000	Disconnect link if there has been no X.25 activity for x seconds
lapb	n	tinact	0-3000	Disconnect link if there has been no activity for x seconds
lapb	n	restartact	1=enabled, 0=disabled	Send X.25 Restart packet on receipt of SABM frame
lapb	n	ans	1=enabled, 0=disabled	Allow this unit to answer calls
lapb	n	msn	text	Only accept calls from calling number ending with
lapb	n	sub	text	Only accept calls with sub-address ending with
lapb	n	ptime	0-60000	Wait x milliseconds before attempting to establish the LAPB link after B-channel becoming active
lapb	n	cli	text	Only answer calls from numbers whose trailing digits match
lapb	n	mux_0710	1=enabled, 0=disabled	Mux 0710 mode
lapb	n	mux_mode	0=Basic, 1=Error Recovery	Mux mode

Entity	Instance	Parameter	Values	Equivalent Web Parameter
lapb	n	dlc	0-63	DLC #
lapb	n	asyport	0-255	ASY port
lapb	n	virt_async	0-255	Virtual ASY port

NUI Mappings parameters

When a TPAD call is taking place, the attached terminal sometimes only specifies a NUI (Network User ID) to call. If the X.25 network requires an NUA instead of an NUI to determine the destination of a call then the NUI Mappings table can be used to convert an NUI to an NUA.

If a TPAD call specifies a call in which the NUI matches an entry the call actually placed on the network will contain the respective NUA and no NUI.

TransPort WR44v2 (SN: 319410) Configuration and Management

Configuration - Network > Legacy Protocols > X.25 > NUI Mappings

▼ X.25
  ▶ General
  ▶ LAPB
  ▼ NUI Mappings

When a TPAD call is taking place the attached terminal sometimes only specifies a NUI to call. If the X.25 network requires a NUA instead of a NUI to d...
destination of a call, then the NUI Mappings table can be used to convert a NUI to a NUA.

(You can specify up to 20 mappings)

NUI	Maps to NUA
No NUI mappings have been configured.	

[Add]

[Apply]

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
nuimap	n	nua	text	Maps to NUA
nuimap	n	nui	text	NUI

NUA / NUI Interface Mappings parameters

For PAD and TPAD instances, the NUA/NUI Interface Mappings table can be used to override the following:

- Interface
- Backup interface
- IP address
- TCP/UDP port number

Based upon data in the call request matching the following comparison fields:

- NUA called
- NUI called
- X.25 Call Data
- PID

All the comparison fields, **NUA**, **NUI**, **Call Data**, and **PID**, can use the wildcard matching characters **?** and *****.

NUA

The Network User Address.

NUI

The Network User Identifier.

Call Data

The X.25 Call Data.

PID

The Protocol Identifier.

IP address

The IP address.

IP Port

The IP port number.

Interface

The Primary interface name.

Backup Interface

The Backup interface name.

Note This table is duplicated in the **Configuration > Network > Protocol Switch > NUA to Interface Mappings** section, as it can also be used by the Protocol Switch. Not all of the fields are visible in the Protocol Switch section, as they do not all apply to the Protocol Switch.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
nuaip	N	nua	text	NUA
nuaip	N	nui	text	NUI
nuaip	N	cud	text	Call Data
nuaip	n	pid	text	PID
nuaip	n	IPaddr	IP address	IP Address
nuaip	n	ip_port	0-65535	IP Port
nuaip	n	swto	0 -15	Interface
nuaip	n	buswto	0 -15	Backup Interface

The interface and backup interface values are as follows:

Parameter Value	Interface Type
0	Default
1	LAPD
2	LAPB 0
3	LAPB 1
4	XOT
5	LAPD x (instance determined by NUA)
6	LAPB 0 PVC
7	LAPB 1 PVC
8	XOT PVC
9	TCP Stream
10	UDP Stream
12	LAPB 2
13	LAPB 2 PVC
14	VXN
15	SSL

Calls Macros parameters

This page allows you to define up to **64** X.25 CALL macros that can be used to initiate ISDN and/or X.25 layer 3 calls. These simple English-like names are mapped to full command strings. For example, the call string:

```
0800123456=789012Dtest data
```

could be given the name **X25test** and then executed simply by entering:

```
CALL X25test
```

To create a macro, enter a name for the macro in the left column of the Call Macros table and in the right column enter the appropriate command string (excluding the ATD). Then click **Add**.

Macro

The name of the macro, this can be any text.

Command

The X.25 call command.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
macro	n	name	text	Macro
macro	n	cmd	text	Command

IP to X.25 Calls parameters

This page contains a table that allows you to enter a series of IP Port numbers and X.25 Call strings as shown below. It is used to configure the router so that IP data can be switched over X.25. For example data that is received on a TCP connection can be answered by a PAD as if it is an X.25 call.

This table is duplicated in the Configure Protocol Switch software on page 567,as it is also used by the protocol switch. It is included at this point in the web user interface as a convenience in case the table is being used in conjunction with PAD and not the protocol switch.

IP Port

Used to set up the port numbers for those IP ports that will listen for incoming connections that are to be switched over X.25 or other protocol. In the case of switching to X.25, when such a connection is made the router will make an X.25 Call to the address specified in the X.25 Call field. Once this call has been connected, data from the port will be switched over the X.25 session.

Number of Sockets

Selects how many IP sockets should simultaneously listen for data on the specified port. The number of available IP sockets will depend on the model you are using and how many are already in use (see note below).

X25 Call

The X.25 call field may contain an X.25 NUA or NUI or one of the X.25 Call Macros defined on the **Configuration > Advanced applications > X25 > Macros page.**

PID

The protocol ID (PID) to use when the router switches an IP connection to X.25. The PID field takes the format of four hexadecimal digits separated by commas, such as **1,0,0,0**, at the start of the **Call User Data** field in the X.25 call.

Confirm Mode

When confirm mode is set to **On**, then the incoming TCP socket is not successfully connected until the corresponding outgoing call has been connected. The incoming TCP socket triggers the corresponding outgoing call either to a local PAD instance or to whatever is configured. The effect of this mode is that the socket will fail if the outbound call fails and so may be useful in backup scenarios. In addition it will ensure no data is sent into a "black hole". (When this setting is not enabled, data that is sent on the inbound TCP connection before the outbound connection has been successful can be lost.)

RFC 1086 Mode:

RFC 1086 specifies a mode of operation in which the IP socket answers and then with a simple protocol in the socket identifies the X.25 address and other X.25 call setup parameters to be used. Then when the X.25 call parameters have been identified the X.25 call is made and if successful then data is then switched between the X.25 call and the IP socket. The protocol selects whether incoming or outgoing support is required.

IP length header

When IP length header is **On**, the IP length indicator field is inserted at the start of each packet. When set to **8583 Ascii 4 byte**, the IP length header conforms to the ISO 8583 format.

In the example above, 3 IP sockets will listen for an incoming connection on IP Port **2004**. Once connected each socket makes an X.25 Call to **jollyroger**. The router recognizes that **jollyroger** is a pre-defined macro (as illustrated below), and translates it into an X.25 Call to address **32423** with the string **x25 data** included as data in the call. The outgoing X.25 call(s) are made over whichever interface is specified by the **Switch from XOT(TCP) to** parameter on the **Configuration > Network > Protocol Switch** page.

Note At the top of the page, the total number of sockets available and the number currently free is shown. Care should be take not to allocate too many of the free sockets unless you are confident that they are not required for other applications.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ipx25	n	ip_port	0-65535	IP Port
ipx25	n	nb_listens	0-software-dependent max	Number of Sockets
ipx25	n	x25call	NUA, NUI or X.25 macro name	X25 Call
ipx25	n	pid	hex numbers	PID
ipx25	n	cnf_mode	1=enabled, 0=disabled	Confirm Mode
ipx25	n	rfc1086_mode	1=enabled, 0=disabled	RFC 1086 Mode
ipx25	n	iphdr	0=Off 1=On 2=8583 Ascii 4 byte	IP length header

PADS parameters

PAD which stands for **P**acket **A**ssembler **D**issembler, is used to interface between a character based serial connection and an X.25 synchronous packet switched network.

There are two main elements to the configuration procedure for accessing X.25 networks:

• General and service related parameters

• PAD parameters (X.3)

Each X.25 PAD configuration page also includes a sub-page detailing the X.3 PAD parameters. Collectively this set of values is known as a PAD profile. Your router contains four pre-defined standard PAD profiles numbered **50**, **51**, **90** and **91**. You can also create up to four custom PAD profiles numbered **1** to **4** for each PAD instance.

Use PAD over interface

Selects whether the PAD instance uses ISDN B-channel X.25, ISDN D-channel X.25, TCP, UDP, VXN, SSL TCP or SSL XoT as the transport protocol.

- For ISDN D-channel operation, select the **LAPD** option is selected.

- For ISDN B-channel operation or operation through a synchronous port, select **LAPB**.

- For LAPB and LAPD, you can also specify an interface number.

This parameter specifies which LAPB or LAPD instance to use for the relevant TPAD instance. Select **0** or **1** for LAPB or **0** or **1** for LAPD.

Use backup interface

A backup interface used automatically if the call to the primary interface fails. The primary interface is tried first for every new call attempt.

X.25 Settings

Default X.25 packet size

The default X.25 packet size. This can be set to **16**, **32**, **64 128**, **256**, **512** or **1024**, but the actual values permitted are normally constrained by your service provider.

Answer incoming calls from NUA

The NUA that the router responds to for incoming X.25 calls.

Only answer calls with CUG

The PAD will only answer calls with this Call User Group (CUG) specified.

Use X.25 Call Macro macroname to an ATD command

The name of an X.25 call macro used when an **ATD** command is received by the router. The **ATD** command is ignored, and a PAD **CALL** command using the macro replaces it. The purpose of this feature is to allow non-PAD terminals to use an X.25 PAD network connection. X.25 call macros are set up in the **Configuration > Network > Legacy Protocols > X.25 > Call Macros** web page, or by using the macro text command.

Use NUA

This NUA is used as the calling NUA when an outgoing X.25 call is made.

LCN

The router supports up to 8 logical X.25 channels. In practice, the operational limit is determined by the particular service to which you subscribe (usually 4). Each logical channel must be assigned a valid Logical Channel Number (LCN). The LCN parameter is the value of the first LCN that will be assigned for outgoing X.25 CALLs. The default is **1027**.

For incoming calls, the router accepts the LCN specified by the caller.

LCN Direction

Whether the LCN used for outgoing X.25 calls is incremented or decremented from the starting value when multiple X.25 instances share one layer 2 (LAPB or LAPD), connection. The default is **Down** and LCNs are decremented, such as if the first CALL uses **1024**, the next will use **1023**, etc. Setting the parameter to **Up** causes the LCN to be incremented from the start value.

NUI/NUA selection

If both an NUI and an NUA are included in the call string, this parameter allows the router to filter one of these out of the X.25 call request. This can be extremely useful in backup scenarios. Consider the following example; the router is configured to do online authorizations via the ISDN D channel and to fall back to B-channel (if the D-channel host did not respond for any reason). Using this parameter in conjunction with the backup equivalent, it is possible to configure the router to use the supplied NUA to connect over D-channel and the supplied NUI to connect over B channel (for backup).

On the backup interface LCN

The LCN parameter is used to set the first LCN that will be used for the backup interface.

On the backup interface LCN Direction

Whether the LCN used for the backup X.25 interface is incremented or decremented from the starting value when multiple X.25 instances share a single layer 2 connection.

On the backup interface NUI/NUA selection

If both an NUI and an NUA are included in the call string, this parameter allows the router to filter one of these out of the X.25 call request.

Enable X.25 Restart Packets

It is normally possible to make X.25 CALLs immediately following the initial SABM-UA exchange. In some cases however, the X.25 network may require an X.25 **Restart** before it will accept X.25 CALLs. The correct mode to select depends upon the particular X.25 service to which you subscribe. The default value is **On**. This means that the router will issue X.25 **Restart** packets. To prevent the router from issuing **Restart** packets, set this parameter to **Off**.

Restart delay

When the **Restarts** parameter is **On**, the **Restart delay** value determines the length of time in milliseconds that the router will wait before issuing a **Restart** packet. The default value is **2000** giving a delay of **2** seconds.

IP Settings

Remote IP address

The destination host that will answer the XOT, TCP, SSL, or UDP call.

Remote IP Address when using the backup interface

The destination host that will answer the XOT, TCP, SSL, or UDP call if a connection via the primary interface has failed and the PAD is configured to backup to a secondary interface that is using an IP based protocol.

IP Stream port

The TCP or UDP port number to use for IP (but not XoT) connections.

IP length header

When set to **On**, and in IP Stream mode, the length of a data sequence is inserted before the data. For the receive direction, it is assumed the length of the data is in the data stream. When set to **8583 Ascii 4 byte**, the IP length header conforms to the ISO 8583 format.

PAD Settings

PAD prompt

Allows you to redefine the standard **PAD>** prompt. To change the prompt, enter a new string of up to **15** characters into the text box.

PAD mode

The PAD Mode parameter can be set to **Normal** or **Prompt Always On**. In Prompt Always On mode, the ASY port attached to the PAD behaves as if it were permanently connected at layer 2, such as it always displays a **PAD>** prompt. AT commands may still be entered but the normal result codes are suppressed. To disable this mode set the parameter to **Normal**.

Use PAD Profile

The PAD profile # allows you to select the PAD profile to use for this PAD instance. There are four pre-defined profiles, numbered **50**, **51**, **90**, and **91**. In addition to the pre-defined profiles, you can also create up to four user-defined profiles numbered **1**, **2**, **3**, and **4**. To assign a particular profile to the PAD select the appropriate number from the list.

Strip Trailing Spaces

If set to **On**, any spaces received at the end of a sequence of data from the network are removed before being relayed to the PAD port.

Enable Leased Line Mode

If set to **On**, causes the PAD to always attempt to be connected using the Auto macro setting as the call command.

Send ENQ on Connect

If set to **On**, the PAD sends an ENQ character on the ASY link when an outgoing call has been answered.

Enable STX / ETX Filtering

If set to **On**, the PAD ignores data that is not encapsulated between ASCII characters **STX** (**Ctrl+B**) and **ETX** (**Ctrl+C**). To disable this feature select the **Off** option.

Delay connect message n x 10 milliseconds

Delay the **Connect** message by the number of milliseconds specified. This is useful when working with equipment that previously connected to slower networks and is upset by the quicker **Connect** when used with modern networks.

Delay data transfer after connection by n x 10 milliseconds

Delays the data delivered from the X.25 or other type of connection to the terminal upon initial connection.

Terminate the PAD call after x seconds if there has been no data transmission

The length of time, in seconds, after which the PAD will terminate an X.25 call if there has been no data transmission.

Disconnect the layer 2 call if there is no layer 3 call in progress for x seconds

The length of time, in seconds, after which the router disconnects a layer 2 link if there are no layer 3 calls in progress. For LAPB sessions, this also terminates the ISDN call.

Create an event when the following data is on the PAD

A string, which if it appears in the received data causes a **Data Trigger** (47) event to be generated and recorded in the event log.

Create an event when there has been no activity on the PAD for x seconds

The time, in seconds, in which if there is no activity on the PAD an event in the event log is posted. This can be used to trigger email exceptions.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
pad	n	l2iface	lapb, lapd, TCP, SSL	Use PAD over interface
pad	n	l2nb	0-255 (instance of LAPB or LAPD)	Use PAD over interface
pad	n	ip_stream	0=off (for XoT), 1=TCP, 2=UDP	Use PAD over interface
pad	n	defpak	16,32,64,128,256,512 or 1024	Default X.25 packet size
pad	n	ansnua	text (valid NUA)	Answer incoming calls from NUA
pad	n	anscug	text (valid CUG)	Only answer calls with CUG
pad	n	amacro	text	Use X.25 Call Macro macroname to an ATD command
pad	n	cingnua	text (valid NUA)	Use NUA
pad	n	lcn	1-4095	LCN
pad	n	lcnup	1=up, 0=down	LCN Direction
pad	n	nuaimode	0=NUI and NUA, 1=NUA only, 2=NUI only	NUI/NUA selection
pad	n	dorest	1=enabled, 0=disabled	Enable X.25 Restart Packets
pad	n	restdel	0 -60000 (ms)	Restart delay
pad	n	IPaddr	text	Remote IP address
pad	n	buipaddr	text	Remote IP Address when using the backup interface
pad	n	ip_port	0-65535	IP Stream port
pad	n	iphdr	0=Off, 1=On, 2=8583 Ascii 4 byte	IP length header
pad	n	prompt	text	PAD prompt

Entity	Instance	Parameter	Values	Equivalent Web Parameter
pad	n	padmode	0=Normal, 1=Prompt Always On	PAD mode
pad	n	profile	1-4, 50, 51,90,91	Use PAD Profile
pad	n	strip_tspaces	1=enabled, 0=disabled	Strip Trailing Spaces
pad	n	llmode	1=enabled, 0=disabled	Enable Leased Line Mode
pad	n	enqcon	1=enabled, 0=disabled	Send ENQ on Connect
pad	n	stxmode	1=enabled, 0=disabled	Enable STX / ETX Filtering
pad	n	delconmsg	0-10	Delay connect message n x 10 milliseconds
pad	n	data_del	0-2147483647	Delay data transfer after connection by n x 10 milliseconds
pad	n	inacttim	0-1000	Terminate the PAD call after x seconds if there has been no data transmission
pad	n	nocalltim	0-60000	Disconnect the layer 2 call if there is no layer 3 call in progress for x seconds
pad	n	trig_str	text	Create an event when the following data is on the PAD
pad	n	inactevent	0-2147483647	Create an event when there has been no activity on the PAD for x seconds

Stopping and starting PADs

PAD instances can be stopped and started using the following CLI commands:

- **stoppads**: Stops all PAD instances from accepting and performing any PAD commands.

- **gopads**: Resumes processing of PAD commands.

The **stoppads** and **gopads** commands can have the PAD number specified in the syntax to stop and start individual PAD instances.

For example:

- To stop PAD 1 from processing PAD commands:

  `stoppads 1`

- To re-enable PAD 1:

  `gopads 1`

X3 parameters

Each PAD configuration page has an attached sub-page that allows you to edit the X.3 PAD parameters. These pages allow you to load one of the standard profiles or edit the individual parameters to suit your application requirements and save the resulting customized user profile to non-volatile memory.

Configuration - Network > Legacy Protocols > X.25 > PADs 0-9 > PAD 0 > X3 Parameters		
▼ X3 Parameters		
Parameter	**Name**	**Value**
1	PAD recall character	1
2	Echo	0
3	Data forwarding characters	0
4	Idle timer delay	5
5	Ancillary device control	0
6	Suppression of PAD service signals	5
7	Action on break (from DTE)	0
8	Discard output	0
9	Padding after CR	0
10	Line folding	0
11	Port speed	15
12	Flow control of PAD (by DTE)	0
13	LF insertion (after CR)	0
14	LF padding	0
15	Editing	0
16	Character delete character	8
17	Line delete character	24
18	Line redisplay character	18
19	Editing PAD service signals	2
20	Echo mask	64
21	Parity treatment	0
22	Page wait	0

Save Profile   1 ▼
Load Profile   1 ▼

Apply

Loading and Saving PAD Profiles

To create your own PAD profiles, edit the appropriate parameters and then select user profile 1, 2, 3 or 4 as required from the list and click the **Save Profile** button. Each PAD profile page includes two list boxes that allow you to load and save PAD profiles. To load a particular profile, select the profile from the list and click the **Load Profile** button. The parameter table is updated with the values from the selected profile.

1 PAD Recall Character

Determines whether PAD recall is enabled. When this facility is enabled, typing the PAD recall character temporarily interrupts the call and returns you to the PAD> prompt where you may enter normal PAD commands as required. To resume the interrupted call, use the **CALL** command without a parameter. The default PAD recall character is **[Ctrl-P]**. This may be changed to any ASCII value in the range 32-125 or disabled by setting it to **0**. When a call is in progress and you need to actually transmit the character that is currently defined as the PAD recall character, simply enter it twice. The first instance returns you to the **PAD>** prompt; the second resumes the call and transmits the character to the remote system.

Option	Description
0	Disabled
1	PAD recall character is CTRL-P (ASCII 16, DEL)
32-126	PAD recall character is user defined as specified

2 Echo

Enables or disables local echo of data transmitted during a call. When echo is enabled, X.3 parameter **20** can be used to inhibit the echo of certain characters.

Option	Description
0	Echo off
1	Echo on

3 Data Forwarding Characters

Defines which characters cause data to be assembled into a packet and forwarded to the network.

Option	Description
0	No data forwarding character
1	Alphanumeric characters (A-Z, a-z, 0-9)
2	CR
4	ESC, BEL, ENQ, ACK
8	DEL, CAN, DC2
16	EXT, EOT
32	HT, LF, VT, FF
64	Characters of decimal value less than 32

Combinations of the above sets of characters are possible by adding the respective values together. For example, to define CR, EXT and EOT as data forwarding characters, set this parameter to **18** (**2** + **16**). If no forwarding characters are defined the Idle timer delay (parameter **4**) should be set to a suitable value, typically **0.2 seconds**.

4 Idle Timer Delay

Defines a time-out period after which data received from the DTE is assembled into a packet and forwarded to the network. If the forwarding time-out is disabled, one or more characters should be selected as data forwarding characters using parameter **3**.

Option	Description
0	No data forwarding time-out
1	Data forwarding time-out in 20ths of a second.

5 Ancillary Device Control

Determines method of flow control used by the PAD to temporarily halt and restart the flow of data from the DTE during a call.

Option	Description
0	No flow control
1	XON/XOFF flow control
3	RTS/CTS flow control (not a standard X.3 parameter)

6 Suppression of PAD Service Signals

Determines whether or not the **PAD>** prompt and/or **Service**/**Command** signals are issued to the DTE.

Option	Description
0	PAD prompt and signals disabled
1	PAD prompt disabled, signals enabled
4	PAD prompt enabled, signals disabled
5	PAD prompt enabled, signals disabled

7 Action on Break (from DTE)

Determines the action taken by the PAD on receipt of a break signal from the DTE.

Option	Description
0	No action
1	Send an X.25 interrupt packet
2	Send an X.25 reset packet to the remote system
4	Send an X.29 indication of break
8	Escape to PAD command state
16	Set PAD parameter 8 to 1 to discard output

Multiple actions on receipt of break are possible, by setting this parameter to the sum of the appropriate values for each action required. For example, when parameter **7** is set to **21** (**16** + **4** + **1**), an X.25 interrupt packet is sent followed by an X.29 indication of break, and then parameter **8** is set to **1**. Do not set this parameter to **16**; doing so would mean the remote system would receive no indication that a break had been issued and output to the DTE would therefore remain permanently discarded. If you need to use the discard output option, use it with the X.29 break option. so that on receipt of the X.29 break, the remote system can re-enable output to your DTE using parameter **8**.

8 Discard Output

Determines whether data received during a call is passed to the DTE or discarded. It can only be directly set by the remote system and may be used in a variety of circumstances when the remote DTE is not able to handle a continuous flow of data at high speed.

Option	Description
0	Normal data delivery to DTE
1	Output to DTE discarded

9 Padding after CR

Slower terminal devices, such as printers, may require a delay after each Carriage Return before they can continue to process data. This parameter controls the number of pad characters (**NUL-ASCII 0**) that are sent after each CR to create such a delay.

Option	Description
0	No padding characters after CR
1-255	Number of padding characters (NUL) sent after CR

10 Line Folding

Controls the automatic generation of a **[CR],[LF]** sequence after a certain line width has been reached.

Option	Description
0	No line folding
1-255	Width of line before the PAD generates [CR],[LF]

11 Port Speed

This is a read only parameter, set automatically by the PAD and accessed by the remote system.

Option	Description
15	19,200 bps
14	9,600 bps
12	2,400 bps
3	2,400 bps

12 Flow Control of PAD (by DTE)

Determines the flow control setting of the PAD by the DTE in the on-line data state.

Option	Description
0	No flow control
1	XON/XOFF flow control
3	RTS/CTS flow control (not a standard X.3 parameter)

13 LF Insertion (after CR)

Controls the automatic generation of a Line Feed by the PAD.

Option	Description
0	No line feed insertion
1	Line Feeds inserted in data passed TO the DTE
2	Line Feeds inserted in data received FROM the DTE
4	Line Feeds inserted after CRs echoed to DTE

The line feed values can be added together to select Line Feed insertion to any desired combination.

14 LF Padding

Some terminal devices, such as printers, require a delay after each Line Feed before they can continue to process data. This parameter controls the number of padding characters (**NUL-ASCII 0**) that are sent after each **[LF]** to create such a delay.

Option	Description
0	No line feed padding.
1-255	Number of NUL characters inserted after LF

15 Editing

Enables (**1**) or disables (**0**) local editing of data input fields by the PAD before data is sent. The three basic editing functions provided are character delete, line delete and line re-display.

The editing characters are defined by parameters **16**, **17**, and **18**. In addition, parameter **19** determines which messages are issued to the DTE during editing. When editing is enabled, the idle timer delay (parameter **4**) is disabled, and parameter 3 must be used to select the desired data forwarding condition.

16 Character Delete Character

The edit mode delete character (ASCII 0-127). The default is backspace (**ASCII 08**).

17 Line Delete Character

The edit mode line buffer delete character (**ASCII 0-127**). The default is **CTRL-X** (**ASCII 24**).

18 Line Redisplay Character

The character that re-displays the current input field when in editing mode (**ASCII 0-127**). The default is **CTRL-R** (**ASCII 18**).

19 Editing PAD Service Signals

The type of service signal sent to the DTE when editing input fields.

Option	Description
0	No editing PAD service signals.
1	PAD editing service signals for printers.
2	PAD editing service signals for terminals.

20 Echo Mask

Defines characters that are not echoed when echo mode has been enabled using parameter 2.

Option	Description
0	No echo mask (all characters are echoed)
1	CR
2	LF
4	VT, HT or FF
8	BEL, BS
16	ESC,ENQ
32	ACK,NAK,STX,SOH,EOT,ETB,ETX
64	No echo of characters set by parameters 16, 17 & 18
128	No echo of characters set by parameters 16, 17 & 18

Combinations of the above sets of characters are possible by adding the respective values together.

21 Parity Treatment

Determines whether parity generation/checking is used.

Option	Description
0	No parity generation or checking
1	Parity checking on
2	Parity generation on
3	Parity checking and generation on

22 Page Wait

Determines how many line feeds are sent to the terminal before output is halted on a page wait condition. In other words, it defines the page length for paged mode output. A page wait condition is cleared when the PAD receives a character from the terminal

Option	Description
0	Page wait feature disabled
1	Number of line feeds sent before halting output

Related CLI commands

The X.3 PAD parameters can be edited from the command line using the **set** command, described in .

Configure X.25 PVCs parameters

A Permanent Virtual Circuit (PVC) provides the X.25 equivalent of a leased line service. With a PVC there is no call setup or disconnect process; you can just start sending and receiving X.25 data on a specified LCN. For each X.25 service connection you may setup up multiple PVCs each of which uses a different LCN (or a mixture of PVCs and SVCs). Digi routers support up to four PVCs numbered 0-3.

Enable this PVC

Enables or disables the PVC.

LCN

The LCN value to be used for this PVC. For an XOT PVC, this parameter defines the **Responder LCN** field in the PVC setup packet, though an LCN of 1 is always used in the XOT PVC connection. For an XOT PVC, this field should contain the remote connection's LCN.

PVC Mode

The lower layer interface use for the PVC. This setting can be set to **LAPB**, **LAPD** or **TCP**, for XOT mode.

Connect this PVC to PAD x

What type of upper layer interface is connected to this PVC and can be set to **PAD** for an X.25 PAD, **TPAD** for a TPAD instance, or **XSW** for X.25 switching. If set to **XSW** for the X.25 switch, the X.25 switch must also be configured regarding the interfaces to switch this PVC to/from. For example, if this is an incoming XOT PVC we are configuring, the Switch from XOT PVC parameter must be set to the desired destination interface.

Use packet size

The packet size for the PVC. Select the appropriate value from the drop down list.

Use window size

The layer 3 window size for the PVC. Select the appropriate value from the drop down list.

Remote IP address

The IP address for outgoing XOT calls.

Use the source IP address from interface x,y

Which Ethernet or PPP interface to use for the source IP address.

Initiator interface

The name of the interface from which the PVC was initiated, such as **Serial 1**. The initiator and responder strings identify the circuit when PVCs are being set up. They must match the names in the remote router that terminates the XOT PVC connection. If the unit terminating the PVC XOT connection is not another Digi router, you must refer to the documentation or the configuration files of the other unit to determine the names of the interfaces.

Responder interface

The name of the interface to which a PVC initiator is connected, such as **Serial 2**.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
pvc	n	l2iface	Blank or lapb, lapd, tcp	Enable this PVC
pvc	n	lcn	0-4096	LCN
pvc	n	uliface	pad, tpad, xsw	Connect this PVC to PAD x
pvc	n	psize	0=default 4=16 5=32 6=64 7=128 8=256 9=512 10=1024	Use packet size
pvc	n	window	1-7	Use window size
pvc	n	ipaddr	IP address	Remote IP address
pvc	n	srcipent	auto, eth, ppp	Use the source IP address from interface x,y
pvc	n	srcipadd	0-255	Use the source IP address from interface x,y
pvc	n	iniface	text	Initiator interface
pvc	n	respiface	text	Responder interface

About X.25 packet switching

X.25 is a data communications protocol used throughout the world for wide area networking across Packet Switched Data Networks (PSDNs). The X.25 standard defines the way in which terminal equipment establishes, maintains and clears Switched Virtual Circuits (SVCs), across X.25 networks to other devices operating in packet mode on these networks.

The protocols used in X.25 operate at the lower three layers of the ISO model.

- At the lowest level the Physical layer defines the electrical and physical interfaces between the DTE and DCE.
- Layer 2 is the Data Link Layer that defines the unit of data transfer as a "frame" and includes the error control and flow control mechanisms.
- Layer 3 is the Network layer. This defines the data and control packet structure and the procedures used to access services that are available on PSDNs.

Another standard, X.31, defines the procedures used to access X.25 networks via the ISDN B and D-channels.

Digi ISDN products include support for allowing connected terminals to access X.25 over ISDN B channels, the ISDN D-channel or over TCP. They can also be configured so if there is a network failure, the router automatically switches to using an alternative service. The Packet Assembler/ Disassembler (PAD) interface conforms to the X.3, X.28, and X.29 standards.

Up to 6 PAD instances, from an available pool of 8, can be created and dynamically assigned to the asynchronous serial ports or the REM pseudo-port.

Each application that uses the router to access an X.25 network has its own particular configuration requirements. For example, you may need to program your Network User Address (NUA) and specify which Logical Channel Numbers (LCNs) should be used on your X.25 service. This information will be available from your X.25 service provider. You also need to decide whether your application uses B or D-channel X.25.

Once you have this information, use the PAD configuration pages to set up the appropriate parameters.

B-channel X.25

The router can transfer data to/from X.25 networks over either of the ISDN B-channels.

Once the router has been configured appropriately, the ISDN call to the X.25 network can be made using an **ATD** command or by executing a pre-defined macro. The format of the **ATD** command allows you to combine the ISDN call and the subsequent X.25 call in a single command. Alternatively, the X.25 call may be made separately from the **PAD>** prompt once the ISDN connection to the X.25 network has been established.

D-channel X.25

The router can transfer data to/from X.25 networks over the ISDN D-channel if your ISDN service provider supports this facility. The speed at which data can be transferred varies depending on the service provider, but is generally **9600bps** or less.

X.28 commands

Once an X.25 session layer has been established the router switches to **PAD** mode. In this mode, operation of the PAD is controlled using the standard X.28 PAD commands listed in the following table:

Command	Description
CALL	Make an X.25 call
CLR	Clear an X.25 call
ICLR	Invitation to CLR
INPAR?	List X.3 parameters of specified PAD instance
INPROF	Load or save specified PAD profile
INSET	Set X.3 parameters of specified PAD instance
INT	Send Interrupt packet
LOG	Logoff and disconnect
PAR?	List local X.3 parameters
PROF	Load or save PAD profile
RESET	Send reset packet
RPAR?	List remote X.3 parameters
RSET	Set remote X.3 parameters
SET	Set local X.3 parameters
STAT	Display channel status

CALL command: Make an X.25 call

The full structure of a **CALL** command is:

```
CALL [<facilities->]<address>[D<user data>]
```

where:

- **<facilities->** is an optional list of codes indicating the facilities to be requested in the call (separated by commas, terminated with a dash)
- **<address>** is the destination network address.
- **<user data>** is any optional user data to be included with the call.

The facility codes supported are:

- **F**: Fast select-no restriction
- **Q**: Fast select-restricted response
- **Gnn**: Closed User Group
- **Gnnnn**: Extended Closed User Group
- **R**: Reverse charging
- **N<NUI>:** Network User Identity code (NUI)

Example

The following command places a call to address **56512120** using reverse charging and specifying **Closed User Group 12**. The string **MYNUI** is your Network User Identity. The string **Hello** appears in the user data field of the call packet.

```
CALL R,G12,NMYNUI-56512120DHello
```

Note The particular facilities available vary among X.25 service providers.

If a **CALL** command is issued without the address parameter, it is assumed you wish to go back on-line to a previously established call, having used the PAD recall facility to temporarily return to the **PAD>** prompt.

Fast select (ISDN B-channel only)

When the standard Fast select facility is requested using the **F** facility code, the call packet generated by the **CALL** command is extended to allow the inclusion of up to 124 bytes of user data. For example:

```
CALL F-1234567890DThis DATA sent with call packet
```

causes an X.25 **CALL** packet to be sent using the Fast select facility including the message **This DATA sent with call packet**. The Carriage Return used to enter the command is not transmitted. If the Fast select facility code is not included, only the first 12 characters are sent.

When a Fast select **CALL** has been made, the PAD accepts an extended format response from the called address. This response, consisting of up to 124 bytes of user data, can be appended to the returning call accepted or call clear packet. When one of these packets is received, the user data is extracted and passed from the PAD to the terminal immediately prior to the **CLR DTE . . .** message in the case of a call clear packet or **CON COM** message in case of a call accepted packet.

When a restricted response Fast select call has been made using the Q facility code, the call packet indicates that a full connection is not required, so that any response to the user data in the **CALL** packet should be returned in a call clear packet.

When the PAD receives an incoming call specifying Fast select, the call is indicated to the terminal in the normal way. For example:

```
IC 1234567890 FAC: Q,W:2 COM
```

indicates that an incoming call had been received requesting Restricted response fast select and a window size of **2**. The user (or system) then has 15 seconds in which to pass up to 124 bytes of data to the PAD to be included in the clear indication packet that is sent in response to the call.

The PAD does not differentiate between standard and restricted response Fast select on incoming calls and, consequently, will always respond with a clear indication.

Network User Identity (NUI)

The N facility code allows you to include your Network User Identity in the call packet. For security reasons, the PAD echoes each character as an asterisk (*****) during the entry of an NUI. Some X.25 services use the NUI field to pass both a username and password for validation. For example, if your username is **MACDONALD** and your password is **ASDF**, a typical CALL command would have the format:

```
CALL NMACDONA;ASDF-56512120
```

where the **;** is used to separate the username from the password.

Closed User Group (CUG)

Most X.25 networks support Closed User Groups. Closed User Groups are used to restrict subscribers to only making calls or receiving calls from other members of the same CUG. The CUG number effectively provides a form of sub-addressing that is used in conjunction with the NUA to identify the destination address for a call. When the G facility code is specified in a CALL packet, it must be followed by the CUG number. This can be a 2- or 4-digit number. If you are a member of a closed user group, the network may restrict you to only making calls to or receiving calls from other members of the same group.

Reverse charging

Reverse charging, specified using the R facility code, allows outgoing calls to be charged to the account of destination address. Whether or not a call is accepted on a reverse charging basis is determined by the service provider and by the type of account held by the called user.

Calling user data

The calling user data field for a normal call can contain up to 12 bytes of user data. If the first character is an exclamation mark (!), the PAD omits the 4-byte protocol identifier, and allows the full 16 bytes as user data. The same is true for a fast select call, except the maximum amount of user data is increased from 124 to 128 bytes. When entering user data, the tilde character (~) can be used to toggle between ASCII and binary mode. In ASCII mode, data is accepted as typed, but in binary mode, each byte must be entered as the required decimal ASCII code separated by commas. For example, to enter the data **Line1** followed by **[CR][LF]** and **Line2**, you would enter:

`DLine1~13,10~Line2`

CLR command: Abort a CALL command

To abort an X.25 CALL, use the X.28 CLR command, do one of the following:

- Press **[Enter]**.
- Drop DTR from the terminal while the call is in progress. Dropping DTR will also terminate an established call.

If a call is terminated by the network or by the remote host, the router returns a diagnostic message before the **NO CARRIER** result code. Messages can be numeric or verbose, depending on the setting of the **ATV** command.

The following table lists the verbose messages and equivalent numeric codes:

Code	Verbose message
1	Unallocated (unassigned) number
2	No route to specified transit network
3	No route to destination
4	Channel unacceptable
6	Channel unacceptable
7	Call awarded and being delivered in an established channel
16	Normal call clearing
17	User busy
18	No user responding
19	No answer from user (user alerted)
21	Call rejected
22	Number changed
26	Non-selected user clearing
27	Destination out of order
28	Invalid number format
29	Facility rejected
30	Response to **STATUS ENQUIRY**
31	Normal, unspecified
34	No circuit/channel available
38	Network out of order
41	Temporary failure
42	Switching equipment congestion

Code	Verbose message
43	Access information discarded
44	Requested circuit/channel not available
47	Resources unavailable, unspecified
49	Quality of service unavailable
50	Requested facility not subscribed
57	Bearer capability not authorized
58	Bearer capability not presently available
63	Service or option not available, unspecified
65	Bearer capability not implemented
66	Channel type not implemented
69	Requested facility not implemented
70	Only restricted digital information bearer
79	Service or option not implemented, unspecified
81	Invalid call reference value
82	Identified channel does not exist
83	A suspended call exists, but this call identity does not
84	Call identity in use
85	No call suspended
86	Call having the requested call identity has been cleared
88	Incompatible destination
90	Destination address missing or incomplete
91	Invalid transit network selection
95	Invalid message, unspecified
96	Mandatory information element is missing
97	Message type non-existent or not implemented
98	Message not compatible with call state or message type nonexistent or not implemented
99	Information element non-existent or not implemented
100	Invalid information element contents
101	Message not compatible with call state

Code	Verbose message
102	Recovery on timer expired
111	Protocol error, unspecified
127	Interworking, unspecified
128	General level 2 call control failure (probable network failure)

Note Some verbose messages may be abbreviated by the router.

CLR command: Clear an X.25 Call

The **CLR** command clears the current call and release the associated virtual channel for further calls. On completion of call clear, the **PAD>** prompt is re-displayed. A call can also be cleared as a result of a number of other situations. If one of these situations occurs, a message is issued to the PAD in the following format:

```
CLR <Reason> C:<n> - <text>
```

where:

- **<Reason>** is a 2/3 character clear down code
- **<n>** is the numeric equivalent of the clear down code
- **<text>** is a description of the reason for clear down

The clear down reason codes supported by the router are listed in the following table:

Reason Code	Numeric Code	Text
DTE	0	by remote device
OOC	1	number busy
INV	3	invalid facility requested
NC	5	temporary network problem
DER	9	number out of order
NA	11	access to this number is barred
NP	13	number not assigned
RPE	17	remote procedure error
ERR	19	local procedure error
ROO	21	cannot be routed as requested
RNA	25	reverse charging not allowed
ID	33	incompatible destination
FNA	41	fast select not allowed
SA	57	ship cannot be contacted

If an unknown reason code is received, the text field is blank.

ICLR command: Invitation To CLR

The **ICLR** command invites the remote X.25 service to CLR the current X.25 session.

INT command: Send interrupt packet

INT causes PAD to transmit an interrupt packet. These packets flow outside normal buffering/ flow control constraints and are used to interrupt the current activity.

LOG command: logoff and disconnect

LOG terminates an X.25 session. It causes the PAD to clear any active X.25 calls, disconnect, and return to AT command mode.

PAR? command: List Local X.3 parameters

PAR? lists the local X.3 parameters for the current session.

PROF command: Load/Save PAD profile

The **PROF** command stores or retrieves a pre-defined set of X.3 PAD parameters, called a PAD profile. The information is stored in system file called **X3PROF**. There are 4 pre-defined profiles, numbered **50**, **51**, **90**, and **91**. Additionally, you can create 4 user PAD profiles, numbered 1 to 4. Profile **50** is automatically loaded when a PAD is first activated. To load one of the other pre-defined profiles, use the **PROF** command, followed by the required profile number. For example:

PROF 90

To create a user PAD profile, use the **SET** command to configure the various PAD parameters to suit your application, then use the **PROF** command in the format:

PROF &nn

where **nn** is the number of the User PAD profile to be stored, such as **03**. Alternatively, you can use the web interface to edit the parameters directly (**Configuration > Network > Legacy Protocols > X.25 > PADs n-n > PAD n > PAD Settings**). The pre-defined profiles (**50**, **51**, **90**, **91**), cannot be overwritten and are permanently configured as shown in the following table:

Parameter	Profile			
	50	51	90	91
1	1	0	1	0
2	0	0	1	0
3	0	0	126	0
4	5	5	0	20
5	0	3	1	0
6	5	5	1	0
7	0	8	2	2
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	15	15	15	15
12	0	3	1	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
16	8	8	127	127
17	24	24	24	24
18	18	18	18	18

19	2	2	1	1
20	64	64	0	0
21	0	0	0	0
22	0	0	0	0

Stored X.25 PAD profiles are held in non-volatile memory, and are not lost when the router is switched off.

When used in the format:

`prof nn`

the **PROF** command loads the stored profile specified by **nn**.

RESET command: Send reset packet

RESET issues a reset for the current call to the network. It does not clear the call, but it does return the network level interface to a known state by re-initializing all Level 3 network control variables. All data in transit is lost.

RPAR? command: Read remote X.3 parameters

RPAR? lists the current X.3 parameter settings for the remote system.

RSET command: Set remote X.3 parameters

RSET sets one or more X.3 parameters for the remote system. It is entered in the format:

`RSET par #:value[,par #:value[,par #:value ...]]`

SET command: Set local X.3 parameters

SET sets one or more of the local X.3 parameters for the duration of the current session. The format of the command is:

`SET par #:value[,par #:value[,par #:value ...]]`

STAT Display Channel Status

STAT displays the current status for each logical channel indicating whether it is free or engaged. For example:

```
stat
PAD  STATE
1    ENGAGED
2    FREE
3    FREE
4    FREE
```

Configure MODBUS Gateway parameters

Digi TransPort routers support conversion from MODBUS serial to MODBUS TCP.

Requirements for MODBUS support in TransPort devices

When converting from MODBUS serial to MODBUS TCP over a WAN link, it is necessary to have intelligence in the router to minimize the effect of the higher latency.

Digi TransPort supports being a MODBUS server only. Clients, such as remote PCs, can send overlapping requests. The router will create a queue of info requests and deal with them appropriately, sending them out over the serial port and relaying the responses back. Overlapping polls from multiple clients are supported.

Modbus Gateway configuration parameters

Modbus Gateway parameters are configured on the **Configuration > Network > Legacy Protocols > MODBUS Gateway** page.

Enable MODBUS Gateway

Enables or disables MODBUS gateway instance.

Async Port

The local serial port number (asynchronous port) for the MODBUS serial interface.

Async Mode

The serial driver for RS232 or RS485 on supported hardware.

Duplex Mode

The duplex mode, which can be **half** or **full**. Use **full** for 4-wire installations; otherwise **half** is required.

Operation mode

The operation mode to master or slave.

Idle Gap

When receiving an modbus response from a station when this idle gap (pause with no reception of characters) is detected the message (currently received from the station) is at that staged forwarded on as the complete response.

Fix slave address

The address of the slave is fixed at this value. An address conversion will occur if a message that does not contain this address is received from the TCP master. If not used, the TCP master must use the correct slave address.

Adjust slave address

The address of the slave is adjusted by this value. If left at **0**, the slave address is not adjusted at all.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
modbus	n	enabled	1=enabled, 0=disabled	Enable MODBUS Gateway
modbus	n	asy_add	0-255	Async Port
modbus	n	op_mode	Master/Slave	Operation mode
modbus	n	async_mode	RS322 or RS422	Async Mode
modbus	n	duplex	0=full, 1=half	Duplex Mode
modbus	n	idle_gap	0-2147483647	Idle Gap
modbus	n	fix_slave_address	0-255	Fix slave address
modbus	n	adj_slave_address	0-255	Adjust slave address
modbus	n	ipport0	0-65535	IP Port (row 1)
modbus	n	nbsocks0	0 -"currently available"	Number of sockets (row 1)
modbus	n	ipmode0	0=TCP, 1=UDP	IP Mode (row 1)
modbus	n	rawmode0	1=enabled, 0=disabled	Raw Mode (row 1)
modbus	n	Ipport1	0-65535	IP Port (row 2)
modbus	n	nbsocks1	0 -"currently available"	Number of sockets (row 2)
modbus	n	ipmode1	0=TCP, 1=UDP	IP Mode (row 2)
modbus	n	rawmode1	1=enabled, 0=disabled	Raw Mode (row 2)
modbus	n	bcasts_on	OFF, ON	Broadcast support.

MODBUS Slaves parameters

This page defines access for the following MODBUS slaves when operating as **act-as-slave**. Up to **32** slave definitions may be defined.

Slave addresses/unit ids

The address of the slave unit.

Remote Host

The IP address of the remote host, such as the slave unit.

IP Port

The IP port number. The default port is **502**.

IP Mode

Select the IP mode using this drop down list. The default mode is **TCP**.

Add

Click on the add button to add the slave.

Configure Protocol Switch software

The Protocol Switch software is available on some of the Digi TransPort models.

About the Protocol Switch software

The Protocol Switch provides X.25 call switching between the various protocols and interfaces that may be available including:

Interface / Protocol	Description
Off/None	Data is note switched from or backed-up to this protocol.
LAPD	Data is switched from or backed-up to LAPD using the X.25 service.
LAPD X	As above, but the actual LAPD instance used is determined by the NUA.
LAPB 0	Data is switched from or backed-up to LAPB 0.
LAPB 1	Data is switched from or backed-up to LAPB 1.
LAPB 2	Data is switched from or backed-up to LAPB 2.
LAPB 0 PVC	Data is switched from or backed-up to an X.25 PVC on LAPB 0.
LAPB 1 PVC	Data is switched from or backed-up to an X.25 PVC on LAPB 1.
LAPB 2 PVC	Data is switched from or backed-up to an X.25 PVC on LAPB 2.
XoT	Data is switched from or backed-up to an XOT (X.25 over TCP/IP) connection.
XoT PVC	Data is switched from or backed-up to an XOT PVC connection.
TCP stream	Data is switched from / backed-up to a TCP socket. The socket's IP address will be determined from the IP stream port setting.
UDP stream	This is similar to the TCP stream setting, but instead of switching onto a TCP socket, data is switched onto a UDP socket. In the case of switching from X.25. the effect is that a UDP frame will be sent for each packet of X.25 data being switched.
VXN	Data is switched or backed-up to Datawire's VXN protocol.
SSL	Datais switched or backed-up to SSL.
DialServ	Data is switched or backed-up to an analog modem via the built-in DiaslServ daughter card.

When this optional feature is included, the device can be configured to pass X.25 calls or data received in a TCP connection to another protocol or interface.

In addition, it is possible to specify a backup protocol or interface so if an outgoing call on one interface fails, the backup interface is automatically tried. LAPB can be used to switch to either ISDN or X.25 over serial, depending on the configuration of the LAPB instance chosen.

Protocol Switch software logic

The logic used in the switching software is outlined in the flowchart below. The following notes provide a more in-depth explanation of the actions taken in each of the numbered boxes.
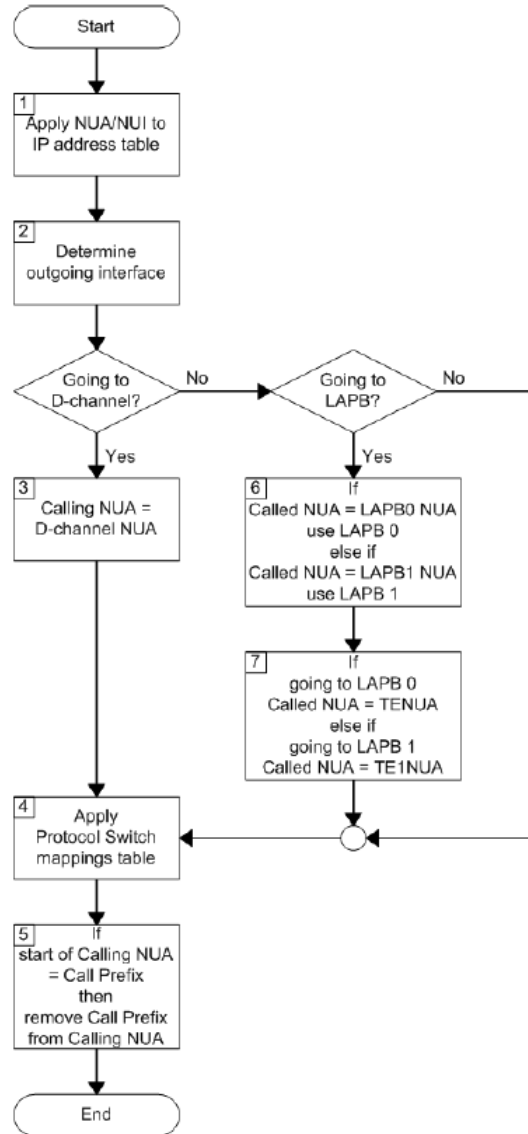
- The router first looks up the Called NUA/NUI in the **Configuration > Network > Protocol Switch > NUA to Interface Mappings** mapping table to determine the IP address to use in the event that the call ends up being switched to a TCP or XOT interface. If a match is found on the Called NUA/NUI the router assigns the matching IP address from the table to the call. If IP address mapping table does not contain an entry for the Called NUA/NUI and the call is eventually switched to a TCP or XOT channel then the default IP address (**IP Stream** or **XOT Remote IP Address**) is used.

- The router then determines from the source interface of the incoming call which interface type it should be switched to, from the **Switch from** parameters on the **Protocol Switch** page.

  - For example, if the call arrived via a LAPB 0 interface and the Switch from LAPB 0 to parameter was set to LAPD, then the outgoing interface would LAPD.

  - If the outgoing interface is LAPD the router changes the Calling NUA field of the incoming call to the D-Channel NUA value (as defined on the **Protocol Switch** page). If the outgoing interface is NOT LAPD processing proceeds as at step 6.

- The router then searches the **Configuration > Network > Protocol Switch > NUA Mappings** table to see if there are any matches for the **Called** or **Calling NUA** values on the specified interface. When the **Interface Description** is **Off**/**None** data is not switched from or backed-up from this protocol is a match, the **NUA In** value is substituted by the **NUA Out** value, as the mapping is applied individually to both the **Calling NUA** and **Called NUA** for the packet.

- The router checks the leading characters of the **Calling NUA** to see if there is a match with the **Call Prefix** parameter. If there is a match, the prefix digits are removed before the outgoing X.25 call is made. Otherwise, the call is made anyway, and the switching process is complete for this call.

- If after step 3, the router has determined that the outgoing interface is not LAPD, it checks if the outgoing interface is LAPB. If it is, it checks to see if the **Called NUA** field in the call packet matches the **LAPB 0** NUA parameter. If it does, it selects **LAPB 0** as the outgoing interface. If the **Called NUA** field does not match **LAPB 0** NUA, it checks for a match with **LAPB 1** NUA. If there is a match, it sets the outgoing interface to **LAPB 1**.

- If the **Called NUA** field in the calling packet matches neither the **LAPB 0** NUA or **LAPB 1** NUA parameters, the outgoing interface is set to the interface specified by the relevant **Switch from** parameter.

- If the call is being switched over **LAPB 0**. the router sets the **Called NUA** to the **TE NUA** (**LAPB 0**) value. If the call is being switched over **LAPB 1**, the router sets the **Called NUA** to the **TE NUA** (**LAPB 1**) value.

Digi TransPort Protocol Switch parameters

The **Configuration > Network > Protocol Switch** menu has the following sub-menu options:

- **CUD Mappings**
- **IP Sockets to Protocol Switch**
- **NUA to Interface Mappings**
- **NUA Mappings**

TCP or XoT

Controls the switching of incoming X.25 calls received via TCP or XOT. Select the interface to which data should be switched from the drop down list, or select **Off** and the protocol switch will not respond to any incoming XOT or TCP connections.

LAPD

Controls the switching of incoming X.25 calls received via ISDN LAPD. Select the interface to which data should be switched from the drop down list, or select **Off** and the protocol switch will not respond to any incoming LAPD calls.

LAPB X

Controls the switching of incoming X.25 calls received via LAPB X. Select the interface to which data should be switched from the drop down list, or select **Off** and the protocol switch will not respond to any incoming LAPB X calls.

LAPB X PVC

Controls the switching of incoming X.25 calls received via LAPB X PVC. Select the interface to which data should be switched from the drop down list, or select **Off** and the protocol switch will not respond to any incoming PVC calls on LAPB X.

XOT PVC

Controls the switching of incoming X.25 calls received via an XOT PVC. Select the interface to which data should be switched from the drop down list, or select **Off** and the protocol switch will not respond to any incoming XOT PVC calls.

TCP XOT backup to interface

If any of the **Switch from** parameters has been set to **XOT**, and XOT is unavailable, this parameter can be used to specify an alternative interface to switch the X.25 call to. Any of the other interfaces can be selected, or **None**. If **None** is selected, no backup call is attempted.

LAPD backup to interface

If any of the **Switch from** parameters has been set to **LAPD**, and LAPD is unavailable, this parameter can be used to specify an alternative interface to switch the X.25 call to. Any of the other interfaces can be selected, or **None**. If **None** is selected, no backup call is attempted.

LAPB X backup to interface

If any of the **Switch from** parameters has been set to **LAPB X**, and LAPB X is unavailable, this parameter can be used to specify an alternative interface to switch the X.25 call to. Any of the other interfaces can be selected, or **None**. If **None** is selected, no backup call is attempted.

VXN backup to interface

If any of the **Switch from** parameters has been set to VXN, and VXN is unavailable, this parameter can be used to specify an alternative interface to switch the X.25 call to. Any of the other interfaces may be selected, or **None**. If **None** is selected, no backup call is attempted.

LAPD Parameters

Calling Prefix

The call prefix to inserted in front of the NUA in calls being switched to LAPD. For example, if the called NUA in the call being received by the **LAPB 0** interface is **56565**, and the call prefix is **0242**, the call placed on the LAPD interface is to NUA **024256565**. Also, for calls in the reverse direction, if the prefix in the calling NUA matches this parameter, it is removed from the calling NUA field.

D-Channel LCN

The value of the first LCN assigned for outgoing X25 calls on LAPD.D-Channel LCN Direction.

Max VCs: Unlimited

The maximum number of Virtual Circuits (VCs) used on an LAPD interface. When the maximum has been reached, the backup call will take place immediately, or the call will clear if there is no backup call. If this parameter is set to **0**, there is no limit.

Default Packet Size

The default packet size for X.25 calls being switched onto LAPD. The default packet size is **128**, other possible values are **256**, **512**, or **1024** bytes.

Default Window Size

The default window size for calls being switched onto LAPD. The default window size is **2**; the valid range is **1** to **7**.

LAPB Parameters

LCN

The value of the first LCN that will be assigned for outgoing X25 calls on LAPB.

LCN direction: Up Down

Determines whether the LCN used for outgoing X.25 calls on LAPB is incremented or decremented from the starting value.

Max VCs: Unlimited

The maximum number of Virtual Circuits (VCs) used on an LAPB interface. When the maximum has been reached, then the backup call occurs immediately, or the call will clear if there is no backup call. If this parameter is set to **0**, there is no limit.

B-Channel Number

An ISDN number used for calls being switched in the direction of **LAPB 0** or **LAPB 1**.

Enable ENQ Char

When this parameter is set to **On**, when an incoming call on LAPB is switched and the router connects to it, the X.25 switch sends a data packet on the LAPB X.25 SVC containing the **ENQ** character.

LAPB 0 Default Packet Size: 128 256 512 1024

The default packet size for calls being switched onto **LAPB 0.** The default packet size is **128**. Other possible values are **256**, **512**, or **1024** bytes.

LAPB 0 Default Window Size: 2 1 3 4 5 6 7

The default window size for calls being switched onto LAPB 0. The default window size is **2**. The valid range is **1** to **7**.

LAPB 1 Default Packet Size: 128 256 512 1024

The default packet size for calls being switched onto **LAPB 1**. The default packet size is **128**. Other possible values are **256**, **512**, or **1024** bytes.

LAPB 1 Default Window Size: 2 1 3 4 5 6 7

The default window size for calls being switched onto **LAPB 1**. The default window size is **2**. The valid range is **1** to **7**.

LAPB 2 Default Packet Size: 128 256 512 1024

The default packet size for calls being switched onto **LAPB 2**. The default packet size is **128**. Other possible values are **256**, **512**, or **1024** bytes.

LAPB 2 Default Window Size: 2 1 3 4 5 6 7

The default window size for calls being switched onto **LAPB 2**. The default window size is **2**. The valid range is **1** to **7**.

IP Stream / XOT Parameters

IP Stream or XOT Remote IP Address:

For calls being switched in the direction of XOT, this parameter specifies the destination IP address used for the outgoing XOT call. This is also used as the destination IP address in the IP/UDP stream modes.

IP Stream or XOT Backup IP Address

If the **Switch from XOT to** parameter is set to **XOT**, this is the IP address the XOT call will be switched to, if the original XOT IP address is unavailable.

IP Stream Port

The IP port number used when **IP stream** or **UDP stream** are selected as the parameter for any of the **Switch from** or **Backup from** parameters.

Note:

The XOT remote IP address and IP stream port parameters are overridden by the values in the NUA/NUI to IP addresses table if the call matches any entry in that table.

IP Length Header: Off On 8583 Ascii 4 byte On (inclusive)

When IP length header is **On**, a length indicator field is inserted at the start of each packet. When set to **8583 Ascii 4 byte**, the IP length header conforms to the ISO 8583 format.

Source IP address interface: Auto Ethernet PPP

The default value for this parameter is **Auto**, which means that the source IP address of an outgoing XOT connection on an un-NATed W-WAN link is the address of the PPP interface assigned to W-WAN. This is because the XOT connection is initiated (automatically) within the router, and does not originate from the local subnet (LAN segment to which the router is attached via the Ethernet interface). However, this means that if you are routing traffic from the local subnet across a VPN tunnel, you would have to set up two Eroutes: one to match the local subnet address, and one to match the XOT source address, such as the address of the PPP interface associated with to the wireless network. If set to **Ethernet**, the router uses the IP address of the Ethernet port instead of that of the PPP interface, so that you need only set up on Eroute.

X.25 Parameters

Don't switch facilities

If this parameter is set to **Off**, the packet size and window size are only switched if they need to, such as if they specify a value different from what is currently being negotiated. If this parameter is set to **On**, the facilities are not switched.

Don't strip facilities

When set to **On**, this parameter stops the X.25 switch from stripping packet size and window size facilities as it switches an X.25 call. When set to **Off**, the X.25 switch strips facilities if the requested facilities match the defined defaults for that interface.

L2 Deactivation Clear Cause

When one side of a switch call fails because layer 2 drops, the other side is usually cleared with a clear **cause 9, out of order**. This parameter allows you to set this code to any value.

X25 Version: 84 88

Allows you to switch between X.25 version 88, and X.25 version 84, in which clear causes are always **0** when issued if the router is the DTE.

Interpret no facilities on Call Accept as P7W2

When this parameter is set to **On**, the X.25 switch interprets any call accept packets that do not include the window size (**W**) or packet size (**P**) as if the call accept has **P7W2**, such as a packet size of **128 bytes** and a windows size of **2**.

Notes on PAD Answering

Because the other interfaces can operate as normal, even when the switch is operating, take special care with regard to answering NUAs programmed on active PADs. For example, when a call is being received on a LAPD or LAPB interface, a PAD instance or remote configuration session can answer and terminate the call in preference to the call being switched. This means that the PADs **Answering NUA** parameters should be left blank to ensure that the router's PADs are not answering calls that need to be switched. If you do want a PAD instance to answer a call, program the **Answering NUA** field with as many digits as you can to ensure it only answers calls destined for that PAD.

These same precautions apply to the **Allow CLI access from X.25 address** parameter on the **Configuration > System > General** page.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
X25sw	0	swfrlapb0	0,1,3- 10,12-15 (see below)	Switch from LAPB 0 to
X25sw	0	swfrlapb0pvc	0-5,7-10,12-15 (see below)	Switch from LAPB 0 PVC to
X25sw	0	swfrlapb1	0-2,4-10,12-15 (see below)	Switch from LAPB 1 to
X25sw	0	swfrlapb1pvc	0-6,8-10,12-15 (see below)	Switch from LAPB 1 PVC to
X25sw	0	swfrlapb2	0-10,13-15 (see below)	Switch from LAPB 2 to
X25sw	0	swfrlapb2pvc	0-10,12, 14, 15 (see below)	Switch from LAPB 2 PVC to
X25sw	0	swfrlapd	0, 2-10,12-15 (see below)	Switch from LAPD to
X25sw	0	swfrxot	0-3,5-10,12-15 (see below)	Switch from XOT (TCP) to
X25sw	0	swfrxotpvc	0-7,9,10,12-15 (see below)	Switch from XOT PVC to
X25sw	0	callprefix	<NUA>	Calling Prefix
X25sw	0	dlcn	0-65535	D-Channel LCN
X25sw	0	dlcnup	off, on Off=Down On=Up	D-Channel LCN Direction
X25sw	0	dmaxvc	0-65535	Max VCs
X25sw	0	lapb0ppar	7,8,9,10 7=128 8=256 9=512 10=1024	Default Packet Size
X25sw	0	lapb0wpar	1-7	Default Window Size
X25sw	0	blcn	0-65535	LCN
X25sw	0	blcnup	off, on Off=Down On=Up	LCN direction
X25sw	0	bmaxvc	0-65535	Max VCs
X25sw	0	bnumber	ISDN number	B-Channel Number

Entity	Instance	Parameter	Values	Equivalent Web Parameter
X25sw	0	benqcon	off, on	Enable ENQ Char
X25sw	0	lapdppar	7,8,9,10 7=128 8=256 9=512 10=1024	LAPB 0 Default Packet Size
X25sw	0	lapdwpar	1-7	LAPB 0 Default Window Size
X25sw	0	lapb1ppar	7,8,9,10 7=128 8=256 9=512 10=1024	LAPB 1 Default Packet Size
X25sw	0	lapb1wpar	1-7	LAPB 1 Default Window Size
X25sw	0	lapb2ppar	7,8,9,10 7=128 8=256 9=512 10=1024	LAPB 2 Default Packet Size
X25sw	0	lapb2wpar	1-7	LAPB 2 Default Window Size
X25sw	0	ipaddr	IP address	IP Stream or XOT Remote IP Address
X25sw	0	buipaddr	IP address	IP Stream or XOT Backup IP Address
X25sw	0	ip_port	0-65535	IP Stream Port
X25sw	0	iphdr	0,1,2 0=Off 1=On 2=8583 Ascii 4 byte	IP Length Header
X25sw	0	srcipadd	Interface number 0-65535	Source IP address interface
X25sw	0	srcipent	<blank>, PPP, ETH	Source IP address interface
X25sw	0	noswfac	off, on	Don't switch facilities
X25sw	0	nostripfac	off, on	Don't strip facilities
X25sw	0	l2deactcc	0-65535	L2 Deactivation Clear Cause
X25sw	0	x25ver84	off, on Off=88 On=84	X25 Version
X25sw	0	accdefp7w2	off, on	Interpret no facilities on Call Accept as P7W2

Interfaces are coded as follows:

Parameter value	Interface type
0	None
1	LAPD
2	LAPB 0
3	LAPB 1
4	XOT
5	LAPD X (actual instance is determined by NUA)
6	LAPB 0 PVC
7	LAPB 1 PVC
8	XOT PVC
9	TCP stream
10	UDP stream
12	LAPB 2
13	LAPB 2 PVC
14	VXN
15	SSL

CUD Mappings parameters

Protocol Switch CUD mappings allow you to map an incoming call's CUD (call user data) from one value to another. The PID (protocol identifier) portion of the CUD, if present, is maintained from input to output and is not involved in the comparison.

The **Configuration > Network > Protocol Switch > CUD Mappings** web page displays a table with four columns in which you can specify the **CUD In** values, corresponding **CUD Out** values and to which interfaces the mappings should be applied. The **interface** field defines which output interfaces this mapping applies to. Wildcard characters are allowed, and In each case the interface type to which the mapping applies can be selected from **ANY**, **LAPD**, **LAPB0**, **LAPB1**, **LAPB2,** or **XOT**.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
cudmap	0-9	cudfrom	0-65536	CUD In
cudmap	0-9	cudto	0-65536	CUD Out
cudmap	0-9	Interface	0,1,2,3,4,12 0=Any 1=LAPD 2=LAPB 0 3=LAPB 1 4=XOT 12=LAPB 2	Interface

IP Sockets to Protocol Switch

This page contains a table for entering a series of IP Port numbers and **X.25 Call** strings, as shown below. It is used to configure the router so that IP data can be switched to any of the protocols support by the protocol switch, including X.25. For example, data received on a TCP connection can be forwarded over SSL, XoT, or a UDP stream. The only columns that must be filled out are **Port** and **Number of Sockets**.

This table is duplicated in the **Configuration > Network > Legacy Protocols > X.25 > IP to X.25 Call** section, as it can also be used to convert an incoming TCP connection to an X.25 session to be answered by PAD without using the protocol switch. It is included at this point in the web user interface as a convenience, in case the table is being used in conjunction with PAD and not the protocol switch.

IP Port

Used to set up the port numbers for those IP ports that will listen for incoming connections to be switched over X.25 or other protocol. In the case of switching to X.25, when such a connection is made, the router makes an **X.25 Call** to the address specified in the **X.25 Call** field. Once this call has been connected, data from the port is switched over the X.25 session.

Number of Sockets

How many IP sockets should simultaneously listen for data on the specified port. The number of available IP sockets depend on your router model and how many are already in use. See note at the end of these settings descriptions.

X25 Call

The X.25 call field may contain an X.25 NUA or NUI or one of the X.25 Call Macros defined on the **Configuration > Advanced applications > X25 > Macros page**.

PID

The Protocol Identifier (PID) to use when the router switches an IP connection to X.25. The **PID** (protocol ID) field takes the format of four hexadecimal digits separated by commas, such as **1,0,0,0,** at the start of the **Call User Data** field in the X.25 call.

Confirm Mode

When set to **On**, the incoming TCP socket is not successfully connected until the corresponding outgoing call has been connected. The incoming TCP socket triggers the corresponding outgoing call either to a local PAD instance or to whatever is configured. The effect of this mode is that the socket fails if the outbound call fails and so may be useful in backup scenarios. In addition it ensures that no data is sent into a "black hole". When this setting is not enabled, data sent on the inbound TCP connection before the outbound connection has been successful can be lost.

RFC 1086 Mode:

RFC 1086 specifies a mode of operation in which the IP socket answers, and then, with a simple protocol in the socket, identifies the X.25 address and other X.25 call setup parameters to be used. When the X.25 call parameters have been identified, the X.25 call is made. If successful, data is switched between the X.25 call and the IP socket. The protocol selects whether incoming or outgoing support is required.

IP length header

When IP length header is **On**, the IP length indicator field is inserted at the start of each packet. When set to **8583 Ascii 4 byte**, the IP length header conforms to the ISO 8583 format.

In the example above, 3 IP sockets will listen for an incoming connection on IP Port **2004**. Once connected, they each make an X.25 Call to **jollyroger**. The router recognizes that **jollyroger** is a pre-defined macro, as illustrated below, and translates it into an X.25 Call to address **32423** with the string **x25 data** included as data in the call. The outgoing X.25 call(s) are made over whichever interface is specified by the **Switch from XOT(TCP)** to parameter on the **Configuration > Network > Protocol Switch** page.

Note At the top of the page, the total number of sockets available and the number currently free is shown. Take care to not allocate too many of the free sockets, unless you are confident they are not required for other applications.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ipx25	n	ip_port	0-65535	IP Port
ipx25	n	nb_listens	0-software-dependent max	Number of Sockets
ipx25	n	x25call	NUA, NUI or X.25 macro name	X25 Call
ipx25	n	pid	hex numbers	PID
ipx25	n	cnf_mode	1=enabled, 0=disabled	Confirm Mode
ipx25	n	rfc1086_mode	1=enabled, 0=disabled	RFC 1086 Mode
ipx25	n	iphdr	0=Off 1=On 2=8583 Ascii 4 byte	IP length header

NUA to Interface Mappings

This page contains a table to enter a series of X.25 NUA or NUI values along with IP addresses/ Ports to which they should be mapped, if you need to override the default settings in the **Configuration > Network > Legacy Protocols > X.25 > NUA/NUI Interface Mappings** page.

(You can specify up to 256 NUA to Interface mappings)

NUA	IP Address	IP Port	Interface	Backup Interface
No NUA to Interface mappings have been configued.				
			Default	Default	Add

If, in the **Protocol Switch** configuration, you had configured the router to switch from **LABP 0** to **TCP**, the **IP Address** and **Port** values would normally be determined from the **XOT Remote IP address** and **IP stream port** parameters. However, having set up the NUA/NUI to IP addresses table as shown in the example above, if an X.25 call with NUA of value **222** is received on **LAPB 0**, it is switched onto a TCP socket using IP address **1.2.3.4** on port **45** instead of the settings configured on the **Configuration > Network > Legacy Protocols > X.25 > NUA/NUI Interface Mappings** page.

Similarly, NUIs can also be matched. In this example, a call with NUI of value **test** is switched onto a TCP socket using IP address **100.100.100.1** on port **678**.

All three comparison fields, NUA, NUI and Call Data can use the wildcard matching characters **?** and *****. In the example shown above, when an X.25 call is received with either the NUA having **1234** followed by any 2 digits or a call being received with call user data with any 4 characters followed by **aa**, the call is switched to a TCP socket on address **100.100.100.52** on port **4001**.

When a connection has been successfully established and data is being switched from the X.25 call to the socket and from the socket to the X.25 connection, it can be terminated by either the socket closing or the X.25 call clearing.

If the connection terminates because of an incoming X25 **CALL CLEAR** packet, the switch terminates the socket connection. If the connection terminates because the socket is closed, the switch clears the X.25 call by transmitting a **CALL CLEAR** packet.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
nuaip	0-255	nua	0-65536	NUA
nuaip	0-255	ipaddr	IP address	IP Address
nuaip	0-255	ip_port	0-65536	IP Port
nuaip	0-255	swto	0-10, 12-15 (see table below)	Interface
nuaip	0-255	buswto	0-10, 12-15 (see table below)	Backup Interface

Interfaces are coded as follows:

Parameter Value	Interface Type
0	Default
1	LAPD
2	LAPB 0
3	LAPB 1
4	XOT
5	LAPD X (actual instance determined by NUA)
6	LAPB 0 PVC
7	LAPB 1 PVC
8	XOT PVC
9	TCP stream
10	UDP stream
12	LAPB 2
13	LAPB 2 PVC
14	VXN
15	SSL

NUA Mappings parameters

Protocol switch NUA mappings allow you to redirect specified NUAs to alternative NUAs for switched X.25 calls. Up to 20 **NUA In** to **NUA Out** mappings are available. These mappings alter the **called NUA** field in any X.25 call. The comparison uses tail matching, so only the rightmost digits in the NUA are compared with the table entry.

You may specify up to 20 NUA mappings

NUA In	NUA Out	Interface	Called / Calling	
No NUA mappings have been configured.				
		ANY ▼	Both ▼	Add

This page displays a table with four columns in which you can specify the **NUA In** values, corresponding **NUA Out** values, to which interfaces the mappings should be applied, and whether the mapping should apply if the router is making the call, receiving the call, or both.

For example, if the called NUA is **123456789345** and there is an NUA In table entry of **9345**, with **Called/Calling** set to either **Both** or **Called**, this will match, and the entire called NUA will be replaced with the corresponding **NUA Out** entry. In each case, the interface type to which the mapping applies can be selected from **ANY**, **LAPD**, **LAPB0**, **LAPB1**, **LAPB2**, or **XOT**.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
X25map	0-19	nuafrom	0-65536	NUA In
X25map	0-19	nuato	0-65536	NUA Out
X25map	0-19	interface	0,1,2,3,4,12 0=Any 1=LAPD 2=LAPB 0 3=LAPB 1 4=XOT 12=LAPB 2	Interface
X25map	0-19	ca_or_ci	0,1,2 0=Both 1=Called 2=Calling	Called / Calling

Configure alarms

You can configure the Alarm parameters of your router with Digi TransPort Web Interface. This section covers configuring alarms on the **Configuration > Alarms** page. It covers the following topics:

- Event Settings parameters on page 587
- Event Logcodes parameters on page 602
- SMTP Account parameters on page 606

Event Settings parameters

The router maintains a log of events in the **LOGCODES.TXT** pseudo file. When an event of a specified or lower priority level occurs, a syslog message, an email alert, or SMS alert can be sent to a pre-defined address. The **Configuration > Alarms > Event Settings** menu has the following sub-menu items:

- **Email Notifications**
- **SNMP Traps**
- **SMS Messages**
- **Local Logging**
- **Syslog Messages**
- **Syslog Server n**

To configure the **Event Settings**, set the following parameter values:

Only log events with a log priority of at least **n**

Enables a filter that ensures that only events having a specified severity or lower level are logged.

Do not log the following events

A numerical list of comma-separated values specifying events to be excluded from the log. These numerical values can be found in the eventlog.txt file on the router.

After power up, wait **s** seconds before sending Emails, SNMP traps, SMS or Syslog messages

The delay, in seconds, after power-up that the router should wait before sending any alert messages. This is useful when the sending of those items would fail if sent too soon after the router powers up because the underlying interface that would be used has not completed initialization.

Include event number in the event log and Email, SNMP traps or Syslog messages

If enabled, event numbers from the **logcodes.txt** file are included.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
event	n	loglevel	0-9 0 none 1 low 9 high	Only log events with a log priority of at least **n**
event	n	ev_filter	Comma-separated list of event numbers	Do not log the following events.
event	n	action_dly	Number of seconds (such as 60)	After power up, wait **s** seconds before sending Email, SNMP traps, SMS or Syslog messages.
event	n	incevnums	0,1	Include event number.

Email Notification parameters

About using email templates

One of the key features provided by the event log function is the ability to configure the router to automatically generate and send an email alert message each time an event of up to a specified priority occurs. The format of the message is determined by the email template specified in the **Use email template file** parameter, normally **EVENT.EML**, in the **Configuration > Alarms > Event Settings > Email Notifications** web page.

If the standard **EVENT.EML** template supplied with the router is not suitable, you can create your own template. An email template is a text file that defines the appearance and content of the email messages generated by the event logger.

Email template structure

An email template consists of a header section followed by a body section. One or more blank lines separate the two sections.

Header section

The header section MUST contain the following three fields:

TO

Used to specify at least one recipient's email address. Multiple addresses may be included and must be separated by a space, comma or semicolon character. For example:

```
To: 123@456.com, 456@123.com; abc.def.com
```

FROM

The email address of the sending unit. Alternatively, you can enter a simple string. This may depend on the SMTP server as to what is accepted. For example:

```
FROM: WR44
```
Or
```
FROM: wr44@mycompany.com
```

SUBJECT

A string describing the subject of the email message. For example:

```
Subject: Automated message from router
```

Other fields

In addition to the required fields described above, the header section of an email can also contain one or more optional fields. Many such fields are defined in the relevant RFCs, but there are some fields the router handles a little differently ,as described below. The router inserts other fields as necessary if it is required to send attachments with the email.

Reply To

If the router discovers this field is not present in the email template, it inserts this field into the header. The string used for this field is the one configured by the **smtp 0 reply_to** CLI command (or the use **Reply To** address parameter in the **Configuration > Alarms > SMTP Account** web page). This allows for different reply addresses, and a simple way of using the same (easily configurable) reply address for all emails.

Date

If this field is present in the header, the router inserts the current date and time into the header. The date and time are values local to the router and do not contain any time zone information.

Body section

The body section can include any text. This text is parsed for any function calls that may be present. Function calls must be enclosed between **<%** and **%>**. These sequences are substituted by text resulting from the function call. The following functions may be used:

Function	Description
TimeSmtp();	Inserts the router's date and time.
serial_number();	Inserts the router's serial number
Smtpip();	Inserts the IP address of the router as seen by the SMTP server during transmission
email_event()	Inserts a formatted description of the event that caused the email transmission.
Smtpid()	Inserts the router ID for this device as configured by the **Router Identity** field in the **Configuration > System > Device Identity** web page, or the **cmd 0 unitid** CLI command.
pppip("instance");	Inserts the IP address for a specific PPP instance, where instance is the PPP instance number.

Example email templates

Following are examples of email templates.

Example 1

```
TO: 123@abc.co.nz
FROM: MyRouter
SUBJECT: Remote Configuration
                              ← This blank line is required

Time: <%timeSmtp();%>
Serial Number: <%serial_number();%>
Req: CFG_RQ
IP Address: <%smtpip();%>
PPP 1 IP address: <%pppip("1");%>
```

Example 2

```
TO: fred@anyco.com, jane@anyco.co.uk
FROM: MyRouter
SUBJECT: automatic email
MIME-Version: 1.0
                              ← This blank line is required

Unit: <%smtpid();%>
Event: <%email_event();%>
This event had sufficient priority to cause the transmission of this email. Please check
the attached logs and review.
```

Include the output from CLI commands in the email body

You can also execute CLI commands and include their output within the email; the output from up to 10 CLI commands will be added to the body of the email. The command to be executed needs to be entered in place of **xxxxx** below. To include the output from multiple commands, use the **run_cmd()** function multiple times.

The **run_command()** function is as follows:

```
<%run_cmd("xxxxx");%>
```

For example,

```
<%run_cmd("ati5");%>
<%run_cmd("bufs");%>
<%run_cmd("msgs");%>
```

For example, here is a template adding CLI commands:

```
TO: fred@anyco.com, jane@anyco.co.uk
FROM: MyRouter
SUBJECT: automatic email
MIME-Version: 1.0


Unit: <%smtpid();%>
Event: <%email_event();%>
This event had sufficient priority to cause the transmission of this email. Please check
the attached logs and review.
<%run_cmd("ati5");%>
<%run_cmd("bufs");%>
<%run_cmd("msgs");%>
```

You can also specify an extra parameter which indicates the required priority of the event before the command is executed. This allows events to be sent off without attachments, but if the event has an equal or higher priority than the value of this parameter, the attachments are included. This ensures that the attachments are not included unnecessarily with non-critical events and using up all the data allowance on a wireless connection.

```
<%run_cmd("chkst","5");%>
```

An example template adding CLI commands with priority values is:

```
TO: fred@anyco.com, jane@anyco.co.uk
FROM: MyRouter
SUBJECT: automatic email
MIME-Version: 1.0


Unit: <%smtpid();%>
Event: <%email_event();%>
This event had sufficient priority to cause the transmission of this email. Please check
the attached logs and review.
<%run_cmd("chkst","5");%>
```

In the example above, the command **chkst** is executed when an event with a priority equal to or higher than **5** is detected.

Email Notifications Parameter descriptions

To use the email alert facility, you must first specify a valid **Dial-out number**, **Username,** and **Password**, and set the SMTP parameters correctly. The **Dial-out number**, **Username** and Password parameters are on the **Configuration > Network > Interfaces > Advanced > PPP n** pages where **n** is the relevant interface number. The SMTP parameters are on **Configuration > Alarms > SMTP Account**.

Send email notifications

Enables the display of the configurable parameters when checked.

Send an email notification when the event priority is at least n

The lowest priority event that will generate an email alert message. For example, if this value is set to **6**, only events with a priority of **6** or lower (**7**, **8**, or **9**) trigger an automated email alert message. To disable email alarms, set this value to **0**.

Send a maximum of n emails per day

The limit on the number of emails that can be sent during any 24-hour period. The intention is to prevent excessive alerts being sent when the event trigger value is set to a high priority / low value (for example, **1**, **2**, or **3**), such as a value that results in a large number of automated email alert messages being generated.

n emails have been sent today

A status message, indicating how many emails have been sent during the last 24-hour period.

Use email template file

The name of a template file used to form the basis of any email alert messages generated by the event logger. The default template is a file called **EVENT.EML** stored in the compressed **.web** file. You can create alternative template, but to be valid, it must have the **.EML** file extension and be stored in the normal file directory. A new template with the name **EVENT.EML** takes precedence over the predefined **EVENT.EML** template, but it is recommended that a new name is used, such as **event1.eml**.

Email To

The standard email address format for the intended recipient of the alert.

Email From

A valid email address that will be accepted by the SMTP server as being authorized to send email.

Email Subject

A short description of the email content.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
event	n	etrig	0-9 0 disables sending alerts	Send an email notification when the event priority is at least n
event	n	emax	0-255	Send a maximum of n emails per day
event	n	etemp	The name of a template file. Default is **EVENT.EML**	Use email template file
event	n	to	A valid email address, such as **you@yourdomain.com**	Email To
event	n	from	A valid email address	Email From
event	n	subject	A brief description of the content of the email	Email Subject

SNMP Traps parameters

The router firmware supports the use of SNMP, with the ability to generate traps. To make the SNMP (Simple Network Management Protocols) functional, a SNMP trap server must be configured. SNMP trap server configuration is in the
Configuration > Remote Management > SNMP > SNMP Traps menu.

Send SNMP Traps

This checkbox, when checked enables the display of the following parameters:

Send a SNMP Trap when the event priority is at least n

The lowest-priority event that will generate an SNMP trap message. For example, if this value is set to **6**, only events with a priority of **6** or lower (**7**, **8** or **9**) will trigger an automated SNMP trap message. To disable SNMP traps, set this value to 0.

Send a maximum of n SNMP taps per day

Sets the limit on the number of emails that may be sent during any 24-hour period. The intention is to prevent excessive alerts being sent when the event trigger value is set to a high priority/low value (for example, **1**, **2**, or **3**), such as a value that results in a large number of SNMP trap messages being generated.

n SNMP traps have been sent today

A status message, indicating how many SNMP trap messages have been sent during the last 24-hour period.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
event	n	trap_trig	0-9 0 disables sending alerts	Send a SNMP trap when the event priority is at least n
event	n	trap_max	0-65535	Send a maximum of n SNMP traps per day

SMS Messages parameters

This menu option has three identical rows, each of which controls the setting of the SMS alert messages.

Note The SMS Messages option is only available on routers with W-WAN capability.

Send SMS messages to

The destination telephone number (MSISDN) for SMS alert messages. The format for this field is the international dialing code followed by the number, but should not contain a **+** prefix. For example, UK mobile **07871 445677** would be **447871445677**.

If the event priority is at least **n**

Sets the trigger level for the alert message. For example, if this field is set to the value **6**, only events with a priority of **6** or higher will trigger an automated SMS alert. Setting this field to **0** disables sending SMS alerts.

Use SMS template

The name of the template file that used to form the basis of any alarm messages generated by the event logger. The default template file is a file called **EVENT.SMS** that is stored in the compressed **.web** file. A new template can be created, and if named **EVENT.SMS, it takes** precedence over the pre-defined **EVENT.SMS** template. However, it is recommended that a new name is used, such as **event1.sms**. Templates should use the **.SMS** file extension.

Send a maximum of **n** SMS messages per day

Limits the number of SMS alert messages sent by the router in any one day.

n SMS messages have been sent today

A status message, indicating how many SMS alert messages have been sent during the last 24-hour period.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
event	n	sms_to	A valid mobile number such as **447871445677**	Send SMS messages to
event	n	sms_trig	0-9	If the event priority is at least n
event	n	sms_to2	A valid mobile number such as **447871445677**	Send SMS messages to
event	n	sms_trig2	0-9	If the event priority is at least n
event	n	sms_to3	A valid mobile number such as **447871445677**	Send SMS messages to
event	n	sms_trig3	0-9	If the event priority is at least n
event	n	sms_temp	event.sms (template file stored in the compressed **.web** file)	Use SMS template
event	n	sms_max	0-65535	Send a maximum of n SMS messages per day

Local Logging parameters

A secondary log file can be created on a USB flash drive. Events will be appended to this log file. Using a secondary log file is useful if an extended logging period is required where, the normal **eventlog.txt** file would overwrite early events before the operator has had a chance to view them. The secondary log file can be limited in size or allowed to fill the USB flash drive. Once the log file is full, earlier events are pruned from the end of the file to allow new events to be added.

To configure the local logging parameters, set the following values in the web interface:

Local Drive to log to

Determines the drive letter where the USB flash drive is located. This is designated **u** for a USB drive.

Log filename

The name of the file for the secondary event log.

Log size

The maximum size of the log file in kilobytes.

XML logs

On platforms that support it, event logs can be saved in XML format. This field specifies the size of the XML log file, in kilobytes. The files created will be named **EVXML1.XML**, **EVXML2.XML**, etc.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
event	n	logdrive	Drive letter, such as **u** for USB flash drive.	Local drive to log to
event	n	logfile	Name of the file, such as **mylog.txt**.	Log filename
event	n	logsizek	Size of log in kilobytes, such as **1048576**, which is 1MB.	Log size
event	n	xmllogs		None

Syslog Messages parameters

As well as logging events to an internal log file and to a file on a USB flash drive, the router can log events to a Syslog server.

To configure the router to send Syslog messages to a Syslog server, set the following values in the web interface:

Send Syslog messages

When this checkbox is checked, the following options are displayed:

Send a Syslog message when the event priority is at least **n**

The lowest-priority event that will generate a syslog message. For example, if this value is set to **6**, only events with a priority of **6** or lower (**7**, **8**, or **9**) will trigger an automated syslog message. To disable syslog messages, set this value to **0**.

Send a maximum of **n** Syslog messages per day

Sets the limit on the number of syslog messages that may be sent during any 24-hour period. The intention is to prevent excessive alerts being sent when the event trigger value is set to a high priority/low value (**1**, **2**, or **3** for example), such as a value that results in a large number of syslog messages being generated.

n Syslog messages have been sent today

A status message that indicates how many Syslog messages have been sent in the last 24-hour period.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
event	n	syslog_trig	0-9	Send a Syslog message when the event priority is at least n.
event	n	syslog_max	0-2147483647	Send a maximum of n Syslog messages per day.

Syslog Server n parameters

This section describes the configuration of the router for defining the Syslog server to send messages to.

Syslog server IP address

The IP address of the server.

Port

The port to use.

Note The following three items (**Mode**, **TCP timeout**, and **Route**) only appear on routers that have the TCP logging software option enabled. This is not a commonly used option.

Mode

There are currently three supported communication modes; these are selected from a drop-down list and are **TCP**, **UDP**, and a protocol described in RFC 3195.

TCP timeout s seconds

For TCP communications, this parameter sets the timeout on the socket.

Route using

These radio buttons select which method of establishing a route to the server to use.

Routing table

When this radio button is selected, the routing table is used to determine the interface that will be used to transmit the syslog message.

Interface x,y

If the routing table is not to be used, an interface type (**PPP** or **Ethernet**) can be selected from the drop-down selection box, and the interface instance number can be typed into the adjoining text entry box. The route is then determined by that interface.

Priority

The checkboxes listed in this section select the event priorities that should cause the event to be logged.

Facility

The checkboxes listed in this section select which of the router facilities should be logged.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
syslog	n	server	IP address	Syslog server IP address
syslog	n	port	IP port number	Port
syslog	n	mode	UDP, TCP, RFC3195	Mode
syslog	n	tcp_to	Timeout in seconds, such as **86400**.	TCP timeout s seconds
syslog	n	source_ent	PPP, ETH	Interface x,y x=Interface type
syslog	n	source_add	0-4	Interface x,y y=interface number
syslog	n	priority	Hyphen separated 0-7 Comma-separated 0,3,5 or **all**	Priority checkboxes.
syslog	n	facility	Hyphen-separated 0-23 Comma-separated 4,3,5,10,15,22 or **all**	Facility checkboxes.

Event Logcodes parameters

On the **Event Logcodes** page, you can edit the logcodes that describe events entered in the **EVENTLOG.TXT** file. If a change is made to the **logcodes.txt** file, the changes are saved in the file **logcodes.d**, so that when a firmware upgrade is performed, the changes to the logcodes are retained.

The **Event Logcodes** page initially shows a table containing the event descriptions and reason. Clicking on any of the items that are links in the table opens a configuration page associated with that item. The newly-opened page allows that item to be configured. The configuration options shown on that page are described below.

Event

This is not a configurable parameter; it is simply the event number, displayed for information only. This is the number to refer to when filtering events in the event log settings **Configuration > Alarms > Event Settings**.

Description

A description of the event code. Clicking on a link in this field brings up the configuration page associated with that event.

Filter

This parameter is for information only. If event filtering is applied to an event, the associated filter is shown as **On**. This is a result of enabling the parameter **Do not log this event** as described below.

Event Priority

Controls the priority of the event and is used to determine whether an event will trigger email, SMS messages or SNMP traps.

Reasons

The reason why the event occurred. Not every event has a list of reasons.

Reason Priority

This parameter is for information only.

Attachment List ID

A fixed list of values that can be used to conveniently refer to the associated list of files to attach to an email.

Files

Allows entering a comma-separated list of names for the files that should be attached to an email.

Configuring Events

This page controls the configuration of the event that is displayed in bold font at the top of the page, just below the blue title bar.

Do not log this event

When checked, this checkbox disables logging of the event.

Note This parameter is **not** saved in the **logcodes.txt** file but in the **config.dan** file. This means that after changing this parameter, you must save the changes by clicking the save changes link when prompted (this appears after clicking the **Apply** button). If you click the **Save All Event Code Changes**, your changes are not reflected.

Log Priority

The priority of the event to determine whether the event will trigger emails, SMS messages or SNMP traps. **0**=disabled, **1**=highest priority, **9**=lowest priority.

Alarm Priority

If the above **Inherit alarm priority from event** checkbox is **not** checked, this parameter selects the priority of the reason. Valid values are **0** to **9**.

Alarm Priority is dependent on the event being logged by Entity

Selecting this checkbox makes the priority conditional on which system entity triggered the event, such as Ethernet, and enables the following two configuration options:

Entity

A list of the system entities.

All

Selecting this radio button causes all of the system entities.

Instance

Selecting this radio button enable a text entry box that allows the user to enter the instance of the selected entity.

Priority only applies to

A set of checkboxes, each checkbox controlling whether the priority is applied to that interface instance. So for example, to apply the priority to PPP interface **1**, click on **PPP 1** checkbox.

Store a snapshot of the Traffic Analyser trace on the log drive

Selecting this checkbox causes a snapshot of the analyser trace to be stored on the USB flash drive

If this event creates an Email alarm

Attach a snapshot of the Traffic Analyser trace

Checking this checkbox causes a snapshot of the analyser trace to be attached to the email.

After this event

Leave the Analyser trace

Leaves the analyser trace unchanged.

Freeze the Analyser trace

Causes the analyser to be frozen, such as no more logging will take place until the email has been sent.

Delete the Analyser trace

Causes the analyser trace to be deleted once the email has been sent.

Attach a snapshot of the Event Log

Causes the event log to be attached to the email.

After this event

Leave the Event Log

Selecting this radio button will leave the event log unchanged.

Delete the Event Log

Selecting this radio button will cause the event log to be deleted after the email has been sent.

Attachment List ID

Which files to attach to the email. The ID refers to the table of files.

Syslog Priority

This drop-down selection box contains the following options:

- **Emergency**
- **Alert**
- **Critical**
- **Error**
- **Warning**
- **Info**
- **Debug**

Syslog Facility

This drop-down selection box contains the following options:

- **Kernel**
- **User**
- **Mail**
- **System**
- **Auth**
- **Syslog**

Configuring Reasons

The page invoked by selecting a reason link in the event logcodes table is very similar to the **Configuring Events** page but with the following differences.

There is no "Do not log this event" checkbox. There is the following additional parameter:

Inherit alarm priority from event

Selecting this checkbox causes the following **Alarm Priority** parameter to be disabled, and causes the priority to be the same as the event that triggered it. The **Alarm Priority** parameter is the same as in the **Configuring Events** page.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
event	n	ev_filter	Comma-separated list of event codes	Do not log this event

There are no CLI commands for editing Event logcodes. However, you can edit the **LOGCODES.TXT** file which holds all the logcode information. For details on how to do this, see View and manage the event log on page 753

SMTP Account parameters

For the router to successfully send emails, an email account (SMTP) must be available. This section describes the configuration of the router to use the email account set up for it.

Hostname or IP address of your SMTP server

The IP address or hostname of the SMTP mail server, such as **smtp.myisp.com**. Sending email requires a connection to the Internet. Depending upon how the router is configured, it may be necessary to check that the PPP configuration allows a connection to the ISP or external SMTP mail server.

Port

The Simple Mail Transfer Protocol (SMTP) uses TCP port **25**, which is the default for this parameter. If the mail server uses a different TCP port, enter it here.

Username

Email accounts are controlled by requiring a username and password in order to send and receive mail. This field is where the account username is set. This information will be provided by the administrator of the email server.

Password

This field is where the account password is set.

Confirm Password

Used to re-enter the password. The two passwords are compared to check that they are the same and that there hasn't been a typographical error when entering them. This check is used since the password characters are not echoed. Therefore, the usual visual feedback is not available.

Display "Email From" as

The text to be used as the **MAIL FROM** parameter which forms part of the protocol when connecting to the email server. Most SMTP servers accept an empty string, while others require that this parameter is present. You may need to consult with the SMTP server administrator (or ISP) to determine whether this parameter is required.

Attachment size limit **n** Kbyte, Mbyte

Some email service providers place a limit on the size of an email attachment that they will accept, this parameter can be used to ensure that the limit is not exceeded. The traffic analyser and event logger can generate substantial files, and it may be required that these files are truncated when sent as email attachments. The size is specified in kilobytes. For example, setting this limit to **250** truncates the attachment to **250kB** before transmission. Setting the size to **0** means that no limits are imposed.

If the email template does not contain one, use "Reply To" address

This address is inserted into the email header if no reply address exists in the appropriate email template. If the email template does contain an address in the **reply to:** field, that will override the default reply address.

Route using Routing table, Interface **x,y**

When selected, the routing code determines the outbound interface, and that interface determines the source IP address. If the **Route using routing table** option is not selected, the settings in the interface and interface instance text boxes determine the outbound interface and source IP address. These are selected from the drop-down selection box and are **None**, **PPP**, and **Ethernet**.

Resend the email after **s** seconds if the first attempt fails

This checkbox and associated text entry box enable the retry mechanism. If the first attempt to deliver the email fails, the router waits the specified number of seconds (which must be non-zero) before making another attempt.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
smtp	n	server	Valid hostname or IP address	Hostname or IP address **mailserver.isp.com 122.134.156.178**
smtp	n	port	Valid port number, such as 25	Port **n**
smtp	n	username	Free text field containing a valid account username such as **my_account**	Username
smtp	n	password	Free text field containing account password, such as **my_password**	Password
smtp	n	mail_from	Free text field	Display **Email From** as
smtp	n	att_lim	0-65535	Attachment size limit This CLI value is entered in Kilobytes only.
smtp	n	reply_to	Free text field	If the email template does not contain one, use **Reply To** address
smtp	n	userouting	0,1	Route using routing table
smtp	n	ll_ent	Blank,PPP,ETH	Route using Interface x,y x=Interface type
smtp	n	ll_add	0-255	Route using Interface x,y y=interface number
smtp	n	retry_dly	0-255	Resend the email after s seconds if the first attempt fails

Configure system settings

The TransPort device has several groups of configuration settings for general behavior of the system, on the **Configuration > Systems** pages. This section covers configuring system settings from the web interface and command line. It covers the following topics:

- Device Identity parameters on page 610
- Date and Time parameters on page 612
- General system parameters on page 621

Device Identity parameters

You can configure the identity of your router with the Digi TransPort web interface.

To configure your router's device identity, set the following values:

Description

A description of the router that can be used to uniquely identify it. This is useful where there are a large number of routers on a site and a descriptive name would be easier to use when referring to the router, rather than having to use the serial number or other unique parameter. This parameter is used by the SNMP function within the router.

Contact

A contact name for the router.

Location

A location string for the router, which again may be helpful when referring to a particular router within a site or for identifying a particular site.

Device ID

This field is taken from the Remote Manager configuration and should not normally need to be changed. When using Remote Manager to manage the router, the configuration procedure assigns a device ID to the router. The device ID is a 64-byte value, with each 8-byte section separated with a **-** character. Valid digits are upper case hexadecimal. The first 16 digits (reading from left to right) are normally set to **0**. The second 16 digits comprise the MAC address of the primary Ethernet interface and the digits **FF** to make up the full 8-digit. The following device ID illustrates the format:

`00000000-00000000-001122FF-FF334455`

This example uses the MAC address **00:11:22:33:44:55**.

Router Identity

A string of up to 20 characters that identify the router in email alert messages generated by the event logger. This string also serves as the prompt string during a remote login. The factory configuration uses the character sequence **%s**. This sequence is replaced by the serial number of the router when the unit identity is displayed. This character sequence can be used when creating a custom identity for the router. For example, if the serial number of the router is **012345**, entering the string **My_Router_%s>** would show the prompt **My_Router_012345**> during a remote login.

Hostname

Assigns a hostname to the local IP address of the router.

Secondary Hostname

Allows a second hostname to be assigned to a router. This is associated with the secondary IP address.

Note Character limitations of the **Description** and **Hostname** fields should be 64 characters.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
snmp	n	Name	Free text field up to 64 characters	Description
snmp	n	Contact	Free text field	Contact
snmp	n	Location	Free text field	Location
cmd	n	Unitid	Free text field	Router Identity
cmd	n	Hostname	Free text field up to 64 characters	Hostname
cmd	n	sec_hostname	Free text field up to 64 characters	Secondary Hostname

Date and Time parameters

The router keeps track of calendar time using an internal real time clock (RTC) device. The clock is used to time/date stamp logfiles. The date and time configuration pages allow the system time to be set and maintained. Since maintaining an accurate system clock can be important for routers on the Internet, NTP and SNTP services are supported and the router may be configured to use one of these protocols for maintaining the internal system time. The router uses the 24-hour clock.

Current system time

The current system time appears at the top of this web page.

Manually set the time h hours, m minutes s seconds, M month D day Y year

These parameters are set using the associated drop-down selection menus.

Hours

Select from the drop-down list to set the hours.

Minutes

Select from the drop-down list to set the minutes.

Seconds

Select from the drop-down list to set the seconds. This setting may have limited use due to human reaction times.

Month

Select from the drop-down list to set the month.

Day

Select from the drop-down list to set the day.

Year

Select from the drop-down list to set the year.

Set

Click this button to cause the above settings to take effect.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
n/a	n/a	time	**hh** [**mm** [**ss** [**DD** [**MM** [**YYYY**]]]]]	Manually set the time.

Autoset Date and Time parameters

Do not auto-set the system time

This is the system default, and this radio button will appear filled in when the router is new unless a different default configuration has been supplied. Click this radio button to close the SNTP or NTP configuration pages.

Auto-set the system time

Selecting this radio button expands the page to include the SNTP settings, described below.

SNTP server

The hostname or IP address of the desired SNTP server.

Check on Power-up

This checkbox, when checked, causes the router to attempt to connect to the SNTP server every time it boots.

Update every h hours

The interval, in hours, the router should wait between updating the system clock.

Randomly between s1 and s2 seconds

It is possible to use a random update interval rather than a fixed interval. There are two text-entry boxes for this purpose. Enter the minimum interval into the left-hand box, and the maximum desired interval into the right-hand box. Selecting the random update clears the fixed interval.

Offset from GMT

This parameter should be set to **+** or **-** the number of hours the router's time should be ahead or behind Greenwich Mean Time.

Update for Daylight Saving Time.

When checked, this checkbox causes the following parameters to appear, the router uses those settings to automatically adjust the system time to ensure that local daylight saving is used.

Start parameters

Month

The month in which to switch to daylight saving time.

Day

The day on which to switch to daylight saving time.

Hour

The hour at which to switch to daylight saving time.

End

Month

The desired month in which to switch back to GMT (UTC).

Day

The desired day on which to switch back to GMT.

Hour

The desired hour at which to switch back to GMT.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
sntp	n	server	Valid hostname or IP address **sntp.timeserve.org**	SNTP Server
sntp	n	pwrchk	0,1	Check on Power-up 0=Off 1=On
sntp	n	interval	0-255	Update every h hours Default=**24**
sntp	n	randintsecs	0-86400	Randomly between s1 and s2 seconds Use format [s1,s2] For example, min **50**, max **500** would be: **[50,500]**
sntp	n	offset	-12 to +13	Offset from GMT.
sntp	n	dstonmon	0-12	Start: Month Update for Daylight Saving Time 0 disables daylight saving.
sntp	n	dstonday	0-31	Start: Day
sntp	n	dstonhr	0-23	Start: Hour
sntp	n	dstoffmon	0-12	End: Month
sntp	n	dstoffday	0-31	End: Day
sntp	n	dstoffhr	0-23	End: Hour
sntp	n	ntp	0,1	0=SNTP 1=NTP Default=OFF

NTP parameters

Use NTP for greater accuracy

Selecting this checkbox expands the page to show the NTP settings, described below.

NTP is much more accurate than SNTP, with NTP an accuracy of 200 microseconds (1/5000 second) can be achieved. The NTP functionality is in accordance with RFC1305.

Up to 4 remote peers can be configured, all the peers are polled at intervals and the best peer is selected for using as the time source. SNTP should be configured prior to using NTP. The router calculates the accuracy of the NTP time servers over a period of time, up to 2 hours. Once the drift compensation is calculated, the NTP client will be used. The drift compensation value is stored in NVRAM and written to the **config.da0** file. If the router loses power or is rebooted, it does not need to re-calculate the accuracy of the NTP servers again. The compensation value is constantly monitored to make sure it remains correct.

Note Using SNTP achieves an accuracy of around 1 second.
Using NTP achieves an accuracy of 200 microsecond.
Not all models support NTP; this option only appears for models that do.

Initial Drift Compensation n ppm

NTP incorporates compensation for clock drift. If this parameter is known, it can be entered here. Otherwise, the router calculates this value over a period of time. Once calculated, the value is displayed in the text box.

Clock Precision Limit

Select the clock precision limit from the drop-down selection box.

Disable NTP when interface x,y is out of service

If the specified interface is out of service, the NTP is disabled until the interface is available again.

NTP Servers 1 - 4

The router can have up to four NTP server connections. The more NTP servers used, the more accurate the time setting will be. The following section describes the configuration of the connections.

NTP Server 1/2/3/4 Hostname

The NTP server hostname or IP address.

Broadcast Mode

When enabled, the NTP client operates in a different manner. Rather than sending out an NTP client message and expecting a reply, the NTP module sends out a broadcast mode packet to the IP address configured in **NTP host** field. The broadcast interval is determined by the value of **Minimum poll interval**.

Poll Interval s1 to s2 seconds

The minimum and maximum intervals between poll broadcasts. The values are time, in seconds, represented as a power of 2. This means that a value of **4** means that the minimum poll interval is **2^4=16** seconds.

Startup burst Interval s seconds

When connecting to an NTP time server in polled mode, it may be necessary to send polls at intervals shorter than the minimum poll interval, to speed up the synchronization process. This parameter controls the interval between polls during the startup process. This feature is useful in situations where the router only has an intermittent Internet connection.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ntp	n	driftppm	-10000-+10000	Initial Drift Compensation
ntp	n	precision	-10-0	Clock Precision Limit
ntp	n	inhibit_int	Blank,PPP,Ethernet	Disable NTP when interface **x,y** is out of service x=Interface type
ntp	n	inhibit_add	0-255	Disable NTP when interface x,y is out of service y=interface number
ntp	n	server	Valid IP address or hostname, such as ntp1@timeserver.org	NTP Server
ntp	n	bcast	0,1	Broadcast Mode 0=disabled 1=enabled
ntp	n	minpoll	3-14	Poll Interval s1, s2 3=8 4=16 5=32 6=64 7=128 8=256 9=512 10=1024 11=2048 12=4096 13=8192 14=16384
ntp	n	maxpoll	3-14	Poll Interval s1, s2 See **minpoll** for values
ntp	n	burstint	0-255	Startup burst Interval s seconds
ntp	n	server2	Valid IP address or hostname, such as **ntp2@timeserver.org**	NTP Server
ntp	n	bcast2	0,1	Broadcast Mode 0=disabled 1=enabled
ntp	n	minpoll2	3-14	Poll Interval **s1, s2** See **minpoll** for values

ntp	n	maxpoll2	3-14	Poll Interval s1, s2 See **minpoll** for values
ntp	n	burstint2	0-255	Startup burst Interval s seconds
ntp	n	server3	Valid IP address or hostname, such as **ntp3.timeserver.org**	NTP Server.
ntp	n	bcast3	0,1	Broadcast Mode 0=disabled 1=enabled
ntp	n	minpoll	3-14	Poll Interval s1, s2 See **minpoll** for values
ntp	n	maxpoll	3-14	Poll Interval s1, s2 See **minpoll** for values
ntp	n	burstint3	0-255	Startup burst Interval s seconds
ntp	n	server4	Valid IP address or hostname, such as **ntp4.timeserver.org**	NTP Server.
ntp	n	bcast4	0,1	Broadcast Mode 0=disabled 1=enabled
ntp	n	minpoll4	3-14	Poll Interval s1, s2 See **minpoll** for values
ntp	n	maxpoll4	3-14	Poll Interval s1, s2 See **minpoll** for values
ntp	n	burstint4	0-255	Startup burst Interval s seconds

ntpstat command: Check NTP client status

To check the status of the NTP client, use the ntpstat command.

View NTP system status information

`ntpstat sys`

View NTP peer information

`ntpstat peers`

Reset system information and allow NTP to recalculate the drift compensation

`ntpstat rst`

General system parameters

The **General system parameters** page has the following settings.

Autorun Commands

The router can be configured to run a number of commands once it has booted. These commands are associated with specific asynchronous serial interfaces. For example, suppose a Script Basic script, **sample.bas**, must be run at boot up. Autorun commands are normally associated with an ASY port, but running a script for example is not ASY port-specific.

To configure the autorun commands, set the following values:

#

The command interface to be associated with the command. In the above example, this would be set to the number **0**.

Command

The CLI command to run on start-up. In the above example, this field would be set to the string **bas sample.bas**.

Related CLI commands.

Entity	Instance	Parameter	Values	Equivalent Web Parameter
cmd	n	autocmd	Valid CLI command	Autorun Commands

Web / command line interface

The router can be configured using several different methods. This section describes how to configure the web GUI and CLI (command line interface) options.

Automatically log user out if idle for h hours m minutes s seconds

To limit the probability of unauthorized users gaining access to the router, login timeouts are applied. These timeouts cause an existing connection to be closed after a predefined period. The default is **20** minutes.

For users connected on the local Async port

Use access level None, Low, Med, High, Super

For security purposes, logging into the router is controlled by a user access level. This parameter controls the access level that applies when logging in via the local asynchronous serial port.

Automatically log user out Never / If idle for h hrs m mins s secs

How long the local port allows access before terminating the connection and requiring the user to log in again. Selecting the **Never** buttons allows permanent access to the router via the local asynchronous serial port. If, for security reasons, it is required that the access should be limited, the appropriate time period can be entered into the text entry boxes.

Disable Remote command echo for Telnet sessions

Enables/disables command echo for remote access. This applies to Telnet and TRANSIP sessions.

CLI Pre-Login Banner

The router can display a banner before any login information is requested. The parameter specifies the name of a file that is stored in the flash filing system and contains the text to be displayed before the request for the username and password. This can be useful for displaying a standard welcome message or any site-specific user instructions.

CLI Post-Login Banner

Once the user has successfully logged on to the router, a second message can be displayed. This parameter specifies the name of a file containing the text to display. As above, the file may contain site-specific instructions to be carried out once the user has logged in.

Allow CLI access from X.25 address **n**

Enables/disables logging into the router over an X.25 connection. The parameter **n** must be a valid X.25 NUA (Network User Address).

With TRANSIP, use access level None, Low, Med, High, Super

Controls the security access level when using TRANSIP to access the router.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
cmd	n	tremto	0-86400 seconds	Automatically log user out if idle for h hrs m mins s seconds This CLI value is entered in seconds only.
local	n	access	0-4	Use access level 0=Super 1=High 2=Medium 3=Low 4=None 8=Read only
local	n	tlocto	Free text field	Never, h hrs, m mins, s secs
cmd	n	noremecho	0,1	Enable Remote command echo 0=Off (default) 1=On
cmd	n	prebanner	Valid filename such as **welcome1.txt**	CLI Pre-Login Banner
cmd	n	postbanner	Valid filename such as **welcome2.txt**	CLI Post-Login Banner
cmd	n	cmdnua	0-1023	Allow CLI access from X.25 address
local	n	transaccess	0-4	With TRANSIP, use access level 0=Super 1=High 2=Medium 3=Low 4=None 8=Read only

Miscellaneous configuration items

This section is for those configuration settings that do not fit neatly into any other group of settings.

Note Depending on the router model, some of these options may not be available.

Use Config n when the router powers up

The router maintains two configuration files, either of which may be invoked on power-up. Select the required one from the drop-down selection box. Use this option with care as selecting the incorrect configuration file can cause confusion.

Allow anonymous FTP login

When checked, this checkbox enables the router to accept anonymous logins. The default state is Off and the security implications of enabling this option should be considered carefully before applying.

Additional FTP NAT port n

Standard FTP uses two well-known ports, a control port and data port. These are low-number ports, and may be blocked by firewall rules. As such, it may be that an FTP server may be listening on a non-standard control port. This parameter is used to specify the port that the router should monitor for the FTP **PORT** and **PASV** commands. These commands contain information relating to IP addresses and Ports which should be modified during the NAT process. The NAT modifications may result in different-sized packets being generated that then require that the TCP sequence numbers be modified to allow for the changes.

SNMP Enterprise number

The value of the OID (Object IDentifier) used by SNMP management tools when accessing the MIB (Management Information Block). This number must form part of the OID used to access individual items in the MIB as a prefix.

For example: **SNMPv2-SMI::enterprises.16378.10001**.

SNMP Enterprise Name

The name corresponding to the above Enterprise Number.

Only resolve DNS request for domain

Entering a domain name here restricts DNS requests to the specified domain only.

W-WAN LED to display W-WAN, ISDN/PSTN

On the front panel of the display of models fitted with a W-WAN module, is an LED that can be used to display the status of the W-WAN module or the status of the PSTN/ISDN connection. Use the drop-down selection box to choose what the LED displays. The ISDN/PSTN settings depend upon which of these two options are available on the router.

Serial LED to display Connection, DTR

On the front panel of the router is an LED dedicated to indicating the status of various signals on the asynchronous serial line. Use the drop-down selection box to choose which signal status to display. On modules fitted with W-WAN, this LED has additional functionality, it can also be used to display the W-WAN signal strength.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
config	n	powerup	0,1	Use Config n when the router powers up
cmd	n	anonftp	0,1	Allow anonymous FTP login 0=Off (default) 1=On
snmp	n	ftpnatport	0-65535	Additional FTP NAT port
snmp	n	ent_nb	0-65535	SNMP Enterprise Number Default 16378
cmd	n	ent_name	Free text field	SNMP Enterprise Name
cmd	n	dnsname	Valid Domain name, such as **mydomain.org**	Only resolve DNS request for domain
cmd	n	gprsled_mode	0,1	W-WAN LED to display W-WAN, ISDN/PSTN 0=W-WAN 1=ISDN/PSTN
cmd	n	asyled_mode	0,1	Serial LED to display Connection, DTR 0=Connection 1=DTR status 2=W-WAN signal strength

Configure Remote Manager

The **Configuration > Remote Manager** page has the following menu options:

About Digi Remote Manager

Digi Remote Manager is a hosted remote configuration and management system that has been designed to facilitate the management of large numbers of routers.

Digi Remote Manager provide a web-based interface that shows the configuration of selected routers allows the configuration to be changed and also facilitates remote firmware upgrade. The Digi Remote Manager servers also provide a data storage facility.

Using Digi Remote Manager requires setting up a Digi Remote Manager account. Applying for an account is a straightforward procedure; the local sales representative will have details. To set up a Digi Remote Manager account and learn more about Digi Remote Manager, go to http://www.digi.com/products/cloud/digi-remote-manager.

Remote Manager parameters

Remote Manager parameters are configured on the **Configuration > Remote Management** pages.

Connection Settings

To configure Digi Remote Manager connection settings parameters, set the following values:

Enable Remote Management using a client-initiated connection

Select this checkbox to display the basic configuration parameters and enable the router to make the connection to the Remote Manager server.

Server Address

The IP address or (more usually) the domain name of the Remote Manager host. This information will be supplied when your Remote Manager account is activated.

Automatically reconnect to the server after being disconnected

The protocol used to communicate with the server allows the router to detect that it is no longer connected to the server. Enabling this checkbox causes the router to attempt a reconnection when it discovers that the connection has been lost.

Reconnect after h hours m minutes s seconds

If the reconnect checkbox is enabled, these parameters specify the interval to wait before attempting to reconnect to the server.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
cloud	n	clientconn	0,1	Enable Remote Management and Configuration using a client-initiated connection 0=Off 1=On
cloud	n	server	Valid IP address such as **1.2.3.4** or domain name such as **login.remotemanager.digi.com**	Server Address
cloud	n	reconnect	0,1	Automatically reconnect the server after being disconnected 0=Off 1=On
cloud	n	reconnectsecs	0-86400	Reconnect after h, m, s This CLI value is entered in seconds only.

SMS Settings

The SMS feature supports sending and receiving SMS messages between Remote Manager and a Remote Manager-registered router. SMS can be used to:

• Send an SMS message to the router in order to have the router dynamically establish its EDP connection with Remote Manager

• Send user defined data to and from Remote Manager and Remote Manager-registered router

• Perform limited device management such as pinging the router, as well as provisioning it properly for SMS functionality with Remote Manager

For more information on the SMS feature, see the *Remote Manager User Guide*, Digi part number 90001436.

You can configure the Remote Manager SMS Settings parameters using the Digi TransPort web Interface.

To configure the Remote Manager SMS Settings, set the following values:

Enable Remote Manager SMS

Check this box to enable Remote Manager SMS feature

Enable Opt-in

Enable the opt-in to ensure that you have subscribed to the SMS service. Check this box to enable opt-in.

Enable Strict Sender

You can enable the Strict Sender mode to ensure that the SMSs from Remote Manager are never blocked. Check this box to enable the Strict Sender framework.

Enable responses to be sent to the sender's phone number

Check this box to enable responses to be sent to the sender's phone number.

Accept Remote Manager client connection requests

Enable client connection requests to accept the incoming connections. Check this box to enable Remote Manager client connection requests.

Accept requests to connect to other Remote Manager servers

Check this box to accept request to connect to other Remote Manager servers.

Override the destination phone number with the following number

Check this box to override the destination phone number with another phone number. Once you check this box, the phone number text box is enabled. You can enter the phone number in this text box.

Override the service ID with the following value

Check this box to specify the service ID value. Once you check this box, the service ID text box is enabled. You can enter your service ID in this text box.

Limit CLI response to

You can specify the maximum CLI response size in this text box.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
cloudsms	n	enable	OFF |ON Default: OFF	Enable Remote Manager SMS
cloudsms	n	optinenable	OFF |ON Default: OFF	Enable Opt-in
cloudsms	n	strictsender	OFF |ON Default: OFF	Enable Strict Sender
cloudsms	n	replytosender	OFF |ON Default: OFF	Enable responses to be sent to the sender's phone number
cloudsms	n	pagedconnect	OFF |ON Default: OFF	Accept Remote Manager client connection requests
cloudsms	n	connectoverride	OFF |ON Default: OFF	Accept requests to connect to other Remote Manager servers
cloudsms	n	phnum	Number	Override the destination phone number with the following number
cloudsms	n	svcid	Number	Override the service ID with the following value
cloudsms	n	maxcliresp	Number Default: 0	Limit CLI responses to the specified number.
cloudsms	n	debug	OFF |ON Default: OFF	

Advanced remote management settings

The settings in the previous section, along with the system defaults are sufficient to establish a connection to the Remote Manager server. The settings in the advanced section allow the connection to be fine-tuned. The parameters described here are concerned with detecting loss of connection. When the router first connects to the Remote Manager server, the link parameters are sent to it. The WAN settings and Ethernet settings described below are identical, but it should be noted in the command line descriptions, the default keepalive intervals are different. This is owing to the different characteristics of PPP and Ethernet links.

Connection Settings

Disconnect when Remote Manager is idle

Once the router has connected to the Remote Manager server, and the server has established that all the settings it holds for the router are current, and no new changes are being requested, the traffic between the router and Remote Manager server reduces to the sending of keep-alive packets. In this situation, it may be advantageous to terminate the connection to reduce bandwidth or to keep data costs down. Enabling this checkbox causes the router to negotiate termination of the connection.

Idle Timeout h hours, m minutes, s seconds

The timeout entered here defines how long the router should wait after detecting the idle condition before negotiating termination of the link. Default is **10** seconds.

WAN Settings

WAN Settings

Remote Manager Management Protocol Keep-Alive Settings:

Receive Interval: 290   seconds   Transmit Interval: 290   seconds

Assume connection is lost after: 3   timeouts

Receive Interval s seconds

The time between keep-alive packets that the router should wait before considering that the connection may be lost.

Transmit Interval s seconds

The interval between transmission of keep-alive packets.

Assume connection is lost after n timeouts

Occasional packet loss is to be expected. This parameter allows for a specified number of lost keep-alive packets before the connection is deemed to have failed.

Ethernet Settings

Ethernet Settings

Remote Manager Management Protocol Keep-Alive Settings:

Receive Interval: 60   seconds   Transmit Interval: 60   seconds

Assume connection is lost after: 3   timeouts

Receive Interval s seconds

The time between keep-alive packets that the router should wait before considering that the connection may be lost.

Transmit Interval s seconds

The interval between transmission of keep-alive packets.

Assume connection is lost after n timeouts

Occasional packet loss is to be expected. This parameter allows for a specified number of lost keep-alive packets before the connection is deemed to have failed.

Related CLI commands

cloud command

Entity	Instance	Parameter	Values	Equivalent Web Parameter
cloud	n	idledisconn	0,1	Disconnect when Remote Manager server is idle 0=Do not disconnect 1=Disconnect
cloud	n	disconnsecs	0-28800	Idle Timeout h,m,s This CLI value is entered in seconds only.
cloud	n	ppprxkeepalive	0-28800	WAN - Receive Interval seconds.
cloud	n	ppptrxkeepalive	0-28800	WAN - Transmit Interval seconds.
cloud	n	pppwaitfor	1-255	WAN - Assume connection is lost after n timeouts.
cloud	n	ethrxkeepalive	0-28800	Ethernet - Receive Interval seconds.
cloud	n	ethtxkeepalive	0-28800	Ethernet - Transmit Interval seconds.
cloud	n	ethwaitfor	1-255	Ethernet - Assume connection is lost after n timeouts.

cloudstat command

There is an additional cloud CLI command, **cloudstat**. Enter this command without parameters to return the status of the socket connections, such as whether there is a live connection to the Remote Manager server.

SNMP parameters

The Simple Network Management Protocol (SNMP) is a well-established way of managing clusters of remote routers. The TransPort routers support versions 1, 2c, and 3 of this protocol.

Supported Management Information Bases (MIBs)

The standard Management Information Bases (MIBs) supported by the router are detailed below. Besides these, there are two other MIBs that are supplied as standard.

- There is a MIB that is generated after the firmware has been installed. This is accomplished using the **mibprint** CLI command and the **MIBEXE** DOS tool, available from the Technical Support Team. This MIB changes with every firmware release, since the firmware revision is embedded in the Object Identifiers (OIDs). This MIB provides access to most of the configuration and statistics that are associated with the router.

- The second MIB is the **Monitor MIB**, which is a standard MIB that gives access to various Digi TransPort proprietary objects. The OIDs in this MIB do not change with every release, although it is possible for new objects to be added to it. This MIB is available from the Technical Support team.

The standard MIBs supported are:

- SNMP MIB (RFC3418)

- Interfaces MIB (RFC2233)*

- IP MIB (RFC2011)

- IP Forwarding Table MIB (RFC2096)

- TCP MIB (RFC2012)

- UDP MIB (RFC2013)

- VRRP MIB (RFC2787)

- SNMP MPD MIB (RFC3412)

- SNMP USM MIB (RFC3414)**

    * The following groups/tables in RFC2233 are not supported: **ifXTable**, **ifStackTable**, **ifRcvAddressTable**.
    ** The following groups/tables in RFC3414 are not supported: **usmUserTable**.
    Other MIBs may be available on request.

Parameter descriptions

Enable SNMPv1

Enables/disables support for version 1 of the protocol.

Enable SNMPv2c

Enables/disables support for version 2c of the protocol.

Enable SNMPv3

Enables/disables support for version 3 of the protocol.

Use UDP Port n

The UDP port number to use. The default is UDP port **161**.

SNMPv3 Engine ID

This is required as part of the SNMP v3 protocol. This is a 24-hexadecimal character string; any trailing zeroes in this string making the value up to 24 characters can be omitted. A remote engine ID is required when a SNMP v3 Inform is configured. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
snmp	n	v1enable	0,1	Enable SNMPv1 0=Off 1= On
snmp	n	v2cenable	0,1	Enable SNMPv2c 0=Off 1=On
snmp	n	v3enable	0,1	Enable SNMPv3 0=Off 1=On
snmp	n	port	0-65535	Use UDP Port Default=**161**
snmp	n	engineid	String	SNMPv3 Engine ID

SNMP User parameters

This page controls the configuration of the SNMP users.

SNMPv1 / SNMPv2c

Community

The text in this text entry box specifies the community string for Version 1 and Version 2c SNMP packets.

Confirm Community

The community string is echoed as dots in the text entry box. Having a second confirmation field where the string is retyped allows a simple check to be performed for correct entry.

SNMPv3

Username

This field is the name of the SNMP user.

Authentication None, MD5, SHA1

These three radio buttons select what authentication algorithm is to be applied to the SNMP transactions.

Authentication Password

The authentication password for the user.

Confirm Authentication Password

The authentication password is not shown as clear text. The confirmation box allows a simple check that the password has been entered correctly.

Encryption None, DES, AES

These three radio buttons select which encryption (privacy) algorithm should be applied to the SNMP data.

Encryption Password

The user's password that is used to control the privacy of the SNMP transactions is entered into this text entry box.

Confirm Encryption Password

The encryption password is not shown as clear text. The confirmation box allows a simple check that the password has been entered correctly.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
snmpuser	n	community	public / private	Community
snmpuser	n	name	**user_name**	Username
snmpuser	n	auth	Off,MD5,SHA1	Authentication, None, MD5, SHA1
snmpuser	n	authPassword	**my_password**	Authentication Password
snmpuser	n	priv	Off,DES,AES	Encryption, None, DES, AES
snmpuser	n	privPassword	**my_password**	Encryption Password

SNMP Filter parameters

SNMP filters allow the system administrator to control access to the router MIBs via SNMP. This functionality is controlled by a table on the web configuration page. This table has three columns, two main headed columns as described below and a control column containing button widgets. The table has a capacity of ten entries, SNMP filter instances range from **0** to **9**.

Username

The username (as configured in the **Configuration > Security > Users** section) of the user to whom the access restriction is applied.

OID Prefix

The Object ID (OID) prefix for the range of objects in the MIB that the user is not allowed to view. such as **1.3.6.1.2.1.4**.

Add

Adds the username and OID prefix into the table.

Delete

Deletes the associated entry in the table.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
snmpfilter	n	user	username	Username.
snmpfilter	n	oid	Valid SNMP OID	OID Prefix.

SNMP Trap parameters

SNMP traps are events that are generated when the specified condition is met. The web page and CLI configuration parameters are described here. The TransPort routers support two trap servers.

Generate Enterprise traps

When this check box is enabled, the router will generate product-specific traps.

Generate Generic traps

SNMP specifies several generic traps (**Cold Start**, **Warm Start**, **Link Down**, **Link Up**, etc). When this checkbox is ticked, generic traps are generated.

Generate Authentication Failure traps

Enables the generation of authentication failure traps.

Generate VRRP traps

Checking this checkbox enables the generation of VRRP traps. For details on VRRP configuration, see Ethernet VRRP Parameters on page 165.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
snmp	n	enterprisetraps	0,1	Generate Enterprise traps 0=Off 1=On
snmp	n	generictraps	0,1	Generate Generic traps 0=Off 1=On
snmp	n	authtraps	0,1	Generate Authentication traps 0=Off 1=On
snmp	n	vrrptraps	0,1	Generate VRRP traps 0=Off 1=On

SNMP Trap Server parameters

Digi TransPort routers support two SNMP trap servers. The following options and description explain how to configure a trap server.

Trap Server IP Address a.b.c.d

The IP address of the server running the SNMP software and determines the destination for the trap notifications.

Port n

The UDP port number that the SNMP server is listening on, the default is **162**, which is the standard port number for this service.

Use SNMP Version

Select the required SNMP version number from this drop-down selection box.

Send "Inform Request" message

If SNMP version 2c or 3 is selected, the router can send a SNMP **Inform Request** message instead of a **Trap** message. **Inform Request** messages are acknowledged by the SNMP Trap server whereas **Trap** messages are not.

If no response, retransmit the Inform Request message after n seconds

The period after which the **Inform Request** message is retransmitted if no response has been received.

Retransmit a maximum n times

The maximum number of times an **Inform Request** message is retransmitted. If no acknowledgment is received after the maximum number of retransmissions, an event is logged.

Community

Enter the desired community string into this text entry box.

Confirm Community

Entering the community string again here enables verification of the string since the string is not displayed.

Trap Server Engine ID

This item will be configured within the application and is the SNMP server software engine ID which is used for authentication and encryption.

SNMP User

The username that should be associated with the trap server. This should match a user from one of the previously configured SNMP users (**Configuration > Remote Management > SNMP > Users**).

User Security Level

Select the desired security level from this drop-down selection box. The choices are these:

- **No Authentication, No Privacy**
- **Authentication, No Privacy**
- **Authentication, Privacy**

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
snmptrap	n	IPaddr	Valid IP address such as **1.2.3.4**	Trap Server IP Address **a.b.c.d**
snmptrap	n	port	0-65535	Port Default=**162**
snmptrap	n	version	v1, v2c, v3	Use SNMP Version
snmptrap	n	sendInforms	on | off	Send "Inform Request" messages
snmptrap	n	informto	Integer	If no response, retransmit the Inform Request message after n seconds
snmptrap	n	informretries	Integer	Retransmit a maximum **n** times
snmptrap	n	community	String	Community
snmptrap	n	engineid	String	Trap Server Engine ID
snmptrap	n	securityname	String	SNMP User
snmptrap	n	securitylevel	noauthnopriv authnopriv authpriv	User Security Level noauthnopriv=No Authentication, No Privacy authnopriv=Auth, No Priv authpriv=Auth & Priv

Configure security settings

This section covers the configuring security settings from the web interface and command line. It covers the following topics:

System security settings

To configure system security settings, go to **Configuration > Security> System**.

This page allows you to configure the USB and miscellaneous security.

Disable the following USB devices

This parameter provides an option of enabling or disabling any of the following USB devices:

- **All devices**
- **Mass storage devices**
- **Serial devices**
- **Hub devices**

Allow autoexec.bat files to run from Mass Storage Devices

Enables/disables running the **autoexec.bat** files from the mass storage devices.

Enable "Factory Default" reset button

Enables/disables execution of a complete hardware reset.

Users security settings

User parameters

To configure system security settings, go to **Configuration > Security> User**.

The **User** parameter pages allow you to configure a number of authorized users. The number of users available depends on the firmware build the router is running. Each user has a password and access level that determines the facilities to which the user has access.

Username

The name of the user. Up to 14 characters are allowed. There are some special usernames that can also be used, these are:

Username	Description
%s	Uses the serial number of the router as the username.
%i	Uses the IMEI of the cellular module as the username.
%c	Uses the ICCID of the SIM as the username.

If a **%** symbol is part of the username, it must be escaped with another '%' symbol. For example **user%1** should be entered as **user%%1**.

Password / Confirm Password

The password for the user. Up to 14 characters are allowed.

Access Level

Selects the access level for the user. There are the following options:

Access level	Access allowed
Super	Allows full access to all facilities.
High	Allows user to reconfigure the general configuration of the router and to change some settings such as the time and date. Not allowed to change user settings.
Medium	Allows user to access medium level configuration commands which allow some configuration of the router.
Low	Allows user to access low level commands which tend to be status and statistics commands.
Read Only	Read only access of the configuration.
None	User is not allowed to login via Web, FTP, SSH, and Telnet.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
user	0	name	String (up to 40 chars)	Username
user	0	password	String (up to 40 chars)	Password
user	0	access	0=Super 1=High 2=Medium 3=Low 4=None 8=Read Only	Access Level

Change the default username and password for a user

By default, the username for each supported user is **username** and the password is **password**. To increase security, change the username and password for device users from these defaults.

Note Record the new password. If the changed password is lost, the router must be reset to the default firmware settings.

In the web interface:

1. From the Main menu, navigate to **Configuration > Security> Users> User n**.

2. In the **Username** field, enter the new user name. Up to 14 characters are allowed in a username. For additional details on the username, see User parameters on page 646.

3. In the Password / Confirm Password field, enter the new password. For additional details on the password, see User parameters on page 646.

4. Select the access level for the user: **Super**, **High**, **Medium**, **Low**, **Read Only,** or **None**. Descriptions of these access levels is in User parameters on page 646.

5. Click **Apply**.

From the command line:

Issue the **user** command, specifying the **name**, **password**, and **access** parameters.

Advanced user settings

To configure system security settings, go to **Configuration > Security> Users> User n> Advanced**.

Allow this user to log in over a PPP network

Enabling this setting allows the user to log in to the router using PPP. Disabling this disables PPP login for the user, no matter their access level.

Use this number x when PPP dial-back is required for this user

The telephone number for the user in the event that dial-back is required. If the username that the remote router uses during the PPP authentication matches the username of the user where a dial-back number is configured, the user's dial-back number overrides any dial-back number configured in the answering PPP interface.

Alternate IKE Key / Confirm Alternate IKE Key

When IKE is the initiator, the responder-supplied HASH is checked using the normal password (above) and if that fails, the Alternate Key (this setting). The initiator remembers which password was successful, and uses that password to create the HASH if it becomes the responder of some new negotiation. If the IKE becomes a responder and IKE negotiations fail after supplying the HASH, the other password is used during the next negotiation. Using this Alternate Key, it should be possible to configure new passwords into both ends of a tunnel, and not have too many failed negotiations. The process would be to add the Alternate Key into the remote router, then update the local router with the Alternate Key. Once that has been done, the administrator could move the Alternate Key to the usual location (**Password**) and remove the Alternate Key (**newpwd**) from the configuration. Should a negotiation take place during the period where the Alternate Key has been entered into the remote router, but not the local router, there should be no more than one failed negotiation, and only if the remote router is the initiator.

Remote Peer IP address

In certain circumstances, it may be desirable for a user connecting in over a PPP connection to be allocated a specific IP address, rather than be allocated an address from a pool configured on a PPP interface. When this parameter is configured, the IP address negotiated on the PPP link will be this one, not an address from the regular IP address pool.

Remote Peer IP subnet

If multiple PPP interfaces are enabled for answering and multiple remote routers can dial into the local router, static routes cannot always be used to ensure that packets which should be routed to the remote network are sent through the correct PPP interface. This parameter can be used in conjunction with the **Remote Peer IP subnet mask** parameter to associate a network subnet with a user. When a remote unit connects in and authenticates with the router, the router creates a dynamic route that will override any static routes for the duration of the PPP session. The interface for the dynamic route is the PPP interface that answered the call. The network address for the dynamic route is taken from the entry in the user table that matches the username that the remote unit used during the PPP authentication.

Remote Peer IP subnet mask

The remote subnet mask parameter is used in conjunction with the **Remote Peer IP subnet** parameter above to fully qualify the network address for the user.

Public Key file

The name of the file containing the public key for that user. If the public key matches the client supplied public key, the user is allowed access.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
user	0	dun_en	on, off	Allow this user to log in over a PPP network
user	0	phonenum	Number	Use this number x when PPP dial-back is required for this user
user	0	newpwd	String (up to 14 chars)	Alternate IKE Key
user	0	fieldip	IP Address	Remote Peer IP address
user	0	ipaddr	IP Address	Remote Peer IP subnet
user	0	mask	IP Mask	Remote Peer IP subnet mask
user	0	keyfile	Filename	Public Key file

Firewall configuration

To configure firewall settings, go to **Configuration > Security> Firewalls**.

About firewalls

All Digi TransPort routers incorporate a comprehensive firewall facility. A firewall is a security system that is used to restrict the type of traffic that the router will transmit or receive based on a combination of IP address, service type, protocol type, port number and IP flags. Firewalls are used to minimize the risk of unauthorized access to the local network resources by external users or to restrict the range of external resources to which local users have access. A more detailed description of how firewalls operate on Digi routers is given in "Firewall scripts on page 655". Refer to this section before attempting to implement a firewall.

The rules governing the operation of the firewall are contained in a pseudo-file called **fw.txt**. This file can be created either by using the controls in the web page described below or by using a text editor on a PC and then loading the resulting file onto the router using FTP or XMODEM. Digi Routers are shipped with a default **fw.txt** file that can be used as the starting point for a custom firewall configuration.

Firewall parameters

On the **Configuration > Security> Firewalls** page, firewall configuration done using settings in the table described below. There are three other buttons that appear just below the table. Their use will also be described.

Since a default file is supplied, when this page loads it will show the rules in the default **fw.txt** file. If **fw.txt** does not exist, a blank table will be shown.

Hits

The numbers that appear in this column of the table are the number of hits for the rule that appears to the right.

#

This is non-editable and is simply the rule number.

Delete

Clicking this button deletes the rule that appears to its left.

Insert

These buttons are used to insert new lines. The insert buttons that appear alongside existing rules insert new blank lines above the line on which they appear. The button at the bottom creates a new blank line at the end of the table. (An empty table will only have the one button at the bottom). To create a new rule, click the button at the point the new rule should appear and a new text box should appear. Type the rule into the text box and once complete, click the **OK** button. To abandon any changes click the **Cancel** button. Once the **OK** button has been clicked the firewall task will validate the rule and if valid, will add it the table. If errors are detected, a warning message will be displayed, at which point the rule may be edited or deleted.

Edit

These buttons that appear to the right of the rule open up the rule in an edit text box which allows the text to be edited. Click on the **OK** button to commit the changes or **Cancel** to abandon the edit.

Reset Hit Counters

Clicking this button resets to zero all the rule hit counts that appear in the left-hand column of the table.

Save

Clicking this button saves changes to the table to the **fw.txt** file. If the changes are not saved using this button, they will be lost if the router is rebooted or loses power.

Restore

If, after reviewing changes to the table it is decided that the edit should be abandoned, clicking this button restores the original **fw.txt** to the table, provided that they have not been saved.

Below the firewall editor table is another table that controls the interfaces to which the firewall rules apply.

Interface

A list of the available interfaces to which the firewall rules may be applied.

Enabled

Check the checkbox next to the interface(s) that the firewall should operate on to enable the firewall for that interface.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
fw	n/a	logclr	-	Reset Hit Counters
fw	n/a	save	-	Save
fw	n/a	-	-	Restore

The firewall rule hits may be viewed from the command line console by using the command:

```
type fwstat.hit
```

Stateful Inspection Settings parameters

Stateful inspection settings are configured on the **Configuration > Security> Firewalls> Stateful Inspection Settings** page. This page contains timer timeout values and other options used by the firewall stateful inspection module. This module establishes firewall rules that last for a single connection only. Typically, the first packet of a TCP connection (SYN packet) is used to create a stateful inspection rule that only allows subsequent packets for that TCP connection through the firewall. The timers described below set limits on how long such rules persist.

Timers

TCP Opening s seconds

The time following receipt of a TCP packet that causes a stateful inspection rule to be created before a TCP connection must be established. If a TCP connection is not established within this period, the associated stateful rule is removed.

TCP Open s seconds

The time an established TCP connection can remain idle before the stateful inspection rule created for it is removed. The timer is restarted each time a packet is processed by the associated stateful inspection rule.

TCP Closing s seconds

The time allowed for a TCP socket to close once the first FIN packet has been received. If the timer expires before the socket has completed closing, the stateful inspection rule is removed.

TCP Closed s seconds

The time that a stateful inspection rule remains in place after a TCP connection has closed.

UDP s seconds

The time that a stateful inspection rule remains in place following the receipt of UDP packet. The timer is restarted each time packets matching the rule pass in each direction. As a consequence, rules based on UDP should only be used if it is anticipated that packets will travel in both directions.

ICMP s seconds

Some ICMP packets, such as the ECHO request, generate response packets. The value in this text box specifies the length of time that a stateful inspection rule created for an ICMP packet will remain in place if the response is not received. The rule is removed immediately following receipt of the response.

Other protocols s seconds

If a stateful inspection rule is created from a packet type other than TCP, UDP or ICMP, a rule timeout should be created for it. The parameter in this text box specifies the length of time such a rule persists. The timer is restarted each time a packet is processed by the rule.

Other Options

Expire entry after n consecutive packets in one direction

The maximum number of consecutive packets that should pass in one direction before the corresponding rule entry is expired.

Count missed UDP echo packets as dropped

When checked, this checkbox causes the firewall to increment the dropped packet count for each failed echo request in the situation where UDP echo is active on an interface that becomes disconnected.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
fwall	0	opening	0-4294967296	TCP Opening s seconds
fwall	0	open	0-4294967296	TCP Open s seconds
fwall	0	closing	0-4294967296	TCP Closing s seconds
fwall	0	closed	0-4294967296	TCP Closed s seconds
fwall	0	udp	0-4294967296	UDP s seconds
fwall	0	icmp	0-4294967296	ICMP s seconds
fwall	0	other	0-4294967296	Other protocols s seconds
fwall	0	maxuni	0-2147483647	Expire entry after n consecutive packets in one direction
fwall	0	cntmissedecho	OFF,ON Default OFF	Count missed UDP echo packets as dropped

Firewall scripts

A firewall is a protection system designed to prevent your local area network from unauthorized external access by other users of the Internet or another wide area network. It can also limit the degree of access local users have to external network resources. A firewall does not provide a complete security solution; it provides only one element of a fully secure system. Consider using additional security methods, such as user authentication and data encryption. Refer to the IPSec section for further information.

A firewall is a packet filtering system that allows or prevents the transmission of data (in either direction) based on a set of rules. These rules allow filtering based on the following criteria:

- Source and destination IP addresses
- Source and destination IP port or port ranges
- Type of protocol in use
- Direction of the data (in or out)
- Interface type
- The eroute the packet is on
- Whether an interface is OOS (out of service)
- ICMP message type
- TCP flags (**SYN**, **ACK**, **URG**, **RESET**, **PUSH**, **FIN**)
- TOS field
- Status of a link and/or data packets on UDP/TCP and ICMP protocols

Besides providing comprehensive filtering facilities, Digi TransPort routers support rules relating to the logging of information for audit/debugging purposes. This information can be logged to a pseudo-file on the router called **FWLOG.TXT**, the **EVENTLOG.TXT** pseudo-file or to a syslog server, and can also be used to generate SNMP traps.

Firewall Script syntax

A firewall must be individually configured to match the needs of authorized users and their applications. On Digi routers, the rules governing firewall behavior are defined in a script file called **FW.TXT**. Each line in this file consists of a label definition, a comment or a filter rule.

Labels

A label definition is a string of up to 12 characters followed by a colon. Labels can only include letters, digits and the underscore character. They used with the break option to cause the processing of the script to jump to a new location.

Comments

Any line starting with the hash character (**#**) is considered a comment and is ignored.

Filter rules

The syntax for a filter rule is:

`[action] [in-out] [options] [tos] [proto] [dnslist] [ip-range] [inspect-state]`

- When the firewall is active, the script is processed one line at a time as each packet is received or transmitted.

- Even when a packet matches a filter-rule, processing still continues and all the other filter rules are checked until the end of the script is reached.

- The action taken on a particular packet is that specified by the last matching rule.

- With the break option, the script processing can be redirected to a new location or to the end of the script if required.

- The default action that the firewall assigns to a packet is to block. This means if the packet does not match any of the rules, it is blocked.

Firewall script rule fields

Firewall script rule fields are as follows:

[action]

Can be specified as **block**, **pass**, **pass-ifup**, **dscp**, **vdscp**, or **debug**. These operate as follows:

block

Prevents a packet from being allowed through the firewall. When block is specified, an optional field can be included that causes an ICMP packet to be returned to the interface from which that packet was received. This technique is sometimes used to confuse hackers by having different responses to different packets or for fooling an attacker into thinking a service is not present on a network.

The syntax for specifying the return of an ICMP packet is:

`"return-icmp" [icmp-type [icmp-code]]`

where **[icmp_type]** is a decimal number representing the ICMP type, or one of the predefined text codes listed in the following table:

ICMP type value	ICMP type
1	Unreach
2	Echo
3	Echorep
4	squench
5	redir
6	timex
7	paraprob
8	timest
9	timestrap
10	inforeq
11	inforep
12	maskreg
13	maskrep
14	routerad
15	routersol

The optional **[icmp-code]** field can also be a decimal number representing the ICMP code of the return ICMP packet but if the **[icmp-type]** is **[unreach]**, then the code can also be one of the following pre-defined text codes:

ICMP code	Meaning
net-unr	Network unreachable
host-unr	Host unreachable
proto-unr	Protocol unrecognized
port-unr	Port unreachable
needfrag	Needs fragmentation
srcfail	Source route fail

For example:

```
block return-icmp unreach in break end on ppp 0
```

This rule causes the router to return an ICMP Unreachable packet in response to all packets received on PPP **0**.

Instead of using the **return-icmp** option to return an ICMP packet, you can use **return-rst** to return a TCP reset packet instead. This would only be applicable for a TCP packet. For example:

```
block return-rst in break end on eth 0 proto tcp from any to 10.1.2.0/24
```

This would return a TCP reset packet when the firewall receives a TCP packet on the Ethernet interface 0 with destination address **10.1.2.***.

pass

Allows packets that match the rule to pass through the firewall.

pass-ifup

Allows outbound packets that match the rule to pass through the firewall but only if the link is already active.

debug

Causes the router to tag any packets matching the rule for debug. This means that for every matching rule that is encountered from this point in the script onwards, an entry will be placed in the pseudo-file **FWLOG.TXT**.

dscp

Causes any packets matching this rule to have its DSCP value adjusted according to this rule. The DSCP value of a packet indicates the type of service required and is used in conjunction with QOS (Quality of Service) functions. A decimal or hex number must follow the dscp keyword to indicate the value that should be set.

vdscp

Similar to the **dscp** action as described above, in that it adjusts the DSCP value in a packet. The difference is that this is a virtual change only, which means that the actual packet is not changed, and that the packet is processed as if it had the DSCP value as indicated. Like the **dscp** action, a decimal or hexadecimal number must follow.

[in-out]

The **[in-out]** field can be in or out and is used to specify whether the action applies to inbound or outbound packets. When the field is left blank, the rule is applied to any packet irrespective of its direction.

[options]

Used to define a number of options that may be applied to packets matching the rule. These are:

log

When the **log** option is specified, the router places an entry in the **FWLOG.TXT** file each time it processes a packet that matches the rule. This log normally details the rule that was matched along with a summary of the packet contents.

- If the log option is followed by the **body** sub-option, the complete IP packet is entered into the log file so when the log file is displayed, a more detailed decode of the IP packet is shown.

- The **log** field can also be followed by a further sub-option that specifies a different type of log output. This may either be **snmp**, **syslog**, or **event**. If **snmp** is specified, an SNMP trap (containing similar information to the normal log entry), is generated when a packet matches the rule. If **syslog** is specified, a syslog message is sent to the configured syslog manager IP address. This message contains the same information as that entered into the log file, but in a different format.

- If the **body** option has also been specified, some of the IP packet information is also included.

- The size of the syslog message is limited to a maximum of **1024** bytes.

- The syslog message is sent with default priority value of **14**, which expands out to facility of **USER**, and priority **INFO**.

- If **event** is specified, the log output is copied to the **EVENTLOG.TXT** pseudo-file and the **FWLOG.TXT** file.

- The event log entry contains the line number and hit count for the rule that caused the packet to be logged.

Example:

Suppose your local network is on subnet **192.168.*.*** and you want to block any packets received on **PPP 0** that were pretending to be on the local network, and log the receipt of any such packets to the **FWLOG.TXT** file and to a syslog server. The filter rule is constructed as follows:

```
block in log syslog break end on ppp 0 from 192.168.0.0/16 to any
```

> break

When the **break** option is specified it must be followed by a user-defined label name or the predefined end keyword. When followed by a label, the rule processor jumps to that label to continue processing. When followed by the **end** keyword, rule processing is terminated and the packet is treated according to the last matching rule.

Example:

```
break ppp_label: on ppp 0
# insert rule processing here for packets that are not on ppp 0
break end
ppp_label:
# insert rule processing here for packets that are on ppp 0
```

> on

The interface to which the rule applies; must be followed by a valid interface name. For example, if you were only interested in applying a particular rule to packets being transmitted or received by **PPP 0**, you would include **ppp 0** in the rule. Valid interface-names are **eth n**, **tun n** or **ppp n**, where **n** is the instance number.

> oneroute

A rule will only match packets associated with the specified eroute. For example, including the option **oneroute 2** causes the rule to only match on packets transmitted or received over Eroute 2. The **oneroute** option can be followed with the keyword **any**, which will match if the packet is on any eroute.

> routeto

When the **routeto** option is specified and the firewall is processing a received packet, if the rule is the last matching rule, the packet is tagged as being required to be routed to the specified interface.

Example

The following filter rule ensures all packets from **10.1.*.*** to **1.2.3.4** on the **telnet** port are all routed to **ETH 1**.

```
pass in break end routeto eth 1 from 10.1.0.0/16 to 1.2.3.4 port=telnet
```

oosed

Used to check the out of service status of an interface. For example, including the option **oosed ppp 1** would cause the rule to match only if interface **PPP 1** is out of service.

[tos]

Used to specify the Type of Service (TOS) to match. If included, the **[tos]** field consists of the keyword **tos** followed by a decimal or hexadecimal code, identifying the TOS to match. For example, to block any inbound packet on **PPP 0** with a TOS of **0**, you would use a rule such as:

```
block in on ppp 0 tos 0
```

[proto]

Used to specify a protocol to match and consists of the **proto** keyword followed by one of the following protocol identifiers:

Identifier	Meaning
udp	UDP packet
tcp	TCP packet
ftp	FTP packets regardless of port number
icmp	ICMP packet
decimal number	decimal number matched to protocol type in IP header

The **[proto]** field is also important when stateful inspection is enabled for a rule (using the **[inspect-state]** field), as it describes the protocol to inspect (see **[inspect-state]** below).

[dnslist]

Used to match packets containing DNS names in a given dnslist. Following **dnslist**, there needs to be a name of a DNS list as specified by the **#dns** command.

For example, consider the following DNS list:

```
#dns gglist www.Digi.co.*,www.*.co.nz
```

The following firewall rule blocks all DNS lockups to DNS names matching the above list:

```
block out break end on ppp 1 proto udp dnslist gglist from any to any port=dns
```

[ip-range]

The range of IP addresses and ports to match upon and may be specified in one of several ways. The basic syntax is:

```
ip-range="all" | "from" ip-object "to" ip-object [flags] [icmp]
```

where **ip-object** is an IP address specification. For full details of the syntax with examples, see Specifying IP Addresses and ranges on page 662.

[inspect-state]

Used in create rules for stateful inspection. This is a powerful option in which the firewall script includes rules that allow the router to keep track of a TCP/UDP or ICMP session and therefore to only pass packets that match the state of a connection.

Additionally, the **[inspect state]** field can specify an optional OOS (Out Of Service) parameter. This parameter allows the router to mark any route as being out-of-service for a given period of time in the event that the stateful inspect engine has detected an error.

A full description of how the **[inspect state]** field works is given below under the heading Stateful Inspection Settings parameters on page 653.

Specifying IP Addresses and ranges

The **ip-range** field of a firewall script rule identifies the IP address or range of addresses to which the rule applies. The syntax for specifying an IP address range is:

```
ip-range = "all" | "from" ip-object "to" ip-object [ flags ] [ icmp ]
where:
ip-object = addr [port-comp | port-range]
flags = "flags" { flags } [ !{ flags } ]
icmp = "icmp-type" icmp-type [ "code" decnum ]
addr = "any" | ip-addr[ "/"decnum ] [ "mask" ip-addr | "mask" hexnum ]
port-comp = "port" compare port-num
port-range = "port" port-num "<>" | "><" port-num
ip-addr = IP address in format nnn.nnn.nnn.nnn
decnum = a decimal number
hexnum = a hexadecimal number
compare = "=" | "!=" | "<" | "<=" | ">" | ">="
port-num = service-name | decnum
service-name = "http" | "telnet" | "ftpdat" | "ftpcnt" | "pop3" | "ike" | "xot"| "sntp" |
"smtp"
```

In the above syntax definition:

• Items in quotes are keywords.

• Items in square brackets are optional.

• Items in curly braces are optional and can be repeated.

• The vertical bar symbol ("|") means **or**.

An **ip-object** consists of an IP address and an IP port specification, preceded by the keyword from or to define whether it is the source or destination address. The most basic form for an **ip-object** is an IP address preceded **by** from or **to**. For example, to block all packets destined for address 10.1.2.98 the script rule is:

```
block out from any to 10.1.2.98
```

An **ip-object** can also be specified using an address mask. This is a way of describing which bits of the IP address are relevant when matching. The script processor supports two formats for specifying masks.

- **Method 1**: The IP address is followed by a forward slash and a decimal number. The decimal number specifies the number of significant bits in the IP address. For example, if you wanted to block all packets in the range **10.1.2.*** the rule would be:

  ```
  block from any to 10.1.2.0/24
  ```

  such as, only the first 24 bits of the address are significant.

- **Method 2**: This same rule could be described another way using the mask keyword:

  ```
  block from any to 10.1.2.0 mask 255.255.255.0
  ```

The IP address can also contain either **addr-ppp n** or **addr-eth n**, where **n** is the **eth** or **ppp** instance number. In this case, the rule specifies that the IP address is that allocated to the PPP interface or to the Ethernet interface. This is useful when IP addresses are obtained automatically and therefore are not known by the author of the filtering rules. For example:

```
block in break end on ppp 0 from addr-eth 0 to any
```

Address/Port translation

One further option for specifying addresses is to use address translation. The syntax for this is:

```
srcdst = "all | fromto [-> [ip-object] "to" object]
```

such as, directly after the IP addresses and port are specified an optional **->** can follow, indicating that the addresses/ports should be translated. The first source object is optional, and is unlikely to be used, as it is more normal to translate the destination address.

The following example reroutes packets originally destined for **10.10.10.12** to **10.1.2.3**:

```
pass out break end from any to 10.10.10.12 -> to 10.1.2.3
```

In addition, complete subnets can have NAT applied. The address bits not covered by the subnet mask are taken from the original IP address. For example, to NAT the destination subnet of **192.168.0.0/24** to be **192.168.1.0/24**, the firewall rule is:

```
pass out break end from any to 192.168.0.0/24 -> to 192.168.1.0/24
```

Filtering on port numbers

Suppose a Telnet server is running on a machine on IP address **10.1.2.63**, and you want to make this accessible. The filter from the previous example blocks all packets to **10.1.2.***. To make the Telnet server available on **10.1.2.63**, add the following line before the blocking rule:

```
pass break end from any to 10.1.2.63 port=23
```

A packet sent to the Telnet server (port **23**) on IP address **10.1.2.63** matches this rule, and further checking is prevented by the break end option.

The above example illustrates the `=` comparison. Other comparison methods supported are:

Symbol	Meaning
!=	not equal
>	greater than
<	less than
<=	less than or equal to
>=	greater than or equal to

You can also specify a port in range or a port out of range with the `><` or `<>` symbols. For example, to pass all packets to addresses in the range **23** to **28**, the rule is:

```
pass break end from any to 10.1.2.63 port 23><28
```

To simplify ports references, some commonly used port numbers are associated with the predefined strings, listed in the table below. For example, in the example above, if we substitute the number **23** with the string **telnet**, the rule would be:

```
pass break end from any to 10.1.2.63 port=telnet
```

Other port keywords that are defined are as follows. The service keywords are predefined based on standard port numbers. These port numbers may have been defined differently on your system, in which case you should use the port numbers explicitly, and not the defined names.

Keyword	Std. Port	Service
Ftpdat	20	File Transfer Protocol data port
Ftpcnt	21	File Transfer Protocol control port
telnet	23	Telnet server port
smtp	25	SMTP server port
http	80	Web server port
pop3	110	Mail server port
sntp	123	NTP server port
ike	500	Source/destination port for IKE key
xot	1998	Destination port for XOT packets

Filtering on TCP flags

An **ip-object** can be followed by an optional **[flags]** field.

[flags]

Allows the script to filter based on any combination of TCP flags. The **[flags]** field is used to specify the flags to check and consists of the flags keyword followed by a string specifying the flags themselves. Each letter in this string represents a particular flag type as listed below:

Code	Flag
f	FIN Flag
r	RESET Flag
s	SYN Flag
p	PUSH Flag
u	URG Flag
a	ACK Flag

These flag codes allow the filter to check any combination of flags.

Following on from the previous example, to block packets that have all the flags set you would need to precede the pass rule with the following block rule:

```
block break end from any to 10.1.2.0/24 port=telnet flags frspua
```

Here, the list of flags causes the router to check that those flags are set. This list may be optionally followed by an exclamation mark (**!**) and a second list of flags that the router should check for being clear.

For example. the following **[flags]** field tests for the **s** flag being on and the **a** flag being off with all other flags ignored.

```
flags s!a
```

As a further example, suppose we want to allow outward connections from a machine on **10.1.2.33** to a Telnet server. We have to define a filter rule to pass outbound connections and the inbound response packets. Because this is an outbound Telnet service we can make use of the fact that all incoming packets will have their **ACK** bits set. Only the first packet establishing the connection will have the **ACK** bit off. The filter rules to do this would look like this:

```
pass out break end from 10.1.2.33 port>1023 to any port=telnet
```

```
pass in break end from any port=telnet to 10.1.2.33 port>1023 flags !a
```

The first rule allows the outward connections, and the second rule allows the response packets back in which the **ACK** flag must always be on. This second rule will filter out any packets that do not have the **ACK** flag on. This will bar any attackers from trying to open connections onto the private network by simply specifying the source port as the Telnet port. Note that there is a simpler way to achieve the same effect using the inspect state option, described below.

Filtering on ICMP codes

An **ip-object** can be followed by an optional **[icmp]** field.

[icmp]

This field allows the script to filter packets based on ICMP codes. ICMP packets are normally used to debug and diagnose a network and can be extremely useful. However, they form part of a low-level protocol and are frequently exploited by hackers for attacking networks. For this reason, most network administrators will want to restrict the use of ICMP packets.

The syntax for including ICMP filtering is:

```
icmp = "icmp-type" icmp-type ["code" decnum]
```

icmp-type

Can be one of the pre-defined strings listed in the following table or the equivalent decimal numeric value:

ICMP Type	ICMP Value
Unreach	3
Echo	8
Echorep	0
Squench	4
Redir	5
Timex	11
Paramprob	12
Timest	13
Timestrep	14
Inforeq	15
Inforep	16
Maskreq	17
Maskrep	18
Routerad	9
Routersol	10

The following two rules are therefore equivalent:

```
pass in break end on ppp 0 proto icmp from any to 10.1.2.0/24 icmp-type 0
```

```
pass in break end on ppp 0 proto icmp from any to 10.1.2.0/24 icmp-type echorep
```

Both of these rules allow echo replies to come in from interface **ppp 0** if they are addressed to our example local network address (**10.1.2.***).

In addition to having a type, ICMP packets also include an ICMP code field. The filter syntax allows for the specification of an optional code field after the ICMP type. When specified the code field must also match. The ICMP code field is specified with a decimal number.

For example, suppose we wish to allow only echo replies and ICMP unreachable type ICMP packets from interface **ppp 0**. Then the rules would look something like this:

```
pass in break end on ppp 0 proto icmp from any to 10.1.2.0/24 icmp-type echorep code 0
```

```
pass in break end on ppp 0 proto icmp from any to 10.1.2.0/24 icmp-type unreach code 0
```

```
block in break end on ppp 0 proto icmp
```

The first two rules in this set allow in the ICMP packets that we are willing to permit and the third rule denies all other ICMP packets in from this interface. Now if we ever expect to see echo replies in on **ppp 0**, we should allow echo requests out on that interface too. To do that we would have the rule:

```
pass out break end on ppp 0 proto icmp icmp-type echo
```

Stateful inspection

The Digi routing code stack contains a sophisticated scripted Stateful Firewall and Route Inspection engine. Stateful inspection is a powerful tool that allows the router to keep track of a TCP/UDP or ICMP session and match packets based on the state of the connection on which they are being carried. In addition to providing sophisticated Firewall functionality the SF/RI engine also provides a number of facilities for tracking the health of routes, marking dead routes as being Out Of Service (OOS) and creating rules for the automatic status checking of routes previously marked as OOS (for use in multilevel backup/restore scenarios).

The firewall can be used to place interface into an OOS state and also control how the interfaces return to service. When an interface goes OOS, all routes configured to use that interface will have their route metric set to **16** (the maximum value), meaning that some other route with a lower metric will be selected.

When a firewall stateful inspection rule expires, a decision is made as to whether the traffic being allowed to pass by this rule completed successfully or not. For example, if the stateful rule monitors **SYN** and **FIN** packets in both directions for a TCP socket then that rule will expire successfully. However, if **SYNs** are seen to pass in one direction but no **SYNs** pass in the other direction, the stateful rule will expire and the router will tag this as a failure.

Conditions tagging a stateful rule as a failure

The following conditions tag a stateful rule as a failure:

- Packets have only passed in one direction.
- 10 packets have passed in one direction with no return packets (for TCP the packets must also be re-transmits) All of these features depend upon the stateful inspection capabilities of the Firewall engine which are explained below.

The [inspect] field

The **[inspect]** field takes the following format:

```
inspect = [“inspect-state” {“oos” {interface-name¦logical-name} secs {t=secs} {c=count}
{d=count}} {r=“ping”¦“tcp”{,secs{secs}}} {rd=x} {dt=secs}{stat}]
```

The field can be used on its own or with an optional **oos** (Out Of Service) parameter.

How stateful rules can improve firewall security

To better understand how to use stateful inspection, consider a simple example of setting up a filter to allow all machines on a local network with addresses in the range **10.1.2.*** to access the Internet on port **80**. This example requires one rule to filter the outgoing packets, and another to filter the responses. The rules are:

```
pass out break end on ppp 0 from 10.1.2.0/24 to any port=80
pass in break end on ppp 0 from any port=80 to 10.1.2.0/24
```

In this example

- The first rule allows outgoing HTTP requests on PPP 0 from any address matching the mask **10.1.2.*** providing that the requests are on port **80** (the normal port address for HTTP requests).
- The second rule allows HTTP response packets to be received on PPP 0 providing they are on port **80** and they are addressed to an IP address matching the mask **10.1.2.***.

However, rule 2 creates a potential security hole. The problem with filtering based on the source port is that you can trust the source port only as much as you trust the source machine. For example, an attacker could perform a port scan and provided the source port was set to **80** in each packet, it would get through this filter. Alternatively, on an already compromised system, a Trojan horse might be set up listening on port **80**.

A more secure firewall can be defined using the **inspect-state** option. The stateful inspection system intelligently creates and manages dynamic filter rules based on the type of connection and the source/destination IP addresses. Applying this to the above example, we can redesign the script to make it both simpler and more effective as described below.

As a consequence of the fact that only the first packet in a TCP handshake will have the **SYN** flag set, we can use a rule that checks the **SYN** flag:

```
pass out break end on ppp 0 from 10.1.2.0/24 to any port=80 flags s inspect-state
block in break end on ppp 0
```

The first rule matches only the first outgoing packet because it checks the status of the **s** (**SYN**) flag and will only pass the packet if the **SYN** flag is set. At first glance however, it appears that the second rule blocks all inbound packets on **PPP 0**. While this may be inherently more secure, it also means users on the network could not receive responses to their HTTP requests making the rule of little use.

The reason that this is not a problem is that the stateful inspection system creates temporary filter rules based on the outbound traffic. The first of these temporary rules allows the first response packet to pass because it also will have the **SYN** flag set. However, once the connection is established, a second temporary rule is created that passes inbound or outbound packets if the IP address and port number match those of the initial rule but does not check the **SYN** flag. It does however monitor the **FIN** flag so that the system can tell when the connection has been terminated. Once an outbound packet with the **FIN** flag has been detected along with a FIN/ACK response, the temporary rule ceases to exist and further packets on that IP address/port are blocked.

In the above example, if a local user on address **10.1.2.34** issues an HTTP request to a host on **100.12.2.9**, the outward packet would match and be passed. At the same time a temporary filter rule is automatically created by the firewall that will pass inbound packets from IP address **100.12.2.9** that are addressed to **10.2.1.34** port **x** (where **x** is the source port used in the original request from **10.1.2.34**).

This use of dynamic filters is more secure, because both the source and destination IP addresses/ports are checked. In addition, the firewall will automatically check that the correct flags are being used for each stage of the communication.

The potential for a security breach has now been virtually eliminated, because even if a hacker could time his attack perfectly he would still have to forge a response packet using the correct source address and port (which was randomly created by the sender of the HTTP request) and also has to target the specific IP address that opened the connection.

Another advantage of **inspect-state** rules is that they are scalable, such as many machines can use the rule simultaneously. In our above example, many machines on the local network could all browse the Internet and the inspection engine would be dynamically creating precise inward filters as they are required and closing them when they are finished with.

The **inspect-state** option can be used on TCP, UDP protocols and some ICMP packets. The ICMP types that can be used with the **inspect-state** option are **echo**, **timest**, **inforeq** and **maskreq**.

Using [inspect-state] with Flags

As can be seen above, the **inspect-state** option can be used with flags. To illustrate this, we will refer back to the earlier example of filtering using flags. It is possible to simplify the script by using the **inspect-state** option. The original script was:

```
pass out break end from 10.1.2.33 port>1023 to any port=telnet
pass in break end from any port=telnet to 10.1.2.33 port>1023 flags a!
```

Using the inspect state option this can be replaced with a single filter rule:

```
pass out break end from 10.1.2.33 port>1023 to any port=telnet flags s!a inspect-state
```

No rule is needed for the return packets because a temporary filter will be created that will only allow inbound packets to pass if they match sessions set up by this stateful inspection rule.

A further point to note about the new rule is that the **flags s!a** specification ensures that it only matches the first packet in a connection. This is because the first packet in a TCP connection has the **SYN** flag on and the **ACK** flag off, and so we only match on that combination. The stateful inspection engine will take care of matching the rest of the packets for this connection.

Using [inspect-state] with ICMP

The **[inspect-state]** option can be also used with ICMP codes. To allow the use of echo request and to allow echo replies you would have just the one rule:

```
pass out break end on ppp 0 proto icmp icmp-type echo inspect-state
```

The advantage of using **inspect-state**, other than just needing one rule, is that it leads to a more secure firewall. For instance with the **inspect-state** option, the echo replies are not allowed in all the time; they are only allowed in once an echo request has been sent out on that interface. The moment that a valid echo reply comes back (or there is a timeout), echo replies will again be blocked. Furthermore, the full IP address is checked; the IP source and destination must exactly match the IP destination and source of the echo request. If you compare this to the rule to allow echo replies in without using **inspect-state,** it would not be possible to check the source address at all and the destination address would match any IP address on our network.

The **inspect-state** option can be used with the following ICMP packet types:

ICMP Type	Matching ICMP Type
Echo	Echo reply
Timest	Timestrep
Inforeq	Inforep
Maskreq	Maskrep

Using [inspect-state] with the Out Of Service option

The **inspect-state** field can be used with an optional **oos** parameter. This parameter allows the stateful inspect engine to mark as **out of service** any routes that are associated with the specified interface and also to control how and the interfaces are returned to service. Such routes will only be marked as **out of service** if the specified **oos** option parameters are met. The **oos** parameter takes the format:

```
oos {interface-name¦logical-name} secs {t=secs} {c=count} {d=count}
{r="ping"|"tcp"{,secs}}
```

where:

interface-name or logical-name

The interface with which the firewall rule is associated, such as **PPP 1**. This can also be a logical interface name which is simply a name that can be created (such as **waffle**). When a logical interface name is specified then this name can become **oos** (**out of service**) and can be tested in other firewall rules with the **oosed** keyword.

secs

The length of time, in seconds, for which the routes that are using the specified interface are marked as out of service.

{t=secs}

An optional parameter that specifies the length of time in seconds the router will wait for a response the packet that matched the rule.

{c=count}

An optional parameter that specifies the number of times that the stateful inspection engine must trigger on the rule before the route is marked as out of service.

{d=count}

An optional parameter that specifies the number of times that the stateful inspection engine must trigger on the rule before the interface is deactivated. This parameters applies to PPP interfaces only.

{r="ping"|"tcp"{,secs{,secs}}}

An optional parameter that specifies a recovery procedure. When a recovery procedure is specified then after the oos timeout has expired instead of bringing the interface back into service immediately the link is tested first. It is tested by either sending a TCP **SYN** packet or a ping packet to the address/port that caused the oos condition. The **secs** field specifies the retry time when checking for recovery. Only when the recovery succeeds will the interface become in service again.

UDP example

```
pass in
pass out
pass out on ppp 1 proto udp from any to 156.15.0.0/16 port=1234 inspect-state oos ppp 1 300
t=10 c=2 d=2
```

The first two rules simply configure the router to allow any type of packets to be transmitted or received (the default action of the firewall is to block all traffic).

The third rule is more complex:

- It configures the stateful inspection engine to watch for UDP packets (with any source address) being routed via the **PPP 1** interface to any address that begins with **156.15** on port **1234**.

- If a hit occurs on this rule, but the router does not detect a reply within 10 seconds (as specified by the **t=** parameter), it increments an internal counter.

- When this counter reaches the value set by the **c=** parameter, the stateful inspection engine marks the **PPP 1** interface (and therefore any routes using it), as being out of service for **300** seconds.

- Similarly, if this counter matches the **d=** parameter, the stateful inspection engine deactivates **PPP 1**.

- The stateful inspection engine marks any routes that use **PPP 1** as out of service AND deactivates **PPP 1** if no reply is detected within 10 seconds for two packets in a row.

- Routes will come back into service when either the specified timeout expires or if there are no other routes with a higher metric in service.

- PPP interfaces will be re-activated when either the routes using them are back in service and there is a packet to route and the AODI mode parameter is set to **On**.

TCP example

```
pass out log break end on ppp 3 proto tcp from any to 192.168.0.1 flags S!A inspect-state
oos 30 t=10 c=2 d=2
pass in
pass out
```

- This rule specifically traces attempts to open a TCP connection on **PPP 3** to the **192.168.0.1** IP address and if it fails within 10 seconds twice in a row, will cause the **PPP 3** interface to be flagged as out of service (such as its metric will be set to 16), for 30 seconds.

- The optional **d=2** entry will also cause the PPP link to be deactivated. Deactivating the link can be useful in scenarios where renegotiating the PPP connection is likely to resolve the problem.

- Again, if a matching route with a higher metric has been defined it will be used while **PPP 3** routes are out of service, thus providing a powerful route backup mechanism.

Using [inspect-state] with the stat option

The **inspect-state** option can be used with the **stat** option. The **stat** option will cause this firewall rule to record statistics associated with this firewall rule. Transaction times, counts and errors are recorded under the PPP statistics with this option.

Assigning DSCP values

When using QOS, packet priorities will be determined by the DSCP values in their TOS fields. These priorities may have already been assigned but if necessary, the router can be configured to assign them by inserting the appropriate rules in the firewall. This is done by using the **dscp** command.

For example, the following rule sets the DSCP value to **46** for almost any type of packet received on **ETH 0** from IP address **100.100.100.25** addressed to **1.2.3.4** on port **4000**. This allows you to set the DSCP value for almost any type of packet.

```
dscp 46 in on eth 0 from 100.100.100.25 to 1.2.3.4 port=4000
```

As a further example, the following rule causes outgoing mail traffic to the same top priority queue (**46** is, by default, a very high priority code in the DSCP mappings):

```
dscp 46 in on eth 0 proto smtp from any to any
```

FWLOG.TXT file

When the log option is specified within a firewall script rule, an entry is created in the **FWLOG.TXT** pseudo-file each time an IP packet matches the rule. Each log entry contains the following information:

Parameter	Description
Timestamp	The time when the log entry is created.
Short Description	Usually **FW LOG** but could be **FW DEBUG** for packets that hit rules with the **debug** action set.
Dir	Either **IN** or **OUT**. Indicates the direction the packet is traveling.
Line	The line number of the rule that cause the packet to be logged.
Hits	The number of matches for the rule that caused this packet to be logged.
Iface	The Interface the packet was to be transmitted/received on.
Source IP	The source IP address in the IP packet.
Dest. IP	The destination IP address in the IP packet.
ID	The value of the ID field in the IP packet.
TTL	The value of the TTL field in the IP packet.
PROTO	The value of the protocol field in the IP packet. This will be expanded to text as well for the well-known protocols.
Src Port	The value of the source port field in the TCP/UDP header.
Dst Port	The value of the source port field in the TCP/UDP header.
Rule Text	The rule that caused the packet to be logged is also entered into the log file.

In addition, port numbers are expanded to text pre-defined port numbers.

Log file examples

Log entry without the body option

```
----- 15-8-2002 16:25:50 ------
FW LOG Dir: IN Line: 11 Hits: 1 IFACE: ETH 0
Source IP: 100.100.100.25 Dest IP: 100.100.100.50 ID: 39311 TTL: 128
PROTO: TCP (6)
Src Port: 4232 Dst Port: WEB (80)
pass in log break end on eth 0 proto tcp from 100.100.100.25 to addr-eth 0
flags S/SA inspect-state
----------
```

Log entry with the body option

```
----- 15-8-2002 16:27:56 ------
FW LOG Dir: IN Line: 7 Hits: 1 IFACE: ETH 0
Source IP: 100.100.100.25 Dest IP: 100.100.100.50 ID: 40140 TTL: 128
PROTO: ICMP (1)
block return-icmp echorep log body break end proto icmp icmp-type echo
From REM TO LOCIFACE: ETH 0
45 IP Ver: 4
Hdr Len: 20
00 TOS: Routine
Delay: Normal
Throughput: Normal
Reliability: Normal
00 3C Length: 60
9C CC ID: 40140
00 00 Frag Offset: 0
Congestion: Normal
May Fragment
Last Fragment
80 TTL: 128
01 Proto: ICMP
0C E1 Checksum: 3297
64 64 64 19 Src IP: 100.100.100.25
64 64 64 32 Dst IP: 100.100.100.50
ICMP:
08 Type: ECHO REQ
00 Code: 0
04 5C Checksum: 1116
----------
```

Text included in the EVENTLOG.TXT pseudo-file when the event sub-option is specified

```
16:26:32, 15 Aug 2002,Firewall Log Event: Line: 10, Hits: 3
```

Syslog message where the body option is not specified

```
2002-09-04 16:30:06 User.Info100.100.100.50Aug 15 16:31:59 arm.1140
IP Filter -
Filter Rule: block return-icmp unreach host-unr in log syslog break end on eth 0 proto tcp
from any to 100.100.100.50 port=telnet
Line: 10
Hits: 4
```

Syslog message with the body option specified

2002-08-30 16:19:59 User.Info100.100.100.50Aug 10 16:21:56 arm.1140

```
IP Filter - Filter Rule: block return-icmp unreach port-unr in log body syslog break end on
eth 0 proto tcp from any to 100.100.100.50 port=telnet
Line: 9
Hits: 3
PKT:
Source IP: 100.100.100.25
Dest IP: 100.100.100.50
ID: 13317
TTL: 128
Protocol: TCP
Source Port: 1441
Dest Port: 23
TCP Flags: S
```

Further [inspect-state] examples

- Here is a basic **inspect-state** rule with no OOS options:

```
pass out break end on PPP 2 proto TCP from 10.1.1.1 to 10.1.2.1 port=telnet flags S!A
inspect-state
```

  This rule allows TCP packets from **10.1.1.1** to **10.1.2.1** port **23** with the **SYN** flag set to pass out on **PPP 2**. Because the **inspect-state** option is used, a stateful rule will also be set up which allows other packets for that TCP socket to also pass.

- Next, we will modify the rule to mark an interface OOS, if a stateful rule identifies a failed connection:

```
pass out break end on PPP 2 proto TCP from 10.1.1.1 to 10.1.2.1 port=telnet flags S!A
inspect-state oos 60
```

  The addition of **oos 60** means if the stateful rule sees a failure, interface **PPP 2** will be set OOS for **60** seconds. If no interface is specified after the **oos** keyword, the interface set to OOS will be the one the packet is currently passing on. It is possible to OOS a different interface by specifying the interface after the **oos** keyword, such as **oos ppp 1 60** to put **PPP 1** out of service for **60** seconds.

- The default time allowed by the stateful rule for a connection to open can be overridden by using the **{t=secs}** option. Such as, to override the default TCP opening time of **60** seconds to **10** seconds:

```
pass out break end on PPP 2 proto TCP from 10.1.1.1 to 10.1.2.1 port=telnet flags S!A
inspect-state oos 60 t=10
```

  A socket will now only have **10** seconds to become established (such as exchange SYNs) before the stateful rule will expire and be tagged as a failure.

- It is possible to configure the firewall so that the interface is only set to OOS after a number of consecutive failures occur. To do this, use the **{c=count}** option. For example:

```
pass out break end on PPP 2 proto TCP from 10.1.1.1 to 10.1.2.1 port=telnet flags S!A
inspect-state oos 60 t=10 c=5
```

  PPP 2 will now only be set OOS after **5** consecutive failures.

- It is possible to deactivate the interface after a number of consecutive failures. This is useful for WWAN interfaces, which may get into a state where the PPP connection appears to be operational, but in fact no packets are passing. In this case, deactivating and reactivating the interface will sometimes fix the problem. For example:

```
pass out break end on PPP 2 proto TCP from 10.1.1.1 to 10.1.2.1 port=telnet flags S!A
inspect-state oos 60 t=10 c=5 d=10
```

  Now, **PPP 2** will be deactivated after **10** consecutive failures.

Keeping a route out of service and using recovery

You may want to keep the interface OOS until you are sure that a future connection will work. To help achieve this, you can specify one or more recovery options. These options get the router to test connectivity between the router and the destination IP address of the packet that established the stateful rule. The recovery can be in the form of a **ping** or a TCP socket connection. An interval between recovery checks must also be specified. For example:

```
pass out break end on PPP 2 proto TCP from 10.1.1.1 to 10.1.2.1 port=telnet flags S!A
inspect-state oos 60 t=10 c=5 d=10 r=tcp,120
```

Now the interface will be set to OOS for **60** seconds after **5** consecutive failures. After the **60** seconds elapses, the recovery procedure is initiated. In this example, the recovery consists of TCP connection attempts executed at **2-minute** intervals. The interface remains OOS until the recovery procedure completes successfully. The destination IP address in this case is **10.1.2.1**.

To override the default socket connection time, you can specify an additional recovery option. For example:

```
pass out break end on PPP 2 proto TCP from 10.1.1.1 to 10.1.2.1 port=telnet flags S!A
inspect-state oos 60 t=10 c=5 d=10 r=tcp,120,10
```

Now, **10 seconds** is allowed for each recovery attempt. If the socket connects within that time, the recovery is successful, else the recovery is unsuccessful.

There is also an option **{rd=x}** to disconnect the interface after a recovery attempt completes. You can use this option to deactivate the interface after a recovery failure, success, or either. **x** is a bitmask indicating the cases where the interface should be deactivated. Bit **0** is used to deactivate the interface after a recovery failure. Bit **1** is used to deactivate the interface after a recovery success, such as:

- **rd=1** means deactivate after a recovery failure.
- **rd=2** means deactivate after a recovery success.
- **rd=3** means deactivate after either recovery success or recovery failure.

Extending our firewall rule to include this option gives:

```
pass out break end on PPP 2 proto TCP from 10.1.1.1 to 10.1.2.1 port=telnet flags S!A
inspect-state oos 60 t=10 c=5 d=10 r=tcp,120,10 rd=3
```

Now the interface will be deactivated after a recovery success or failure.

If the **{rd=x}** option is not used, the interface remains up until its inactivity timer expires, or it is deactivated by some other means.

The **{dt=secs}** option can be used to indicate that the interface is to remain OOS when it is disconnected, and that it should be reactivated some time after it last disconnected. Recovery procedures start after the interface connects.

Extending our firewall rule to include this option gives:

```
pass out break end on PPP 2 proto TCP from 10.1.1.1 to 10.1.2.1 port=telnet flags S!A
inspect-state oos 60 t=10 c=5 d=10 r=tcp,120,10 rd=3 dt=60
```

Now, the interface is reconnected **60** seconds after it disconnects and recovery procedures start after the interface connects. This option would normally be used with the **{rd=x}** option so that recovery has control over when the interface connects and disconnects.

Keeping a route out of service and using recovery with a list of addresses

This expands on the functionality above, and gives the ability to check connectivity to a range of addresses using a **ping** command. It is possible to specify an address list that the recovery mechanism will ping in turn to see if any respond. This helps ensure that even when one, two, or three destinations cannot be reached due to an outage on the remote network, the connection will be made available again if at least one of the addresses in the list responds.

The address lists are created using the following syntax:

```
#addrs <list-name> <address1,address2,address3,address4>
```

Address lists can span multiple lines if required, for example:

```
#addrs <list-name> <address1,address2>
#addrs <list-name> <address3,address4>
```

The address list is called using the recovery option **pingl**. An example firewall rule is:

```
pass out break end on PPP 1 proto ICMP from 10.1.1.1 to 10.1.2.1 inspect-state oos 60 t=10
c=5 d=10 r=pingl listA ,120,10 rd=3 dt=60
```

This rule allows pings outbound, and on detecting a communication failure it uses pings to a address list named **listA**. The address list named **listA** could look like this:

```
#addrs listA 10.1.2.1,10.1.3.1,10.1.4.1,10.1.5.1
#addrs listA 10.1.6.1,10.2.1.1,10.2.2.1
```

This causes the recovery to ping the range of address shown in the list above.

Debugging a firewall

When creating and managing firewall scripts, the scripts may need debugging to ensure that packets are being processed correctly. To assist in this, a rule with the debug action can be used.

If a rule with the **debug** action is encountered, an entry is made in the **FWLOG.TXT** pseudo-file each time the packet in question matches a rule from that point on. This gives the administrator the ability to follow a packet through a rule set, and can help determine what, if any, changes are required to the rule set. Rules that specify the debug action are typically placed near the top of the rule set, so all matching rules from that point on are entered into the log file.

Entries created in the **FWLOG.TXT** file as the result of a debug rule can be identified by the short description **FW_DEBUG** at the top of the log entry.

An example rule set using a `debug` rule:

```
debug in on ppp 2 proto tcp from any to any port=http
```

```
pass in break end proto tcp from any to any port=http flags s/sa inspect state
```

```
pass out break end proto udp
```

If placed at the top of the rule set, any packet received on interface **PPP 2** to destination port **80** generate a debug entry in the log file for each subsequent rule that it matches. In the example rule set above, a packet that matched the second rule would also match the first rule, and would therefore create two log entries. The same packet would not match the third rule, and so no log entry would be made for this rule.

Because of the extra processor time required to add all of these additional log entries, debug rules should be removed (or commented out) once the rule set is operating as desired.

RADIUS parameters

RADIUS parameters are configured on the **Configuration > Security > Radius** pages.

About using a RADIUS client for authentication

A RADIUS client may be used for authentication purposes at the start of remote command sessions, SSH sessions, FTP sessions, HTTP sessions and Wi-Fi client connections (PEAP & EAP-TLS). Depending on how the RADIUS client is configured, the router may authenticate with one or two RADIUS servers, or may authenticate a user locally using the existing table configured on the router.

There are 2 RADIUS client configurations: **RADIUS Client 0** and **RADIUS Client 1**. Both have specific functions and the correct instance (0, 1, or both) should be configured depending on the requirements.

To use RADUIUS for authenticating router administration access, configure **RADIUS Client 0**. To use RADIUS for authenticating Wi-Fi clients, configure **RADIUS Client 1**.

When the router has obtained the remote user username and password, the RADIUS client is used to pass this information (from the Username and Password attributes) to the specified RADIUS server for authorization. The server should reply with an **ACCEPT** or **REJECT** message.

The RADIUS client may be configured with up to two Network Access Servers (NAS). It may also have local authentication turned on or off depending on system requirements.

When a user is authenticated, the configured RADIUS servers are contacted first. If a valid **ACCEPT** or **REJECT** message is received from the server, the user is allowed or denied access respectively. If no response is received from the first server, the second server is tried (if configured). If that server fails to respond, local authentication is used unless disabled. If both servers are unreachable and local authentication is disabled, all authentication attempts fail.

If a RADIUS server replies with a **REPLY-MESSAGE** attribute (**18**), the message is displayed after the login attempt and after any configured "post-banner" message. The router will then display a **Continue Y/N?** prompt to the user. If **N** is selected, the remote session is terminated. This applies to remote command sessions and SSH sessions only.

If the login attempt is successful and the server sends an **IDLE-TIMEOUT** attribute (**28**), the idle time specified will be assigned to the remote session. If no **IDLE-TIMEOUT** attribute is sent, the router applies the default idle timeout values to the session.

The access level is determined by the value of the **SERVICE-TYPE** attribute returned by the RADIUS server. Administrative access is determined by the value **6** being returned by the server. Any other value or no value returned will result in the access level **low** being assigned.

When the session starts and ends, the router will send the RADIUS accounting **START/STOP** messages to the configured server. Again, if no response is received from the primary accounting server, the secondary server will be tried. No further action is taken if the secondary accounting server is unreachable.

As a consequence of the fact that the router has separate configurations for authorization and accounting servers, it is possible to configure the router to perform authorization functions only, accounting only, or both. An example of how this might be used could be to perform local authorizations but send accounting start/stop records to an accounting server.

RADIUS Client n parameters

Configuration > Security> Radius > RADIUS Client n

The following pages describe the configuration parameters available for setting up a RADIUS client on the router.

Authorization

Primary Authorization Server

IP Address a.b.c.d

The IP address of the primary authorization NAS.

NAS ID

An identifier passed to the primary authorization NAS and is used to identify the RADIUS client. The appropriate value will be supplied by the primary authorization NAS administrator.

Password

The password supplied by the primary authorization NAS administrator and is used in conjunction with the primary authorization NAS ID to authenticate RADIUS packets.

Confirm Password

Type the above password into this text box so that the router can determine if the two are identical.

Secondary Authorization Server

IP Address a.b.c.d

The IP address of the secondary authorization NAS server.

NAS ID

An identifier passed to the secondary authorization NAS and is used to identify the RADIUS client. The appropriate value will be supplied by the secondary authorization NAS administrator.

Password

The password supplied by the secondary authorization NAS administrator and is used in conjunction with the secondary authorization NAS ID to authenticate RADIUS packets.

Confirm Password

Type the above password into this text box so the router can determine if the two are identical.

Enable local authorization if there is no response from the authorization server(s)

Enables or disables local authorization if the RADIUS servers are unreachable or not configured. Default is enabled. Un-check the box to disable local authorization.

Accounting

Primary Accounting Server

IP Address

The IP address of the primary accounting NAS.

NAS ID

An identifier that is passed to the primary accounting NAS and is used to identify the RADIUS client. The appropriate value will be supplied by the primary accounting NAS administrator.

Password

The password that is supplied by the primary accounting NAS administrator and is used in conjunction with the primary accounting NAS ID to authenticate RADIUS packets.

Confirm Password

Type the above password into this text box to enable the router to check that they are identical.

Secondary Accounting Server

IP Address

The IP address of the secondary accounting NAS.

NAS ID

An identifier that is passed to the secondary accounting NAS and is used to identify the RADIUS client. The appropriate value will be supplied by the secondary accounting NAS administrator.

Password

The password that is supplied by the secondary accounting NAS administrator and is used in conjunction with the secondary accounting NAS ID to authenticate RADIUS packets.

Confirm Password

Type the above password into this text box to enable the router to check that they are identical.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
radcli	0,1	server	Valid IP Address **a.b.c.d**	Primary Authorization Server IP Address
radcli	0,1	nasid	Up to 80 characters	Primary Authorization Server NAS ID
radcli	0,1	password	Up to 40 characters	Primary Authorization Server Password
radcli	0,1	server2	Valid IP Address a.b.c.d	Secondary Authorization Server IP Address
radcli	0,1	nasid2	Up to 80 characters	Secondary Authorization Server NAS ID
radcli	0,1	password2	Up to 40 characters	Secondary Authorization Server Password
radcli	0,1	localauth	OFF,ON Default ON	Enable local authorization if there is no response from the authorization server(s)
radcli	0,1	aserver	Valid IP Address a.b.c.d	Primary Accounting Server IP Address
radcli	0,1	anasid	Up to 80 characters	Primary Accounting Server NAS ID
radcli	0,1	apassword	Up to 40 characters	Primary Accounting Server Password
radcli	0,1	aserver2	Valid IP Address a.b.c.d	Secondary Accounting Server IP Address
radcli	0,1	anasid2	Up to 80 characters	Secondary Accounting Server NAS ID
radcli	0,1	apassword2	Up to 40 characters	Secondary Accounting Server Password

Advanced RADIUS client n parameters

Configuration > Security> Radius> Radius Client n> Advanced

If there is no response from the server

Use Source IP Address

If required, you can select an alternative source interface and instance here. Select the required interface from the drop-down list and enter the instance of that interface into the adjacent text box. The available interface options are

- **Auto**
- **PPP**
- **Ethernet**

Retransmit the request after **s** seconds

The interval between retransmissions of RADIUS packets.

Stop the negotiation after **n** retransmissions

The maximum number of times RADIUS data should be transmitted to the NAS before the negotiation is deemed to have failed.

Stop the negotiation if there is no activity for **s** seconds

The inactivity period after which the negotiation procedure is deemed to have failed.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
radcli	0	ip_ent	Blank,ETH,PPP Blank=Auto	Use Source IP Address
radcli	0,1	retranint	0-2147483647 Default 5	Retransmit the request after s seconds
radcli	0,1	retran	0-2147483647 Default 3	Stop the negotiation after n retransmissions
radcli	0,1	inactto	0-2147483647 Default 30	Stop the negotiation if there is no activity for s seconds

TACACS+ parameters

The Digi TransPort range of routers supports Terminal Access Controller Access-Control System Plus (TACACS+) for controlling access to the router.

About TACACS

TACACS+ provides authentication, authorization and accounting (AAA) services.

TACACS+ can be used to control the following access methods:

- Secured asynchronous serial (ASY) ports
- Telnet
- SSH
- FTP
- HTTP/HTTPS
- SNMP

When any sort of request is performed by the TACACS+ client, the client first checks to see if a socket to the server (primary or backup) is already open. If a socket is already open, that socket is used for the TACACS+ request. If no socket is open, the primary server is tried first. If the primary server socket fails to open, the backup server will be tried. Regardless of whether the primary or backup socket connected, the primary server is always tried first on the next connection attempt. Once the connection to the TACACS+ server opens, all pending requests are sent to the TACACS+ server.

If a connection to the TACACS+ server is not possible due to network or server problems, all requests by applications are denied.

Functions of the AAA services

If TACACS+ authentication is enabled, the request is sent to the TACACS+ server. If disabled, the router performs the authentication. At this point authorization is also performed. If TACACS+ authorization is disabled, the user access level is obtained from the local user table on the router. If TACACS+ authorization is enabled, an authorization request is sent to the TACACS+ server. The server returns a privilege level and may also return other attributed such as a new idle time for this session, which takes precedence over locally configured values.

When the user has been authenticated and access has been authorized, the login is allowed. If the connection is via telnet or SSH, a welcome message showing the access level and the method of authentication is displayed. If the access level was assigned locally the following message is displayed:

```
Welcome. Your access level is SUPER
```

If the access level was assigned by the TACACS+ server, the following message is displayed:

```
Welcome. Your access level is obtained remotely
```

If accounting is enabled, session start and stop messages are sent to the TACACS+ server when the session opens and closes. During the session, details of commands executed and denied due to access level control will be sent to the TACACS+ server. At the end of the session the stop message is sent to the TACACS+ server with the elapsed session time included.

TACACS+ to local privilege level mappings

TACACS+ level	Local level
>= 15	Super
12-14	High
8-11	Medium
4-8	Low
0-3	None

TACACS configuration parameters

Primary TACACS+ Server

Hostname or IP address of Server a.b.c.d Port n

The IP address or hostname of the primary TACACS+ server is entered into the left-hand text box. If required a port number may also be specified using the right-hand text box. TACACS+ uses TCP port **49** by default. Entering a different number into this text box will cause the router to use that port instead. The port number is used by both the primary and secondary TACACS+ servers.

Server Key

The encryption key to use when communicating with the primary server.

Confirm Server Key

The key is typed into this text box to allow the router to confirm that the two strings are identical.

Secondary TACACS+ Server

Hostname or IP address of Server

The IP address or hostname of the secondary (backup) TACACS+ server. This will be used if a socket to the primary server cannot be opened.

Server Key

The encryption key to use when communicating with the secondary server.

Confirm Server Key

Enter the key into this text box to allow the router to confirm that the two entries are identical.

Enable local authentication if there is no response from the server(s)

When checked, this checkbox will allow local authentication if TACACS+ authentication fails.

Enable TACACS+ Authentication

When checked, this checkbox enables authentication. When authentication is enabled, user authentication takes place on the TACACS+ server. When disabled, user authentication takes place locally on the router.

Enable TACACS+ Authorisation

When checked, this checkbox enables authorization which means that authorization of the application takes place and authorization of application-related commands also takes place.

Enable TACACS+ Accounting

When checked, this checkbox enables accounting. When accounting is enabled, accounting messages are sent at the start and end of application sessions, where applicable, and update messages are also sent from command sessions when commands are denied locally or after they are executed.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
tacplus	0	svr	Up to 64 characters for hostname or valid IP address **a.b.c.d**	Hostname or IP address of server
tacplus	0	port	0-2147483647 Default 49	Port
tacplus	0	key	Up to 20 characters	Server Key
tacplus	0	svr2	Up to 64 characters or valid IP address **a.b.c.d**	Hostname or IP address of server
tacplus	0	key2	Up to 20 characters	Server Key
tacplus	0	localauth	OFF,ON	Enable local authentication if there is no response from the server(s)
tacplus	0	authent	OFF,ON	Enable TACACS+ Authentication
tacplus	0	author	OFF,ON	Enable TACACS+ Authorization
tacplus	0	acct	OFF,ON	Enable TACACS+ Accounting
tacplus	0	debug	OFF,ON	n/a
tacplus	0	tacacspageauth	OFF,ON	n/a

Advanced security settings

The parameters described in this section should not normally need to be adjusted.

Use source IP Address x,y

If required, due to the TACACS+ server being accessed via a VPN tunnel, an alternative source interface and instance may be selected here. Select the required interface from the drop-down list and enter the instance of that interface into the adjacent text box. The available interface options are

- **Auto**
- **PPP**
- **Ethernet**

Response Timeout s seconds

Text box

Stop the negotiation if there is no activity for s seconds

The amount of time (in seconds) before an inactive socket is closed.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
tacplus	0	ip_ent	Blank,ETH,PPP Blank=Auto	Use source IP Address x,y
tacplus	0	ip_add	0-2147483647	Use source IP Address x,y
tacplus	0	respto	0-2147483647 Default=30	Response Timeout s seconds
tacplus	0	inact	0-2147483647 Default=30	Stop the negotiation if there is no activity for s seconds

Command filters

When this feature is enabled, commands will not reach the router's command interpreter unless they are defined in the Command Filters table. Terminal devices may send commands that the router will not necessarily understand but that require a basic **OK** or **ERROR** response.

With command filtering turned on, any command entered will be responded to with a MODEM-like **OK** or **ERROR** response (depending on settings below) unless the command is found in the Command Filters table. The command filter uses wild-card character matching so that command filters such as **cmd*** are permitted which would allow all **cmd 0 ...** commands to be executed. Note that the command mapping table is checked first and the command filter table is only checked if there was not a match in the command matching table.

For more information on command filtering, see *Application Note 17, Command Line Response Manipulation*, which is available on the Digi web site (**www.digi.com**).

The table is generated by typing the desired command into the text box and clicking the **Add** button. Once a command has been entered into the table, it can be removed by clicking the **Delete** button that appears on the right hand side.

Command

This text box contains the command to filter.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
cfilter	n	cmd	Valid command line command	Command
cmd	n	cfilton	0,1 0=Off 1=On	n/a
cmd	n	cfilterr	0,1 0=Off-OK 1=On-ERROR	n/a

Command filtering is enabled from the command line for any particular instance of the command interpreter with the following command:

`cmd <n> cfilton 1`

The default action is to respond with the **OK** response. If the response needed is **ERROR**, use the parameter:

`cmd <n> cfilterr 1`

Where **n** is the instance number.

> **Note**   If the command string contains blank characters, it must be enclosed by double quotation marks. When substituting a command, upper case characters are considered the same as the corresponding lower case characters.

Calling Numbers

This page has a table that accepts a series of telephone numbers, each of which has an associated **Answer** or **Reject** parameter, and, for numbers from which calls are to be rejected, a user-defined reason code. For each number set to **Reject**, the router rejects incoming calls from that number using the reason code specified. The reason code is a numeric value chosen to suit the particular application. If any of the entries is set to **Answer**, the router only answers incoming calls from that number and rejects calls from other numbers using a standard ISDN reject code.

Note	This feature is intended for use by experienced personnel for network testing and fault diagnosis. It is not required for normal use. To use this feature, the ISDN circuit must support the Calling Line Identification (CLI) facility. If CLI is supported, incoming calls from specified numbers can be answered normally or rejected with an optional reject code.

Number

The telephone number to either answer or reject.

Mode

The drop-down list in this column selects either **Answer** to answer calls or **Reject** to reject calls.

Reject Code

The reason code pertaining to the rejection of the call.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
rejlst	n	num	up to 20 digits	Number
rejlst	n	ans	OFF,ON	Mode Answer,Reject
rejlst	n	code	0-255	code

Command line examples:

To display an entry in the calling numbers list enter the command:

```
rejlst <instance> ?
```

where *<instance>* is 0-9.

Such as, `rejlst 5 ?`

To set up an entry to reject a number, use the following commands:

```
rejlst 0 num 1234567
rejlst 0 ans OFF
rejlst 0 code 42
```

To set up an entry to answer a number, use the following commands:

```
rejlst 1 num 1234567
rejlst 1 ans ON
```

Configure position (GPS) settings

This section describes configuring position (GPS) settings from the web interface and command line. It covers the following topics:

About the GPS module on TransPort routers

One of the options available on some models is the ability to connect a GPS receiver which enables the router access to geographical position information. The GPS module may be internal or external. In either situation, an internal asynchronous serial (ASY) port is used for the connection. The standard way that GPS modules send the data is using National Marine Electronics Association (NMEA) standard 0183 messages. This protocol is usually simply referred to as NMEA. Routers offering this functionality support the most common NMEA data messages. These messages are described below. GPS receiver modules normally accept configuration commands which specify which of the NMEA messages should be sent to the requesting host.

GPS parameters

GPS parameters are configured on the **Configuration > GPS** page.

The following descriptions show how to configure a router to accept and forward GPS data using the web interface and by using CLI commands.

Enable local monitoring

When checked, this checkbox allows messages from the GPS receiver may be viewed on the **Management > Position > GPS** status page. Which messages are displayed is configured via entries in a table.

GPS Module Initialization String

Some GPS receivers may require configuration via an initialization message at start-up in order to send the appropriate messages in the required format, at the required data rate. Any such required command string is entered into the text entry box and will be sent to the attached GPS receiver module when the router initializes the module.
The table described here controls which NMEA messages should be sent from the module. The default is to enable all messages.

Fix data (GGA)

When the associated checkbox is checked, the fix data (2D, 3D or no fix) will be output.

Position (GLL)

This checkbox, when checked, causes the Geographic position (Latitude/Longitude) sentence to be output.

Active Satellites (GSA)

Checking this checkbox causes the NMEA sentence containing the number of active satellites used to calculate the position, to be output.

Satellites in view (GSV)

Checking this checkbox causes the NMEA sentence containing the number of satellites in view to be output.

Position and Time (RMC)

Checking this checkbox causes the NMEA sentence containing the current position and time, to be output.

Course over Ground (VTG)

Checking this checkbox causes the NMEA sentence containing the course data to be output.

UTC and local date/time data (ZDA)

Checking this checkbox causes the NMEA sentence containing the current local time and date, to be output.

All other messages

The above messages are the most common and useful NMEA sentences. Many GPS modules support additional messages. Checking this checkbox causes the modules to output any other supported messages.

IP Connection 1

GPS data may be sent to up to two IP destinations. These are specified in the following two sections of the web page.

Send GPS messages to IP address a.b.c.d

The IP address to which the GPS data should be sent.

Port n

The required TCP/UDP port number that the GPS data should be sent to is specified here.

Every n interval(s)

Controls how often the GPS data is transmitted to the specified host.

- A value of **1** cause collected GPS data to be transmitted each time a UTC and local date/time data (ZDA) message is received from the GPS receiver module.

- A value of **2** causes every second message to be sent and so on.

For this feature to work over a TCP/IP connection, the ZDA message must be enabled.

Use TCP / UDP

The protocol to use for sending the messages.

Prefix the message with t

A text string that should precede the NMEA data, if desired.

Suffix the message with t

A text string that should follow the NMEA data, if desired.

IP Connection 2

Send GPS messages to IP address a.b.c.d

The IP address to which the GPS data should be sent.

Port n

The required TCP/UDP port number to which the GPS data should be sent.

Every n interval(s)

How often the GPS data is transmitted to the specified host.

- A value of **1** causes collected GPS data to be transmitted each time a UTC and local date/time data (ZDA) message is received from the GPS receiver module.

- A value of **2** causes every second message to be sent and so on.

For this feature to work over a TCP/IP connection, the ZDA message must be enabled.

Use TCP / UDP

The protocol to use for sending the messages.

Prefix the message with t

A text string that should precede the NMEA data, if desired.

Suffix the message with t

A text string that should follow the NMEA data, if desired.

Related CLI commands

gps command

Entity	Instance	Parameter	Values	Equivalent Web Parameter
gps	0	asy_add	The ASY port to which the GPS receiver is connected	n/a
gps	0	gpson	On, Off	Enable local monitoring
gps	0	init_str	Valid command for GPS receiver	GPS Module Initialization string
gps	0	gga_on	0,1 0=Off 1=On	Fix data (GGA)
gps	0	gll_on	0,1 0=Off 1=On	Position (GLL)
gps	0	gsa_on	0,1 0=Off 1=On	Active Satellites (GSA)
gps	0	gsv_on	0,1 0=Off 1=On	Satellites in view (GSV)
gps	0	rmc_on	0,1 0=Off 1=On	Position and time (RMC)
gps	0	vtg_on	0,1 0=Off 1=On	Course over Ground (VTG)
gps	0	zda_on	0,1 0=Off 1=On	UTC and local date/time (ZDA)
gps	0	oth_on	0,1 0=Off 1=On	All other messages
gps	0	IPaddr1	Valid IP address **a.b.c.d**	Send GPS message to IP address (1)
gps	0	IPport1	Valid IP port **n**	port n
gps	0	nsecs1	Time s seconds	every n interval(s)

Entity	Instance	Parameter	Values	Equivalent Web Parameter
gps	0	udpmode1	0,1 0=TCP 1=UDP	Use TCP/UDP
gps	0	IPprefix1	Free text	Prefix the message with
gps	0	IPsuffix1	Free text	Suffix the message with
gps	0	IPaddr2	Valid IP address **a.b.c.d**	Send GPS message to IP address (2)
gps	0	IPport2	Valid IP port **n**	port n
gps	0	nsecs2	Time **s** seconds	every n interval(s)
gps	0	udpmode2	0,1 0=TCP 1=UDP	Use TCP/UDP
gps	0	IPprefix2	Free text	Prefix the message with
gps	0	IPsuffix2	Free text	Suffix the message with

The following CLI parameters are not available on the web interface:

Entity	Instance	Parameter	Values	Equivalent Web Parameter
gps	0	gga_int	s seconds 0–255	n/a
gps	0	gll_int	s seconds 0-255	n/a
gps	0	gsa_int	s seconds 0-255	n/a
gps	0	gsv_int	s seconds 0-255	n/a
gps	0	rmc_int	s seconds 0-255	n/a
gps	0	vtg_int	s seconds 0-255	n/a
gps	0	zda_int	s seconds 0-255	n/a

gpson command

```
cmd <instance> gpson {on|off}
```

When **gpson** is set to **on**, this indicates an instance of the command line interpreter is connected to the GPS receiver. The instance number should be the ASY port number to which the GPS receiver is connected. This parameter has two purposes:

- It tells a particular command interpreter instance that it is connected to a GPS receiver so that commands received by that instance should be ignored, rather than being treated as invalid commands.

- It is used by the **at\gps** command to determine where the GPS messages originate.

at\gps command

```
at\gps
```

- This command causes messages from the GPS receiver to be sent directly to the ASY port from which the command has been entered.

- This requires that the **gpson** parameter (above) is set to **on** for one of the command interpreter instances.

- As soon as the **at\gps** command has been issued, data from the GPS receiver will be sent to that ASY port.

- To stop the GPS data, the **+++** escape sequence must be entered, followed by a pause, followed by **at**.

Configure GPS support for the GOBI3000 module

GOBI3000 module supports the use of the GPS functionality. To configure the GOBI3000 module with GPS functionality:

Configure the GPS **init** string should be configured with **$GPS_START** command:

```
 gps 0 init_str $GPS_START
```

Set the GPS **asy_add** parameter to **3**.

Manage applications

This section describes how to manage applications written in the ScriptBasic and Python languages from the web interface and command line. It covers the following topics:

Manage ScriptBasic applications

To allow end users to extend and enhance the functionality of the TransPort routers, scripting support is provided. ScriptBasic is a scripting language supported by Digi TransPort routers. This section describes how to run simple ScriptBasic scripts.

To manage ScriptBasic application files, go to **Applications > Basic > ScriptBasic**. On this page,

- The main configuration setting is a table containing a list of reference numbers and associated user parameters.

- The second setting is a text box containing the name of the script to run.

Initially, the table is displayed empty, with a row that states **No parameters have been defined**. The leftmost column contains the number **1**.

n

The number of the parameter that appears in the next column. Up to 30 parameters can be configured. It is best to enter the numbers in a consecutive, ascending sequence since this is how the parameters will be referred to in any ScriptBasic script.

Parameter

Type the name of the parameter you wish to create. This can be any alphanumeric string. These parameters can then be referenced by a ScriptBasic script. For example, a script using parameter **string1** will use the string defined in the text entry box associated with command index **1**.

Add

Adds the parameter to the list of parameters. Parameters are added consecutively, with each parameter number referring to the string in the adjacent column.

Run Script

The name of the ScriptBasic file to run. This script must exist within the filing system. Conventionally, ScriptBasic scripts use the **.sb** file extension, such as **myscript.sb**.

Run

Causes the ScriptBasic interpreter to run the named script.

Stop

Stops the execution of the ScriptBasic script.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
basic	0	string1-string30	Free-form alphanumeric text	Parameter
basic	0	n/a	kill	Stop
bas	n/a	n/a	Name of ScriptBasic script	Run Script

Examples

To set User parameter 1 to IPv4 address 10.1.1.1, enter the command:

```
basic 0 string1 10.1.1.1
```

To execute a script from the CLI, enter the command:

```
bas <myscript.sb>
```

To kill a running script from the CLI, enter the command:

```
Basic 0 kill
```

Manage Python applications

About Python programming for Digi TransPort devices

Some of the Digi TransPort routers support the Python scripting language. Python allows users to extend and enhance the basic functionality of the router through programming. The routers contain a Python interpreter which may be invoked from the command line. This can be useful for developing scripts. The more usual way to use Python is to write a script to implement a required function and to run this script autonomously. It is common practice for Python scripts to use the file extension **.py**, such as **myscript.py**. A Python script is a text file containing Python commands and may be created using a normal plain text editor. Python is a powerful language and obtains some of its power from the many modules that are available for it. A description of the Python language is outside the scope of this manual. For more information on Python programming see the *Digi Python Programmer's Guide* on www.digi.com.

Python Files page

To manage Python application files, go to **Applications > Python > Python Files**.

This page has the following settings:

Module search path

Sets the search path for Python modules that are not in the default search path. Multiple locations may be specified by separating pathnames with colons, such as **pymod1.zip:python21.zip**. This causes the interpreter to search for the two compressed files **pymod1.zip** and **python21.zip**. Note that TransPort routers have a flat filing system structure that does not support subdirectories.

Redirect the Python output to debug

When checked, this checkbox allows the redirection of the **stdout** file handle to the debug output (**stderr**) file handle. The default state of this parameter is **Off**. The easiest way to see this in action is to issue the command to start the Python interpreter from a debug/CLI terminal, and note that the screen remains blank. Stop the interpreter (using the **exit()** command), set this parameter to **On**, and re-issue the command to start the interpreter. This time, the familiar Python welcome message and prompt should appear on the console.

Unbuffered output to stdout

When checked, this checkbox allows redirection of unbuffered output to file handle to the debug output (**stderr**) file handle.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
pycfg	0	modpath	valid search path, such as **mymod.py**	Module search path
pycfg	0	stderr2stdout	0,1 0=Off 1=On	Redirect the Python output to debug

The following additional command line informational/debugging commands are helpful when developing Python scripts.

- **pycfg files**: Displays the status of any Python files.
- **pycfg mem**: Shows the memory usage for the router.
- **pycfg scripts**: Shows the status of any scripts and change count.

Manage networks and connections

This chapter covers how to manage networks and connections the web interface and command line. It covers the following topics:

- View network interface status on page 706
- Manage connections on page 743
- Manage position (GPS) information on page 751
- View and manage the event log on page 753
- Use the Analyser on page 754
- Monitor and manage network top talkers on page 763

View network interface status

The **Management-Network Status> Interfaces** menu has the following sub-menu options:

Ethernet (ETH n) parameters

This page displays the current status and statistics of the selected Ethernet interface.

IP Address

The IP address of the Ethernet interface. This could be either manually configured or assigned via DHCP.

Mask

The mask of the Ethernet interface. This could be either manually configured or assigned via DHCP.

DNS Server / Secondary DNS Server

The primary and secondary DNS Server IP addresses of the Ethernet interface. These could be either manually configured or assigned via DHCP.

Gateway

The IP gateway of the Ethernet interface. This could be either manually configured or assigned via DHCP.

MAC Address

The Ethernet interface's MAC address.

Speed

The current speed of the Ethernet interface.

Duplex

The current duplex mode of the Ethernet interface.

Bytes Received

The number of bytes received on the Ethernet interface.

Bytes Sent

The number of bytes sent on the Ethernet interface.

Packets Received

The number of packets received on the Ethernet interface.

Packets Sent

The number of packets sent on the Ethernet interface.

Unicast Packets Received

The number of unicast packets received on the Ethernet interface.

Unicast Packets Sent

The number of unicast packets sent on the Ethernet interface.

Broadcast Packets Received

The number of broadcast packets received on the Ethernet interface.

Broadcast Packets Sent

The number of broadcast packets sent on the Ethernet interface.

Multicast Packets Received

The number of multicast packets received on the Ethernet interface.

Multicast Packets Sent

The number of multicast packets sent on the Ethernet interface.

Rx Overruns

The number of receive overruns that have occurred on the Ethernet interface. An Rx overrun occurs when there are not enough buffers to receive incoming packets which results in the received packets being dropped.

Collisions

The number of times the router has detected a packet collision on the Ethernet network when transmitting a packet.

Late Collisions

The number of times the router has detected a late packet collision on the Ethernet network when transmitting a packet.

Flood Protection

The number of times the router has detected an Ethernet packet flood on the network and has enabled the Flood Protection mechanism. Flood protection is designed to stop the router from being overwhelmed by the sudden large increase in packets on the Ethernet network.

Alignment Errors

The number of alignment errors that have been detected when receiving an Ethernet packet.

FCS Errors

The number of Ethernet packets that have been received but had an invalid FCS.

Tx Deferred

The Ethernet packets successfully transmitted after being initially deferred.

Long Frames

The number of Ethernet packets that have been received which are too long.

Carrier Sense Error

The number of carrier sense errors that have occurred. These occur when the router attempts to transmit an Ethernet packet but cannot detect the carrier sense condition on the Ethernet network.

Rx MAC Errors

The number of internal errors that have occurred when receiving an Ethernet packet.

Tx MAC Errors

The number of internal errors that have occurred when attempting to transmit an Ethernet packet.

Other Errors

The number of errors that have occurred which are not counted by the other statistics.

Related CLI commands

Command	Instance	Parameter	Equivalent Web Parameter
eth	n	status	Displays the current configuration and status of Ethernet interface n.
ethstat	n	n/a	Displays the statistics for Ethernet interface n.
at\mibclr=eth.n.stats	n/a	n/a	Clears the statistics for Ethernet interface n.

Wi-Fi interfaces

Module Detected

Indicates that the Wi-Fi hardware has been detected by the router.

Admin Status

The current administrative state of the Wi-Fi interface. It indicates whether there is sufficient configuration to bring the Wi-Fi interface up. It can be either **Up** or **Down**.

Operational Status

The current operational state of the Wi-Fi interface. It can be either **Up** or **Down**.

Channel Mode

The Wi-Fi channel mode that is being used. The possible values for this parameter are **B/G** and **A**.

Channel

The Wi-Fi channel being used.

Bytes Received

The number of bytes received on the Wi-Fi interface.

Bytes Sent

The number of bytes sent on the Wi-Fi interface.

Packets Received

The number of packets received on the Wi-Fi interface.

Packets Sent

The number of packets sent on the Wi-Fi interface.

Receive Errors

The number of receives errors that have occurred on the Wi-Fi interface.

Transmit Errors

The number of transmit errors that have occurred on the Wi-Fi interface.

Received Packets Dropped

The number of received packets that have been dropped on the Wi-Fi interface.

Wi-Fi Client Connections table

The **Wi-Fi Client Connections** table gives information on the Wi-Fi clients that are connected to the router's Wi-Fi Access Point interface.

Number of Connected Wi-Fi Clients: 2

Node	Wi-Fi Node	RSSI	Flags	Power Save	Neg. Rates (Mbps)	Capability Info	
00:27:10:d8:cf:c4	0	37	ERP,	Awake	1.0, 2.0, 5.5, 6.0, 9.0, 11.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0	ESS, Privacy, Short Preamble, Short Slottime,	Disconnect
00:80:48:66:36:65	0	36	ERP,	Awake	1.0, 2.0, 5.5, 6.0, 9.0, 11.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0	ESS, Privacy, Short Preamble, Short Slottime,	Disconnect

Disconnect All Clients

Node

The MAC address of the connected Wi-Fi client.

Wi-Fi Node

The Wi-Fi node on the router the client is connected to.

RSSI

The signal strength experienced by the Wi-Fi client.

Flags

The state information for the Wi-Fi client connection.

Power Save

The current power saving state of the Wi-Fi client. The possible values are **Awake** and **Sleep**.

Neg. Rates (Mbps)

The transmission rates that have been negotiated with the Wi-Fi client.

Capability Info

The capabilities the router has advertised to the Wi-Fi client.

Access Point Connections Table

This **Access Point Connections** table gives information on the Wi-Fi Access Points that the router is connected to.

Number of Access Point Connections: 1

Access Point	Wi-Fi Node	RSSI	Flags	Power Save	Neg. Rates (Mbps)	Capability Info	
JPHOME (00:18:4d:67:c5:c8)	0	28	-	Awake	1.0, 2.0, 5.5, 6.0, 9.0, 11.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0	ESS, Privacy,	Disconnect

Disconnect All Clients

Access Point

The name and MAC address of the Wi-Fi Access Point that the router is connected to.

Wi-Fi Node

The Wi-Fi node that has been used to connect to the Access Point.

RSSI

The signal strength experienced by the router when connected to the Wi-Fi Access Point.

Flags

The state information for the Wi-Fi Access Point connection.

Power Save

The current power saving state of the router. The possible values are **Awake** and **Sleep**.

Neg. Rates (Mbps)

The transmission rates that have been negotiated with the Wi-Fi Access Point.

Capability Info

The capabilities of the Access Point that the router is connected to.

Related CLI commands

Command	Options	Parameter	Equivalent Web Parameter
wificonn	n/a		Displays the Wi-Fi connection table.
wificonn	x	cscan	Performs wifi network scan
wifistat	n/a		Displays the Wi-Fi statistics.

Mobile interfaces

The **Mobile interfaces status** page displays the current mobile connection, network and module information.

Management - Network Status > Interfaces > Mobile

Mobile Connection

Registration Status: Registered, home network lac:00DF ci:01B0BD51
Signal Strength: ▁▃▅ (-63 dBm)

Mobile Statistics

IP Address: 10.138.175.115
Primary DNS Address: 88.82.13.12
Secondary DNS Address: 88.82.13.12
Data Received: 2582 bytes
Data Sent: 2462 bytes

Mobile information

Results of Last Module Status Poll at 4 Sep 2012 14:42:26
Outcome: Got modem status OK

SIM status: Ready (PIN checking disabled)
Signal strength: -63 dBm
Radio technology: UMTS
Signal quality (UMTS): RSSI -63 dBm, Ec/Io -10.0 dB
Radio band: WCDMA 2100
Channel: 10712
Manufacturer: HUAWEI Incorporated
Model: Huawei EM680 w/Gobi Technology
IMEI: 354976040164587
ESN: 8026D8C6
MEID: A000003361201A
IMSI: 234159043530649
MDN: Not provisioned
ICCID: 89441000001802166072
Firmware: D3200-STSUGN-1575 1 [Nov 22 2010 09:00:00]
Bootcode: D3200-STSUXN-1577
Hardware version: 30500000
GPRS Attachment Status: Attached
GPRS Registration: Registered, home network lac:00DF ci:01B0BD51
Network: voda UK, 23415
Preferred system: Auto

Mobile Connection

Registration Status

The GSM registration status of the mobile module with respect to the GSM network. It may be one of the following

- **Not Registered, not searching**

- **Not registered, searching**

- **Registered, home network**

- **Registered, roaming**

- **Registration denied**

- **Unknown**

- **ERROR**

The registration status may sometimes be followed by additional information about the **Location Area Code (LAC)** and the **Cell Identifier (CI)**.

Signal Strength

The signal strength in dBm being received by the mobile module. The range is **-113dBm** (min) to **-51dBm** (max). The signal strength bars should match the **Signal Strength LEDs** on the front of the router.

Mobile Statistics

IP Address

The IP address of the mobile interface.

Primary DNS Address / Secondary DNS Address

The primary and secondary DNS addresses used by the mobile interface.

Data Received

The number of data bytes received on the mobile interface while it has been connected.

Data Sent

The number of data bytes sent on the mobile interface while it has been connected.

Mobile Information

For GSM networks, the Mobile Information section can have the following items.

SIM Status

This indicates whether or not a valid SIM card has been installed in the router. It may be one of the following

- **READY**: SIM is OK.

- **SIM PIN**: PIN number required.

- **SIM PUK:** SIM blocked (unblocking code required).

- **ERROR**: SIM is not installed or is faulty.

Radio Technology

The current network technology in use. It may be one of the following

- **GSM**

- **GPRS**

- **EDGE**

- **UMTS**

- **HSDPA**

- **HSUPA**

- **CDMA**

Manufacturer

The manufacturer of the mobile module.

Model

The model of the mobile module.

IMEI

The International Mobile Equipment Identification (IMEI) of the mobile module.

ESN

The Electronic Serial Number (ESN) of the mobile module.

MEID

The Mobile Equipment Identifier (MEID) of the mobile module.

IMSI

The International Mobile Subscriber Identity (IMSI) of the mobile module.

ICCID

This field specifies Integrated Circuit Card Identifier (ICCID) of the SIM card.

Firmware

This specifies firmware running on mobile module.

Bootcode

This field specifies bootcode firmware running on the mobile module.

Hardware Version

The hardware version of the mobile module.

GPRS Attachment Status

This is the current status of the mobile module with respect to the Mobile service. It may be one of the following

• **Not attached**: The router has not connected to a mobile service.

• **Attached**: The router has connector to a mobile service.

• **ERROR**: Unknown response from the mobile module.

GPRS Registration

See Registration Status.

Network

The name of the GSM network to which the mobile module is currently connected to or ERROR if no network is available.

Preferred system

The preferred technology. It can be one of following:
• **Auto**
• **GSM only**
• **WCDMA only**
For CDMA networks, the Mobile Information can have the following items.

Current system ID

The current system ID reported by the mobile module.

Current network ID

The current network ID reported by the mobile module.

Network

The current network reported by the mobile module.

Signal strength 1xRTT

The signal strength in dBm being received by the mobile module from 1xRTT networks.

Signal strength EVDO

The signal strength in dBm being received by the mobile module from EVDO networks.

Manufacturer

The manufacturer of the mobile module.

Model

The model of the mobile module.

MDN

The Mobile Directory Number (MDN) of the mobile module.

MIN

The Mobile Identification Number (MIN) of the mobile module.

ESN

The Electronic Serial Number (ESN) of the mobile module.

MEID

The Mobile Equipment Identifier (MEID) of the mobile module.

Firmware

The firmware running on mobile module.

Bootcode

The bootcode firmware running on the mobile module.

Hardware version

The hardware version of the mobile module.

Registration State

See Registration Status.

Roaming status

The current roaming status of the mobile module.

Radio interfaces in use

It can be one of the following

- **CDMA 1x**
- **EVDO**
- **No service**
- **Unknown**

PRL version

The version of the Preferred Roaming List (PRL) loaded on the mobile module.

Activation status

The activation state of the mobile module. It can be of the following:

- **0-Not activated**
- **1-Activated**

Related CLI commands

Command	Option	Equivalent Web Parameter
modemstat	?	Mobile Information
modemstat	s	Scan for Networks
pppstat	n	Mobile Statistics (where n is the PPP interface being used by the mobile interface)
at\mibs=ppp.n.stats	n	Displays the current interface statistics
at\mibclr=ppp.n.stats	n	Clears the current interface statistics

DSL interface

This page displays the current status and statistics of the DSL interface.

```
▼ DSL

              Modem Status: Up
                Link Uptime: 0 Hrs 0 Mins 10 Secs
           Firmware Version: 2227:0
           Operational Mode: G.dmt Annex A
           Remote Vendor ID: TSTC

                                    Downstream        Upstream
              Speed (kbps): 7808              832
                   Channel: Interleave        Interleave
       Relative Capacity (%): 87               71
            Attenuation (dB): 29.0             13.0
          Noise Margin (dB): 16.5             11.0
         Output Power (dBm): 15.5             12.5
             Indicator Bits: 0x0000           0x0000
                      Cells: 7                9
                        CRC: 1                0
                        HEC: 0                0
                        LOS: 0                0
                        SEF: 0                0
            Corrected Blocks: 0
          Uncorrected Blocks: 0
               Overrun Cells: 0
                  Idle Cells: 0

             [ Refresh ]  [ Clear Stats ]
```

Modem Status

The current status of the DSL modem. On the DR64 platform, the values can be one of the following:

- **Idle**

- **Activating**

- **Ghs**

- **Training**

- **Up**

Link Uptime

The amount of time the modem has been in the **Up** state.

Firmware Version

The version of the firmware running on DSL modem.

Operational Mode

The operational mode that the DSL modem is in when in the Up state. It is in the format of:

`<Mode> Annex <A | B | M>`

where the **<Mode>** can be one the following:

*   **ANSI**
*   **ETSI**
*   **G.dmt**
*   **G.lite**
*   **ADSL2**
*   **ADSL2+**

Remote Vendor ID

The remote vendor ID of the DSLAM that the DSL interface connected to.

Speed

The current speed the downstream and upstream DSL channels in Kbps.

Channel

The channel type being used. It can be either **Fast** or **Interleaved**.

Relative Capacity

The current relative capacity on the downstream and upstream DSL channels. The relative capacity is the percentage of your overall available bandwidth used to obtain your ATM service rate.

Attenuation

The current attenuation, in decibels, on the downstream and upstream DSL channels. Attenuation is the measure of how much the signal has degraded between the DSLAM and the DSL modem. The lower the attenuation, the better the performance will be.

Noise Margin

The current noise margin, in decibels, on the downstream and upstream DSL channels. The noise margin (aka Signal to Noise Ratio) is the relative strength of the DSL signal to noise. The larger the noise margin, the better the performance will do. In some instances, interleaving can help raise the noise margin.

Power Output

The current amount of power, in dBm, that the DSL modem (upstream) and DSLAM (downstream) are using. The lower the power output, the better the performance will be.

Indicator Bits

The indicator bit values being used on the downstream and upstream DSL channels.

Cells

The number of cells that have received (downstream) and transmitted (upstream).

CRC

The number of CRC errors that have occurred downstream and upstream.

HEC

The number of Header Error Controls (HEC) errors that have occurred downstream and upstream.

LOS

The number of Loss of Signal (LOS) errors that have occurred downstream and upstream.

SEF

The number of Severely Errored Frame (SEF) errors that have occurred downstream and upstream.

Corrected Blocks

The number of blocks received and corrected by the forward error correction (FEC) code.

Uncorrected Blocks

The number of blocks that were received and could not be corrected by the forward error correction (FEC) code.

Overrun Cells

The number of cells lost because of overrun errors.

Idle Cells

The number of idle cells received.

Related CLI commands

Command	Instance	Equivalent Web Parameter
adslst	n/a	Displays the current DSL interface status.
at\mibs=adsl.0.stats	n/a	Displays the current DSL interface statistics.
at\mibclr=adsl.0.stats	n/a	Clears the current DSL interface statistics.
pppstat	n	DSL Statistics (where n is the PPP interface being used by the DSL PVC).

GRE parameters

This page displays a summary table of the configured GRE interfaces.

#	Description	Oper. Status	IP Address	Mask	Source	Destination
0	Paris Office	Up	47.1.2.3	255.255.255.0	ETH 0 (10.1.47.30)	47.47.1.2
1	New York Office	Up	47.2.2.2	255.255.255.0	10.1.47.30	192.168.44.3

Refresh

#

The GRE interface number.

Description

The configured GRE interface description.

Oper. Status

The current operational status of the GRE interface. It can be one of the following values:

• **Up**: The GRE interface is up.

• **Lower Layer Down**: The GRE interface has keepalives enabled, but is not getting any response from the configured destination.

IP Address

The configured IP address for the GRE interface.

Mask

The configured IP subnet mask for the GRE interface.

Source

The configured source IP address or interface of the GRE interface.

Destination

The configured destination IP address or domain name of the GRE interface. Further information on particular GRE interfaces can be obtained by selecting the appropriate GRE interface submenu underneath the GRE summary table.

Besides the above information, the following statistics are also displayed:

Bytes Received

The number of bytes received on the GRE interface.

Bytes Sent

The number of bytes sent on the GRE interface.

Packets Received

The number of packets received on the GRE interface.

Packets Sent

The number of packets sent on the GRE interface.

Keepalives Received

The number of GRE keepalive packets received on the GRE interface.

Keepalives Sent

The number of GRE keepalive packets sent on the GRE interface.

Rx Errors

The number of receive errors that have occurred on the GRE interface. These can include the received being an invalid GRE packet.

Tx Errors

The number of transmit errors that have occurred on the GRE interface. These can include an internal error due to no packet buffers being available.

Rx Unknown

The number of packets that have been received with an unknown IP protocol and have been dropped.

Tx Discards

The number of packets that have been discarded during transmission due to the GRE interface not being up or if a routing loop has been detected.

Related CLI commands

Entity	Instance	Options	Equivalent Web Parameter
tunstat	n	n/a	Displays the GRE interface specific status and statistics.
tunstat	n	clear	Clears the statistics for the GRE interface.

ISDN parameters

This section contains the status information for the ISDN interface.

ISDN BRI

The status information is presented as a simple table having three or four columns as described below:

Channel

There are three supported channels; the D-channel, B1, and B2 channels that appear in this column. Each channel row has an associated status, protocol and (for data channels) action. The **Action** column will only appear when the associated channel becomes active.

Status

The status of each channel. The status is either **ON** or **OFF**.

Protocol

The protocol in use by the channel. This should be as set up in the configuration procedure. For D-channels, this will be **LAPD**. If the associated channel is not active, this entry will be blank.

Action

When the link becomes active, a button should appear in this column. The text on the button will be **Drop Link**. Clicking the button deactivates the channel.

Related CLI commands

If a PPP instance has been associated with a B-channel, the statistics for that PPP instance will be available using the normal **pppstat** command.

PSTN parameters

This section contains the network status information for the PSTN interface.

Link Name

A description of the interface, if one was assigned during the configuration.

This PSTN interface is using PPP n

When configuring the PSTN module, a PPP instance is assigned. This field is the instance number of the assigned PPP interface.

IP Address

The IP address assigned to the interface.

Mask

The subnet mask being used by the interface.

DNS Server

The IP address of the DNS server being used by the interface.

Bytes Received

The number of bytes received by the interface.

Bytes Sent

The number of bytes sent by the interface.

LCP Packets Received

The number of Link Control Protocol (LCP) packets received.

LCP Packets Sent

The number of LCP packets sent by the interface.

PAP Packets Received

The number of Password Authentication Protocol (PAP) packets sent by the interface.

PAP Packets Sent

The number of PAP packets sent by the interface.

IPCP Packets Received

The number of IP Control Protocol (IPCP) packets received by the interface.

IPCP Packets Sent

The number of IPCP packets sent by the interface.

Receive Errors

The number of frames received that contain an error (CRC etc).

Transmit Errors

The number of frames the interface attempted to transmit, but were found to contain an error.

Refresh

Clicking this button causes the status page to be refreshed with the updated statistics.

Clear PPP n Statistics

Clicking this button causes the statistics to be reset to zero.

Related CLI commands

The CLI commands are the same as for other interfaces and are described in the PPP status section. The command to obtain the status is:

`pppstat <n>`

where **<n>** is the interface number for the PPP interface assigned to the PSTN module and is shown at the top of the web page.

Serial parameters

This page displays the current status and statistics of the selected serial interface.

DTR

The current status of the Data Terminal Ready (DTR) signal.

Bytes Received

The number of bytes received on the serial interface.

Rx Overruns

The number of receive overruns that have occurred on the serial interface. A receive overrun occurs when there are not enough buffers to receive incoming data which results in the received data being dropped.

Tx Underruns

The number of transmit underruns that have occurred on the serial interface. A transmit underrun occurs when there is not enough data available when it is about to be transmitted.

Breaks Received

The number of times a break signal has been received.

Framing Errors Received

The number of framing errors that have been detected when receiving data on the serial interface.

Parity Errors Received

The number of parity errors detected when receiving data on the serial interface.

Buffer Shortages

The number of times data received on the serial interface has been dropped because of a lack of system buffers.

Message Shortages

The number of times data received on the serial interface has been dropped because of a lack of system messages.

Related CLI commands

Command	Instance	Parameter	Equivalent Web Parameter
at\mibs=asy.n	n/a	n/a	Displays the statistics for serial interface n.
at\mibclr=asy.n	n/a	n/a	Clears the statistics for serial interface n.

Advanced PPP n parameters

This page displays the current status and statistics of the selected PPP interface.

▼ **PPP 1**

[Raise Link] [Drop Link]

Name: W-WAN

Uptime:	4 Hrs 8 Mins 41 Seconds	
Option	**Local**	**Remote**
MRU:	1500	1500
ACCM:	0x0	0x0
VJ Compression:	OFF	OFF
Link Active With Entity:	ASY 7	
IP Address:	178.106.229.53	
DNS Server IP Address:	149.254.230.7	
Secondary DNS Server IP Address:	149.254.192.126	
Outgoing Call To:	*98*1#	

Total Data Transferred:	33940	Total Up Time Today (mins):	628
Bytes Received:	18418	Bytes Sent:	15522
LCP Packets Received:	64	LCP Packets Sent:	48
PAP Packets Received:	2	PAP Packets Sent:	2
IPCP Packets Received:	110	IPCP Packets Sent:	111
BACP Packets Received:	0	BACP Packets Sent:	0
BAP Packets Received:	0	BAP Packets Sent:	0
Unknown Packets Received:	0		
Receive Errors:	0	Transmit Errors:	0
CRC Errors Received:	0	Framing Errors Received:	0

Transaction Stats.

Last Counter Reset Timestamp:	10:07:25, 13 Dec 2010		
Successful Transaction Count:	0	Dropped Transaction Count:	0
Minimum Transaction Time (ms):	0	Maximum Transaction Time (ms):	0
Average Transaction Time (ms):	0	Route OOS Count:	0

[Refresh] [Clear PPP 1 Statistics] [Clear Total Data Transferred] [Clear Transaction Statistics]

Name

The name assigned to the PPP interface.

Uptime

The amount of time the PPP interface has been up.

MRU

The maximum receive unit (MRU) that has been negotiated by each peer on the PPP connection.

ACCM

The Asynchronous Control Character Map (ACCM) that has been negotiated by each peer on the PPP connection.

VJ Compression

The Van Jacobson (VJ) compression that has been negotiated by each peer on the PPP connection.

Link with Active Entity

The entity this PPP interface is using for connectivity.

IP Address

The IP address assigned to this PPP interface. This could be either statically configured or assigned by the remote PPP peer.

DNS Server IP Address / Secondary DNS Server IP Address

The primary and secondary DNS server IP addresses that are being used by the PPP interface.

Outgoing Call To

If this is dial-out PPP interface, this is the number it used to make the call.

Total Data Transferred

The total amount of data bytes received and transmitted on the PPP interface, including PPP headers and payload.

Total Up Time Today

The total amount of time, in minutes, the PPP interface has been connected in the current 24-hour period.

Bytes Received

The number of bytes received on the PPP interface.

Bytes Sent

The number of bytes sent on the PPP interface.

LCP Packets Received

The number of Link Control Protocol (LCP) packets received on the PPP interface.

LCP Packets Sent

The number of Link Control Protocol (LCP) packets sent on the PPP interface.

PAP Packets Received

The number of Password Authentication Protocol (PAP) packets received on the PPP interface.

PAP Packets Sent

The number of Password Authentication Protocol (PAP) packets sent on the PPP interface.

IPCP Packets Received

The number of IP Control Protocol (IPCP) packets received on the PPP interface.

IPCP Packets Sent

The number of IP Control Protocol (IPCP) packets sent on the PPP interface.

BACP Packets Received

The number of Bandwidth Allocation Control Protocol (BACP) packets received on the PPP interface.

BACP Packets Sent

The number of Bandwidth Allocation Control Protocol (BACP) packets sent on the PPP interface.

BAP Packets Received

The number of Bandwidth Allocation Protocol (BAP) packets received on the PPP interface.

BAP Packets Sent

The number of Bandwidth Allocation Protocol (BAP) packets sent on the PPP interface.

Unknown Packets Received

The number of packets received with an unknown or unsupported PPP protocol.

Receive Errors

The number of receive errors that have occurred on the PPP interface.

Transmit Errors

The number of transmit errors that have occurred on the PPP interface.

CRC Errors Received

The number of packets received on the PPP interface with invalid CRCs.

Framing Errors Received

The number of packets received on the PPP interface with invalid framing.

Transaction Stats

Last Counter Reset Timestamp

The time when the PPP transaction statistics where last reset.

Successful Transaction Count

The number of successful PPP transactions.

Dropped Transaction Count

The number of transactions sent but no response has been received.

Minimum Transaction Time

The shortest response time, in milliseconds, for a PPP transaction.

Maximum Transaction Time

The longest response time, in milliseconds, for a PPP transaction.

Average Transaction Time

The average response time, in milliseconds, for the successful PPP transactions.

Route OOS Count

The number of Route **Out Of Service** messages sent by the firewall to the routing code. These messages put routes out of service for a period of time and are sent when enough failed PPP transactions have occurred.

Related CLI commands

Command	Instance	Parameter	Equivalent Web Parameter
ppp	n	status	Displays the current status of PPP interface n.
at\mibs=ppp.n.stats	n/a	n/a	Displays the statistics for PPP interface n.
at\mibclr=ppp.n.stats	n/a	n/a	Clears the statistics for PPP interface n.

View the IP routing table

The **IP Routing Table** page displays the IPv4 routing table.

IP Routing Table

Destination	Src Addr	Gateway	Metric	Protocol	Idx	Interface	Status
10.1.0.0/16	0.0.0.0/0	10.1.47.30	1	Local	-	ETH 0	UP
47.1.2.0/24	0.0.0.0/0	47.1.2.3	1	Local	-	TUN 0	UP
192.168.0.0/24	0.0.0.0/0	192.168.0.100	1	Local	-	ETH 1	UP
192.168.47.0/24	0.0.0.0/0	0.0.0.0	1	Static	0	PPP 1	DOWN

Default Routes

Destination	Src Addr	Gateway	Metric	Protocol	Idx	Interface	Status
0.0.0.0/0	0.0.0.0/0	0.0.0.0	1	Static	0	PPP 1	DOWN

Refresh   Toggle Src Addr

Destination

The destination IP network of the route. The destination needs to match the destination IP address of an IP packet for the route to be used. For default routes, the destination IP network is always **0.0.0.0/0**. Default routes are used when no other route matches the destination IP address of an IP packet.

Src Addr

When source address routing is being used, the **Src Addr** value needs to match the source IP address of an IP packet for the route to be used.

Gateway

The IP address of the next router to which the IP packet will be routed to in order to reach the destination network. On **PPP** and **TUN** interfaces, and **ETH** interfaces that have the gateway configured, this parameter can be blank.

Metric

The route metric defines the cost of the route. If CIDR routing is enabled and there are two routes to the same destination, the route with the lower metric is used.

Protocol

The protocol that created the route. This setting can be one of the following:

Local	The route is for a network connected directly to the router.
Remote	The route is for a remote network accessed via a PPP connection.
Static	The route is a static route.
Static/RIP	The route is a static route that has been updated by RIP.
RIP	The route is a RIP route.
IBGP	The route is an interior BGP route.
EBGP	The route is an exterior BGP route.
OSPF	The route is an OSPF route.

Idx

Used for static routes only. The index of the configured static route.

Interface

The interface over which the IP packet will be routed when the route is used.

Status

The current status of the route. This setting can be one of the following:

UP	The route is up and can be used for routing.
DOWN	The interface that the route uses is currently down. The interface can be activated if the route is required.
OOS	The interface that the route uses is currently "Out of Service".

Related CLI commands

Command	Options	Equivalent Web Parameter
route	print	Displays the IPv4 routing table.
route	printsrc	Displays the IPv4 routing table with the **src addr** information.

View the IP hash table

The router uses a routing hash table to improve IPv4 routing performance by reducing route lookup times.

The **IP Hash Table** contains information on recently routed IP packets such as source and destination IP address, IP protocol, etc, plus information on the interface and gateway used when routing the IP packet.

When the router receives an IP packet to route, it looks in the IP hash table before looking in the IPv4 routing table.

Whenever the IPv4 routing table changes (such as a route is added, deleted or modified), all entries in the IP hash table are flushed out.

The IP hash table can be flushed manually using the **Flush** button.

Entries in the IP hash table are automatically deleted if it is not used for 10 seconds.

▼ IP Hash Table

Src IP Address	Src Port	Dest IP Address	Dest Port	Next Hop	IP Protocol	Interface	Age	Idx	Usage
10.1.3.14	50983	10.1.47.30	80	0.0.0.0	TCP	-	0	2	5
10.1.255.115	138	10.1.255.255	138	0.0.0.0	UDP	-	0	10	3
10.1.3.14	50976	10.1.47.30	80	0.0.0.0	TCP	-	1	25	37
10.1.63.1	137	10.1.255.255	137	0.0.0.0	UDP	-	0	49	3
10.1.3.14	50973	10.1.47.30	80	0.0.0.0	TCP	-	1	53	13
10.1.3.14	50977	10.1.47.30	80	0.0.0.0	TCP	-	1	58	17
10.1.3.14	50981	10.1.47.30	80	0.0.0.0	TCP	-	0	63	11
0.0.0.0	68	255.255.255.255	67	0.0.0.0	UDP	-	0	66	1
10.1.3.14	50971	10.1.47.30	80	0.0.0.0	TCP	-	1	114	11
10.1.3.14	50979	10.1.47.30	80	0.0.0.0	TCP	-	1	124	11

[Refresh] [Flush]

Src IP Address

The source IP address of the routed IP packet.

Src Port

The source TCP/UDP port of the routed IP packet. If the IP protocol is not TCP or UDP, then this field is **0**.

Destination IP Address

The destination IP address of the routed IP packet.

Dest Port

The destination TCP/UDP port of the routed IP packet. If the IP protocol is not TCP or UDP, this field is **0**.

Next Hop

The next hop gateway to which the routed IP packet was sent to.

IP Protocol

The IP protocol field in the routed IP packet.

Interface

The interface that was used when the IP packet was routed.

Age

The age, in seconds, of the entry in the IP hash table.

Idx

The index in the IP hash table of the entry.

Usage

The number of times the entry has been used.

Related CLI commands

Command	Options	Equivalent Web Parameter
route	hash	Displays the IP hash table.
route	flush	Flushes the IP hash table.

View the Port Forwarding table

This page displays the Port Forwarding / NAT table. The router uses this table to keep track of IP packets that have been modified via NAT or NAPT to be routed over a particular network.

When the router receives a response to a previously modified IP packet, it looks up the matching entry in the Port Forwarding table to correctly modify the response IP packet.

▼ **Port Forwarding Table**

Src IP Address	Dest IP Address	IP Protocol	Src Port	NAPT Port	Dest Port	TTL
192.168.0.120	10.1.2.100	ICMP	512	512	0	10
10.1.48.17	10.1.48.255	UDP	138	57345	138	56

2 current entries
78 free entries

[Refresh]

Src IP Address

The source IP address of the modified IP packet.

Dest IP Address

The destination IP address of the modified IP packet.

IP Protocol

The IP protocol field of the modified IP packet.

Src Port

The source TCP/UDP port of the modified IP packet. For ICMP packets, this defines the ICMP Echo identifier value.

NAPT Port

The new destination TCP/UDP of the modified IP packet. For ICMP packets, this defines the ICMP Echo identifier value.

Dest Port

The original destination TCP/UDP port of the modified IP packet.

TTL

The time to live, in seconds, for the Port Forwarding entry. If the entry is not used for the specified amount of time, the entry is deleted from the Port Forwarding table.

Related CLI commands

Command	Options	Equivalent Web Parameter
nat	list	Displays the Port Forwarding / NAT table.

View firewall statistics

This page displays the current firewall statistics and the Firewall Stateful Inspection table.

Passed Packets

The number of packets the firewall has passed.

Blocked Packets

The number of packets the firewall has blocked.

Logged Packets

The number of packets the firewall has logged.

Stateful Packets

The number of packets that have matched a stateful rule.

Undersized Packets

The number of packets received by the firewall that are too small.

Oversized Packets

The number of packets received by the firewall that are too large.

Return TCP RST

The number of times the firewall has returned a TCP Reset packet.

Return ICMP

The number of times the firewall has returned an ICMP packet.

Stateful rule shortages

The number of times there has been a shortage of entries stateful inspection table.

HASH table errors

The number of times there has been a hashing error when looking into the stateful inspection table.

In use stateful rules reused

The number of times an in-use stateful inspection table has been reused.

Firewall Stateful Inspection Table

The Firewall Stateful Inspection table is a sophisticated, scripted stateful firewall and route inspection engine. Stateful inspection is a powerful tool allowing the router to keep track of a TCP/UDP or ICMP session and match packets based on the state of the connection on which they are being carried.

The table contains a list of dynamic firewall rules that have been created when packets have matched a configured firewall with the **inspect-state** keyword specified.

For more information on the **inspect-state** keyword, see Stateful Inspection Settings parameters on page 653.

▼ **Firewall Stateful Inspection Table**

TTL	Hits	Direction	Src IP Addr	Src Port	Dst IP Addr	Dst Port	Trans. Src IP Addr	Trans. Src Port	Trans. Dst IP Addr	Trans. Dst Port	Protocol	Interface
7	2	OUT	213.152.58.85	1093	212.104.130.9	53	0.0.0.0	0	0.0.0.0	0	UDP	PPP 1

Refresh

TTL

The number of seconds for the table entry to live. When this reaches zero, the entry is removed from the table.

Hits

The number of times an IP packet has been matched against the firewall rule.

Direction

The direction of the IP packets that match the firewall rule.

Src IP Addr

The source IP address of the IP packets that match the firewall rule.

Src Port

The source TCP/UDP port of the IP packets that match the firewall rule.

Dest IP Addr

The destination IP address of the IP packets that match the firewall rule.

Dest Port

The destination TCP/UDP port of the IP packets that match the firewall rule.

Trans. Src IP Addr

If the firewall is configured to modify (such as NAT or NAPT) the source IP address of the IP packets that match the firewall, this defines the new source IP address of the IP packets.

Trans. Src Port

If the firewall is configured to modify (such as NAPT) the source TCP/UDP port of the IP packets that match the firewall, this defines the new source TCP/UDP port of the IP packets.

Trans. Dest IP Addr

If the firewall is configured to modify (such as NAT or NAPT) the destination IP address of the IP packets that match the firewall, this defines the new destination IP address of the IP packets.

Trans. Dest Port

If the firewall is configured to modify (such as NAPT) the destination TCP/UDP port of the IP packets that match the firewall, this defines the new destination TCP/UDP port of the IP packets.

Protocol

The IP protocol of the IP packets that match the entry.

Interface

The interface over which the IP packets that match the entry are sent or received.

Related CLI commands

Command	Options	Equivalent Web Parameter
fwall	show	Displays the Firewall Stateful Inspection table.

View firewall trace output

The firewall trace output is appended to when the **log** keyword is used in the firewall. Most commonly, the **log** keyword is used in the last rule in the form block log break end to log a summary of all packets that did not match one of the preceding allow rules. The **log** keyword is much more versatile in its usage and what can be logged. For more information see the description of the **log** action in

Example firewall trace output

Here is example firewall trace output from the commonly used firewall rule:

```
block log break end
----- 5-10-2009 23:12:08 ------
FW LOG Dir: IN Line: 37 Hits: 4730 IFACE: ETH 3
Source IP: 222.45.112.59 Dest IP: 217.34.133.21 ID: 256 TTL: 106 PROTO: TCP (6)
Src Port: 12200 Dst Port: 8118
block log break end
----------
----- 5-10-2009 23:13:15 ------
FW LOG Dir: IN Line: 37 Hits: 4731 IFACE: ETH 3
Source IP: 218.61.22.42 Dest IP: 217.34.133.21 ID: 35372 TTL: 136 PROTO: TCP (6)
Src Port: FTP CTL (21) Dst Port: 16794
block log break end
----------
```

This output shows two example logged packets. The output of the 1st logged packet is as follows:

```
----- 5-10-2009 23:12:08 ------
```

This is the time stamp of the blocked packet.

```
FW LOG Dir: IN Line: 37 Hits: 4730 IFACE: ETH 3
```

- `Dir:` is the direction of the packet that was logged, either IN or OUT of the router.
- `Line:` is the line number within the firewall rules that caused this packet to be logged.
- `Hits:` is the number of packets that have matched this rule.
- `IFACE:` is the interface which the packet was logged on.

```
Source IP: 222.45.112.59 Dest IP: 217.34.133.21 ID: 256 TTL: 106 PROTO: TCP (6)
```

- `Source IP:` is the source IP address of the packet that was logged.
- `Dest IP:` is the destination IP address of the packet that was logged.
- `ID:` is the ID of the packet, this is taken from the packet header.
- `TTL:` is the Time To Live value.
- `PROTO:` is the layer 3 protocol of the logged packet.

```
Src Port: 12200 Dst Port: 8118
```

- `Src Port` is the source TCP or UDP port number of the packet that was logged.
- `Dst Port` is the destination TCP or UDP port number of the packet that was logged.

- `block log break end` This is the actual rule that caused the packet to be logged.

Related CLI commands

Command	Options	Equivalent Web Parameter
type fwlog.txt	n/a	Displays the current Firewall trace.

View DHCP status

This page displays the current DHCP status table.

IP Address

The IP address assigned to the hostname.

Hostname

The hostname to which the IP address has been assigned.

Lease time left (mins)

The length of time, in minutes, the IP address lease is valid for. After this time, the DHCP client will need to renew its IP address.

Mac Address

The MAC address.

Related CLI commands

Entity	Instance	Parameter	Equivalent Web Parameter
dhcp	0	status	Displays the current status of the DHCP table.
dhcp	0	clear	Deletes all the entries in the DHCP table.

View DNS status

This page displays DNS status table.

DNS Status		
Hostname	**IP Address**	**TTL**
www.bbc.co.uk	212.58.244.70	18
www.google.com	173.194.36.104	282
www.digi.com	172.16.1.69	287

Clear

Hostname

The hostname that has been resolved.

IP Address

The IP address of the hostname.

TTL

The time to live, in seconds, for the DNS entry. When the TTL reaches zero, the entry is deleted.

Related CLI commands

Entity	Instance	Parameter	Equivalent Web Parameter
dns	0	status	Displays the current status of the DNS table.
dns	0	clear	Deletes all the entries in the DNS table.

View QoS status

This page displays the current Quality of Service (QoS) status table for a particular interface.

Priority Q

The priority queue in the table.

TX rate (kbps)

The current transmit rate in kbps of the queue.

Limit

The current transmit rate limit in kbps of the queue.

Weighted Q length

The weighted queue length using the Weighted Random Early Discard (WRED) algorithm.

Q length

The number of packets on the queue.

Manage connections

The **Management- Connections** page has several menu options:

Manage IP connections

This page displays the current status of the TCP sockets on the router.

The router has two types of sockets:

Socket type	Use
TCP Sockets	Reserved for WEB and FTP connections.
General Purpose Sockets	Can be used by any application for TCP connections.

TCP Sockets

```
TCP Sockets
 ID   SID        State         Local IP Addr    Local Port    Remote IP Addr    Remote Port
  0    2         LISTEN          0.0.0.0             21          0.0.0.0              0
  1    3         LISTEN          0.0.0.0             80          0.0.0.0              0
  2   286        ESTAB          10.1.47.30           80         10.49.16.16        54209
  3   -1   CLOSED Closed ( FW2 ) 10.1.47.30          80         10.49.16.16        54207
  4   -1   CLOSED Closed ( FW2 ) 10.1.47.30          80         10.49.16.16        54191
  5   -1   CLOSED Closed ( FW2 ) 10.1.47.30          80         10.49.16.16        54194
  6   -1   CLOSED Closed ( FW2 ) 10.1.47.30          80         10.49.16.16        54196
  7   -1   CLOSED Closed ( FW2 ) 10.1.47.30          80         10.49.16.16        54197
  8   -1   CLOSED Closed ( FW2 ) 10.1.47.30          80         10.49.16.16        54198
  9   -1   CLOSED Closed ( FW2 ) 10.1.47.30          80         10.49.16.16        53754
 10   -1   CLOSED Closed ( FW2 ) 10.1.47.30          80         10.49.16.16        53755
 11    0         LISTEN          0.0.0.0              0          0.0.0.0              0
 12    0         LISTEN          0.0.0.0              0          0.0.0.0              0
 13    0         LISTEN          0.0.0.0              0          0.0.0.0              0
 14    0         LISTEN          0.0.0.0              0          0.0.0.0              0
SYNs waiting : 0
Free SYN entries : 40, min 35
```

ID

The TCP socket identifier.

SID

An internal socket identifier.

State

The current state of the socket.

Local IP Addr

The IP address on the router that is being used for the TCP connection.

Local Port

The TCP port on the router that is being used for the TCP connection or is being listened on.

Remote IP Address

The IP address of the remote device that has the TCP connection to the router.

Remote Port

The TCP port being used by the connected remote device.

SYNs Waiting

The number of TCP SYN packets that are currently being processed by the router.s

Free SYN entries

The number of entries available to process an incoming TCP SYN packet.

Related CLI commands

Command	Options	Description
socks		Displays the current status of the TCP sockets.

General Purpose Sockets

General Purpose Sockets

ID	Owner	Protocol	Mode	State	Local Port	Remote IP Addr	Remote Port	Inactivity Timeout (secs)
0	ASY 0	TCP	Normal	Listening	4000			300
1	ASY 1	TCP	Normal	Listening	4001			300
2	ASY 2	TCP	Normal	Listening	4002			300
3	ASY 3	TCP	Normal	Listening	4003			300
4	ASY 4	TCP	Normal	Listening	4004			300
5	ASY 5	TCP	Normal	Listening	4005			300
6	ASY 6	TCP	Normal	Listening	4006			300
7	ASY 7	TCP	Normal	Listening	4007			300
8	ASY 8	TCP	Normal	Listening	4008			300
9	ASY 9	TCP	Normal	Listening	4009			300
10	ASY 10	TCP	Normal	Listening	4010			300
11	X25 75	TCP	XOT	Listening	1998			300
12	X25 76	TCP	XOT	Listening	1998			300
13	X25 77	TCP	XOT	Listening	1998			300
14	X25 78	TCP	XOT	Listening	1998			300
15	X25 79	TCP	XOT	Listening	1998			300
16	X25 80	TCP	XOT	Listening	1998			300
17	X25 81	TCP	XOT	Listening	1998			300
18	X25 82	TCP	XOT	Listening	1998			300
19	X25 83	TCP	XOT	Listening	1998			300
20	X25 84	TCP	XOT	Listening	1998			300
21	X25 85	TCP	XOT	Listening	1998			300
22	X25 86	TCP	XOT	Listening	1998			300
23	X25 87	TCP	XOT	Listening	1998			300
24	X25 88	TCP	XOT	Listening	1998			300
25	X25 89	TCP	XOT	Listening	1998			300
26	X25 90	TCP	XOT	Listening	1998			300
27	SSH 1	TCP	Normal	Listening	22			300
28	SSH 3	TCP	Normal	Listening	22			300
29	SSH 5	TCP	Normal	Listening	22			300
30	SSH 7	TCP	Normal	Listening	22			300
31	SSH 9	TCP	Normal	Listening	22			300
35	REALPORT 3	TCP	Normal	ESTAB	771	10.49.16.16	60564	300
43	CMD	TCP	Normal	Listening	23			300

Total Number of Sockets : 44
Number of Free Sockets : 10

ID

The ID of the general purpose socket.

Owner

The software task that created the socket.

Protocol

The protocol being used by the socket.

Mode

The mode of operation of the socket.

State

The current state of the socket.

Local Port

The port of the router that is being used by the socket.

Remote IP Addr

The IP address of the remote device that has a TCP connection with the socket.

Remote Port

The TCP port being used by the remote device.

Inactivity Timeout

The socket's inactivity timeout, in seconds. If the timer reaches zero seconds, the TCP connection is closed.

Total Number of Sockets

The total number of general purpose sockets available on the router.

Number of Free Sockets

The number of free general purpose sockets available on the router.

Related CLI commands

Command	Options	Description
gpstat		Displays the current status of the general purpose sockets.
gpstat	close <ID>	Closes the GP Socket connection with the ID number specified.

Manage Virtual Private Networking (VPN) connections

The **Management-Connections> VPN** menu has the following sub-menu options:

- **IPsec > IPsec Tunnels**
- **OVPN**

IPsec > IPsec Tunnels

This page displays the current status of the IPsec tunnels.

Outbound V1 SAs

#	Peer IP Addr	Local Network	Remote Network	AH	ESP Auth	ESP Enc	IP Comp	KBytes Delivered	KBytes Left	Time Left (secs)	Interface	
0	217.34.XXXXX	1.1.1.1/32	1.1.1.2/32	N/A	SHA1	AES(128)	N/A	1	0	86188	PPP 3	Remove

Remove All

Inbound V1 SAs

#	Peer IP Addr	Local Network	Remote Network	AH	ESP Auth	ESP Enc	IP Comp	KBytes Delivered	KBytes Left	Time Left (secs)	Interface	
0	217.34.XXXXX	1.1.1.1/32	1.1.1.2/32	N/A	SHA1	AES(128)	N/A	0	0	86188	PPP 3	Remove

Remove All

Outbound V2 SAs
No Tunnels
Inbound V2 SAs
No Tunnels

Refresh

#

IPsec tunnel number.

SPI

The Security Parameters Index (SPI) is a pointer that references the session key and algorithm used to protect the data in the IPsec tunnel.

Peer IP

The IP address of the remote device that is the other end of the IPsec tunnel.

Local Network

The local IP network of the IPsec tunnel that is connected to the router.

Remote Network

The remote IP network of the IPsec tunnel that is connected to the remote device.

First Rem. IP / Last Rem. IP

For IPsec tunnels that have been negotiated using IKEv2, this is the range IP addresses available on the remote IP network.

First Loc. IP / Last Loc. IP

For IPsec tunnels that have been negotiated using IKEv2, this is the range IP addresses available on the local IP network.

AH

The AH algorithm in use, if any.

ESP Auth

The ESP authentication algorithm in use, if any.

ESP Enc

The ESP encryption algorithm in use, if any.

IPComp

The data compression algorithm in use, if any.

KBytes Delivered

The total amount of data that has been transferred (in both directions) over this IPsec tunnel.

KBytes Left

The amount of data left to be transferred over the IPsec tunnel before the data duration limit is reached. The data duration is negotiated between the router and the remote device.

Time Left

The time left, in seconds, before the time duration limit is reached. The time duration is negotiated between the router and the remote device.

Interface

The interface over which the IPsec tunnel operates.

Related CLI commands

Command	Options	Description
sastat	[dyn]	Displays the current status of all of the IPsecs tunnels. The optional **dyn** parameter can be used to display the status of the dynamic IPsec tunnels.
sastat	[dyn] \<first\> \<last\>	Displays the current status of the IPsec tunnels in the range from **\<first\>** to **\<last\>**. such as **sastat 0 49** or **sastat dyn 0 49**.
sastat	[dyn] peer \<peer\>	Displays the current status of the IPsec tunnels that match the given peer. The **\<peer\>** value can contain the ***** wildcard character. such as **sastat peer uk-north-*** or **sastat dyn peer uk-north-***.

IPsec peers

This page displays the current status of the IPsec peers. This is the list of remote devices that have successfully negotiated an IPsec tunnel with the router.

Peer IP Address	Our ID	Peer ID	Dead Peer Detection (DPD)	NATT Local Port	NATT Remote Port
217.34.✖✖✖✖✖	REM-TEST	SARIAN-BG	Inactive. Next REQ in 119 secs	4500	4500

Remove all unused

Peer IP Address
The IP address of the remote device.

Our ID
The ID of the router.

Peer ID
The ID of the remote device.

Dead Peer Detection (DPD)
The DPD status and the time until the next DPD request.

NATT Local Port
The local NAT-Traversal port.

NATT Remote Port
The remote NAT-Traversal port.

IKE SAs

This page displays the current status of the IKE Security Associations (SA).

IKEv1 SAs

Our ID	Peer ID	Peer IP Address	Our IP Address	Time Left (secs)	Session ID	Internal ID	
REM-TEST	SARIAN-BG	217.34.XXXXXX	10.94.60.189	85599	0x0	6	Remove

Remove All V1 SAs

IKEv2 SAs

No SAs

Our ID

The ID of the router.

Peer ID

The ID of the remote device with which the IKE SA has been negotiated.

Peer IP Address

The IP address of the remote device.

Our IP Address

The IP address the router used to negotiate the IKE SA.

Time Left

The time remaining, in seconds, for the IKE SA to remain in force.

Session ID

The ID of the IKE SA.

Internal ID

An internal identifier for the IKE SA.

Manage position (GPS) information

GPS

This page displays a summary of the most recent information received from the GPS module (if fitted) and the status of the IP connections.

Longitude

The current longitude contained in the last GGA, GLL or RMC message from the GPS module.

Latitude

The current latitude contained in the last GGA, GLL or RMC message from the GPS module.

No of Satellites

The current number of satellites being used as indicated in the last GGA message from the GPS module.

Type of fix

The current fix status as indicated in the last GGA, GLL or RMC message, followed by the type of fix (such as 2D, 3D or no fix) as indicated in the last GSA message.

UTC

The current UTC time as indicated in the last ZDA, GGA, GLL or RMC message from the GPS module.

True Heading

The current true heading as indicated in the last RMC message from the GPS module. If the router is not moving, this value is not available.

Speed

The current speed, as indicated in the last RMC message from the GPS module.

Integrity

The current data integrity as indicated in the last RMC message from the GPS module. It can be either **Valid** or **Not Valid**.

IP Connections

The current IP address, port number, connection type and status of the IP connections.

Related CLI commands

Command	Options	Description
at\mibs=gps.0.stats		Displays the current status of the GPS receiver.

View and manage the event log

The **Management > Event Log** page displays the current contents of the event log on the router.

The event log is stored in a pseudo-file named **eventlog.txt**. It acts as a circular buffer, so when there is no space available for new entries, the oldest entries are overwritten.

Each entry in the log normally consists of a single line containing the date, time and a brief description of the event. In some case it may also identify:

- The type/number of the protocol instance the generated the message, such as **PPP 0**.
- A reason code.
- Additional information such as an X.25 address or ISDN telephone number.

The specific events that generate a log entry are pre-defined and cannot be altered although the text and priority of each event can be modified. This can be done via the **Configuration > Alarms > Event Logcodes** page.

Related CLI commands

Command	Options	Description
type eventlog.txt		Displays the contents of the event log.
clear_ev		Clears the contents of the event log.

Use the Analyser

The router can be configured to capture a trace of the data being transmitted and received on the various interfaces. It can capture the layer 1, 2, and 3 protocol data and present it in an easily read format.

Analyser settings

Enable Analyser

Enables or disables the analyser.

Maximum packet capture size

The number of bytes that are captured and stored for each packet. If the packet is bigger than the configured size, the packet is truncated. Bear in mind that the larger this value, the quicker the pseudo file **ana.txt** will become full so that the effective length of the analyser trace is reduced.

Log Size

The maximum size of the pseudo file **ana.txt** used to store the captured data packets. Once the maximum size is reached, the oldest captured data packets are overwritten when new packets are captured. The maximum value is **180Kb**, but the data is compressed so more than 180Kb of trace data will be captured.

Protocol layers

The check-boxes under this heading specify which protocol layers are captured and included in the analyzer trace. You can choose to capture **Layer 1** (physical / PPP), **Layer 2** (Layer protocol, the Network Layer (**Layer 3**) protocol or any combination, by checking or clearing the appropriate check-boxes. In addition, you may select **XOT** (X.25 over TCP/IP) tracing if this feature is included on the router.

Enable IKE debug

Enables or disables including IKE packets in the analyser trace when using IPsec.

Enable QMI trace

Enables or disables including data from the Qualcomm Management Interface in the analyser trace.

Enable SNAIP trace

Enables or disables including the SNAIP packet in the analyser trace.

ISDN Sources

The checkboxes under this heading select the ISDN channels (**D**, **B1** and **B2**) over which packets will be captured and included in the analyser trace.

LAPB Links

The checkboxes under this heading are used to select the LAPB links over which packets will be captured and included in the analyser trace.

Serial Interfaces

The checkboxes under this heading select the serial interfaces over which packets will be captured and included in the analyser trace. The list of available interfaces include the physical serial interfaces, internal virtual serial interfaces (if present), and interfaces used by built-in WWAN and/or PSTN modems.

Ethernet Interfaces

The checkboxes under this heading select the Ethernet interfaces over which packets are captured and included in the analyser trace.

Raw SYNC Sources

The checkboxes under this heading select the synchronous sources over which packets are captured and included in the analyser trace.

DSL PVC Sources

The checkboxes under this heading select the ADSL ATM PVCs over which packets are captured and included in the analyser trace.

PPP Interfaces

The checkboxes under this heading select the PPP interfaces over which packets are captured and included in the analyser trace.

IP Sources

The checkboxes under this heading select the IP sources over which packets are captured and included in the analyser trace. These sources include IP packets transmitted and received over Ethernet, PPP and OpenVPN (OVPN) interfaces. It is also possible to select GRE Tunnels via the advanced sections of the individual GRE Tunnel configuration pages.

IP Options

Trace discarded packets

Enables or disables the capture of packets that are discarded by an interface along with a reason for why the packet was discarded.

Trace loopback packets

Enables or disables the capture of IP loopback packets.

IP Packet Filters / Discarded IP Packet Filters

TCP/UDP Ports

This parameter filters out TCP or UDP packets with particular source or destination port numbers. The format of this parameter is a comma-separated list of port numbers. For example, you may wish to exclude the capture of Telnet and HTTP traffic that would otherwise swamp the data of interest. This can be done by entering **23,80** for this parameter. Conversely, you may want to capture traffic on a specific source or destination port only. To do this, use a tilde (**~**) symbol before the list of ports. For example, to only capture Telnet and SSH packets, enter **~22,23** for this parameter.

IP Protocols

This parameter is used to filter out IP packets with particular IP protocol numbers. The format of this parameter is a comma-separated list of protocol numbers. For example, you may wish to exclude the capture of TCP traffic that would otherwise swamp the data of interest. This can be done by entering **6** for this parameter. Conversely, you may want to capture traffic with a specific IP protocol number only. To do this, use a tilde (**~**) symbol before the list of protocol numbers. For example, to only capture UDP traffic, enter **~17** for this parameter.

This parameter is used to filter out IP packets with particular source or destination IP addresses. The format of this parameter is a comma-separated list of IP addresses. For example, you may want to exclude the capture of traffic from IP hosts **10.1.2.3** and **10.2.2.2**. This can be done by entering **10.1.2.3,10.2.2.2** for this parameter.

Conversely, you may want to capture traffic to and from particular IP hosts only. To do this, use a tilde (**~**) symbol before the list of IP addresses. For example, to only capture packets to and from IP host **192.168.47.1**, enter **~192.168.47.1** for this parameter.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ana	0	anon	on, off	Enable Analyser
ana	0	maxdata	16-2000	Maximum packet capture size
ana	0	logsize	3 -180	Log Size
ana	0	l1on	on, off	Protocol Layers / Layer 1
ana	0	l2on	on, off	Protocol Layers / Layer 2
ana	0	l3on	on, off	Protocol Layers / Layer 3
ana	0	xoton	on, off	Protocol Layers / XOT
ana	0	ikeon	on, off	Enable IKE debug
ana	0	qmion	on, off	Enable QMI trace
ana	0	snaipon	on, off	Enable SNAIP trace
ana	0	lapdon	0-7 See below	ISDN Sources
ana	0	lapbon	0-7 See below	LAPB Links
ana	0	asyon	Bitmap See below	Serial Interfaces
ana	0	syon	Bitmap See below	Raw SYNC Sources
ana	0	discardson	on, off	IP Options / Trace discarded packets
ana	0	loopon	on, off	IP Options / Trace loopback packets
ana	0	ipfilt	Comma separated list	IP Packet Filters / TCP/UDP Ports
ana	0	ipprotfilt	Comma separated list	IP Packet Filters / IP Protocols

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ana	0	ipaddfilt	Comma separated list	IP Packet Filters / IP Addresses
ana	0	discportfilt	Comma separated list	Discarded IP Packet Filters / TCP/UDP Ports
ana	0	discprotofilt	Comma separated list	Discarded IP Packet Filters / IP Protocols
ana	0	discipaddfilt	Comma separated list	Discarded IP Packet Filters / IP Addresses
eth	n	ethanon	on, off	Ethernet Interfaces
eth	n	ipanon	on, off	IP Sources
ovpn	n	ipanon	on, off	IP Sources
ppp	n	ipanon	on, off	IP Sources
ppp	n	pppanon	on, off	PPP Interfaces
tun	n	ipanon	on, off	GRE IP Sources
tun	n	tunanon	on, off	GRE Tunnel Interfaces

Related CLI commands (not available via the Web Interface)

Entity	Instance	Parameter	Values	Description
ana	0	fcon	on, off	Enable serial flow control tracing.
ana	0	stopbufs	0-255	Stop analyser when number of free system buffers matches this value.
ana	0	stopmsgs	0-255	Stop analyser when number of free system messages matches this value.
ana	0	stopflood	0-1	Stop analyser when Ethernet flood protection is activated.
ana	0	lowbufcmd	Command String	Run this command when the number of free system buffers match **lowbuflvel**.
ana	0	lowbuflev	Integer	Free system buffer threshold used by **lowbufcmd**.
ana	0	lowmsgcmd	Command String	Run this command when the number of free system messages match **lowmsglvel**.
ana	0	lowmsglev	Integer	Free system message threshold used by **lowmsgcmd**.
ana	0	logdrive	String	Specifies an alternate file system drive on which to store the analyser trace. To use an external USB flash device, this should be set to **u:** If the router has an internal SDIO flash device, it can be selected with **s:**
ana	0	logfile	Filename	The file on the alternate drive to which the analyser trace will be stored.
ana	0	contfile	Filename	The file on the alternate drive to which the analyser trace will be stored once the file indicated by **logfile** is reaches its max size as specified by **logsizek**.
ana	0	logsizek	Value in Kbytes	The maximum size in Kbytes of the file on the alternate drive. When set to **0**, the file size is only limited by the flash device.

ISDN Sources

LAPD2	LAPD1	LAPD0	Value
OFF	OFF	OFF	0
OFF	OFF	ON	1
OFF	ON	OFF	2
OFF	ON	ON	3
ON	OFF	OFF	4
ON	OFF	ON	5
ON	ON	OFF	6
ON	ON	ON	7

LAPB Links

LAPD1	LAPD0	Value
OFF	OFF	0
OFF	ON	1
ON	OFF	2
ON	ON	3

Serial Interfaces

Interface	Value
Serial 0	1
Serial 1	2
Serial 2	4
Serial 3	8
Serial 4	16
Serial 5	32
Serial 6	64
Serial 7	128
Serial 8	256
Serial 9	512
Serial 10	1024
Serial 11	2048
Serial 12	4096

To enable the analyser on multiple serial interfaces, add the appropriate values together. For example, to enable the analyser on serial interfaces **2** and **3**, the value should be **12** (**4**+**8**).

The number of serial interfaces can vary on different depending on which hardware and software options are available.

Raw Sync Interfaces

Interface	Value
ISDN D	1
ISDN B1	2
ISDN B2	4
Physical Port 0	8
Physical Port 1	16

To enable the analyser on multiple serial interfaces, add the appropriate values together. For example, to enable the analyser on Physical Ports **0** and **1**, the value should **24** (**8**+**16**).

Display analyser trace

Management > Analyser > Trace displays the current analyser trace.

Related CLI commands

Command	Options	Description
type ana.txt		Displays the contents of the event log.
ana 0 anaclr		Clears the contents of the event log.

Set PCAP (such as Wireshark) traces

The traffic captured by the Analyzer is also available in PCAP format. To display this PCAP format, select **Management > Analyser > PCAP (e.g. Wireshark) traces**. This format can be read by a network protocol analyzer, such as Wireshark. This powerful feature gives a network engineer the ability to diagnose network protocol issues with relative ease.

There are several PCAP files which are available to download. Each file contains a different set of captured packets.

Option	PCAP File	Contents
IP	anaip.pcap	IP traffic captured from all enabled IP sources.
Ethernet	anaeth.pcap	Ethernet traffic captured from all enabled Ethernet sources.
PPP	anappp.pcap	PPP traffic captured from all enabled PPP sources.
Wi-Fi	anawifi.pcap	Wi-Fi traffic captured from the enabled Wi-Fi source.

Wireshark is free software and can be obtained from http://www.wireshark.org.
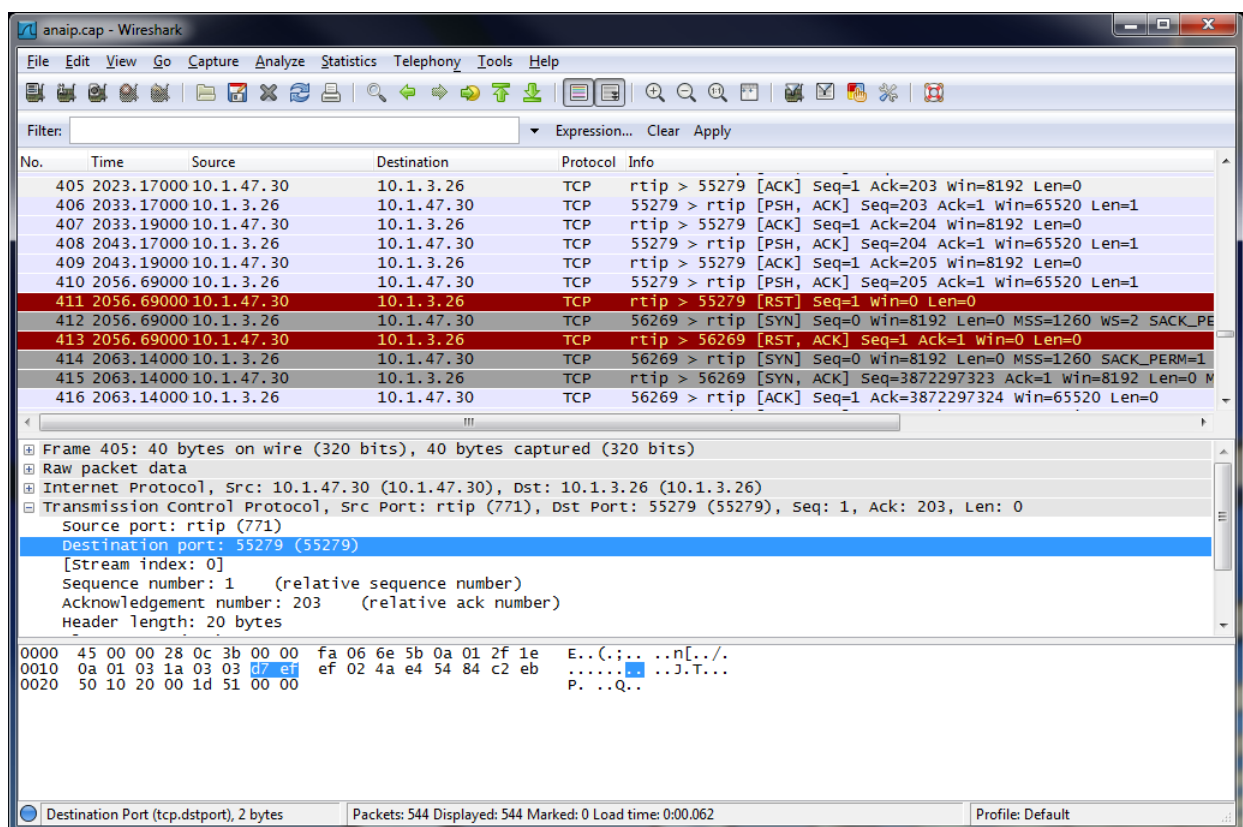
Monitor and manage network top talkers

The router can be configured to monitor the data being transmitted and received on the various interfaces. It is able to report which IP hosts are generating the most traffic over a period of one minute and 30 minutes.

Top Talkers also allows you to block particular IP traffic flows to stop them from using bandwidth. The **Management > Top Talkers** page has the following menu options:

Top Talkers settings

Management > Top Talkers > Settings displays the current settings for the Top Talkers monitor.

Ethernet Interfaces

The checkboxes under this heading are used to select the Ethernet interfaces that Top Talkers will monitor.

PPP Interfaces

The checkboxes under this heading are used to select the PPP interfaces that Top Talkers will monitor.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
eth	n	ttalker	on | off	Ethernet Interfaces
ppp	n	ttalker	on | off	PPP Interfaces

Display Top Talkers trace

Management > Top Talkers > Trace displays the current top talkers trace. For example:

Device administration tasks

This section describes the administration tasks that need to be performed on Digi devices periodically. It covers performing the following topics from the web interface and command line:

- View system information on page 766
- Manage files on page 769
- Manage X.509 certificates and host key pairs on page 788
- Update firmware on page 797
- Reset the router to factory default settings on page 798
- Execute a command on page 799
- Save configuration settings to a file on page 800
- Reboot the router on page 801

View system information

The **Administration > System Information** page gives an overview of the status of the router.

Model

The model of the router.

Part Number

The Digi part number of the router.

Ethernet 0 MAC Address

The MAC address of the **Ethernet 0** interface.

Firmware Version

The firmware version that is currently running on the router.

SBIOS Version

The SBIOS firmware version that is currently running on the router.

Build Version

The build configuration of the firmware that is currently running on the router.

HW Version

The hardware version on the router. This item may be blank.

CPU Utilization

The current and historical CPU utilization since the router booted up.

Up Time

The amount of time since the router booted up.

Date and Time

The current date and time on the router.

Total Memory

The total amount of RAM that is fitted on the router.

Used Memory

The amount of RAM that is currently being used on the router.

Free Memory

The amount of RAM that is currently free on the router.

Mobile Module

Which mobile module is fitted on the router.

SW Opts

Which firmware options are enabled on the router.

SW Cnts

Configuration parameters used by firmware.

Switch Mode

The current setting of the Ethernet switch on routers with multiple Ethernet interfaces. It can be either **Hub** or **Port Isolate**.

Related CLI commands

Command	Options	Equivalent Web Parameter
ati5	n/a	Model Firmware Version SBIOS Version Build Version Mobile Module SW Opts
hw	n/a	Part Number Ethernet 0 MAC Address HW Version
cpu	n/a	CPU Utilization
uptime	n/a	Up Time
time	n/a	Date and Time
mem	n/a	Total Memory Used Memory Free Memory

Manage files

The TransPort file system

The **dir** command described below is used to display a list of the currently stored files. A typical file directory will include the following files:

Filename	Description
ana.txt	Pseudo file for Protocol Analyser output
config.da0	Data file containing Config.0 settings
direct	File directory
eventlog.txt	Pseudo file for Event Log output
fw.txt	Firewall script file
fwstat.txt	Firewall script status file
image	Main system image
*.web	File containing compressed Web pages for your model
logcodes.txt	Text file containing Event Log config. info.
pwds.da0	File containing obfuscated passwords
sbios	TransPort BIOS and bootloader
sregs.dat	Data file containing AT command & S register settings
x3prof	X.25 PAD profile parameters

Once you have configured the router, you must save the chosen settings to non-volatile memory to avoid losing them when the power is removed.

- Application command settings are stored in one of two **CONFIG** files.

- AT command and S register settings are stored in one file named **SREGS.DAT**.

Config Files

Most configuration information is stored in one of two files called **CONFIG.DA0** and **CONFIG.DA1**. This allows two different sets of configuration information to be stored using the **Save** option in the directory tree at the left of the web interface, or by using the **config** command from the command line.

The **Save All** button saves the following files:

File name	Configuration held in file
config.da0	Main configuration parameters
pwds.da0	Encrypted passwords
fw.txt	Firewall rules
sregs.dat	Serial port S registers
x3prof	X.25 PAD profiles

You can select which of the two config files is loaded when the router is powered-up or rebooted by setting the parameter **Configuration > System > General > Miscellaneous > Use Config n when the router powers up** as required, or by using the **config n powerup** CLI command.

Note The **CONFIG** files only contain details of settings that have been changed from the default values.

SREGS.DAT file

A combined set of AT command and S register settings are called a profile. Two such profiles, profile **0** and profile **1**, can be stored for each **ASY** port in a file called **SREGS.DAT**. To save the file, use the **Save Profile** button on the relevant **Configuration > Network > Interfaces > Serial > Serial Port n** web page, or use the **AT&W** command.

Saving the settings for one ASY port does not save the settings for the other ports. You must save the settings for each port individually.

For each ASY port, the profile to be loaded at reboot or power-up is specified in the **Power-up Profile** setting on the relevant **Configuration > Network > Interfaces > Serial > Serial Port 0** web page, or use the **AT&Y** command).

You can load a profile for a particular **ASY** port to take immediate effect, using the **Load Profile** button on the ASY port's web page, the **ATZ** command.

PWDS.DA0 file

As of firmware version 4981, the encrypted forms of passwords entered into the configuration are stored in a separate file named **pwds.da0**. This file can only be accessed by users with **Super** level privileges. The file can be read with the type command, such as, type **pwds.da0**.

The **pwds.da0** file is only created when a password is changed from default and the configuration is saved. The encrypted versions of the default passwords are then removed from the **config.da0** file and the new **pwds.da0** is created and used instead.

If the **pwds.da0** file is deleted, all remote access to the router that requires authentication will fail, a serial cable connection will be required to re-configure passwords to gain access to the router. If both the **pwds.da0** file exists and the **config.da0** contains passwords also, the passwords in the **config.da0** take precedence and will overwrite the passwords in the **pwds.da0** when a **save** command is issued.

Manage files from the web interface

Following is information about managing files from the web interface's
Administration > File Management pages**.**

FLASH directory

The **Administration > File Management > FLASH Directory** web page displays a listing of files held on the router's flash file system.

The router has its own flash memory fling system that uses DOS-like filenames of up to 12 characters long: 8 characters, followed by the **.** separator, and a 3-character extension. The filing system is used to store the system software, Web pages, configuration information and statistics in a single root directory.

Files appear as hyperlinks, which can be downloaded and displayed in the web browser as long an appropriate viewer is installed and a file association with the viewer has been made.

The directory listing of files on the FLASH directory also shows the file size, the access of **rw** (read write) or **ro** (read only) and the date the file was last modified.

Below the file list is a summary of the FLASH file system, including the number of files, FLASH free, and FLASH used.

For example:

Action	File Name	Size	Access	Last Modified
	user	<DIR>		
	direct	52224 bytes	ro	12:56:14, 30 Mar 2011
	sbios	262144 bytes	ro	23:07:49, 22 Jan 2000
	mirror	52224 bytes	ro	12:56:14, 30 Mar 2011
☐	privpy.enc	61524 bytes	rw	23:05:40, 22 Jan 2000
☐	CAcert.cer	1371 bytes	rw	12:56:14, 30 Mar 2011
☐	x3prof	4096 bytes	rw	12:57:51, 30 Mar 2011
☐	sregs.dat	4096 bytes	rw	00:11:37, 01 Jan 2000
	config.fac	8395 bytes	ro	12:56:14, 30 Mar 2011
☐	LOGCODES.TXT	20008 bytes	rw	23:05:37, 22 Jan 2000
☐	passcng.py	836 bytes	rw	14:44:23, 05 Apr 2011
	sregs.fac	4096 bytes	ro	12:56:14, 30 Mar 2011
☐	python.zip	1631612 bytes	rw	23:06:04, 22 Jan 2000
☐	cert01.pem	3285 bytes	rw	12:56:14, 30 Mar 2011
☐	image4.c1	215801 bytes	rw	23:07:32, 22 Jan 2000
☐	privrsa.pem	887 bytes	rw	12:56:14, 30 Mar 2011
☐	config.da0	8520 bytes	rw	22:51:45, 07 Jan 2000
☐	manual.sb	26826 bytes	rw	12:56:14, 30 Mar 2011
☐	activate.sb	33685 bytes	rw	12:56:14, 30 Mar 2011
☐	gobiact.sb	22519 bytes	rw	12:56:14, 30 Mar 2011
☐	prlupdate.sb	31523 bytes	rw	12:56:14, 30 Mar 2011
☐	provision.sb	19501 bytes	rw	12:56:14, 30 Mar 2011
☐	pppfcs.sb	7784 bytes	rw	12:56:14, 30 Mar 2011
☐	queryimsi.sb	10661 bytes	rw	12:56:14, 30 Mar 2011
☐	wizards.zip	276265 bytes	rw	23:15:44, 22 Jan 2000

51 Files, Flash Used: 8375467 Bytes, Flash Free: 57753600 Bytes

Delete selected files

Sub-directories are not supported. Depending on the router mode, a maximum of **80-300** files,can be stored, including system files, providing there is sufficient memory remaining.

New files can be uploaded into the router from a local terminal or from a remote system over the WAN connection. Existing files can be renamed or deleted using DOS-like commands.

Although the file system will only store a limited number of files, all those files associated with the web interface are stored in a single file with the **.WEB** extension and extracted as required.

Action

Selects each read/write file for deletion.

File

The name of the file in the flash file system.

Size (bytes)

The size of the file, in bytes. This is not a fixed value. When downloaded, the size of the downloaded file will be different.

Access

This is the access settings for the file.

rw	Read / Write access
ro	Read Only access

Last Modified

The date and time of when the file was last modified.

Delete Selected Files

This button is used to delete the selected files.

Related CLI commands

Command	Options	Equivalent Web Parameter
dir		Displays the entire contents of the router's flash file system.
dir	<filter>	Displays a filtered view of the router's flash file system. The filter can contain wildcards using the *****. such as **dir *.pem** to display all the files ending in **.pem**.
dir	u:	Displays the contents of an USB flash stick if inserted into the USB port of the router.

WEB Directory

The **WEB** directory contains a list of the files held within the active web file. The web file is shown on the FLASH file system as a single file. This file is compressed and holds approximately 300 files.

Direct access to these files by an engineer is not normally required.

File	Size (bytes)	Compressed Size (bytes)
DIR.ASP	790	542
FLASHDIR.ASP	895	567
STYLE.css	5548	1964
GOAHEAD.GIF	1359	1526
red.GIF	821	592
green.GIF	813	583
ana.htm	452	290
ANATOP.HTM	1168	811
BGPHelp.html	4175	2173
eventtop.htm	1186	818
execmd.htm	961	658
fwcfg.htm	1324	850
fwlog.htm	462	294
fwlogTOP.HTM	321	248
GEN.HTM	460	281
snadescr.htm	640	495
STYLE.HTM	2561	951
tansdescr.htm	776	581
TIME.HTM	458	272
updfwTOP.htm	7777	3580
advnetcfg.asp	15702	6825
AIINCFG.ASP	3792	1658
AMMCFG.ASP	1972	1082
ANA.ASP	674	486

File

The name of the file in web file.

Size (Bytes)

The size of the file, in bytes.

Compressed Size (Bytes)

The compressed size of the file, in bytes.

File Editor

The file editor allows the user to edit text files on the router.

Filename

The name of the file to edit. In this field, you can create a new file by typing in the filename and clicking on the **Save File** button.

Load File

Load the file specified in the **Filename** field into the editor box.

Save File

Save the file to the flash file system.

Manage files from the command line interface

Use the following commands from the command line to perform file management tasks.

COPY command: Copy a file

The **copy** command makes a copy of a file. The format is:

copy <filename> <newfilename>

<filename>

The name of an existing file.

<newfilename>

The name of the new copy that will be created.

DEL command: Delete a file

The **del** command deletes files from the filing system. The format is:

del <filename>

<filename>

The name of an existing file.

You can also use wild cards in the filename in order to delete several files at once. The *****
character can represent one or more characters in the filename. For example, **del fw*.txt** will
delete files **fw.txt** and **fwstat.txt**. The **del** command returns **OK** if files have been deleted, or
ERROR if no matching files have been found.

DIR command: List the file directory

The dir command displays the file directory. For example:

```
dir
      direct      60720 ro   11:30:41, 31 Jan 2011 CRC  ???
       sbios     524288 ro   11:30:43, 31 Jan 2011 CRC 6ba8
      mirror      60720 ro   11:30:41, 31 Jan 2011 CRC  ???
       image    4300995 rw   15:22:23, 31 Jan 2011 CRC ab19
   sregs.dat       4096 rw   11:30:41, 31 Jan 2011 CRC 08b2
      x3prof       4096 rw   11:30:41, 31 Jan 2011 CRC bb5f
   CAcert.cer       1371 rw   11:30:41, 31 Jan 2011 CRC 6764
```

Each line shows:

- The file name and extension, if any
- The file size, in bytes
- The read/write status: **ro**=read only; **rw**=read/write
- The time/date of creation and the CRC value

Note File write operations are carried out as a background task and can be relatively slow due
to the constraints of FLASH memory. As a result, the file directory may only be updated
several seconds after a particular file operation has been carried out.

You can also use wildcards with the dir command in order to narrow your search. The ***** character can represent one or more characters in the filename. For example, **dir fw*.txt** will list only the **fw.txt** and **fwstat.txt** files, if they are present on the TransPort.

FLOCK command: Lock files

The **flock** command prevents any further writing to the FLASH memory. This means that no files can be written to, added to or deleted from the filing system.

FUNLOCK command: Unlock files

The **funlock** command unlocks the FLASH memory if it had been locked using the flock command. Files can then be added, deleted or copied to the filing system.

MOVE command: Move a file

The **move** command replaces one file with another while retaining the original filename. The format is:

```
move <fromfile> <tofile>
```

For example, the command:

```
move fw-temp.txt fw.txt
```

deletes the file called **fw.txt** and then rename the file called **fw-temp.txt** as **fw.txt**.

REN command: Rename a file

The **ren** command renames files in the filing system. The format is:

```
ren <oldfilename> <newfilename>
```

SCAN/SCANR command: Scan the file system

The **scan** command performs a diagnostic check on the file system and reports any errors that are found. For example:

```
scan
Please wait...
      direct ....ok
       sbios ....ok
      mirror ....ok
       image ....ok, data ok
   sregs.dat ....ok
      x3prof ....ok
  CAcert.cer ....ok
```

The scanning process may take several seconds so you should not enter any other commands until the results are listed.

The **scanr** command works in a similar fashion, except that it will return **ERROR** if any file is in error. This is useful when used with scripts that can look for the **ERROR** failure result.

TYPE command: Display a text file

The **type** command displays the contents of a text file. The format is:

```
type <filename>
```

For example:

```
type config.da0
[CFG]
config last_saved "12:04:45, 31 Jan 2011"
config last_saved_changes "1"
config last_saved_user "ASY 0"
eth 0 descr "LAN 0"
eth 0 IPaddr "10.1.51.3"
eth 0 mask "255.255.0.0"
eth 0 bridge ON
eth 1 descr "LAN 1"
eth 2 descr "LAN 2"
eth 3 descr "LAN 3"
eth 4 descr "ATM PVC 0"
```

XMODEM command: Initiate an XMODEM file upload

The xmodem command initiates an XMODEM file upload from the port at which the command is entered. The format is:

```
xmodem <filename>
```

<filename>

The name under which the file will be saved when the upload is complete.

After the **xmodem** command is entered, the router waits for your terminal program to start transmitting the file. When the upload is complete and the file has been saved, the router responds with the **OK** result code.

To initiate a remote XMODEM upload, establish a Telnet session over ISDN, and then issue the **xmodem** command from the remote terminal.

USB support

Most TransPort routers come equipped with USB ports that you can use to connect Mass Storage Devices (MSDs) such as external hard drives or flash-memory pen drives. All the files on the USB device are listed under the **USB Directory Listing** heading on the **Administration > File Management > FLASH Directory** page.

WARNING! For the TransPort WR31, the USB port is for use in a normal location only, not a hazardous location.

Note The USB storage device must be formatted using the FAT16 or FAT32 file system.

When the USB storage device is first inserted into the router, the operating system looks for a file named **autoexec.bat**, and if found, executes it. Other batch files can be executed by pressing the reset button one or more times. The batch file to be executed must be called **pb<n>.bat**, where **<n>** is the number of times the reset button is to be pressed to execute the file.

SD memory card support

Some TransPort routers are available with internal SD memory card, the drive letter assigned to this card is **s:**. To access the SD memory using an FTP client, the subdirectory assigned is **sdmmc**. The SD card can be used in the same way as USB MSDs. The SD card is internal and cannot be removed.

Batch control commands

Any batch file can contain one of the following two control lines: **ERROR_EXIT** or **ERROR_RUN**. If **ERROR_EXIT** is specified in a batch file, any commands run after that point in the file will cause the termination of the batch file if that command causes an error; for example, attempting to delete a file that does not exist. **ERROR_RUN** can be used to return the operation to default, which is to continue the execution of the batch file commands.

USB filing system commands

The USB storage device will respond to any of the standard filing system commands. For all filing system commands, the USB storage device is regarded as drive **u:**.

Note The router does not support sub-directories. Any sub-directories on the USB device will appear with a size of **0 bytes** on the **Administration > File Management > FLASH Directory** page.

Example 1:

To display the contents of the USB storage device, enter the command:

```
dir u:
SERIALS.TXT 1843
EVENTL~1.TXT 1449
USB.TXT 4278
MASSR1~1.TXT 1255
OK
```

If the USB storage device is empty, the following message is displayed:

```
No files
```

If no USB device is present, the following message is displayed:

```
No USB flash directory
```

Example 2:

To copy a file named **image** from the main flash memory onto the USB device, enter the command:

```
copy image u:image
```

To copy a file named **Logcodes.TXT** from the USB device to the main flash memory, enter the command:

```
copy u:Logcodes.TXT Logcodes.TXT
```

or

```
copy u:Logcodes.TXT
```

If no destination file is specified, the destination is set to the FLASH directory and the file name remains the same.

Use a USB devices to upgrade firmware

The following functionality is available from firmware version 4891 onwards.

The TransPort firmware can be upgraded using the USB storage device. To perform an upgrade:

1. Create a simple batch file named **pb2.bat**

2. Place the relevant firmware upgrade files into the **root** directory of the USB storage device.

3. Insert the USB device into the TransPort router.

4. Press the reset button twice. The firmware upgrade will begin. You will see output similar to the following:

```
ERROR_EXIT
del *.web
copy u:sbios1 sbios1
copy u:logcodes.txt logcodes.txt
copy u:image image
copy u:image4.c3 image4.c3
copy u:Y4890wVS.web Y4890wVS.web
move sbios1 sbios
scanr
flashleds
```

5. When the LEDs on the TransPort start flashing, the upgrade is complete.

6. Reboot the TransPort router to activate the new firmware.

Use USB devices with .all files

The following functionality is available from firmware version 4910 onwards.

A **.all** file is a special file that contains all of the firmware and configuration files in a single file that has the file extension .all and is an exact copy of the TransPort router in its current state. This **.all** file can then be applied to another TransPort router, as long as it is the same model.

1. To extract a **.all** file, use the Digi Flash Writer software.

2. Copy the extracted **.all** file to a USB storage device and insert the device into the TransPort router.

3. Issue the command **dir u:** to confirm that the TransPort can access the USB device.

4. To copy the **.all** file onto the TransPort router, from the command line enter this **copy** command:

```
copy u:mr4110.all t.all
```

Replace **mr4110.all** with the correct **.all** file name. The **t.all** destination name can be any destination. The source file (in this example, **mr4110.all**) must adhere to the 8.3 filename convention, owing to limits of the FAT file system, or the process will fail.

USB security

To prevent unauthorized access to a TransPort router using a USB storage device, such as inserting a USB storage device with an **autoexec.bat** file designed to copy usernames and passwords, etc., there are several commands available:

1. Use the **usbcon** command to define an access key. If the **.bat** file does not contain the matching key, it will not be allowed to execute.

2. Use the **uflash** command's **put** parameter to encode the matching key onto the file.

Note When using the **uflash** command, the filename should not be prefixed with **u:**, as the **uflash** command can only act on files stored on a USB storage device.

For example:

- To create a key, enter the command:

    usbcon 0 flashkey

- To encode this key onto a file called **autoexec.bat** on the USB storage device, enter the command:

    uflash autoexec.bat put

- To remove a key from a file, use the **uflash** command parameter **clr**:

    uflash autoexec.bat clr

Note To use the **uflash** command, you must be logged onto the router with **Super** access level.

By default, an **autoexec.bat** file is executed if found when a USB drive is inserted. Other batch files can also be executed. To control this behavior, issue the following command:

usbcon 0 batfile <off|on>

Disable/enable the USB ports

If required, you can disable the external USB ports. Disabling the USB ports prevents any unauthorized copying of files to or from the router, or unauthorized use of flash drives or serial devices connected to the USB ports.

To disable the USB ports, use the **usbcon** command.

The parameters to use on the **usbcon** command are:

dislist

Disables the USB port.

enalist

Explicitly enables a list of USB drivers. The driver list can be comma-separated to specify more than one driver if required.

The format of the **usbcon** command to disable the USB port is:

```
usbcon 0 usb-x-p<.p>.<DRIVER>
```

Where:

- **x=1** for the bottom USB port and 2 for the top port.
- **p=<port #>** (if connected to a USB hub the port numbers can increase).
- **DRIVER=MSD** for Mass Storage Device, **SERIAL** for serial devices, or **HUB** for hub devices.

For example:

- To disable a Flash Stick on the top port only:

```
usbcon 0 dislist usb-2-2.MSD
```

- To use wildcards to disable flash devices entirely:

```
usbcon 0 dislist usb-*.MSD
```

This will match on ALL MSD devices even if in another HUB.

- To disable both external USB ports on a DR64x0, enter the following commands:

usbcon 0 dislist "usb-1-2*,usb-2-2*"

or

```
usbcon 0 dislist "usb-?-2*"
```

The final **-2** is important in both cases. Otherwise, the command disables the internal USB devices, which could include connections to the wireless module or other components.

- To disable serial devices from using either external USB port on a DR64x0, or on a port connected to a hub on either these ports:

```
usbcon 0 dislist "usb-1-2*.SERIAL,usb-2-2*.SERIAL"
```

or

```
usbcon 0 dislist usb-?-2*.SERIAL
```

- The **enalist** takes the same format but when matches occur, it causes the device to be specifically enabled. If a device matches the enable list as well as the disable list the enable list will take preference. When a device matches a list an event is written to the event log of the form:

  ```
  "USB device usb-1-2.4.MSD disabled"
  ```

  or, if the device matches the **enalist**:

  ```
  "USB device usb-1-2.4.MSD enabled"
  ```

- These events can be used to debug the correct matching string to match on when trying to configure these parameters.

- If both lists are left blank, all drivers are enabled and no extra events appear in the event log.

Universal config.da0 using tags

The **config.da0** contains a list of commands, one per line that are parsed at boot. The commands in this file differ, depending on the model of the router, the firmware in use and the hardware options installed.

You can create a single universal configuration file using tags, defining sections that only relate to a specific hardware type or firmware version.

The tag values that can be used are:

- The base model, for example: **DR6410**
- The complete model, for example: **DR6410-H0A**
- The platform build string, for example: **8W**
- The type of DSL, for example: **DSL2**, **2+**
- The type of WWAN module detected, for example: **E** (Edge), **C** (CDMA)
- The complete WWAN module string, for example: ,**MOTO_G24 SIEMENS_GPRS**, **SIEMENS_MC75**, **NOVATEL_3G**, **SIERRA_3G**, **OPTION_3G**, **NOVATEL_CDMA**, **CMOTECH_CDMA**, **SIERRA_CDMA**
- PSTN or ISDN module, for example: **PSTN**, **ISDN**

Enclose the tags within angle brackets. Open AND close the configuration sections with the relevant tag.

For example, to open: **<DR6410>**

To close: **</DR6410>**

Note the use of the **/** in the closing tag.

To view a list of defined tags on a router, use the CLI command **tags**. Following is example output of the **tags** command:

```
Router>tags
tags defined:..
TransPort
DR64
dr6410
8W
OPTION_3G
ISDN
DSL
61690
OK
```

Example scenario:

A single configuration file is required for a range of DR6410 routers, there is a mix of three types of 3G WWAN modules and some have GPRS modules installed. Different W-WAN modules need different modemcc commands to correctly configure the ASY ports. All these modules can have their own specific commands in one config file.

Example configuration using tagged sections:

You can use in configuration files to make them easier to read. Comments are in red and prefixed with a **#** symbol. In the example below, the **info_asy_add** parameters are for illustration purposes only and are not the actual ASY port numbers used.

```
<DR6410-H0A>
#Start of DR6410-H0A config

<NOVATEL_3G>
#Start of Novatel specific config
modemcc 0 asy_add 7
modemcc 0 info_asy_add 8
#End of Novatel specific config
</NOVATEL_3G>

<OPTION_3G>
#Start of Option specific config
modemcc 0 asy_add 7
modemcc 0 info_asy_add 9
#End of Option specific config
</OPTION_3G>

<SIERRA_3G>
#Start of Sierra specific config
modemcc 0 asy_add 7
modemcc 0 info_asy_add 10
#End of Sierra specific config
</SIERRA_3G>

#End of DR6410-H0A config
</DR6410-H0A>

<DR6410-E0A>
#Start of DR6410-E0A config
modemcc 0 asy_add 7
modemcc 0 info_asy_add 11
#End of DR6410-E0A config
</DR6410-E0A>

#Rest of generic config goes below here
modemcc 0 apn internet"
eth 0 ipaddr 192.168.0.99
```

Manage X.509 certificates and host key pairs

The X.509 Certificate Management pages are for loading and managing X.509 certificates and public/private host key pairs that are public key infrastructure (PKI) based security.

Certificate Authorities (CAs)

- A certificate authority (CA) is a trusted third party that issues digital certificates for use by other parties. digital certificates issued by the CA contain a public key.

- The certificate also contains information about the individual or organization to which the public key belongs.

- A CA verifies digital certificate applicant's credentials.

- The CA certificate allows verification of digital certificates and the information contained therein, issued by that CA.

Installed Certificate Authority Certificates

Subject	Issuer	Expiration	Filename		
testCA	testCA	Jul 7 15:12:49 2015 GMT	ca0.pem	View	Delete

This table lists the current CA certificates that have been installed onto the router. Use the **View** button to view the contents of each certificate.

Upload CA Certificates

Upload certificate authority (CA) certificates. Files may be in ASN.1 DER or PEM Base64 encoded formats.

Upload File: [_____] Browse...

Upload

Use the **Browse** and **Upload** buttons to upload CA Certificates from a host PC onto the router.

Obtain CA certificates from a SCEP Server

The Simple Certificate Enrollment Protocol (SCEP) allows the user to request and enroll CA certificates from a CA server.

The CA certificate files are automatically stored with the name **CA<n>.pem**, where **n** increments with each certificate.

SCEP Server IP address

The IP address of the SCEP server/CA server.

Port

The port on which SCEP server is listening. If the port is **0**, the default port of **80** will be used.

Path

The path on the server to the SCEP application. The path can either be entered manually if known, or select from cgi-bin or Microsoft SCEP from the drop-down list.

Application

The SCEP application running on the server.

CA identifier

The identifier for the CA server. The CA identifier to use to identify a particular CA when multiple CAs might be running on the server.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
scep	0	host	IP Address	SCEP Server IP address
scep	0	port	0-65535	Port
scep	0	path	String	Path
scep	0	app	String	Application
scep	0	caident	String	CA Identifier

IPsec/SSH/HTTPS certificates

- The **IPsec/SSH/HTTPS certificates** page contains fields that required when sending a certificate request to a Certificate Authority (CA).

- This information forms part of the certificate request, and thus part of the signed public key certificate.

- The router can use certificates to establish IPsec tunnels with other routers and support SSH and HTTPS connections. For more information on using certificates with the router,

- See the *Application Note 22, IPSec VPN tunnel between two Digi Routers using Certificates and SCEP*, available at www.digi.com.

Installed Certificates

This table lists the current certificates that have been installed onto the router. It is possible to view the contents of each certificate using the **View** button.

Installed Certificates

Subject	Issuer	Expiration	Key Size	Filename		
DigiCA_demo	testCA	Jul 7 15:22:35 2011 GMT	1024	cert0.pem	View	Delete
DigiCA_demo	testCA	Jul 7 15:22:36 2011 GMT	1024	cert1.pem	View	Delete

Upload Certificate or Private Keys

In the Upload Certificate or Private Keys section, you can upload certificates and private key files from a host PC onto the router using the **Browse** and **Upload** buttons.

Upload Certificate or Private Keys

Upload RSA keys and certificates. Certificate and key files may be in ASN.1 DER or PEM Base64 encoded formats.

Upload File: [_____] Browse...

Upload

Create, enroll, and install certificate requests

The following parameters allow you to create a certificate request, enroll them and to install the certificates on the router.

SCEP Server IP address

The IP address of the SCEP server / CA server.

Port

The port on which the SCEP server is listening. If the port is **0**, the default port of **80** is used.

Path

The path on the server to the SCEP application. You can either enter your own path or select from cgi-bin or Microsoft SCEP from the drop-down list.

Application

The SCEP application running on the server.

CA identifier

The identifier for the CA server. The CA identifier to use to identify a particular CA when multiple CAs might be running on the server.

CA certificate

The filename of the CA certificate.

CA encryption certificate

Sometimes when you get a CA certificate, a CA encryption certificate is installed on the router at the same time. You can identify a CA encryption certificate by looking at the **X.509 Key Usage** section in the certificate. It should display something like the following:

```
X509v3 Key Usage: critical
    Key Encipherment, Data Encipherment
```

If a CA encryption certificate has been installed by the CA you wish to use for the certificate request, enter the CA encryption certificate. If no CA encryption certificate has been installed for the CA, leave this file blank.

CA signature certificate

Sometimes when you get a CA certificate, a CA signature certificate is installed on the router at the same time. You can identify a CA signature certificate by looking at the **X.509 Key Usage** section in the certificate. It should say something like the following

```
X509v3 Key Usage: critical
    Digital Signature, Non Repudiation
```

If a CA signature certificate has been installed by the CA you wish to use for the certificate request, enter the CA signature certificate. If no CA signature certificate has been installed for the CA, leave this file blank.

RSA Private key

Selects either using an existing private key or generating a private key for each certificate request.

Private key filename

The filename of the private key file to use.

Enrolment Password

Before you can create a certificate request you must first obtain a challenge password from the Certificate Authority Server. This password is generally obtained from the SCEP CA server by way of a WEB server or a phone call to the CA Server Administrator. For the Microsoft® SCEP server, you browse to a web interface. If the server requires a challenge password, it will be displayed on the page along with the CA certificate fingerprint. This challenge password is usually only valid once and for a short period of time, in this case 60 minutes, meaning a certificate request must be created after retrieving the challenge password.

Common Name (CN)

A name for the router. This parameter is important, as the common name will be used as the router's ID for IKE negotiations.

Country Code (C)

The two-character county code of where the router is located. A list of valid country codes can be found at http://www.iso.org/iso/english_country_names_and_code_elements.

State or Province (ST)

The state, county, or province of where the router is located.

Locality (L)

The town or city of where the router is located.

Organisation (O)

The company to whom the router belongs to.

Organisational Unit (OU)

The company department maintaining the router.

E-mail

An appropriate email address of a contact for the router.

Unstructured Name

This parameter is optional. It can contain some descriptive to help identify the certificate.

Digest Algorithm

The digest algorithm used (MD5 or SHA1) when signed the certificate request.

Ignore NONCE in SCEP response

The parameter instructs the router to ignore the **NONCE** field in the SCEP response. The **NONCE** field is primarily used to prevent replay attacks.

Related CLI commands

scep command

Entity	Instance	Parameter	Values	Equivalent Web Parameter
scep	0	host	IP Address	SCEP Server IP address
scep	0	port	0-65535	Port
scep	0	path	String	Path
scep	0	app	String	Application
scep	0	caident	String	CA Identifier
scep	0	cafile	Filename	CA certificate
scep	0	caencfile	Filename	CA encryption certificate
scep	0	casigfile	Filename	CA signature certificate
creq	0	challenge_pwd	String	Enrolment Password
creq	0	commonname	String	Common Name (CN)
creq	0	country	String	Country Code (C)
creq	0	state	String	State or Province (ST)
creq	0	locality	String	Locality (L)
creq	0	orgname	String	Organisation (O)
creq	0	org_unit	String	Organisational Unit (OU)
creq	0	email	Email Address	E-Mail
creq	0	unstructname	String	Unstructured Name
creq	0	digest	MD5 or SHA1	Digest Algorithm

creq command

You can use the **creq** command to generate the certificate request using the configured parameters. If the private key does not already exist and appropriate parameters are entered, the key will be generated at the same time.

- To generate a certificate request, enter the command:

  ```
  creq new -k<priv key file> -o<cert request file>
  ```

- To generate a private key and a certificate request, enter the command:

  ```
  creq new ?b<priv key length> -k<priv key file> -o<cert req file>
  ```

  For example, to generate a certificate request file called **request.pem** from a private key called **priv001.pem**, enter:

  ```
  creq new -kpriv001.pem -o request.pem
  ```

  To generate a 512 bit private key called **private.pem**, and generate a certificate request called **certreq.pem** using that file, enter:

  ```
  creq new -b512 -kprivate.pem -ocertreq.pem
  ```

Key Generation

The **Key Generation** page allows you to generate a private key. You must create a private key before a certificate can be requested, as the private key is used in the request. The fields on this page are as follows:

Key filename

A name for the private key. The filename must be prefixed with **priv** and have a **.pem** extension.

Key size

The size of the private key, in bits. The larger the key, the more secure the connection. But also, the larger the key, the slower the connection. The key size can be one of the following:

- **384**

- **512**

- **768**

- **1024**

- **1536**

- **2048**

Save in SSHv1 format

If this checkbox is checked the private key will be generated in SSH version 1 format. If it is cleared, the private key will be generated in SSH version 2 format.

Related CLI commands

You can use the **genkey** command to generate a private key file.

To generate a private key, enter the command:

```
genkey 0 <keysize> <filename> <-ssh1>
```

where

- **<keysize>** is the size of the key in bits.
- **<filename>** is the name of the private key file.
- **<-ssh1>** is optional, and will generate the private key file in SSH version 1 format.

Note IPsec requires SSH version 2 private keys.

For example, to generate a 1024 bit SSH version 2 key called privkey.pem, enter:

```
genkey 1024 privkey.pem
```

You will see the following output:

```
OK
Starting 1024 bit key generation. Please wait. This may take some time...
Key generated, saving to FLASH file privkey.pem
Closing file
Private key file created
All tasks completed
```

Private key files: Splitting certificates

For increased security, you can split the private key file between the router flash and an USB memory stick. Once a private key has been split and stored in two parts, the USB memory stick must be present for any successful IKE negotiations that involve the private key. Because the USB memory stick only contains a part of the private key, it cannot be used in another router.

The command to split a private key is:

```
privsplit <certificate filename>
```

Update firmware

The **Administration > Update Firmware** page allows the user to update the router's firmware. The router will download a zip file onto the router, uncompress it, validate each file within the zip file and then update the files in its flash file system.

The zip file containing the latest firmware version is available from the Digi website (http://transport.digi.com/digi/firmware/ftp/). Download the zip file to your PC before starting the firmware update.

Note Do not navigate away from the **Update Firmware** page while an update is in progress, as that action can cause the update to abort prematurely.

CAUTION! Do not remove the power from the router while an update is in progress, as it can corrupt the router's flash file system and might leave the router unable to boot up.

Model

The model of the router.

Firmware Version

The current firmware version running on the router.

Select Firmware

Select the zip file on your PC containing the firmware version to you wish to update to.

Once the firmware update is complete, reboot the router.

Reset the router to factory default settings

The **Administration > Factory Default Settings** page resets the router's configuration back to the factory defaults. You must reboot the router before the configuration changes take effect.

Keep network settings

Selecting this option preserves certain network settings does not revert them back to the factory defaults. The network settings that are preserved are:

- Ethernet 0 IP address
- Ethernet 0 Mask
- Ethernet 0 Gateway
- Ethernet 0 DHCP Client
- Ethernet 0 DNS Server
- Default Route 0 Interface
- PPP 1 Username
- PPP 1 Password
- PPP 3 Username
- PPP 3 Password
- Mobile APN
- Mobile SIM PIN

Restore

Initiates a factory reset of the router.

Related CLI commands

To reset the router's configuration to the factory defaults, use the following commands:

```
del pwds.da0
```
```
copy config.fac config.da0
```

These commands assume you are using configuration profile **0**. If you are using configuration profile **1**, use the suffix **.da1** instead.

Using these commands does not preserve any network settings.

Reset the router using the hardware reset button

- Most routers have a reset button on the underside of the router.
- To perform a factory reset on the router, press and hold the reset button for 5 seconds.
- When the reset is initiated in this manner, the LEDs on the front of the router flash to indicate a reset is in progress.
- The router automatically reboots once the factory reset is complete. Do not remove the power while the router is running this reset procedure.
- Using this method will not preserve any settings.
- To disable the reset button, enter:

  cmd 0 pbreset off

- To re-enable the reset button functionality, enter:

  cmd 0 pbreset on

Execute a command

- The **Administration > Execute a Command** page allows CLI commands to be entered via the web browser.
- Almost all of the CLI commands detailed in this reference guide can be entered from this page.
- Enter the command name and click the **Execute** button.
- The command output is displayed, as shown in the following example.

Save configuration settings to a file

Once you have configured the router, save your chosen settings to non-volatile memory to avoid losing them when the power is removed.

Save current configuration to Config n

Sets the configuration file to which the current configuration will be saved when the **Save** button is clicked. There are two options: **profile 0** and **profile 1**. The configuration profile used when the router powers up is indicated in the selection box. The default power-up profile is **profile 0**.

Save all configuration

The **Save All** button saves the router's entire configuration.

- The current configuration parameters are saved to **config.da0** or **config.da1** file**.

- The ciphered versions of the passwords are saved to the **pwds.da0** or **pwds.da1** file**.

- The Firewall configuration is saved to the **fw.txt** file.

- The serial port configuration is saved to **profile 0** of the **sregs.dat** file.

- The PAD parameters on all the PADs are saved to **profile 0** of the **x3prof** file

Related CLI commands

Parameter	Options	Equivalent Web Parameter
config	save	Save current configuration to Config n
saveall	n/a	Save all configuration

** The default power up profile is **profile 0**. ***.da0**=profile 0, ***.da1**=profile 1.

Reboot the router

To reboot the router immediately or at a scheduled time, select **Administration > Reboot**.

A reboot will be performed after any FLASH write operations have been completed. Also, one second each is allowed for the following operations to be completed before reboot will take place:

- IPSec SA delete notifications have been created and sent
- TCP sockets have been closed
- PPP interfaces have been disconnected

Immediately

Causes the router to reboot after a few seconds. The router will cleanly terminate any TCP and VPN connections before rebooting.

In h hrs m mins s secs

Cause as reboot to be scheduled after the configured period of time.

A scheduled reboot can be canceled by clicking the **Cancel** button.

Related CLI commands

Command	Options	Equivalent Web Parameter
reboot	n/a	Immediately
reboot	0-86400	In h hrs m mins s secs. This CLI value is entered in minutes only.
reboot	cancel	Cancel reboot

Troubleshooting

This section provides information on resources and processes available for troubleshooting your Digi TransPort device, and covers resolution of several common issues.   It covers the following topics:

Troubleshooting Resources

There are several resources available to you for support of your Digi product or resolving configuration difficulties at Digi's Support site, http://www.digi.com/support

On Digi's Support site, you can access:

- Digi's Support knowledge base

- Digi TransPort support documents

- If the knowledge base or support forums do not have the information you need, fill out an Online Support Request via: https://mydigi.secure.force.com/customers/. You will need to create a user account if one is not already set up.

When submitting a support request, please include a copy of the **debug.txt** file from the device's flash. This will greatly improve the quality of the initial response you receive. It will help the Digi Support team to provide accurate answers to your queries.

Download the debug.txt file

To download the debug.txt file from your Digi TransPort device:

1. Browse to the router's IP address to connect to the web interface.

2. Navigate to **Administration > File Management > FLASH Directory**.

3. The **debug.txt** file is usually the last file listed. Right-click on **debug.txt** and click **Save target as**.

4. Send the **debug.txt** file as an attachment.

Note For Digi TransPort WR44 RR, there are several ways to download the **debug.txt** file. For information on the other methods, see *Quick Note 24 - Extracting the debug.txt file from a Digi TransPort or Sarian router*, available on www.digi.com.

Cannot open the web interface

If you cannot open the web interface:

1. Make sure that the LAN cable is properly connected to the LAN port and that the LAN status indicator on the front of the device is illuminated.

2. If it is not, then there is a problem with either the LAN cable or the device to which the TransPort device is connected. If the status indicator is illuminated, check that the PC can communicate with the device. To do this, open the Command Prompt window on your PC and enter the command ping **192.168.1.1**. If you do not get a response, you may have a connection problem. Try one or more of the following methods to establish a connection:

   • Use the Digi Device Discovery Utility. The IP address of the device may have been changed from its default IP address of **192.168.1.1**. The Digi Device Discovery Utility can usually discover the device on a network, unless your system's firewall is enabled.

   • Check the PC's IP configuration. Make sure it is set to obtain an IP address automatically. If not, configure it to automatically obtain the IP address.

   • Refresh the PC's IP settings by opening a command window and entering the following commands:

     ipconfig/release

     ipconfig/renew

   • Check the PC's LAN connection and any LAN device (such as an Ethernet switch) that connects to the router. Make sure the PC is connected to the network.

   • Clear the PC's ARP cache with the command **arp –d ***, then retry the **ping** command. If you do get a response but are unable to view the web interface, then there is most likely a problem with your web browser configuration.

Cannot log into the web interface

If you cannot log in to the web interface, you will need to access the device via Telnet or SSH in order to configure it using the Command Line Interface (CLI). See Use the Digi TransPort command-line interface on page 111for more information.

Troubleshoot the LTE-MIMO antenna orientation

The two LTE antennas should be separated at the maximum distance possible, taking into consideration the available space of the installation. There should be a minimum distance of 1.5 inches between two antennas.

Glossary

0-9

3DES   Triple Data Encryption Standard

A

ACCM   Asynchronous Communication Channel Multiplexer

ACFC   Address Control Field Compression

ADSL   Asymmetric Digital Subscriber Line

AES   Advanced Encryption Standard

AFE   Analogue Front End

AH   Authentication Header

AIS   Alarm Indication Signal

AODI   Always On Dynamic ISDN

APACS   Association of Payment Clearing Services, the UK payments association

APN   Access Point Name

ATM   Asynchronous Transfer Mode or Automatic Teller Machine

ARFCN   Absolute Radio Frequency Channel Number

B

BACP	Bandwidth Allocation and Control Protocol
BAP	Bandwidth Allocation Protocol
BCC	Base station Colour Code
BCCH	Broadcast Control Channel
BGP	Border Gateway Protocol

C

CA	Certificate Authority
CHAP	Challenge Handshake Authentication Protocol
CLI	Calling Line Identification or Command Line Interface
CRC	Cyclic Redundancy Code
CTS	Clear To Send
CUD	Call User Data
CUG	Call User Group

D

DCE	Data Communication Equipment
DER	Distinguished Encoding Rules
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DLSw	Data-Link Switching
DNS	Domain Name Server
DPD	Dead Peer Detection
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
DTE	Data Terminal Equipment
DUN	Dial-Up Networking

E

EDGE	Enhanced Data GSM Environment
ESP	Encapsulating Security Payload protocol

F

FCS	Frame Check Sequence
FEC	Forward Error Correction
FIFO	First In First Out
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol

G

GPRS	General Packet Radio System
GPS	Global Positioning System
GRE	Generic Routing Encapsulation
GSM	Global System for Mobile Communications

H

HDLC	High-Level Data Link Control
HEC	Header Error Control
HMAC	Hash Message Authentication Code
HSDPA	High Speed Downlink Packet Access
HSUPA	High Speed Uplink Packet Access

I

ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IKE	Internet Key Exchange
IMEI	International Mobile Equipment Identification
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPCP	Internet Protocol Control Protocol
IPSec	Internet Protocol Security
ISAKMP	Internet Security Association and Key Management Protocol
ISDN	Integrated Services Digital Network

L

L2TP	Layer 2 Tunnelling Protocol
LAC	Location Area Code
LAI	Location Area Identity
LAN	Local Area Network
LAPB	Link Access Procedure Balanced
LAPD	Link Access Protocol D-channel
LCN	Logical Channel Number
LCP	Link Control Protocol
LRC	Longitudinal Redundancy Check
LSA	Link State Advertisement

M

MAC	Media Access Control
MCC	Mobile Country Code
MD5	Message-Digest algorithm 5
MIB	Management Information Base
MIME	Multipurpose Internet Mail Extensions
MLPPP	Multi-Link Point-to-Point Protocol
MNC	Mobile Network Code
MPPE	Microsoft Point to Point Encryption
MRU	Maximum Receive Unit
MSN	Multiple Subscriber Number
MSS	Maximum Segment Size
MTU	Maximum Transmit Unit

N

NAPT	Network Address and Port Translation
NAS	Network Access Server
NAT	Network Address Translation
NCC	Network Colour Code
NOM	Network Operation Mode
NUA	Network User Address
NUI	Network User Identifier

O

OAM	Operation, Administration and Maintenance
OOS	Out Of Service
OPNS	Online PUK Negotiation Service
OSPF	Open Shortest Path First

P

PANS	Polling Answering Service
PAD	Packet Assembler/Disassembler
PAP	Password Authentication Protocol
PAT	Priority Access Threshold
PBCCH	Packet Broadcast Control Channel
PEM	Privacy Enhanced MIME
PFC	Protocol Field Compression
PFS	Perfect Forwarding Security
PID	Protocol Identifier
PIN	Personal Identity Number
PLMN	Public Land Mobile Network
PPP	Point-to-Point Protocol
PPPoA	Point-to-Point Protocol over ATM
PPPoE	Point-to-Point Protocol over Ethernet
PSDN	Packet Switched Data Network
PSI	Packet System Information
PSTN	Public Switched Telephone Network
PUK	Power Up Key
PVC	Permanent Virtual Circuit

Q

QOS	Quality of Service

R

RAC | Routing Area Code

RACH | Random Access Channel

RADIUS | Remote Authentication Dial-In User Service

RAT | Radio Access Technology

RDI | Remote Defect Indication

RIP | Routing Information Protocol

RSSI | Received Signal Strength Indication

RTS | Request To Send

S

SA | Security Association

SABM | Set Asynchronous Balanced Mode

SABME | Set Asynchronous Balanced Mode Extended

SCEP | Simple Certificate Enrolment Protocol

SDLC | Synchronous Data Link Control

SHA-1 | Secure Hash Algorithm 1

SMS | Short Message Service

SMTP | Simple Mail Transfer Protocol

SNA | Systems Network Architecture

SNAIP | Systems Network Architecture over Internet Protocol

SNMP | Simple Network Management Protocol

SNTP | Simple Network Time Protocol

SPF | Shortest Path First

SPI | Security Parameters Index

SSH | Secure Shell

SSL | Secure Socket Layer

SVC | Switched Virtual Circuit

T

TANS	TPAD Answering
TCH	Traffic Channel
TCP	Transmission Control Protocol
TEI	Terminal Endpoint Identifier
TOS	Type of Service
TPAD	Transaction Packet Assembler/Disassembler

U

UBR	Unspecified Bit Rate
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus

V

VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol

W

WAN	Wide Area Network
WCDMA	Wide-band Code-Division Multiple Access
WRED	Weighted Random Early Dropping
W-WAN	Wireless Wide Area Network

X

XOT	X.25 Over TCP