Digi TransPort User's Guide

90001019_H
9 July 2012

Contents

Introduction

Thank you for choosing a data communications product from Digi International. Digi products are extremely versatile and may be used in a wide variety of applications. It would not be possible to describe in detail all such applications in a single guide. Consequently, this guide has been written for use by technically competent personnel with a good understanding of the communications technologies used in the product, and of the requirements for their specific application.

Digi International designs and manufactures a wide range of both wireline and wireless network routing products. For a complete, up-to-date list of current products, please visit the Digi International web site at www.digi.com.

Whilst each of these models provide a different combination of hardware and software features, the basic method of configuration using the web interface or command line is the same in each case. This guide describes the operation of standard features available across the whole product range. Consequently, some of the features described in this guide may only be available on certain models or must be purchased as optional "feature packs". You should refer to the specification of the particular model you have purchased to ascertain which features are supported as standard.

In addition to a comprehensive range of communications capabilities, our products provide a combination of powerful, yet easy to use, configuration, management and diagnostic tools. These include a protocol analyser, a time-stamped event log and remote management via the web interface or via a Telnet session.

In many applications, the serial ports will be configured to appear as if they were standard "AT" modems and behave accordingly. However, many other standard protocols are supported (e.g. B- and D-channel X.25, PPP, TPAD, V.120, etc.). This makes it simple and cost-effective to migrate existing terminal equipment, which uses the analogue telephone network, to faster, more reliable and cost effective "wireline" or wireless digital services.

All major features of the unit can be configured using a standard Web browser. This can be done locally (via a serial or LAN port), or remotely via a WAN connection. A built-in Web-server and flexible FLASH-memory based filing system mean that the unit can also be customised to provide application specific functions, statistics and diagnostic information.

Requests for corrections or amendments to this guide are welcome and should be addressed to:

Digi International
11001 Bren Road East
Minnetonka, MN 55343

Typographical Conventions

Throughout this manual certain typographical conventions are used as follows:

Text Type	Meaning
Text like this	… is standard text.
Note: Text like this …	indicates points that are of particular importance.
Text like this …	indicates commands entered by the user at the command line.
Text like this …	indicates responses from the unit to commands you enter at the command line.
Configuration – Network > Interfaces	refers to the unit's web-based menu system.

Warnings

Radio Equipment - Canadian Warning Statements

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

- This device may not cause interference.
- 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.

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: MCQ55M1644' placed on it in line with FCC labelling regulations.

Obtaining Technical Support

Technical support for your Digi Transport router is readily available using the following methods.

Self help

Visit the Technical Support section of the Digi website at www.digi.com

From here, you can gain access to FAQs, knowledge base articles, application guides, quick setup guides, installation guides, software applications, firmware upgrades, product literature, warrantyregistration & a support forum.

Assisted help

To obtain support from the Digi Technical Support team, use one of the options below. The preferred method is either via the web portal or via email. This is because the support teams will ask for certain technical information which is required at the time the query is logged.

The support teams request that the following information is included with every support request:

- Hardware model
- Firmware revision
- Current configuration (config c show)
- Firewall configuration
- ADSL / Mobile status and relevant PPP status
- The event log

This information and more can be quickly and easily obtained from the router by downloading the single file debug.txt from ***Administration - Directory Listings > FLASH directory*** using the GUI, or, via the CLI with the command **`type debug.txt`** and send the output to a log file.

The file contents are created when the file is requested, so it may take a few seconds to create and download the file. **Please zip this file and include it with your support request.**

For more complex technical support queries, a detailed network diagram may also be requested.

Web portal

To log a support request online using the web portal, browse to www.digi.com and hover your mouse over the 'Support' link at the top of the page, select 'Online Support Request' from the dropdown list. The direct URL for the web portal is http://www.digi.com/support/eservice

You will need to create an account to use this service.

Remember to upload the debug.txt zip file!

Email

Email support is available from 2 locations:

UK

uksupport@digi.com

USA

support.wizards@digi.com

Remember to attach the debug.txt zip file to your email!

Telephone

Telephone support is available from 2 locations:

UK

Telephone support is available 09:00 - 17:30 GMT.

From within the UK: 0870 350 0035

International: +44 1943 605 055

USA

Telephone support is available 07:00 - 17:30 CST (GMT -6 Hours).

From within the Americas: 952 912 3456

International: +1 952 912 3456

Please be aware, we may ask you to submit your technical support query by email and include the debug.txt zip file.

Using the Web Interface

To access the built-in web pages using a web browser (e.g. Internet Explorer), there are two options.

To access the LAN port follow the instructions below. To access the web interface over a serial connection,see Web Access via Serial Connection.

Access Via a LAN Port

By default, the Digi Transport has a static IP address of 192.168.1.1 with DHCP server enabled. To acess the unit using a web browser (e.g. 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, i.e. 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

Using the 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 unit and this process is described in the next chapter. However, if you do not have access to a Web browser, the unit 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.

To use the serial ports you will need a PC and some communications software such as HyperTerminal ™ (supplied with Windows) or TeraTerm™. The same commands may also be used to configure the unit remotely via Telnet, X.25 or V.120.

There are several types of text command:

AT Commands & S Registers

AT commands (pronounced "ay tee") and Special registers (S registers) are supported in order to maintain compatibility with modems when the unit is used as a modem replacement.

Application Commands

Application commands are specific to Digi International products and are used to control most features of the unit when not using the Web interface.

X.3 Commands

These are standard X.3 commands which are used only in X.25 PAD mode

TPAD Commands

These are used only in TPAD mode.

The "AT" Command Interface

Command Prefix

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

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

Unless you have previously configured the unit to automatically connect to a remote system on powerup, it will now be ready to respond to commands from an attached terminal and is in "command mode".

Now type "AT" (in upper or lower case), and press [Enter]. The unit should respond with the message "OK". This message is issued after successful completion of each command. If an invalid command is entered, the unit 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 you may use the "ATE0" command (which will appear as "AATTEE00"), to prevent the unit from providing command echo. After this command has been entered, further commands will be displayed without the echo.

The "AT" command prefix and the commands that follow it can be entered in upper or lower case. After the prefix, you may enter one or more commands on the same line of up to 40 characters. When the line is entered, the unit will execute each command in turn.

CLI parameter tables and how to use them

After every section, there will be a table that details the CLI parameters that relate to the web based parameters.

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…

An example CLI parameter table would look like the following for Ethernet parameters.

Entity	Instance	Parameter	Values	Equivalent Web Parameter
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 the values as appropriate. Only the first 4 columns are needed for the CLI parameters, the right hand column shows the equivalent web based parameter.

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:

```
eth 0 descr "Local LAN"
```

Take note that 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
```

The Escape Sequence

If you enter a command such as "ATD", which results in the unit 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 unit to the remote system. In the same way, data from the remote system will pass straight through to your terminal.

The unit 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 unit 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.

Result Codes

Each time an AT command line is executed, the unit 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 unit 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 section heading "S registers".

Digi Application Commands

The unit 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 i.e. they are related to the general operation of the unit; others are application or protocol specific.

Application commands may 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 unit is responding to AT commands correctly and then enter the command:

```
AT\LS
```

The speed will remain locked until the unit goes on-line and then off-line again, the power is removed or the unit 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.

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 but 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.

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.

Wildcards in the CLI

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' then command is:

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
```


The Reboot Command

The **reboot** command is used to reboot the unit after altering the configuration. It has three modes of operation:

reboot - will reboot the unit 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> - will reboot the unit in <n> minutes where n is 1 to 65,535

reboot cancel - will cancel a timed reboot if entered before the time period has passed.

The Active Port

When entering "AT" or text commands it is important to understand that 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.

Establishing a Remote Connection

- Once you have finished configuring the unit, there are several ways of establishing a link to a remote system:
- An outgoing V.120 call may be made using the "ATD" command
- You can initiate a DUN session to establish a dial-up PPP connection.
- An outgoing X.25 call may be made using the "ATD" command followed by the X.28 CALL command.
- An outgoing TPAD (Transaction PAD) call may be made by using the TPAD "a" (address) command followed by the appropriate NUA (this is normally only carried out under software control).

Similarly, incoming calls will be handled according to which protocols have been bound to the ASY ports and whether or not answering is enabled for each protocol.

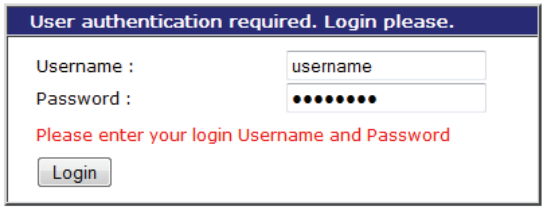
Configuring your TransPort router

This section describes the various configuration parameters for the unit and how to set or change them using the built-in web pages or the text commands. Configuration using the Web pages is achieved by entering the required values into text boxes or tables on the page, or by turning features on or off using checkboxes. The same results can be achieved entering the appropriate text commands via one of the serial ports.

Logging In

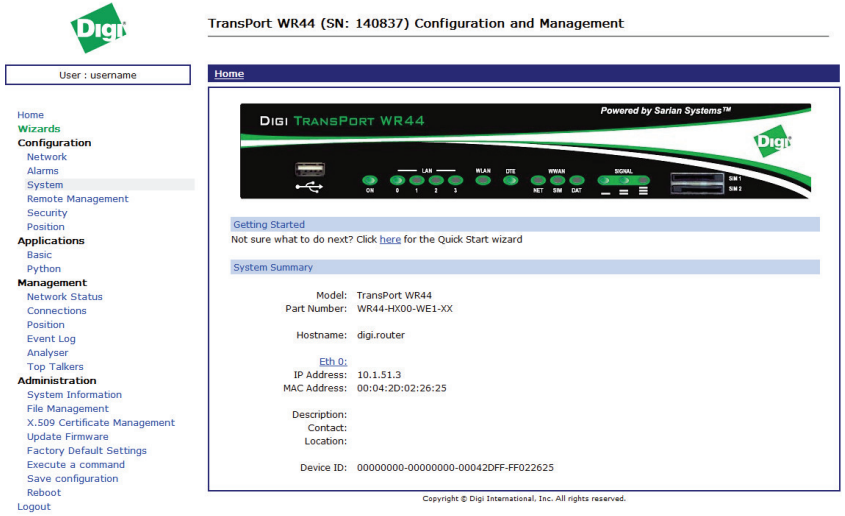
To configure the unit via the Web interface, either establish a DUN connection to it and then open your web browser and enter 1.2.3.4 for the web address, or enter the unit's Ethernet IP address (192.168.1.1) into your web browser after configuring your PC to have an address on the same subnet.

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



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

Correct entry of the username and password will display the main operations page similar to that shown below.

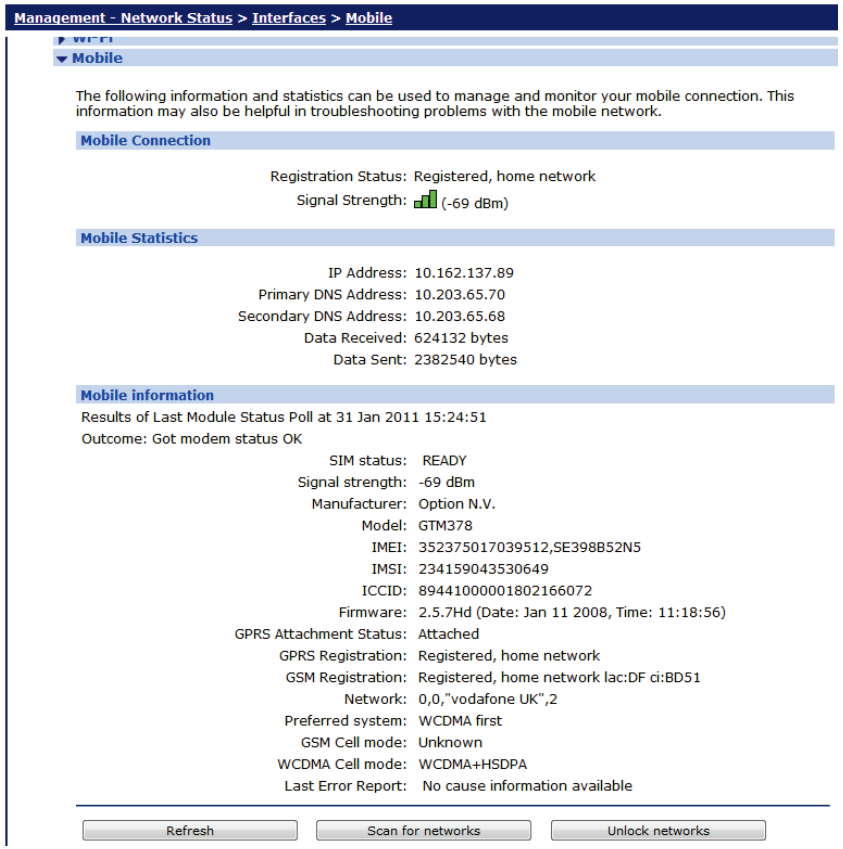


Clicking on the **Click to load Applet graphics!** button will display a representation of the front panel of your unit that will be updated every few seconds to show the actual status of the LED indicators. The model number of your unit will be shown at the top of the screen. The unit's serial number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

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

Configuring and Testing W-WAN Models

Refer to the ***Configuration - Network > Interfaces > Mobile*** section of this guide to configure your router for the correct APN and PIN code (if any). You can now power up your unit and test connection to the wireless network. 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. The unit will now attempt to log on to the specified mobile network and if it is able to do so, the W-WAN NET indicator will illuminate steady. Data passing to and from the network will be reflected by the status of the DAT indicator, which will flash green. If you are unable to connect to the network, go to the ***Management - Network Status > Interfaces > Mobile*** web page and press the Refresh button. The page should appear similar to the following:



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

Signal Strength Indicators

On units 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)

The minimum recommended strength indication is 2 LEDs. If you have no or 1 LEDs lit, it is recommended that you fit an external antenna to the unit.

Wizards

This page contains wizards that simplify common configuration tasks. These wizards will change the minimum number of parameters to complete the required configuration task. However, due to the generic nature of the wizards they may not be suitable for all circumstances.

Quick Start Wizard

The Quick Start Wizard will display the options required for basic configuration of the Eth 0, WLAN and WWAN interfaces.

LAN to LAN IPsec Tunnel Wizard

This wizard will help you to configure an aggressive mode LAN to LAN IPsec tunnel to a remote host.

GOBI Module Carrier Wizard

Used with routers that have a GOBI 2000 module installed, to configure the router for a specified WWAN carrier.

Dual SIM Wizard

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. There are more options detailed in Application Note 7 which can be found on the TransPort Support pages of the Digi website.

Note:

The wizards are designed to assist users. For very specific or uncommon requirements then further manual configuration may be required after completing any of the above wizards.

Configuration – Network > Interfaces > Ethernet

Underneath the Ethernet sub menus, there are configuration parameters for:

Physical Ethernet interfaces

Logical Ethernet interfaces

MAC address filtering

MAC address bridging between routers

Spanning Tree Protocol (RSTP)

VLANs

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

On units 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 units with more than one physical Ethernet port, the Ethernet instances refer to the different physical Ethernet ports. These units 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".

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

Configuration - Interfaces > Ethernet > 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
This parameter allows you to enter a name for this Ethernet instance, to make it easier to identify.

Get an IP address automatically using DHCP
Selecting this option enables the DHCP client on this interface.

Use the following IP address
Selecting this option enables manual configuration of the IP addressing parameters

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

Mask
This parameter specifies the subnet mask of the IP subnet to which the unit is attached via this Ethernet port. Typically, this would be 255.255.255.0 for a Class C network.

Gateway
This parameter specifies the IP address of a gateway to be used by the unit. IP packets whose destination IP addresses are not on the LAN to which the unit is connected will be forwarded to this gateway.

DNS Server / Secondary DNS Server
These parameters specify the IP address of DNS servers to be used by the unit 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 Parameter
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

Configuration - Interfaces > Ethernet > ETH n > Advanced

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

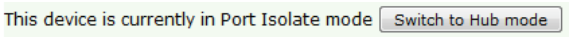
In HUB mode all the Ethernet ports are linked together and behave like an Ethernet hub or switch. This means that the router will respond to all of its Ethernet IP addresses on all of its ports (as the hub/ switch behaviour links the ports together).

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 behaviour 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 will be displayed, with an option to switch to Port Isolate mode.

Ethernet Hub group

On units 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 unit 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 unit is configured for Port Isolate mode.

Metric
This parameter specifies 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
This parameter is used to set the Maximum Transmit Unit for the specified interface. The default value is 0 meaning that the MTU will either be 1504 (for units 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 unit will automatically adjust invalid values entered by the user. So, if the MTU is set to 1000, the largest IP packet that the unit will send is 1000 bytes.

Enable auto-negotiation
Selecting this option 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)
This parameter is used to select "10Base-T", "100Base-T" or "Auto" mode. The currently selected mode will be 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
This parameter is used to select "Full Duplex", "Half Duplex" or "Auto" mode.
Note, 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 may be used to specify a maximum data rate in kbps that the unit will receive 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 may be used to specify a maximum data rate in kbps that the unit 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 (e.g. cable removed or broken)
This parameter is used to specify the length of time (in seconds) that 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 i.e. routes using the interface will not be marked as out of service if the cable is removed.

Enable NAT on this interface
This parameter is used to select 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
This parameter is used to enable or disable 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 will be 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 will match that of the Ethernet or PPP interface specified.

Enable the firewall on this interface
This parameter is used to turn 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 & return RST". When set to "No restrictions", users on this interface can access the unit's Telnet, FTP and web services for the purpose of managing the unit.

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

Disable return RST - whenever a unit receives a TCP SYN packet for one of its own IP addresses with the destination port set to an unexpected value, i.e. a port that the unit would normally expect to receive TCP traffic on, it will reply with a TCP RST packet. This is normal behaviour.

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 unit transmits data (but not when it receives data), the standard response of the unit to SYN packets i.e. transmitting an RST packet, will restart the inactivity timer and prevent the unit 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 units, or where you are not using a firewall, the same result can be achieved by selecting this option, i.e. when this option is selected the normal behaviour of the unit in responding to SYN packets with RST packets is disabled. The option will also prevent the unit from responding to unsolicited UDP packets with the normal ICMP destination unreachable responses.

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

Multihome additional consecutive addresses
This parameter 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
This parameter is used to enable or disable 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 will create an Ethernet bridge between the Wi-Fi access point and the physical Ethernet interface.

Generate Heartbeats on this interface
Enabling this option will display 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
Where:
a.b.c.d specifies the destination IP address for heartbeat packets.
h, m & 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 will be 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 will choose 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 will include the IMSI of the cellular module.

Include GPS information in the Heartbeat message
When enabled and the appropriate GPS hardware is installed, the heartbeat will include the GPS co-ordinates of the router.

Generate Ping packets on this interface
Enabling this option will display 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 webpage.

Send n byte pings to IP host a.b.c.d every h hrs m mins s seconds
Where:
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.
a.b.c.d specifies the destination IP address for auto-ping ICMP echo request.
h, m & 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
Where:
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.
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
This parameter is used to specify the length of time in (s) 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
This parameter is used to specify the length of time in (s) 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

Entity	Instance	Parameter	Values	Equivalent Web Parameter
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
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

Entity	Instance	Parameter	Values	Equivalent Web Parameter
				Heartbeat message
eth	n	hbgps	0,1	Include GPS information in the Heartbeat message
eth	n	pingsiz	value in bytes	Send n byte pings to IP host a.b.c.d every h hrs m mins s seconds
eth	n	pingip	IP address	Send n byte pings to IP host a.b.c.d every h hrs m mins s seconds
eth	n	pingint	0 - 86400	Send n byte pings to IP host a.b.c.d every h hrs m mins s seconds This CLI value is entered in seconds only.
eth	n	pingip2	IP address	Switch to sending pings to IP host a.b.c.d after n failures
eth	n	ip2count	0 - 255	Switch to sending pings to IP host a.b.c.d after n failures
eth	n	pingis	0,1	Only send Pings when this Ethernet interface is "In Service"
eth	n	pingoos	0 - 86400	Take this interface "Out of Service" after receiving no responses for s seconds
eth	n	oossecs	0 - 86400	Keep this interface out of service for s seconds

Configuration - Interfaces > Ethernet > ETH n > QoS

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
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, 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

Configuration - Interfaces > Ethernet > ETH n > VRRP

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
This parameter enables VRRP on this interface.

VRRP Group ID
The VRRP group ID parameter is used to identify 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
This parameter is used to set 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, i.e. 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
This parameter 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 is used to determine which interface should be used. This allows the unit 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 isn't 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
These parameter control 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
These parameters can be used to override the routing code and force the probe packets to be sent out of a specific interface.

Get the source IP address from interface x,y
These parameters can be used to the probe packets have 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

Entity	Instance	Parameter	Values	Equivalent Web Parameter
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

Configuration - Interfaces > Ethernet > Logical Ethernet Interfaces

The logical Ethernet interfaces are virtual Ethernet interfaces. They can be configured as per the standard Ethernet interfaces except for the Speed and Duplex settings which require a physical interface.

Logical Ethernet interfaces can be used for assigning extra IP addresses to the router on the same or an alternate subnet using the same physical Ethernet connection.

Logical Ethernet interfaces can also be used for bridging features (such as used in a Wi-Fi configuration) where it is desirable to not use a physical interface for the bridging.

Configuration - Interfaces > Ethernet > ETH n > MAC Filtering

Ethernet MAC filtering can be used to restrict 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
Enable MAC filtering on a specific Ethernet interface.

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. E.g. "00:04:2d" will allow all Ethernet packets with a source MAC address starting with "00:04:2d".

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

Configuration - Interfaces > Ethernet > ETH n > MAC Bridging

The Ethernet MAC bridge function will create 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
Enable MAC bridging on the Ethernet interface.

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. E.g. "00042d" will allow all Ethernet packets with a source MAC address starting with "00:04:2d".

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

Configuration - Interfaces > Ethernet > ETH n > 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 will use 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
Sets the RSTP priority.

Group
Sets 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

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:

Disabled	The port is not functioning and cannot send or receive data.
Listening	The port is sending and receiving BPDU's 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 BPDU's 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

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 BPDU's.
Forwarding	The port receiving and sending data, normal operation. STP still monitors incoming BPDU's 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.

Configuration - Interfaces > Ethernet > ETH n > VLANs

VLANs (Virtual LANs) facilitate splitting a single physical LAN into separate Virtual LANs. This is useful for security reasons, and will also help cut down on broadcast traffic on the LAN.

Enable VLAN support on Ethernet interfaces
Enables VLAN support on the Ethernet interface.

VLAN ID
The ID of the Virtual LAN. This parameter is used in the TCP header to identify the destination VLAN for the packet.

Ethernet Interface
The Ethernet port that will tag the outgoing packets. Packets sent from this interface will 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.

Related 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 Addess	Source IP Address
vlan	n	srcmask	IP Mask	Source Mask

Configuration - Network > Interfaces > Wi-Fi

This is the section of the web interface that contains the configuration options required in order to configure and enable the Wi-Fi features.

Configuration - Network > Interfaces > Wi-Fi > Global Wi-Fi settings

Due to 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 will restrict 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" will allow 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.

Related 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

This table lists the licensed channels that will be used by the Digi 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.

Configuration - Network > Interfaces > Wi-Fi > Global Wi-Fi settings > 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
This 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 allow the splashscreen to access these locations in order to display them to the client when authenticating.

Related 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

Configuration - Network > Interfaces > Wi-Fi > Global Wi-Fi settings > 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.

Related 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 *e.g.* 112233445566	MAC Address

Configuration - Network > Interfaces > Wi-Fi > Wi-Fi n

When a Wi-Fi interface is configured to be an Access Point, an SSID must be configured in order 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
This parameter allows you to enter 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 will be 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 be 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
The 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 will use the selected Ethernet interface.

Hide SSID
When enabled, the SSID will not be 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 will not be able to communicate with other Wi-Fi clients or Ethernet hosts connected to this AP.

Related 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

Configuration - Network > Interfaces > Wi-Fi > Wi-Fi n - Wi-Fi Security

This section is used to configure the security settings for the Wi-Fi interface.

If using multiple Wi-Fi interfaces at the same time then the interfaces will need to use the same security settings (except for the pre-shared key (PSK)). The only alternative is that the Wi-Fi is be used with no security.

Use the following security on this Wi-Fi interface
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 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
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.

WPA Encryption
The encryption algorithm to use. The options are:

- TKIP
- AES (CCMP)

RADIUS NAS ID
NAS ID of the RADIUS server.

RADIUS Server IP Address
IP address of the RADIUS server

RADIUS Server Password / Confirm RADIUS Server Password

The password of the RADIUS server.

Related 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, e.g.,

- Wi-Fi 0 uses radcli 1
- Wi-Fi 1 uses radcli 2
- Wi-Fi 2 uses radcli 3 and so on.

The table below 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
WPA-PSK	AES	wifinode 0 security wpapsk wifinode 0 wpatype aes

Network Authentication	Data Encryption	CLI Commands
		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>

Configuration - Network > Interfaces > Wi-Fi > Rogue Scan

In Rogue Scan mode, the router will perform 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 authorised Access Point is detected, an event log entry is created and an alarm (e.g. email, SMS, SNMP Trap) can be triggered.

It is possible to configure a list of the MAC addresses of the authorised Access Points that will not be reported when detected.

MAC Address
The MAC address of an authorised Access Point.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
macrogue	n	mac	MAC address with no separators *e.g.* 112233445566	MAC Address

Configuration – Network > Interfaces > Mobile

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 unit 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 units).

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.

Configuration – Network > Interfaces > Mobile

SIM:

Select a SIM to configure. SIM 1 relates to the SIM card fitted to the slot marked SIM 1 on the router's front panel. SIM 2 relates to the SIM card fitted to the slot marked SIM 2.

Note:

When using a single SIM card only, the default action is for the router to use PPP 1 as the mobile interface.

To configure 2 SIM's for fail-over browse to ***Configuration - Network > Interfaces > Mobile > SIM Selection*** to launch the Dual SIM wizard.

Configuration – Network > Interfaces > Mobile > Mobile Settings > Mobile Service Provider Settings

Select the service plan and connection settings used in connecting to the mobile network.

The ***Configuration – Network > Interfaces > Mobile > Mobile Settings*** option opens to show the following parameters:-

Service Plan / APN:
Enter the APN (Access Point Name) given by the service provider.

Use backup APN
Tick to enable this option then enter the backup APN in the free text field

e.g. "your.apn"
This parameter may be used to specify an alternative service APN for use in the event that the unit cannot connect using the primary APN specified by the APN parameter. The unit 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 is used to define how long the unit 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 unit 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 i.e. 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.

Related 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

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

Configuration – Network > Interfaces > Mobile > Mobile Settings > 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
This parameter specifies the amount of time the unit will wait without receiving any PPP packets before disconnecting. An inactivity timeout reset with each received PPP packet.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	1	rxtimeout	0 – 86400 (seconds)	Re-establish connection when no data is received for a period of time. Inactivity Timeout: h hrs m mins s seconds

Configuration – Network > Interfaces > Mobile > Mobile Settings > Mobile Network Settings

Enable NAT on this interface
This parameter is used to enable or disable IP Network Address Translation (NAT) on the mobile 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
This parameter is used to enable or disable 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
This checkbox will configure 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
The Firewall parameter is used to enable or disable 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.

Related 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	on/off	Enable the firewall on this interface

Configuration – Network > Interfaces > Mobile > 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
Click the hyperlink to launch the Dual SIM wizard.

CDMA Provisioning

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.

See Quick Note 25 – "CDMA Provisioning on a Digi TransPort Router" for example configuration.

Automatic Provisioning

If required, enter the MSL/PTN/MSID parameters before clicking Start

MSL:
Master subsidy lock (MSL) code. Obtain this from the mobile operator.
PTN:
Personal Telephone Number. Obtain this from the mobile operator.
MSID:
Mobile Station Identifier. Obtain this from the mobile operator.

Related 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:
Master subsidy lock (MSL) code. Obtain this from the mobile operator.
MDN:
Personal Telephone Number. Obtain this from the mobile operator.
MIN/MSID:
Mobile Station Identifier. Obtain this from the mobile operator.

Related 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:
Enter the Mobile IP profile number
Network Access ID (NAI):
Enter the Network Access ID

MIP Home Address:
Enter the MIP Home Address
Primary Home Agent:
Enter the Primary Home Agent
Secondary Home Agent:
Enter the Secondary Home Agent
HA shared secret: 0xn (Hex strings must start 0x)
Enter the HA shared secret

AAA shared secret: 0xn (Hex strings must start 0x)
Enter the AAA shared secret
HA SPI:
Enter the HA SPI
AAA SPI:
Enter the AAA SPI
Enable Reverse tunnelling:
Enable Reverse tunnelling if required.

Related 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:

Master subsidy lock (MSL) code. Obtain this from the mobile operator.

PRL filename:
Preferred Roaming List file name. Obtain this from the mobile operator.

Note: With the exception of 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.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
provision	0	string1	Free text field	MSL
provision	0	string20	Free text field	PRL Filename

Configuration – Network > Interfaces > Mobile > Advanced

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) 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. Initialisation strings are not normally required for most applications as the unit 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, e.g. 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 Initialisation strings, it is not necessary to include the "AT" as this is inserted automatically by the router

Post Hang-up string:
This parameter allows you to specify additional "AT" commands that is 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
This parameter is used to specify the length of time (in n 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 unit 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 will periodically collect 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
When configured, the signal strength will be written to the eventlog every *n* minutes.

If registration is lost for 5 minutes
This parameter controls whether the unit 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:

This parameter 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. For GSM: 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

Entity	Instance	Parameter	Values	Equivalent Web Parameter
				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

Entity	Instance	Parameter	Values	Equivalent Web Parameter
				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

Configuration – Network > Interfaces > Mobile > Advanced > Mobile Network Settings

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 unit 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
This parameter 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 will choose 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 will include the IMSI of the wireless module.

Include GPS information in the Heartbeat message
When enabled, the heartbeat will include 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".
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" can be used to configure the unit 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
If this parameter is set, the router will use 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
This 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 2nd 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
If this parameter is set to a non-zero value the unit will wait 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 this parameter, ICMP echo requests will only be sent from this interface 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 the mobile interface has been de-activated and then re-activated. 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
This parameter specifies an amount of time after which if no ping response has been received, the unit will terminate the mobile connection in an attempt to re-establish communications. Because by default the mobile link is always on, the unit will automatically attempt to re-establish a PPP connection that has been terminated.

Use the ETH 0 IP address as the source IP address
Enabling this parameter causes the unit to use 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 if you want 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 will be 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	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	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

Entity	Instance	Parameter	Values	Equivalent Web Parameter
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
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

Mobile routers can be configured 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
This specifies the interval in minutes that the unit will wait in between checks for incoming SMS messages. Setting this interval to "0" turns off checking.

Enable command replies via SMS
This parameter 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 not usually required. It is the number of the SMS message center (sometimes referred to as the Service Centre Address), to be used to relay SMS messages or alarms. This number must include the international dialling code, e.g. 44 for the UK, but not the "+" prefix or leading 0's, e.g. 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

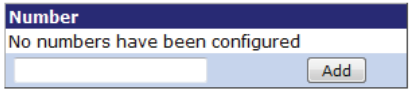
If no number is specified it is possible that the unit will operate using the default message centre for the GSM service to which you have subscribed.

SMS access level:
The access level for SMS commands. The access level set here will need 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)
This parameter specifies the character to be used to separate multiple command lines when a remote SMS sender is controlling the unit. The default separator is <CR> but some SMS capable devices are not equipped with <CR> keys so 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	SMS access level:

Entity	Instance	Parameter	Values	Equivalent Web Parameter
			5 = HighLow 6 = HighMedium 7 = CheckPar	
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)

Configuration – Network > Interfaces > DSL

Router models incorporating a DSL broadband interface will include a configuration page having the title shown above. By default, the configuration in this section will be 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
This checkbox gives the facility to enable or disable the use of DSL/ADSL functionality on the router.

Configure PVC
Select the required PVC instance from the drop-down selection box. Subsequent settings will apply to the selected instance (see below).

Configuration – Network > Interfaces > DSL > PVC Configuration

The PVC (Permanent virtual circuit) parameters are described here.

Enable this PVC
Tick the box to enable PVC settings

Encapsulation
This parameter is used to select 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
This parameter is used to set the Virtual Path Identifier for this APVC in the range 0 - 255.

VCI
This parameter is used to set 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

Configuration – Network > Interfaces > DSL > DSL Network Settings

This DSL PVC is using PPP 1
The default interface for DSL is PPP 1

Description
Enter a description for the DSL if required

Username
Enter ADSL Username

Password
Enter the password for the DSL account

Confirm password
Enter the password for the DSL account

Enable NAT on this interface
This parameter is used to select 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
Enable standard Network Address Translation (NAT).

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
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 has been 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 is used to enable or disable IPSec processing on this interface. If this box is ticked, 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
This checkbox will configure 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
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 Configuration – Security > Firewall

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 may be used to specify a data limit after which the unit 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 unit 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

Enter the maximum data to be transmitted before a warning entry is generated in the eventlog. You have the option to select Kbytes, Mbytes or GBytes via the drop-down box.

Stop data from being transmitted after

This parameter is used to set the maximum amount of data that may be transferred before the unit will "lock" the interface and prevent further transfer. As with the *Issue a warning event after* parameter it is used on networks where the tariff is based on the amount of data transferred to help prevent excess charges being incurred. You have the option to select Kbytes, Mbytes or GBytes 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, this parameter should be set to the appropriate day of the month (from 1 to 28). When this date is reached the unit 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 text will appear.
"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. The 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

Configuration – Network > Interfaces > DSL > PVC Traffic Shaping

Service category

Each ATM PVC may now be configured 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 characterised by the various traffic parameters as follows:
UBR: PCR, which may be zero for no limit
VBR-nrt: PCR, SCR, MBS
VBR-rt: PCR, SCR, MBS
CBR: PCR

Peak cell rate (cells/sec)

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)

Configuration – Network > Interfaces > DSL > Advanced

Operational mode
This parameter is used to specify 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 (i.e. PSTN / POTS) this option provides automatic selection between G.dmt, G.lite and ANSI (in the order listed). For Annex B models (i.e. 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)
This checkbox enables the 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.

Configuration - Network > Interfaces > GRE

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 will be created between 2 devices.

Configuration - Network > Interfaces > GRE > Tunnel n

Description:
This parameter allows you to enter a name for this GRE instance, to make it easier to identify it.

IP address:
This is the IP address of the virtual interface that will be 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:
Used 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 will allow 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:
These 2 parameters allow you to select the GRE tunnel source interface, so the tunnel end point can 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. e.g. 1.1.1.1. This option is normally used in conjunction with IPSec. This parameter should not be used if the interface is selected as the source using the "Use Interface" options above.

Destination IP Address or Hostname:
This is 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. e.g. 2.2.2.2

Enable keepalives on this GRE tunnel

Selecting this checkbox will 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 will be marked as down.

Send a keepalive every s seconds

When configured to a non-zero value, keepalive packets will be 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

This parameter specifies 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
This specifies 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

Configuration - Network > Interfaces > GRE > Tunnel n > Advanced

Metric:
This parameter specifies 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:
Maximum Transmission Unit. The value entered here will be the greatest amount of data that can be transferred in one physical packet. Default value is 1400

Tunnel Key:
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 is used to turn 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, e.g.:

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:
This parameter selects whether to add GRE checksums to GRE packets when the unit is terminating a GRE tunnel. "Off" disables checksums, "On" enables checksums.

Enable IGMP on this GRE tunnel:
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.

Enable IP analysis:
When set to ON, the un-encapsulated IP traffic will be captured into the analyser trace.

Enable Tunnel analysis:
When set to ON, the GRE encapsulated packets and keepalives will be 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

RIP Routing Parameters – CLI only

Please note that under the CLI commands for GRE Tunnels you will find parameters specifically relating to RIP. Please see the **Configuration – Network > IP Routing / Forwarding > RIP > Interfaces > Ethernet / PPP / GRE** section on RIP routing for configuration of these sub parameters.

Configuration - Network > Interfaces > ISDN > ISDN Answering

This page allows you to configure the ISDN interface to receive incoming calls.

Button:- Load answering defaults

Clicking this button resets the default answering PPP interface (PPP 0) to the factory answering defaults.

Description:
This parameter allows you to enter a name for this PPP instance, to make it easier to identify it.

Only accept calls from calling numbers

ending with
This parameter is used to restrict the range of numbers from which ISDN will answer incoming calls, i.e. 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.
This parameter 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 unit 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 unit 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.
This parameter 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 unit 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 unit from answering any calls to numbers that do not end in 123.

Use the following local IP configuration

Local IP Address:
This is the IP address of the unit'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 it is required that the remote system have an address supplied. An attempt to negotiate an IP address from the IP address pool will be made. 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
This is 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:
This specifies 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 allows you to specify an alternative DNS IP address.

Secondary DNS server:
This parameter can supply a secondary DNS server IP address to the peer for DNS requests if required.

Enable NAT on this interface
This parameter is used to enable or disable 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
This parameter is used to enable or disable 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
This checkbox will configure 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
The Firewall parameter is used to enable or disable 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 see Configuration > Security > Firewall

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

Configuration - Network > Interfaces > ISDN > ISDN Answering > Advanced

These are the advanced settings for the ISDN interface.

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.

Enable "Always On" mode of this interface

On
This parameter is used to configure the PPP instance so that in the event that it is disconnected the unit will try 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
As above "On" but the unit will try and connect immediately and without delay.

Put this interface "Out of Service" when an always-on connection attempt fails
Usually, always-on interfaces will not go out of service unless they have connected at least once. When this option is turned "On", the interface will go out of service even if the first connection attempt fails.

Attempt to re-connect after n seconds
This parameter specifies the length of time in seconds that the unit 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 would typically be used to reduce 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 will activate. After that, the usual always-on activation timers apply.

Control when this interface can connect using Time band n

This parameter specifies the Time Band number to use for this ISDN instance (see ***Configuration - Network > Timebands***).

Keep this interface up for at least n seconds
If this parameter is set to a non-zero value, then ISDN will not close the connection for the specified period, even if the link is inactive.

Close this interface

After n seconds
This parameter specifies 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
This parameter specifies 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 will close the connection if the link is inactive for the length of time specified by this parameter.

Alternative idle timer for static routes n seconds
This parameter may be used to specify 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
The value in this text box specifies 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 value in this text box specifies 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 value in this textbox specifies 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 value in this text box specifies 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 reveals 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 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 units
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 value in this text box defined 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

Entity	Instance	Parameter	Values	Equivalent Web Parameter
				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

Configuration – Network > Interfaces > ISDN Dialling

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
The value in this text box is 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
These four text boxes contain the telephone numbers that should be used, in sequence, to make an outgoing connection.

Prefix n to the dial out number
The value in this text box specifies the dialling prefix to use, if needed. This may be necessary when using a PABX.

Username
The text string text box is 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
This text box contains 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 value in this text box is 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 value in this text box specifies 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 will reveal 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 value in this text box is 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 value in this text box is 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 will cause the PPP instance to answer an incoming call.

Only allow calling numbers ending with n
When set to answer calls, the value in this textbox 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 checked, this checkbox will enable Network Address Translation to operate on this interface. This is the same as for other PPP interfaces.

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.

Enable IPsec on this interface
When checked, this checkbox will cause 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 checked, this checkbox causes the router to maintain (i.e. not flush) the SA when the interface becomes disconnected. The normal behaviour 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 (i.e. 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 checked, this checkbox 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

Configuration – Network > Interfaces > ISDN > Advanced

Metric
The value in this text box specifies the route metric that should be applied to this interface. (see ***Configuration – Network > Interfaces > Advanced > PPP n*** for more detail.)

Enable "Always On" mode of this interface
When checked, this checkbox 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 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 parameter in this text box 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 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 value in this text box is 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 ***Configuration – Network > Interfaces > Timebands*** section of this manual.

Keep this interface up for at least s seconds
The value in this textbox specifies 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 value in this text box specifies 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 will deactivate 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 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
The value in this text box specifies 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 value in this text box specifies 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 value in this textbox specifies 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 value in this text box specifies 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 reveals 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 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 units
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 value in this text box defined 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

Entity	Instance	Parameter	Values	Equivalent Web Parameter
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

Configuration - Network > Interfaces > ISDN > LAPD > LAPD n

This page allows you to configure the ISDN LAPD interfaces. Link Access Protocol D (LAPD) is the protocol used for ISDN D-channel signalling and call setup.

LAPD 0 and LAPD 1 can be used as required for SAPI 16 traffic (i.e. X.25 over D-channel). LAPD 2 is normally reserved for ISDN call control.

Enable LAPD n
Un-checking this parameter will disable the LAPD instance. This may be necessary if you have an installation where two or more units are connected to the same ISDN "S" bus. In this case, only one of the units may be configured for D-channel X.25 on TEI1, SAPI16. On each of the other units 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 unit.
When checked, this check box will also reveal the following configuration parameters

Mode
When the DTE/DCE mode parameter is set to DTE, the unit will behave 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 units back-to-back, one of the units should have the DTE mode value set to DCE.

N400 Counter
This is 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
This is 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 n msecs
This is 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
This is 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
This specifies the transmit window size when using D-channel X.25. The default is 7.

Tx Throughput
The Tx Throughput parameter is 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 unit 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 unit will limit the rate at which data is transmitted over the LAPD link.

Note:
Note that if multiple PAD or IP instances are sharing this LAPD instance, the maximum transmission rates of all instances will be limited.

Rx Throughput
The Rx Throughput parameter is 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 unit 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 unit 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:
Note that 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 this parameter is enabled, the unit will try 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 unit will not attempt to reactivate a D-channel link following deactivation by the network.

Reactivate after n secs
This parameter specifies 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
This parameter determines if to deactivate or not the LAPD session when an X.25 PAD session is terminated

Deactivate the LAPD session
This parameter enables automatic deactivation of a LAPD session when an X.25 PAD session is terminated.

Do not deactivate the LAPD session
This parameter ensures the unit will 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, Tick the D64S mode parameter checkbox and ensure that the **TEI** parameter is set to 255. This means that for any application that uses ISDN (e.g. PPP) then it will use D64S mode.

First D64S B-channel
When using D64S mode there is no dialling protocol to negotiate which B-channel to use. This must therefore be specified using this parameter. Check B1 radio button to select channel B1 and Check 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

Configuration – Network > Interfaces > PSTN

This section of the web interface appears when the router is fitted with an optional internal PSTN MODEM card. When first powered up, navigating to the ***Configuration – Network > Interfaces > PSTN*** 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 > 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
This message simply states which PPP instance has been assigned to the interface.

Description
The value in this text box is 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
These four text boxes contain the telephone numbers that should be used, in sequence, to make an outgoing connection.

Prefix n to the dial out number
The value in this text box specifies the dialling prefix to use, if needed. This may be necessary when using a PABX.

Username
The text string text box is 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
This text box contains 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.