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 PSTN 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
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

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	transDNS	Valid IP address a.b.c.d	Primary DNS server a.b.c.d
ppp	n	sectransDNS	Valid IP address a.b.c.d	Secondary DNS server a.b.c.d
ppp	n	ans	OFF,ON	Allow this PPP interface to answer incoming calls
ppp	n	cingnb	up to 25 digits	Only allow calling numbers ending with n
ppp	n	do_nat	0,1,2 0 = Disabled 1 = IP address 2 = IP address and port	Enable NAT on this interface IP address/IP address and Port
ppp	n	nat_ip	Valid IP address a.b.c.d	NAT Source IP address a.b.c.d
ppp	n	ipsec	0 = Disabled 1 = Enabled 2 = Enabled and Keep SAs	Enable IPsec on this interface/ Keep Security Associations when this PSTN interface is disconnected
ppp	n	firewall	OFF,ON	Enable the firewall on this interface

Configuration – Network > Interfaces > PSTN > 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 useage 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 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 > DialServ

The Dialserv option module mimics a telephone exchange in that it supplies the required voltages on the line, generates a RING signal and has off-hook detection circuitry. It can be used to provide similar functionality to dialling into an ISP using an analogue MODEM. The card also contains an analogue MODEM to handle data on the line.

Use PPP/Protocol Switch
These radio buttons select whether the DialServ card uses a PPP instance or the protocol switch functionality to control traffic on the interface. If PPP is selected, the web page expands to reveal the standard PPP configuration settings. If Protocol Switch is selected, only the four settings described immediately below are visible.

Max time to RING line s seconds
The value in this text box specifies the maximum number of seconds that the RING signal should be generated for.

RING frequency n Hz
The DialServer module generates a RING signal – the frequency of the RING is selected from this drop-down list. The available options are:

- 20Hz
- 25Hz
- 30Hz
- 40Hz
- 50Hz.

Initialisation string 1
The text string in this text box contains any required MODEM initialisation commands.

Initialisation string 2
The text string in this text box contain initialisation commands that will be issued to the MODEM after the first initialisation string.

Configuration – Network > Interfaces > DialServ > DialServ Network Settings

The DialServ card may be configured to use PPP as the protocol to connect to the remote peer and as such should be assigned a free PPP instance to use as part of the configuration. If no PPP instance has been assigned and the module has been configured to use PPP, a link to the PPP mappings page and message appear.
If a PPP instance has been assigned, the following configuration options appear:

This DialServ interface is using PPP n
This message simply indicates which PPP instance (n) is being used by the DialServ card.

Description
The value in this text box is a short string that describes the interface and is used as a convenience when referring to 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. These can be used to provide a dialback facility.

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.

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 PSTN 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	“	Dial out using numbers
ppp	n	ph3	“	Dial out using numbers
ppp	n	ph4	“	Dial out using numbers
ppp	n	prefix	0 – 9999999999	Prefix
ppp	n	username	Up to 60 characters	Username
ppp	n	password	Up to 40 characters	Password
ppp	n	IPaddr	0.0.0.0	Allow the remote device to assign a local IP address to this router
ppp	n	IPaddr	Valid IP address a.b.c.d	Try to negotiate a.b.c.d as the local IP address for this router (in conjunction with l_addr)
ppp	n	l_addr	OFF,ON When ON, allows negotiation when OFF force	Use a.b.c.d as the local IP address for this router (not negotiable)

Entity	Instance	Parameter	Values	Equivalent Web Parameter
			use of specified IP address	
ppp	n	DNSserver	Valid IP address a.b.c.d	Primary DNS server
ppp	n	secDNS	Valid IP address a.b.c.d	Secondary DNS server
ppp	n	IPmin	Valid IP address a.b.c.d	Assign remote IP addresses from a.b.c.d to a.b.c.d
ppp	n	IPrange	0 - 255	Assign remote IP addresses from a.b.c.d to a.b.c.d
ppp	n	transDNS	Valid IP address a.b.c.d	Primary DNS server a.b.c.d
ppp	n	sectransDNS	Valid IP address a.b.c.d	Secondary DNS server a.b.c.d
ppp	n	ans	OFF,ON	Allow this PPP interface to answer incoming calls
ppp	n	do_nat	0,1,2 0 = Disabled 1 = IP address 2 = IP address and port	Enable NAT on this interface IP address/IP address and Port
ppp	n	natip	Valid IP address a.b.c.d	NAT Source IP address a.b.c.d
ppp	n	ipsec	0 = Disabled 1 = Enabled 2 = Enabled and Keep SAs	Enable IPsec on this interface/ Keep Security Associations when this DialServ interface is disconnected
ppp	n	firewall	OFF,ON	Enable the firewall on this interface

Configuration – Network > Interfaces > DialServ > 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 textbox 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 textbox 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 useage 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 – 2147483648	Close this interface after s seconds
ppp	n	maxuptime	0 – 2147483647	if it has been up for m minutes in a day
ppp	n	timeout	0 – 2147483648	if the link has been idle for s seconds
ppp	n	timeout2	0 – 2147483648	Alternative idle timer for static routes s seconds
ppp	n	rxtimeout	0 – 2147483648	if the link has not received any packets for s seconds
ppp	n	maxneg	0 – 2147483648	if the negotiation is not complete in s seconds
ppp	n	uplogmins	0 – 2147483647	Generate an event after this interface has been up for m mins
ppp	n	dlwarnkb	0 – 2147483647	Issue a warning after n units
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 > Serial

Digi routers support a variety of serial interfaces, either inbuilt or as optional add-on modules. Each asynchronous serial (ASY) port may be configured to operate at different speed, data format etc. These parameters may be changed using the web interface or from the command line using AT commands and S registers.

The ***Configuration – Network > Interfaces > Serial*** menu item opens out when clicked, to show the list of supported serial interfaces.

> **Note:**
> On models fitted with W-WAN modules, one of the interfaces (and its associated web page) will be dedicated to the W-WAN module. The title will reflect this. Similarly, on models fitted with an analogue MODEM, one of the interfaces will be entitled PSTN port.

Configuration – Network > Interfaces > Serial > Serial Port n

This section describes the basic configuration of a serial port.

Enable this serial interface
When this checkbox is unchecked, this is the only item that appears in the section. Clicking the checkbox causes the various associated configuration parameters to appear.

Description
This free-form text entry box allows a description for the interface to be added. For example, if the serial interface is connected to a card payment device, the description could read "Till 1" or similar appropriate text.

Baud Rate
This drop-down selection box selects the required Baud rate for the associated serial port.

Data Bits / Parity
This drop-down selection box selects the required data format for the interface, 8 data bits, no parity being a very common configuration.

> **Note:**
> When the serial port is not in 8-bit parity mode (i.e. it is in either 8-bit no parity, or 7-bit with parity), the router will continually check for parity when receiving AT commands and adjust and match accordingly.

Flow Control
The unit supports software flow control using XON/XOFF characters and hardware flow control using the RS232 RTS and CTS signals. Use this drop-down list to select "Software", "Hardware" or a combination of "Both". To disable flow control select the "None" option.

Enable echo on this interface
Check this checkbox to enable command echo to be enabled when using the command line interpreter, uncheck it if the attached terminal provides local echo.

CLI result codes
Select the required level of verbosity for command result codes. The available options are:

- Verbose
- Numeric
- None.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
asy	n/a	descr	Free text – description of interface	Description
S31=n	n/a	n/a	Where n = 3 = 115200 4 = 57600 5 = 38400 6 = 19200 7 = 9600 8 = 4800	Baud rate
S23=n	n/a	n/a		Data Bits / Parity
&Kn	n/a	n/a	Where n = 0 = None 1 = Hardware 2 = Software 3 = Both	Flow Control
&En	n/a	n/a	Where n = 0 = No echo 1 = echo	Enable echo on this interface
&Vn	n/a	n/a	Where n = 0 = numeric 1 = verbose	CLI result codes

Configuration – Network > Interfaces > Serial > Serial Port n > Advanced

The configuration parameters in this section are changed less frequently than those in the basic section and so are given a separate page in order to reduce screen clutter.

Answer V.120 calls after n rings (0 = Don't answer)
This parameter controls the answering of incoming V.120 calls. When set to zero, V.120 answering is disabled, otherwise V.120 answering is enabled on this interface. Enter the number of rings to wait before answering the call into this text box. This is equivalent to setting the value of the "S0" register for the associated serial port.

DCD
This drop-down selection box selects how the Data Carrier Detect (DCD) signal is controlled. The available options are:

- Auto
- On
- Off
- Pulse Low.

Selecting "Auto" configures the router so that it will only assert the DCD line when an ISDN connection has been established (this is equivalent to "AT&C1").
Selecting "On" configures the router such that the DCD line is always asserted when the router is powered-up (this is equivalent to "AT&C0").

Selecting “Off” configures the router such that the DCD line is normally asserted but is de-asserted for the time period specified by the “S10” register after a call is disconnected (this is equivalent to “AT&C2”).

DTR Control

This drop-down selection box controls how the router responds to the DTR signal. The available options are:

- None
- Drop call
- Drop line and call
- Drop call on transition
- Drop line & call on transition.

Selecting “None” configures the router to ignore the DTR signal (this is equivalent to “AT&D0”).

Selecting “Drop call” configures the router to disconnect the current call and return to AT command mode when the DTR signal from the attached terminal (DTE) is de-asserted (this is equivalent to “AT&D1”).

Selecting “Drop line and call” configures the router to disconnect the current call, drop the line and return to AT command mode when the DTR signal is de-asserted (this is equivalent to “AT&D2”).

DTR de-bounce time s x 20 milliseconds

This parameter determines the length of time (in multiples of 20ms) for which the DTR signal must be de-asserted before the router acts on any options that are set to trigger on loss of this signal. Enter the desired multiple into the text box. Increasing this value makes the router less sensitive to “bouncing” of the DTR signal. Conversely, decreasing this value makes the router more sensitive. The default of 100ms (5 times 20ms) is a reasonable value.

Escape Character

This parameter determines the character used in the escape sequence. The default is the “+” symbol (ASCII value 43, 0x2b). Changing this value has the same effect as changing the “S2” register.

Escape Delay s x 20 milliseconds

This parameter defines the required minimum length of the pause (in multiples of 20ms) in the escape sequence. The default is 50 x 20ms which means that the escape sequence becomes “+++”, a pause of 1 second and then “AT” in order to drop back to AT command mode. Enter the desired delay into the text box if a delay of some other value is required.

Forwarding Timeout s x 10 milliseconds

This parameter defines the length of time that the router will wait for more data after receiving at least one octet of data through the serial port and transmitting it onwards. This timer is reset each time more data is received. The router will forward data onwards when either the forwarding timer expires or the input buffer becomes full. This parameter applies to ADAPT, TCPDIAL, TCPPERM and PANS.

Break Transmit Escape Character c

This parameter determines the character used in the escape sequence. The “-” symbol (ASCII value 45, 0x2d) is a recommended value. Changing this value has the same effect as changing the “S3” register. To use the break sequence, type “-” 3 times, with a 1 second pause either side of the 3 “-” characters.

When the Async port detects the following sequence....

```
        <guard time 1 sec>---<guard time 1 sec>
```

instead of outputting the three minus characters (they are removed from the output stream) a BREAK condition is placed on the Async transmitter for 1 second.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
S0=n	n/a	n/a	Where n = 0 - 255	Answer V.120 call after n rings
&Cn	n/a	n/a	Where n = 0 = On 1 = Auto 2 = Off 3 = Pulse low	DCD
&Dn	n/a	n/a	Where n = 0 = None 1 = Drop line 2 = Drop line & call 3 = Drop call on transition 4 = Drop line & call on transition	DTR
S45=n	n/a	n/a	Where n = 0 - 255	DTR de-bounce
S2=n	n/a	n/a	Where n = ASCII value	Escape Character
S12=n	n/a	n/a	Where n = 0 - 255	Escape delay
S15=n	n/a	n/a	Where n = 0 - 255	Forwarding Timeout
S3=n	n/a	n/a	Where n = ASCII value	Break Transmit Escape Character

Configuration – Network > Interfaces > Serial > Serial Port n > Profiles

Each serial port can have two profiles which can be configured differently. Which profile is in force when the router powers-up is selected here.

Power-up profile n
Select "0" from the drop-down selection box to choose profile 0 to be active when the router powers-up. Select "1" from the selection box to make profile 1 the active profile.

Load Profile n
Select "0" from the drop-down selection box and click the button to load profile 0.

Save Profile
Select "0" from the drop-down selection box and click the button to save profile 0 after making any changes.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
&Yn			Where n = 0,1	Power-up profile n
&Zn			Where n = 0,1	Load Profile n
&Wn			Where n = 0,1	Save Profile n

Configuration – Network > Interfaces > Serial > Sync

The most common form of serial communications these days is asynchronous. Synchronous serial communications links are still in use and the Digi routers can support these. HDLC is a synchronous protocol that is still in use and can be used with Digi routers. This section describes how to configure the synchronous communications interfaces. To enable synchronous mode, a protocol such as LAPB must be configured to use a synchronous port as its lower layer interface. On certain models, an informational message will appear on the web page which states that jumper settings may need to be changed in order to support synchronous serial operation.

> **Note:**
> The number of synchronous serial ports available will vary depending on the model and any optional modules fitted.

Description
This text entry box is for a description of the interface, should one be required.

Clock source Internal / External
These two radio buttons select between internal or external clock sources for the interface.

Mode
The radio buttons that appear here select the specific serial protocol to use. Which buttons appear depend upon the capabilities of the interface. The options available are; V.35, EIA530, RS232, EIA530A, RS449 and X.21.

Invert RX clock
When checked, this checkbox will cause the router to invert the voltage level of the receive clock signal.

Invert TX clock
When checked, this checkbox will cause the router to invert the voltage level of the transmit clock signal.

Encoding NRZ / NRZI
These two radio buttons select between non-return to zero (NRZ) and non-return to zero (inverted) (NRZI) signal encodings.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
sy	0	descr	Text description of interface	Description
sy	0	clksrc	int,ext	Clock source
sy	0	rxclkinv	OFF,ON	Invert RX clock
sy	0	txclkinv	OFF,ON	Invert TX clock
sy	0	encode	nrz,nrzi	Encoding

Configuration – Network > Interfaces > Serial > Rate Adaption

The router supports two rate adaptation protocol (Adapt) instances. Each instance enables the selection and configuration of the protocol to be used for rate adaptation over an ISDN B channel. The supported protocols are; V.110, V.120 and X.75. Depending on which protocol is selected, there may be an associated LAPB instance (distinct from the two general purpose LAPB instances), as for example, when V.120 is used in error-corrected (multi-frame) mode. Clicking the triangle at the left of the blue bar opens up the two instances described below.

Configuration – Network > Interfaces > Serial > Rate Adaption n

This page displays the configuration parameters directly relevant to the rate adaptation protocol only, LAPB configuration pages are to be found here: ***Configuration – Network > Legacy Protocols > X.25 > LAPB***. When configuring LAPB parameters, be aware that LAPB 2 is used for adapt 0 and LAPB 3 is used for adapt 1.

Attempt to redial the connection n times if rate adaption has not been negotiated
If an ISDN connection is established, but rate adaption is not negotiated, the value in this text box specifies how many times the router should drop the connection and redial it.

Drop the connection if it is idle for h hrs m mins s secs
The values in these text entry boxes specify the time to wait before dropping the connection if the connection becomes idle.

Leased line mode
When checked, this checkbox will allow the router to attempt to maintain the connection automatically once it has been established.

Enable TCP rate adaption
Check this checkbox to enable the use of rate adaptation when using a TCP connection rather than an ISDN line. When enabled, the following controls become enabled:

Connect to IP Address a.b.c.d Port n
When using a TCP connection, these text entry boxes allow the user to specify the IP address and port number that the protocol should use.

Listen on Port
This text entry box contains the port number that the router is listening on when in socket mode.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
adapt	0,1	dial_retries	0 - 255	Attempt to redial the connection n times
adapt	0,1	tinact	0 - 86400	Drop the connection if it is idle for h hrs m mins s secs
adapt	0,1	leased_line	OFF,ON	Leased line mode
adapt	0,1	sockmode	0,1 0 = disable 1 = enable	Enable TCP rate adaption
adapt	0,1	ip_addr	valid IP address a.b.c.d	Connect to IP Address a.b.c.d Port n
adapt	0,1	ip_port	valid TCP port	Connect to IP Address a.b.c.d

Entity	Instance	Parameter	Values	Equivalent Web Parameter
			number	Port n
adapt	0,1	lip_port	valid TCP port number	Listen on Port n

Configuration – Network > Interfaces > Serial > Command Mappings

The router supports a number of command "aliases" which specify strings to be substituted for commands entered at the command line. The table on this page contains two text entry boxes and an "Add" button. Up to 23 command mappings may be specified. An example may make this clear. Suppose, a user coming from a Unix™ background feels more comfortable typing "ls" rather than the native "dir" command in order to list the files in a directory. To achieve this aliasing, enter "ls" into the "From" column in the table, "dir" into the "To" column and then click the "Add" button.

From
This text entry box contains the substitute text.

To
This text entry box contains the command that should be substituted.

Add
Click this button to add the command mapping.

Delete
When the mapping has been added, a "Delete" button will appear in the right-hand column. Clicking this button removes the binding from the table.

> **Note:**
> If either string contains spaces, the entire string must be enclosed within double quotation marks. When substituting a command, upper case characters are considered the same as the corresponding lower case characters.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
cmd	n	cmdmapi	Replacement command	From
cmd	n	cmdmapo	Command to be substituted	To

Configuration – Network > Serial > Protocol Bindings

Digi routers are soft configurable to allow different protocols to be used on different interfaces. The process of selecting which protocol will be used on a particular interface is referred to as "binding". So, for example Serial (ASY) port 0 may be used for an ISDN B channel X.25 connection in which case PAD 0 would be bound to Serial 0 (assuming that PAD 0 is the required PAD). (To complete this example, it would also be necessary to associate the PAD with a LAPB instance using the appropriate page). Protocols are bound to serial interfaces using a table with a drop-down list box for selecting the protocol and a drop-down list for selecting the serial port.

By default, if no specific protocol has been bound to a serial interface, a PPP instance will automatically be associated with that port. This means that PPP is treated as the default protocol associated with the serial ports.

Protocol
Select the desired protocol from this drop-down list.

Bound to
Select the desired serial port from this drop-down list.

Add
Click this button to add the binding.

Delete
When a binding has been added, it appears in the table and a "Delete" button appears in the right-hand column. Click this button to remove the binding. (Remember that the binding does not come into force until the "Apply" button at the bottom of the page has been clicked).

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
bind	n	prot1	Valid protocol, e.g. PAD 0	Protocol
bind	n	id1	Valid serial port e.g. ASY 5	Bound to

To display a list of the current bindings enter the command:

```
bind ?
```

Command line examples:

```
bind pad 0 asy 0
```

binds PAD 0 to serial port 0.

```
bind v120 0 asy 3
```

binds V.120 instance 0 to asynchronous serial port 3.

To access the Internet using PPP via a terminal connected to serial interface 2, enter the command:

```
bind ppp 1 asy 2
```

Currently it is only possible to bind a TANS instance to an ADAPT instance using the bind command. The format of the command is:

```
bind adapt <instance> tans <instance>
```

Configuration – Network > Serial > TRANSIP Serial Ports

TransIP is a way of using virtual serial ports for serial connections over an IP socket, in effect multiplying the number of concurrent serial connections to a router. TransIP can be configured to actively connect on a TCP socket (i.e. make outgoing connections).

Configuration – Network > Serial > TRANSIP Serial Ports > TRANSIP n

The message at the top of this page states which serial interface is being used for the TransIP connection.

Listen on port n
This parameter is the TCP port number that the router should listen on.

Connect to IP Address or Hostname a.b.c.d Port n
The IP address or hostname text entry box should contain a valid IP address or the hostname which the router should use to make the outgoing TransIP connection.
If this parameter is set (i.e. non-zero), the number defined the TCP port number to use when making TCP socket connections. When zero, TransIP is listening only on the port defined above.

Send TCP Keep-Alives every s seconds
The value in this text entry box is the amount of time (in seconds) a connection will stay open without any traffic being passed.

Enable Stay Connected mode
When checked, this checkbox causes the router to refrain from clearing the TCP socket at the end of a transaction, data call or data session (depending on what the TansIP serial port was bound to and what protocol it was using). Leaving this checkbox unchecked allows the router to clear the socket. For example, if the TransIP port is bound to a TPAD and the box is unchecked, the TransIP TCP socket will be cleared at the end of the TPAD transaction.

Disable command echo
When this checkbox is checked command echo for the TransIP port is disabled. When unchecked all commands issued will be echoed back to the TransIP TCP socket.

Escape char c
The parameter in this text entry box is the ASCII character used as the escape character which is by default "+". Entering this escape character three times followed by a pause of at least the "Escape delay" parameter below and then an "AT" command will cause the router to switch back to command mode from online mode. This is equivalent to the "S2" register setting.

Escape delay s milliseconds
The parameter in this text entry box defines the delay required between entering the escape sequence (default "+++") and the "AT" command in order for the router to drop back into command mode. This is equivalent to the "S12" register setting.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
transip	n	port	Valid port number 0 – 65535	Listen on port
transip	n	host	Valid IP address a.b.c.d or hostname	Connect to IPaddress a.b.c.d or Hostname
transip	n	remport	Valid port number 0 – 65535	Port
transip	n	keepact	0 – 255	Send TCP Keep-Alives every s seconds
transip	n	staycon	ON,OFF	Enable Stay Connected mode
transip	n	cmd_echo_off	ON,OFF	Disable command echo
transip	n	escchar	Valid ASCII character	Escape char c
transip	n	esctime	0 – 255	Escape delay s milliseconds

Configuration – Network > Serial > RealPort

Digi devices use the patented RealPort COM/TTY port redirection for Microsoft Windows.

RealPort software provides a virtual connection to serial devices, no matter where they reside on the network. The software is installed directly on the host PC and allows applications to talk to devices across a network as though the devices were directly attached to the host. Actually, the devices are connected to a Digi device somewhere on the network. RealPort is unique among COM port re-directors because it is the only implementation that allows multiple connections to multiple ports over a single TCP/IP connection. Other implementations require a separate TCP/IP connection for each serial port. Unique features also include full hardware and software flow control, as well as tunable latency and throughput. Access to RealPort services can be enabled or disabled.

Encrypted RealPort

Digi devices also support RealPort software with encryption. Encrypted RealPort offers a secure Ethernet connection between the COM or TTY port and a device server or terminal server.

Encryption prevents internal and external snooping of data across the network by encapsulating the TCP/IP packets in a Secure Sockets Layer (SSL) connection and encrypting the data using Advanced Encryption Standard (AES), one of the latest, most efficient security algorithms. Access to Encrypted RealPort services can be enabled or disabled. Digi's RealPort with encryption driver has earned Microsoft's Windows Hardware Quality Lab (WHQL) certification. Drivers are available for a wide range of operating systems, including Microsoft Windows Server 2003, Windows XP, Windows 2000, Windows NT, Windows 98, Windows ME; SCO Open Server; Linux; AIX; Sun Solaris SPARC; Intel; and HP-UX. It is ideal for financial, retail/point-of-sale, government or any application requiring enhanced security to protect sensitive information.

Enable RealPort
Selecting this option enables RealPort on the router.

Listen on port
This configures the TCP port on which the router will listen for RealPort connections.

Maximum number of sockets
This defines the maximum number of RealPort connections that the router will support.

Enable encrypted RealPort
Selecting this option enables encrypted RealPort on the router.

Encryption mode to listen on port
This configures the TCP port on which the router will listen for encrypted RealPort connections.

Maximum number of encryption sockets
This defines the maximum number of encrypted RealPort connections that the router will support.

Enable Device Initiated RealPort
Selecting this option enables router to make a RealPort connection to a host PC.

Connect to host a.b.c.d Port n
This configures the IP address or hostname and TCP port that the router should use when making a device initiated connection.

Allow s seconds between connection attempts

This configures the interval in seconds between device initiated connection attempts.

Send TCP Keep-Alives every s seconds
This configures the interval at which TCP Keep-Alives are sent over the RealPort connection. A value of 0 means that Keep-Alives are not sent.

Send RealPort Keep-Alives every s seconds
This configures the interval at which RealPort Keep-Alives are sent over the RealPort connection. A value of 0 means that Keep-Alives are not sent.

Enable exclusive mode
Selecting this option enables exclusive mode. Exclusive mode allows a single connection from any one RealPort client ID to be connected only. If this setting is enabled and a subsequent connection occurs that has the same source IP as an existing connection, the old existing connection is forcibly reset under the assumption that it is stale.

Enable authentication
Selecting this option enables RealPort authentication.

Authentication secret
This configures the RealPort authentication secret.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
rport	0	enabled	OFF,ON	Enable RealPort
rport	0	ipport	0 - 65535	Listen on port
rport	0	maxnbsocks	0 - 255	Maximum number of sockets
rport	0	encryption	OFF,ON	Enable encrypted RealPort
rport	0	encport	0 - 65535	Encryption mode to listen on port
rport	0	maxnbencsocks	0 - 255	Maximum number of encryption sockets
rport	0	initiate	OFF,ON	Enable Device Initiated RealPort
rport	0	IPaddr	Valid IP address a.b.c.d	Connect to host a.b.c.d Port n
rport	0	initiateport	0 - 65535	Connect to host a.b.c.d Port n
rport	0	initiatebackoff	0 - 255	Allow s seconds between connection attempts
rport	0	tcpkeepalives	0 - 255	Send TCP Keep-Alives every s seconds
rport	0	rportkeepalives	0 - 255	Send RealPort Keep-Alives every s seconds
rport	0	exclusive	OFF,ON	Enable exclusive mode
rport	0	auth	OFF,ON	Enable authentication
rport	0	secret	Up to 30 characters	Authentication secret

Configuration - Network > Interfaces > Advanced

Point-to-Point Protocol (PPP) is a standard protocol for transporting data from point to multipoint networks (such as IP) across point-to-point links (such as a serial or ISDN connection). This functionality is essential for dial-up Internet access.

As data is transferred across IP networks in synchronous format, the router supports asynchronous to synchronous PPP conversion. This allows asynchronous terminals connected to the units to communicate with remote synchronous PPP devices. Normally, this is carried out using a single ISDN B-channel so that data can be transferred at speeds up to 64kbps. This is known as ASYNC to SYNC PPP operation and is supported as standard by most terminal adaptors. To use ASYNC to SYNC PPP operation all that is necessary is to ensure that the PPP protocol is bound to the ASY port to which the terminal or PC is connected. (see ***Configuration – Network > Interfaces > Serial***).

> **Note:**
> In order to use ASYNC to SYNC PPP the attached terminal must also support PPP (Windows dial-up networking supports PPP).

In addition to ASYNC to SYNC operation (where the router only converts the PPP from one form to another) the router can initiate its own PPP sessions. This is used for example when:

The router is configured as a router to connect an Ethernet network to the Internet via ISDN or W-WAN

The router is answering an incoming ISDN call with PPP either for remote management or remote access to the Ethernet network to which the router is connected

The router is accessed locally through the serial port for configuration purposes by setting up a Windows Dial-Up-Networking connection to the "phone number" 123

> **Note:**
> With the exception of MLPPP the parameters in this section are only relevant when the router is generating the PPP, i.e. they are NOT relevant for ASYNC to SYNC PPP operation.

The unit also supports Multi-link PPP (MLPPP). MLPPP uses both ISDN B-channels simultaneously (and two PPP instances), to provide data transfer speeds up to 128Kbps for applications such as email or establishing a point-to-point connection between two units.

Configuration – Network > Interfaces > Advanced > PPP Mappings

The PPP Mappings page contains two columns of as many interfaces as are supported by the router (this varies between models). Each row in the column contains a drop-down list box that allows the user to select what function should be associated with each PPP instance. The PPP instance number is the left-most column. So, for example, to assign a W-WAN interface to PPP instance 3, select "Mobile SIM1 or SIM2" from the drop-down box to the right of instance "3". If a W-WAN interface is fitted to the router, this is the default mapping.

Configuration – Network > Interfaces > Advanced > PPP n > Multilink PPP

As mentioned above, the routers may support multilink PPP – this section describes the configuration of MLPP functionality.

The PPP interface must be configured with "Always On" mode enabled and an AODI NUA.

Desired local ACCM c
The value in this textbox defines the Asynchronous Control Character Map (ACCM). The default value of 0x00000000 should work in most cases. Changing this value is for advanced users only.

Desired remote ACCM c
The value in this textbox defines the ACCM for the remote peer. As above, the default value of 0xffffffff should work in most cases and should only be changed if it is known that other characters should be used.

Username
The value in this textbox is the username that should be used for logging on to the remote system.

Password
The value in this textbox is the password that should be used for authentication with the remote system when using MLPP. This password is used for both B-channel PPP connections.

Confirm password
When changing the password, the new password should also be typed into this text box. The router will check that both fields are the same before changing the value.

Enable remote CHAP authentication
When checked, this checkbox causes the router to authenticate itself with the remote system using CHAP. If this parameter is set, the connection will fail if authentication fails. Generally, this checkbox should be left unchecked.

Enable short sequence numbers
When checked, this checkbox enables the use of 12-bit, rather than the more usual 16-bit data packet sequence numbers.

Bring up the second ISDN B-channel

Never
When selected, this radio button will cause the router not to activate the second B-channel.

When the data rate is greater than n bytes/sec for s seconds

When this radio button is selected, the two associated textboxes become enabled and allow the user to enter the desired data rate (default 2000 bytes/second) that will trigger activation of the second B-channel and the period for which the data rate exceeds that value, before the channel is activated.

Drop the second ISDN B-channel

When the connection is terminated
When this radio button is selected, the second B-channel is only deactivated when the connection is terminated.

When the data rate is less than n bytes/sec for s seconds
When this radio button is selected, the above two text boxes are enabled. The value in the left-hand one specifies the data rate below which the traffic must fall before the secondary B-channel will be deactivated. The second box contains the time in seconds for which the data rate must be below threshold before the second B-channel is deactivated.

Note:
The following parameters are for use with "Always On Dynamic ISDN".

Bring up the first ISDN B-channel

When the data rate is greater than n bytes/sec for s seconds
When "Always On" mode is enabled, these two textboxes specify the data rate and duration for which the data rate must be sustained before the B-channel is activated.

Drop the first ISDN B-channel

When the data rate is less than n bytes/sec for s seconds
When "Always On" mode is enabled, these two textboxes specify the data rate below the traffic must fall and the duration for which it is below the threshold before the B-channel is deactivated.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
mlppp	0	l_accm	0x00000000 – 0xFFFFFFFF	Desired local ACCM
mlppp	0	r_accm	0x00000000 – 0xFFFFFFFF	Desired remote ACCM
mlppp	0	username	Valid username	username
mlppp	0	password	Valid password	password
mlppp	0	epassword	Encrypted password	None – this parameter is not configurable
mlppp	0	r_chap	ON, OFF	Enable remote CHAP authentication
mlppp	0	l_shortseq	ON, OFF Default OFF	Enable short sequence numbers
mlppp	0	up_rate	0 – 2147483648 Default 2000	When the data rate is greater than n bytes/sec
mlppp	0	up_delay	0 – 2147483648 Default 10	for s seconds
mlppp	0	down_rate	0 – 2147483648 Default 1000	When data rate is less than n bytes/sec
mlppp	0	down_delay	0 – 2147483648 Default 10	for s seconds
mlppp	0	dup_rate	0 – 2147483648 Default 500	When data rate is greater than n bytes/sec
mlppp	0	dup_delay	0 – 2147483648 Default 5	for s seconds

Entity	Instance	Parameter	Values	Equivalent Web Parameter
mlppp	0	ddown_rate	0 – 2147483648 Default 500	When data rate is less than n bytes/sec
mlppp	0	ddown_delay	0 – 2147483648 Default 5	for s seconds

Configuration – Network > Interfaces > Advanced > PPP n

This section contains those parameters which may need to be adjusted when setting up a PPP connection but in general can be left at their default values.

Load answering defaults
Clicking this button will cause the router to read the default PPP answering default parameters from a default configuration stored in memory.

Load dialling defaults
Clicking this button causes the router to read the PPP dialling parameters from a default configuration stored in memory.

Description
This text box holds a description of the PPP instance that may make it easier to refer to. For example the PPP instance used to connect to an ISP may be named "MyISP".

This PPP interface will use
If the PPP mappings have been set up previously using the PPP mappings page, this box will contain the name of the protocol that has been assigned to this PPP instance. If the mapping has not been set up previously and if no default mappings apply, the text in the box should read "Not Assigned". Select the required the required physical interface from the drop-down selection box.

Dial out using numbers
To allow the router to automatically make outgoing calls, the ISDN number must be specified. The four text boxes allow four telephone numbers to be entered. The first one is required, the others are optional and will be used in rotation. These numbers may be the number of the Internet Service Provider (ISP) or another router.

Prefix n to the dial out number
When making outgoing PPP calls, the value specified in this text box is inserted before the actual number being called. This may be required if a PABX system is in use which requires a prefix to be used in order to get an outside line. For example, when using AODI or BACP, the remote peer may provide a number to be used for raising an additional B-channel to increase the bandwidth. However, such a number will not normally include the digits needed to connect to an outside line via a PABX.

Username
The value in this text box is the username to be used for MLPPP login.

Password
This is the password to be used for MLPPP login. This password is used for both B-channel PPP connections.

Confirm password
Type the password in this text box to confirm that the password has been correctly typed in.

Note:

The following three radio buttons control how the IP address for the router is assigned.

Allow the remote device to assign a local IP address to this router

When this radio button is selected, the remote peer will assign this PPP interface an IP address.

Try to negotiate a.b.c.d as the local IP address for this router

If it would be useful, but not essential, to have a predefined IP address for the interface, the second radio button should be selected and the desired IP address entered into the text box to the right.

Use a.b.c.d as the local IP address for this router

If it is essential that the PPP interface has a specific IP address, this radio button should be selected and the IP address entered into the text box.

Use mask a.b.c.d for this interface
The default value in this text box will normally work and should only be changed if it is known that the default is not appropriate. Since PPP is a peer-to-peer protocol this value makes sense in most situations.

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

Close the PPP connection after s seconds
The value in this textbox 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 it has been idle for h hrs m mins s secs
The router will deactivate the PPP instance after the time specified in these text boxes if it detects that the link has not seen traffic.

Alternative idle timer for static routes s seconds
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.

Enable NAT on this interface
When checked, this checkbox causes the router to apply Network Address Translation (NAT) to IP packets on this interface. When enabled, the following additional parameters appear:

IP address/IP address and Port
These radio buttons select whether IP address translation only should be applied or whether port number translation should also be applied to IP packets.

NAT Source IP address a.b.c.d
This text box contains the IP address of the interface that should be used as the source address in IP packets crossing the NAT interface.

Enable IPsec on this interface
When checked, this checkbox causes the router to use the IPsec protocol to secure the connection. When enabled, the following additional parameters appear:

Keep Security Associations (SAs) when this PSTN 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

Checking this checkbox causes the router to apply the firewall settings to traffic using this interface. When debugging connections issues it is often helpful to ensure that this checkbox is NOT checked, as incorrect firewall rules will prevent a connection from passing network traffic. If the connection works when the firewall is turned off but fails when turned on, a good place to start checking parameters would be in the firewall settings page, ***Configuration – Security > Firewall***.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	name	Free text field	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	Valid username	Username
ppp	n	password	Valid password	Password
ppp	n	epassword	The encrypted password	None – this parameter is not configurable
ppp	n	IPaddr	Default 0.0.0.0 set automatically	Allow the remote device to assign a local IP address to this router
ppp	n	IPaddr	Valid IP address a.b.c.d	Try to negotiate a.b.c.d as the local IP address for this router
ppp	n	IPaddr	Valid IP address Default 1.2.3.4	Use a.b.c.d as the local IP address for this router
ppp	n	mask	Valid IP address Default 255.255.255.255	use mask a.b.c.d for this interface
ppp	n	DNSserver	Valid IP address	Primary DNS server
ppp	n	secDNS	Valid IP address	Secondary DNS server
ppp	n	DNSport	Valid IP address Default 53	DNS Port
ppp	n	IPmin	Valid IP address Default 10.10.10.10	Assign remote IP addresses from a.b.c.d to a.b.c.d
ppp	n	IPrange	0 – 255 Default 5	Assign remote IP addresses from a.b.c.d to a.b.c.d Note that these are not directly equivalent. This address is obtained by adding the range value to the minimum.
ppp	n	transDNS	Valid IP address	Primary DNS server
ppp	n	sectransDNS	Valid IP address	Secondary DNS server
ppp	n	cingnb	up to 25 digits	Only allow numbers ending with n
ppp	n	msn	up to 9 digits	with ISDN MSN ending with n

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	sub	up to 17 digits	with ISDN sub-address ending with n
ppp	n	maxup	0 – 2147483648	Close the PPP connection after s seconds
ppp	n	maxuptime	0 – 2147483647	if it has been up for m minutes in a day
ppp	n	timeout	Default 300s (5 minutes)	if it has been idle for h, m, s
ppp	n	timeout2	0 – 2147483648	Alternative idle timer for static routes s seconds
ppp	n	rxtimeout	0 – 2147483648	if the link has not received any packets for s seconds
ppp	n	maxneg	0 – 2147483648	if the negotiation is not complete in s seconds
ppp	n	do_nat	0,1 0 = Off 1 = On	Enable NAT on this interface
ppp	n	natip	Valid IP address a.b.c.d	NAT Source IP address a.b.c.d
ppp	n	ipsec	0,1 0 = Off 1 = On	Enable IPsec on this interface
ppp	n	ipsecent	Default PPP Ethernet	Use interface x,y for the source address of IPsec packets
ppp	n	ipsecadd	Valid interface number	Use interface x,y for the source address of IPsec packets
ppp	n	firewall	OFF, ON	Enable the firewall on this interface

Configuration – Network > Interfaces > Advanced > PPP n > Mobile

Mobile telephone modules fitted into the router use PPP to connect to the network and send and receive traffic. This section describes parameters relevant to setting up a mobile telephone module.

Use SIM Any, SIM1, SIM2
These radio buttons are used to select which of the SIM cards fitted should be used by the module.

Detach W-WAN if the link fails
When checked, this checkbox will cause the router to issue the command to detach the mobile telephone module from the wireless network if it detects that the link has failed. Link failure is detected by a PPP ping response timer or by a firewall request.

Detach W-WAN between connection attempts
This checkbox controls whether or not the module stays attached to the network if multiple connection attempts are required to establish a connection. This functionality may be useful if the connection to the mobile telephone network is not very reliable. Connecting to the mobile telephone network to send and receive data is a two-stage process. The first stage is where the module signals its wish to join the network and is accepted by the local cell. The second stage involves negotiating the link parameters and transferring data. Sometimes it may be necessary to cleanly detach from the network in order to start the process from the ground up.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	gprs_sim	0 – 2 0 = Any 1 = SIM1 2 = SIM2	Use SIM, Any, SIM 1, SIM 2
ppp	n	detach_on_fail	OFF,ON	Detach W-WAN if the link fails
ppp	n	detach	OFF,ON	Detach W-WAN between connection attempts

Configuration – Network > Interfaces > Advanced > PPP n > Advanced

This section contains PPP configuration parameters that do not normally need changing from the defaults and are therefore placed in a separate section to reduce clutter on the web pages.

Metric
This parameter specifies the connected metric of the interface. The default metric of a connected interface is 1. By allowing the interface to have a higher value (lower priority), static routes can take precedence over interfaces. For normal operation, leave the value in this textbox unchanged.

Allow this PP interface to settle for s x 100 milliseconds
On wireless links it is possible that the initial packets sent to the interface by the TCP layer may be dropped by the network if they are sent too quickly after PPP negotiation has completed. The value in this textbox defines the delay in notification sent to the TCP layer that PPP negotiation has completed.

Enable "Always On" mode of this interface
If the "always on" option is available on the interface, checking this checkbox reveals the following two radio buttons. When this functionality is enabled, the router will automatically try to reconnect after about 10 seconds if the link becomes disconnected. This parameter should be enabled when using AODI or W-WAN.

On
Default action, the interface will always try and raise this PPP link.

On and return to service immediately
These two radio buttons enable the "always-on" functionality and additionally the facility to return to the in-service state after a disconnect event.

Put this interface "Out of Service" when an always-on connection attempt fails
Normally, always-on interfaces will not go out of service unless they have connected at least once. When checked, this checkbox causes the router to put the interface out of service even if the first connection attempt fails.

Attempt to re-connect after s seconds
The parameter in this textbox 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 a PPP interface that would be inhibited by this PPP is connected, attempt reconnection after s seconds
The value in this textbox 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 textbox 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.

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.

Enable Multilink PPP on this interface
When checked, this checkbox enables the multilink PPP capability of the router. (See above for configuration details).

Click here to assign a timeband to this interface
Clicking this link redirects the browser to the timeband configuration page ***Configuration – Network > Timebands***.

Add a route to a.b.c.d if the peer's IP address is not negotiated
Normally, the IP address for a device connecting to a remote peer is assigned by the remote peer. If this is not the case then the router will need a route to the remote peer. The value in this textbox is set to the IP address of the remote peer so that it can be added to the routing table.

Forward IP broadcasts over this interface if the interface is on the same IP network as an Ethernet interface
When checked, this checkbox causes the router to route broadcast packets to and from Ethernet interfaces. This will only occur if the PPP instance has issued an address which is part of the Ethernet interface network.

Send LCP echo request packet to the remote peer
When checked, this checkbox reveal the configuration parameters that cause the router to send Link Control Protocol (LCP) packets to the remote peer at specified intervals. This facility can be useful for keeping a link active (W-WAN, for example).

Send LCP echo requests every s seconds
The value in this text box sets the interval at which to send the packets. When set to zero, the transmission of LCP packets is disabled.

Disconnect the link after n failed echo requests
The value in this text box set the number of consecutive failed echo requests that are allowed before the router terminates the link. When set to zero, this functionality is disabled, i.e. the router will not terminate the link if the LCP echo requests do not elicit a response from the remote.

Generate Heartbeats on this interface
When checked, this checkbox reveals the configuration options that control how the router sends heartbeat packets. Generating a valid configuration enables the router to send heartbeat packets to the specified destination. Heartbeat packets are UDP packets that contain various items of information about the router and which may include status information that may be used to locate its current dynamic IP address. Heartbeats may also contain GPS position information and mobile telephone module information.

Send Heartbeat messages to IP address a.b.c.d every h hrs, m minutes, s secs
The left-hand text box contains the IP address of the destination for the heartbeat packets. The remaining text boxes specify the desired interval between sending heartbeat packets.

Use interface x,y for the source IP address
These two text boxes allow selection of the source interface for the UDP heartbeats. Selecting an Ethernet source will allow the packets to follow the routing table instead of being sent out from the PPP interface on which they are set.

Select transmit interface using the routing table
When checked, this checkbox causes the router to choose the best route from the routing table. If unchecked, the exit interface will be the interface on which the heartbeat is configured.

Include IMSI information in the Heartbeat message
When checked, this checkbox causes the router to include the IMSI of the wireless MODEM module in the heartbeat packet.

Include GPS information in the Heartbeat message
When checked, this checkbox causes the router to include the GPS co-ordinates in the heartbeat packet.

Generate Ping packets on this interface
When checked, this checkbox causes the router to reveal the configuration parameters that enable the sending of ICMP echo request (ping) packets. This feature can be used as part of a backup interface strategy.

Send n byte pings to IP host a.b.c.d every h hrs, m mins, s secs
These parameters control how the ICMP echo requests are generated. The value in the left-hand text box specifies the number of data bytes in the echo request. Typical values are 32 or 64 octets. The IP host text box specifies the IP address of the host to which the ping packets are sent. The remaining parameters specify how often the ping should be sent.

Send pings every h hrs, m mins, s seconds if ping responses are not being received
These three text boxes specify the interval at which to send pings when more than one ping request is outstanding. When left at the default of zero this function is disabled.

Switch to sending pings to IP host a.b.c.d after n failures
These parameters allow for more reliable problem detection before failover occurs. If the value in the first text box is a valid IP address, and the value in the second text box is greater than zero, when a ping failure is detected on the primary host address, this secondary host is tried. This is to ensure that should the primary host become unavailable for any reason and stops responding to the ICMP echo requests, the router will check an alternative IP address before initiating the failover procedure. The value in the second text box is the number of pings that should be allowed to fail before checking the secondary IP address.

Ping responses are expected within s seconds
When the value in this text box is set to a non-zero value, the router will wait for that specified interval for a response from a ping request before applying the timeout specified in the "**Send pings every … if ping responses are not being received**" setting above. If the value is set to 0 (the default) then the router applies the timeout without modification.

Only send Pings when this interface is "In Service"
When checked, this checkbox causes the router to only send ICMP requests when the PPP instance is in service. The default setting is unchecked which means that ICMP requests are sent when the interface is in service and out of service.

New connections to resume with previous Ping interval
When checked, this checkbox causes the router to use the ping interval that was in force when the PPP interface last disconnected.

Reset the link if no response is received within s seconds
The value in this text box specifies the period for which the router should wait before terminating the PPP connection if no response to the auto-pings has been received. This behaviour is useful in the attempt to re-establish communications, since the router will automatically attempt to restart an always-on link that has been terminated. This function is primarily used where IP traffic is being carried over a W-WAN link and where the associated PPP instance has been configured into the always-on mode.

Use ETH 0 IP address as the source IP address
When checked, this checkbox causes the router to use the IP address of interface ETH 0 as the source address for ICMP echo requests instead of the current IP address of the PPP interface.

Defer sending pings if IP traffic is being received
One of the uses for sending ICMP echo requests is as a keepalive mechanism. When this checkbox is checked, it causes the router to defer sending the ping packets out if IP traffic is being received, since in this case, separate keepalives are not needed.

Limit the data transmitted over this interface
Some service providers impose a (usually monthly) limit on the amount of data sent over a link and levy additional charges if the limit is exceeded. This is fairly common practice for W-WAN links. When checked, this checkbox causes the router to stop sending data on the interface when the preset data limit has been exceeded. The interface is unlocked manually by clicking the "**Clear Total Data Transferred**" button on the ***Management – Network Status > Interfaces > Advanced > PPP > PPP n*** page. Alternatively, it may be reset automatically on a certain day of the month – see below.

Issue a warning event after n Kbytes/Mbytes/GBytes
The value in this text box is the amount of traffic which will cause a warning event to be generated in the event log stating that the specified amount of data has been transferred. The units are specified by a drop-down list, having the following options; KBytes, MBytes, GBytes. For example, if the monthly tariff includes up to 5MB of data before excess useage charges are levied, it would be useful to set this threshold to 4MB. This would cause the router to create a warning entry in the event log once 4MB of data had been transferred. This event could then be used to trigger an email alert, SNMP trap or SMS alert message.

Stop data from being transmitted after n Kbytes/Mbytes/GBytes
The value in this text box specifies the total amount of data that may be transmitted by this PPP instance before the link is blocked for further traffic, and the value in the drop-down list specifies the units which are; KBytes, MBytes, GBytes.

Reset the data limit on the n day of the month
The value in this text box defined the day of the month on which the data limit is reset to zero.

Reset this interface if n packets are transmitted and the connection has been up for at least s seconds
The values in these text boxes control the circumstances under which the link may be reset. If the number of packets text box has a value greater than zero, the router will reset the link if that many IP packets have been transmitted but none have been received, and the link has been active for at least the value specified in the second text box.

Reboot the router after n consecutive resets
If the value in this text box is non-zero, the router will reboot if the PPP link has been reset the specified number of times as a consequence of the value n packets (described immediately above) being exceeded.

Reboot the router after n consecutive connection failures
If the value in this text box is non-zero, the router will reboot if it fails to establish a connection over this PPP instance after the specified number of consecutive attempts.

Allow this PPP interface to attempt to connect n times before allowing other PPP interfaces inhibited by this interface to connect
The value in this textbox specifies the number of connection attempts this PPP instance is allowed to make before other PPP instances that are inhibited by this instance may make connection attempts.

If this PPP interface gets disconnected, allow it to attempt to reconnect n times before allowing other PPP interfaces inhibited by this interface to connect
On W-WAN routers, the value in this textbox specifies the number of times that a PPP instance which was connected and is then disconnected, is allowed to attempt to reconnect before other PPP instances that were inhibited by this PPP instance will be allowed to connect.

Inhibit this PPP interface if the following PPP instances n are Active | Active and not out of service | Not out of service | Connected and not out of service
Inhibition of this PPP interface may be controlled by the state of other PPP instances. This behaviour is controlled by the options in this drop-down menu box.

If this PPP interface is inhibited and data needs to be sent
The options in this drop-down selection box control the behaviour of the router in the situation where the PPP instance is in its inhibited state but there is data waiting to be sent over the interface. The options are:

Do not bring up interface
This option leaves the situation as it is with the interface remaining inhibited.

Bring up interface and use normal idle period
This option removes the inhibit state from the interface and uses the normal idle time associated with it to control when it deactivates.

Bring up interface and use idle period of s seconds
This option causes the interface to become activated but rather than using the idle timer associated with the interface, specify the idle timeout.

Inhibit other PPP interface if this PPP interface is disconnected but operational
When checked, this checkbox enables this PPP instance to inhibit other PPP instances if it is operational but not currently active.

Attempt to negotiate DEFLATE compression on this interface
When checked, this checkbox causes the router to compress the data transferred over this link. When unchecked, compression is disabled. The effectiveness of data compression will vary with the type of data but a typical ratio achieved for a mix of data such as web pages, spreadsheets, databases, text files and (uncompressed) image files would be between 2:1 and 3:1. Using compression has the effect of increasing the effective throughput. Using compression may offer cost savings on a network where charges are based upon the amount of data transferred (e.g. W-WAN networks). If the data is already compressed (e.g. .zip files or JPEG images) then the compression algorithm will detect this and send the data without attempting further compression.

Attempt to negotiate MPPE encryption on this interface
When checked, this checkbox causes the router to attempt to negotiate Microsoft Point-to-Point Encryption (MPPE) with the remote peer. If the remote peer is unable to negotiate MPPE, negotiations will fail. When negotiated, the PPP instance will encrypt the PPP frames as per the MPPE specification.

MPPE key size
The values in this drop-down list select the length (in bits) of the encryption key. The options are:

- Auto
- 40 bits
- 56 bits
- 128 bits.

"Auto" indicates that the router will accept whatever the remote suggests. For the other values, the remote must accept and request the key size specified, else the PPP negotiations will fail.

Enable MPPE stateless mode
When this checkbox is checked, the router will negotiate stateless mode in which the session key is changed after the transmission of each packet. Stateless mode may be useful for lossy links.

Note:
MPPE does not provide authentication, only encryption. This is because the encryption keys are determined by the PPP engines themselves on start-up.

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

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	metric	0 - 255	Metric
ppp	n	settledly	0 - 200	Allow this PPP interface to settle for s seconds after the connection has come up
ppp	n	aodion	0 – 2 0 = disabled 1 = enabled 2 = On and return to service immediately	Enable "Always On" mode of this interface, On, On and return to service immediately
ppp	n	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 a PPP interface that would be inhibited by this PPP is connected, attempt to re-connect after s seconds
ppp	n	pwr_dly	0 - 2147483647	Wait s seconds after power-up before activating this interface
ppp	n	minup	0 - 2147483647	Keep this interface up for at least s seconds
ppp	n	multi	OFF, ON	Enable Multilink PPP on this interface
ppp	n	netip	Valid IP address a.b.c.d	Add a route to a.b.c.d if the peer's IP address is not negotiated
ppp	n	rbcast	OFF, ON	Forward IP broadcasts over this interface if this interface is on the same IP network as an Ethernet interface
ppp	n	echo	0 - 2147483648	Send LCP echo requests every s seconds
ppp	n	echodropcnt	0 - 2147483648	Disconnect the link after n failed echo requests
ppp	n	hrtbeatip	Valid IP address a.b.c.d	Send Heartbeat messages to IP address a.b.c.d every h hrs, m mins, s secs
ppp	n	hrtbeatint	0 - 2147483648	Send Heartbeat messages to IP address a.b.c.d every h hrs, m mins, s secs
ppp	n	hbipent	Blank, PPP, ETH Blank is default	Use interface x,y for the source IP address
ppp	n	hbipadd	Valid interface number 0 - 2147483648	Use interface x,y for the source IP address
ppp	n	hbiproute	OFF, ON	Select transmit interface using the routing table

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	hbimsi	OFF, ON	Include IMSI information in the Heartbeat message
ppp	n	hbgps	OFF, ON	Include GPS information in the Heartbeat message
ppp	n	pingsiz	0 - 2147483648	Send n byte ping to IP host a.b.c.d every h hrs, m mins, s secs
ppp	n	pingip	Valid IP address a.b.c.d	Send n byte ping to IP host a.b.c.d every h hrs, m mins, s secs
ppp	n	pingint	0 - 2147483648	Send n byte ping to IP host a.b.c.d every h hrs, m mins, s secs
ppp	n	pingint2	0 - 2147483648	Send pings every h hrs, m mins, s seconds if ping responses are not being received
ppp	n	pingip2	Valid IP address a.b.c.d	Switch to sending pings to IP host a.b.c.d after n failures
ppp	n	ip2count	0 - 2147483648	Switch to sending pings to IP host a.b.c.d after n failures
ppp	n	pingresp	0 - 2147483648	Ping responses are expected within s seconds
ppp	n	pingis	OFF, ON	Only send Pings when this interface is "In Service"
ppp	n	ping2cont	OFF, ON	New connections to resume with previous Ping interval
ppp	n	pingdeact	0 - 2147483648	Reset the link if no response is received within s seconds
ppp	n	pingfreth0	OFF, ON	Use ETH 0 IP address as the source IP address
ppp	n	pingresetint	OFF, ON	Defer sending pings if IP traffic is being received
ppp	n	dlwarnkb	0 - 2147483647	Issue a warning event after n XBytes
ppp	n	dlstopkb	0 - 2147483647	Stop Data from being transmitted after n XBytes
ppp	n	dlrstday	0 – 255	Reset the data limit on the n day of the month
ppp	n	sscnt	0 - 2147483648	Reset this interface if n packets are transmitted and the connection has been up for at least s seconds

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	sssecs	0 - 2147483648	Reset this interface if n packets are transmitted and the connection has been up for at least s seconds
ppp	n	lscnt	0 - 2147483648	Reboot the router after n consecutive resets
ppp	n	rebootfails	0 - 2147483648	Reboot the router after n consecutive connection failures
ppp	n	acttries	0 - 255	Allow this PPP interface to attempt to connect n times before allowing other PPP interfaces inhibited by this interface to connect
ppp	n	pdacttries	0 - 255	If this PPP interface gets disconnected, allow it to attempt to reconnect n times before allowing other PPP interfaces inhibited by this interface to connect
ppp	n	inhibitno	0 - 2147483648	Inhibit this PPP interface if the following PPP instances n are Active, Active and not out of service, not out of service, Connected and not out of service
ppp	n	inhmode	0 - 3	Inhibit this PPP interface if the following PPP instances n are Active, Active and not out of service, not out of service, Connected and not out of service
ppp	n	actmode	OFF,ON	Inhibit other PPP interface if this PPP is interface is disconnected but operational
ppp	n	trafficto	0 - 2147483648	If this PPP interface is inhibited and data needs to be sent do not bring up the interface, bring up interface and use normal idle period, bring up interface and use idle period of s seconds
ppp	n	deflate	0,1 0 = Off 1 = On	Attempt to negotiate DEFLATE compression on this interface
ppp	n	mppebits	0, 40, 56, 128	MPPE key size

Entity	Instance	Parameter	Values	Equivalent Web Parameter
			0 = Auto	
ppp	n	mppeless	OFF, ON	Enable MPPE stateless mode
ppp	n	tcptxbuf	0 - 2147483648	TCP transmit buffer size n bytes

Configuration – Network > Interfaces > Advanced > PPP n > PPP Negotiation

When PPP starts up, the devices at both ends of the link negotiate the link parameters, in order to find a common subset that both devices can use. The negotiation may be summarized by saying that both ends send negotiation packets that say "these are the values that I wish to use and these are the values that I wish you to use"

Restrict the negotiation time to s seconds
The parameter in this text entry box specifies the maximum time allowed for a PPP negotiation to complete. If negotiations have not completed in this time, the PPP instance is disconnected.

Desired local ACCM
The value in this text box is the local Asynchronous Control Character Map which has the default value 0x00000000. Changing this value is for advanced users.

Desired remote ACCM
This text box holds the remote ACCM which has the default value 0xffffffff. As above, the default will work in nearly all circumstances and should be changed only where really necessary.

Desired local MRU n bytes
The value in this text box is the desired local Maximum Receive Unit (MRU), the default value of 1500 octets will work fine in most cases.

Desired remote MRU n bytes
The value in this text box is the desired MRU for the remote end of the link. The default value of 1500 octets will be fine in most cases.

Request local ACFC
When checked, this checkbox causes the router to request Address Control Field Compression (ACFC). When negotiated, the address/control fields are removed from the start of the PPP header.

Request remote ACFC
When checked, this checkbox causes the router to ask the remote device to request ACFC.

Request local PAP authentication
When checked, this checkbox causes the router to use the Password Authentication Protocol (PAP) before allowing a connection to be made. Generally, this parameter is enabled for incoming connections and disabled for outgoing connections.

Request remote PAP authentication
When checked, this checkbox causes the router to authenticate itself with the remote device using PAP. If this parameter is set, the connection will fail if authentication is not successful. Generally, this parameter is disabled.

Request local CHAP authentication

When checked, this checkbox causes the router to use the Challenge Handshake Authentication Protocol (CHAP) for local authentication. As with PAP, this parameter is generally enabled for incoming connections and disabled for outgoing connections.

Request remote CHAP authentication
As with PAP above, this checkbox controls whether or not the router should authenticate itself with the remote device using CHAP. The connection will fail if authentication fails. Generally, this parameter is enabled for outgoing connection and disabled for inbound connections.

Request local (VJ) compression
When checked, this checkbox causes the router to request the use of Van Jacobson compression which compresses TCP/IP headers to about 3 rather than the standard 40 octets. This is generally only used to improve efficiency on slow links.

Request remote (VJ) compression
When checked, this checkbox causes the router to send a negotiation packet that requests that the remote device requests VJ compression.

Request local PFC
When checked, this checkbox causes the router to request Protocol Field Compression (PFC) which compresses PPP protocol fields from 2 to 1 octet.

Request remote PFC
When checked, this checkbox causes the router to ask the remote device to request Protocol Field Compression.

Request BACP
When this checkbox is checked, the router will use the Bandwidth Allocation Control Protocol (BACP) to determine the ISDN number to dial for the seconds or third multi-link connection.

Request callback
When checked, this checkbox will request a callback when it dials into a remote device. Note that the answering PPP instance of the remote unit must also be configured with the telephone number of the calling unit and a suitable username, password combination.

Allow remote end to request callback
This drop-down list controls whether or not the router will respond to incoming callback requests. The options are:

- Off
- Desired
- Required.

Allow this unit to authenticate using

CHAP-MD5
Selecting enabled from the drop-down menu will allow the router to authenticate logins using the CHAP MD-5 algorithm.

MS-CHAP
Selecting enabled from the drop-down menu will allow the router to authenticate logins using Microsoft's proprietary MS-CHAP algorithm.

MS-CHAPv2
Selecting enabled from the drop-down menu will allow the router to authenticate logins using version 2 of Microsoft's proprietary MS-CHAP algorithm.

Allow a remote unit to authenticate using

CHAP-MD5

When checked, this checkbox will allow the router to authenticate with a remote unit using the CHAP-MD5 algorithm.

MS-CHAP
When checked, this checkbox will allow the router to authenticate with a remote unit using Microsoft's MS-CHAP algorithm.

MS-CHAPv2
When checked, this checkbox will allow the router to authenticate with a remote unit using version 2 of Microsoft's MS-CHAP algorithm.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	maxneg	0 - 2147483648	Restrict the negotiation time to s seconds
ppp	n	l_accm	0x00000000 – 0xFFFFFFFF Default 0x00000000	Desired local ACCM
ppp	n	r_accm	0x00000000 – 0xFFFFFFFF Default 0xFFFFFFFF	Desired remote ACCM
ppp	n	l_mru	0 – n Default 1500	Desired local MRU
ppp	n	r_mru	0 – n Default 1500	Desired remote MRU
ppp	n	l_acfc	OFF, ON	Request local ACFC
ppp	n	r_acfc	OFF, ON	Request remote ACFC
ppp	n	l_pap	OFF, ON	Request local PAP authentication
ppp	n	r_pap	OFF, ON	Request remote PAP authentication
ppp	n	l_chap	OFF, ON	Request local CHAP authentication
ppp	n	r_chap	OFF, ON	Request remote CHAP authentication
ppp	n	l_comp	OFF, ON	Request local (VJ) compression
ppp	n	r_comp	OFF, ON	Request remote (VJ) compression
ppp	n	l_pfc	OFF, ON	Request local PFC
ppp	n	r_pfc	OFF, ON	Request remote PFC
ppp	n	l_bacp	OFF, ON	Request BACP
ppp	n	l_callb	OFF, ON	Request callback
ppp	n	r_callb	0 – 2 0 = Off 1 = Desired 2 = Required	Allow remote end to request callback
ppp	n	l_md5	0 - 2 0 = Disabled 1 = Enabled 2 = Preferred	Allow this unit to authenticate using CHAP-MD5
ppp	n	r_md5	0,1 0 = Off 1 = On	Allow remote unit to authenticate using CHAP-MD5
ppp	n	l_ms1	0,1 0 = Disabled 1 = Enabled 2 = Preferred	Allow this unit to authenticate using MS-CHAP
ppp	n	r_ms1	0,1 0 = On 1 = Off	Allow remote unit to authenticate using MS-CHAP
ppp	n	l_ms2	0 - 2 0 = Disabled 1 = Enabled 2 = Preferred	Allow this unit to authenticate using MS-CHAPv2
ppp	n	r_ms2	0,1 0 = Off 1 = On	Allow remote unit to authenticate using MS-CHAPv2

Configuration – Network > Interfaces > Advanced > PPP n > QoS

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

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

Configuration – Network > Interfaces > Advanced > PPP Sub-Configs

PPP sub-configs can be used as an alternative to using an entire PPP instance if only a few parameters are different to those in an existing PPP instance. Using PPP sub-configs saves on system memory. Up to 50 sub-configs may be defined.

Nb

This is the instance number for a sub-config.

Description
The text in this text box is used as a name to easily identify the sub-config.

Username
The value in this text box is the username that should be used when authenticating with the remote system and is usually only required for outgoing PPP calls.

Password
The value in this text box is the password used for authentication with the remote system.

Confirm
When changing the password, it should be entered into this text box also to allow the router to check for simple typing errors.

Dialout Number
The value in this text box is the ISDN number used to make outgoing calls. This must be a valid number in order to allow the router to make outgoing calls. This number could be the number of the Internet Service Provider (ISP) or another router.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
pppcfg	1 - 50	name	Up to 25 characters	Description
pppcfg	1 - 50	username	Valid username up to 60 characters	Username
pppcfg	1 - 50	password	Valid password up to 40 cahracters	Password
pppcfg	1 - 50	phonenum	Up to 25 digits	Dialout Number

Configuration – Network > DHCP Server

Digi routers incorporate one or more Dynamic Host Configuration Protocol (DHCP) servers, one for each Ethernet port. DHCP is a standard internet protocol that allows a DHCP server to dynamically distribute IP addressing and configuration information to network clients.

This section contains a web page for each of the DHCP servers. Additionally, there is a separate page for mapping MAC addresses to fixed IP addresses.

Configuration – Network > DHCP Server > DHCP Server for Ethernet n

Enable DHCP Server
When checked, this checkbox opens up the page to reveal the following parameters:

IP Addresses a.b.c.d to a.b.c.d
There are six text boxes in this part of the page; three rows of two. The values in these specify the starting and ending addresses for the range of IP addresses that will be handed out by the DHCP server. Each of the three rows can be used to specify a different IP address pool, all pools should be within the same subnet. When the minimum IP address text box is clear, the DHCP service will be disabled. In other words, in order to enable the DHCP service, there must be at least one minimum IP address and a range.
Using the CLI, this is specified slightly differently, a starting address and a range are specified instead.

Mask
The value in this text box specifies the subnet mask used to on the network to which the router is connected.

Gateway
A gateway is required in order to route data to IP addresses that are not on the local subnet. The value in this text box specifies the IP address of the gateway (which is usually the IP address of the router itself as configured by the IP address of the Ethernet interface associated with this DHCP instance). Alternatively, this may be set to the IP address of another router on the LAN.

DNS Server
The value in this text box specifies the IP address of the primary DNS server to be used by clients on the LAN. This will usually be the IP address of the route itself. Alternatively, this may be set to the IP address of an alternative DNS server on the LAN.

Secondary DNS Server
The value in this text box specifies the IP address of a secondary DNS server (if available) to be used by DHCP clients on the LAN.

Domain Name
The value in this text box specifies the domain name which will be returned to clients.

Lease Duration d days h hrs m mins
The values in these three text boxes specify how long a DHCP client may use the assigned IP address before it must renew its configuration with the DHCP server. When configuring this value using the command line interface be aware that this parameter is specified in minutes. The three boxes here are for convenience when using long lease durations.

Wait for s milliseconds before sending DHCP offer reply
When the checkbox box is checked, the router will use the value in the text box as the delay to use prior to sending out the DHCP_OFFER message. Enabling this functionality and setting the delay to a non-zero value will allow other DHCP servers on the network to respond first.

Only send offers to Wi-Fi clients
When checked, this checkbox causes the router to only send DHCP offers to Wi-Fi clients. This is useful if the router is being used as an access point and there is a separate DHCP server on the Ethernet LAN.

DHCP Relay

Forward DHCP requests to a.b.c.d
The values in these two text boxes specify the IP addresses of the two supported DHCP relay agents. If the DHCP server is on a different subnet, specifying the IP address of the server in this text box will cause the router to forward DHCP requests to the IP address specified. The DHCP server must be within 4 hops.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
dhcp	n	IPmin	Valid IP address a.b.c.d	IP Addresses a.b.c.d
dhcp	n	IPrange	0 – 2147483647 Default 20	to a.b.c.d
dhcp	n	IPmin2	Valid IP address a.b.c.d	IP Addresses a.b.c.d
dhcp	n	IPrange2	0 – 2147483647 Default 0	to a.b.c.d
dhcp	n	IPmin3	Valid IP address a.b.c.d	IP Addresses a.b.c.d
dhcp	n	IPrange3	0 – 2147483647 Default 0	to a.b.c.d
dhcp	n	mask	Valid IP address a.b.c.d	Mask
dhcp	n	gateway	Valid IP address a.b.c.d	Gateway
dhcp	n	DNS	Valid IP address a.b.c.d	DNS Server
dhcp	n	DNS2	Valid IP address a.b.c.d	Secondary DNS Server
dhcp	n	domain	Up to 64 characters	Domain Name
dhcp	n	lease	0 – 2147483648 minutes Default 20160 minutes (14 days)	Lease Duration d days, h hrs, m mins
dhcp	n	respdelms	0 - 2147483647	Wait for s milliseconds before sending DHCP offer reply
dhcp	n	wifionly	OFF,ON	Only send offers to Wi-Fi clients
dhcp	n	fwdip	Valid IP address	Forward DHCP requests to

Entity	Instance	Parameter	Values	Equivalent Web Parameter
			a.b.c.d	a.b.c.d
dhcp	n	fwdip2	Valid IP address a.b.c.d	Forward DHCP requests to a.b.c.d

Configuration – Network > DHCP Server > DHCP Server for Ethernet n > Advanced

Next Bootstrap Server a.b.c.d
The value in this text box specifies the IP address of a secondary configuration server. This server does not have to be on the same logical subnet as the client.

Server Hostname
The value in this text box specifies the name of a host that the DHCP client can make contact with in order to download a boot file.

Boot file
The value in this text box specifies the name of the boot file the client can download from the host specified in the Server Hostname text box.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
dhcp	n	nxtsvr	Valid IP address a.b.c.d	Next Bootstrap Server
dhcp	n	sname	Up to 64 characters	Server Hostname
dhcp	n	file	Up to 64 characters	Boot file

Configuration – Network > DHCP Server > DHCP Server for Ethernet n > Advanced DHCP Options

NetBIOS Name Server a.b.c.d
The value in this text box specifies the IP address of the primary WINS server address.

Secondary NetBIOS Name Server a.b.c.d
The value in this text box specifies the IP address of the secondary WINS server address.

TFTP Server Address a.b.c.d
The value in this text box specifies the IP address of a TFTP server. This is mainly used for boot images.

FTP Server Address a.b.c.d (for WYSE Terminals)
The value in this text box specifies the IP address of an FTP server and is a custom option for use with WYSE terminals.

FTP Root Dir (for WYSE Terminals)
The value in this text box specifies the root directory for FTP transfers. This is also a custom option for use with WYSE terminals.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
dhcp	n	NBNS	Valid IP address a.b.c.d	NetBIOS Name Server a.b.c.d
dhcp	n	NBNS2	Valid IP address a.b.c.d	Secondary NetBIOS Name Server a.b.c.d
dhcp	n	tftp	Valid IP address a.b.c.d	TFTP Server Address a.b.c.d
dhcp	n	ftp	Valid IP address a.b.c.d	FTP Server Address a.b.c.d
dhcp	n	ftproot	Up to 64 characters	FTP Root Dir

Configuration – Network > DHCP Server > Logical Ethernet Interfaces

The web pages in this section are simply a duplicate of the above pages but applying to logical, rather than physical Ethernet interfaces.

Configuration – Network > DHCP Server > DHCP Options

The DHCP Option pages allow custom (or non-standard) DHCP options to be configured and sent to the DHCP client when requesting an IP address and other DHCP parameters. This is useful for devices such as IP telephones that use specific strings. On the web page, these (up to ten) options are configured using a table. The table contains the following fields:

Option
The value in this box specifies the DHCP option number.

Data type
The value in this text box specifies the data type for the option and can be any one of the following; 1,2 or 4 byte value, IPv4 address, text string or hexadecimal data.

Value
The value in this text box specifies the actual data that will be sent in the DHCP option message.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
dhcpopt	n	optnb	0 - 2147483647 Default 0	Option

dhcpopt	n	type	i1 = 1 byte value
			i2 = 2 byte value
			i4 = 4 byte value
			ipv4 = IPv4 address
			string = string
			hex = hexadecimal
				Data type

dhcpopt	n	value	Up to 127 octets	Value

Command line examples

To set the option number to “9” for LPR Server, the command is:

```
dhcpopt 0 optnb 9
```

Configuration – Network > DHCP Server > Static Lease Reservations

The table on this web page controls the configuration of MAC address to IP address mappings and is used to assign a specific IP address to a particular Ethernet MAC address. This is particularly useful for mobile applications, e.g. W-WAN where a particular item of mobile equipment should be issued with the same IP address regardless of when it was last connected to the network. Up to ten MAC to IP address reservations may be specified.

Note:
It is important to ensure that the IP addresses specified her DO NOT fall within the IP address ranges specified in the DHCP server page.

IP Address a.b.c.d
The value in this box specifies the IP address to be assigned.

MAC Address aa.bb.cc.dd.ee.ff
The value in this box specifies the MAC address which is to be given the above IP address.

As is usual with the configuration tables, clicking the **Add** button adds the entry to the table and clicking the **Delete** button removes an existing entry from the table.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
mac2ip	n	IPaddr	Valid IP address a.b.c.d	IP Address a.b.c.d
mac2ip	n	mac	Valid MAC address aa.bb.cc.dd.ee.ff	MAC Address aa.bb.cc.dd.ee.ff

Two separate commands are required to set up a mapping, these are:

```
mac2ip <instance> mac <MAC address>
```

```
mac2ip <instance> IPaddr <IP address>
```

where *<instance>* can be 0 – 9.

Configuration – Network > Network Services

The web page described here collects together a number of services that are provided by the router into one section to enable the user to quickly enable or disable these services without having to navigate to multiple sections of the menu. Detailed configuration is performed within the specific section.

Enable Network Management Protocol (SNMP)
Click on this checkbox to enable and disable remote management of the router using SNMP. This checkbox does not actually directly control the SNMP functionality, but enables or disables the remaining SNMP controls on this page.

> **Note:**
> Simply clicking on this checkbox may not be sufficient to allow this service to start working. Depending upon the version selected below, additional configuration may be required.

Detailed configuration, including setting up command filters, users and SNMP traps are to be found at ***Configuration > Remote Management > SNMP***

Enable SNMP v1
When this checkbox is checked, the router will use version 1 of the protocol.

UDP Port n
The standard UDP port that is used by this service is 161 which is used as the default. If a different port is required, enter the port number into the text entry box.

Enable SNMP v2c
When this checkbox is checked, the router will use version 2c of the protocol.

Enable SNMP v3
When this checkbox is checked, the router will use version 3 of the protocol.

Enable Simple Network Timer Server (SNTP)
When checked, the router will act as an SNTP time server.

Source
This drop-down selection menu selects the source used to supply time data for the SNTP server. The usual options are:

- internal real time clock (RTC) device
- a GPS module (if supported)
- an NTP client (if supported).

Enable Secure Shell Server (SSH / SFTP)
The simplest way to check the status or configuration of the router or to upload new firmware is to use the CLI over a directly connected ASY port or via a telnet session. Both of these options have security implications. If a user wishes to gain access to the command line interface of the router but using a more secure protocol, then selecting this checkbox will enable a secure shell to start. This option also enables support for SFTP for secure file transfers.

Enable Telnet Server
This radio button selects between a simple telnet server or telnet over SSL. When this option is selected, the simple, insecure version of telnet is enabled.

Enable Telnet over SSL
If security is an issue, then selecting this option with the radio button disables the simple version and enables telnet over the secure socket layer (SSL) protocol.

Enable Web Server (HTTP)
Much of the configuration of the router may be performed using the web GUI as described here. However, HTTP is an insecure protocol and so for security reasons, this service may be disabled by deselecting this radio button and hence, enabling the following secure web server. If security is not such an issue, selecting this option allows the simpler and slightly more convenient web server to be used.

Enable Secure Web Server (HTTPS)
Select this radio button to disable the insecure HTTP protocol and enable the HTTPS service.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
snmp	n	v1enable	0,1 0 = Off 1 = On	Enable SNMP v1
snmp	n	port	Default 161	UDP Port n
snmp	n	v2cenable	0,1 0 = Off 1 = On	Enable SNMP v2c
snmp	n	v3enable	0,1 0 = Off 1 = On	Enable SNMP v3
sntp	0	srvr_mode	ON,OFF	Enable Simple Network Time Server (SNTP)
sntp	0	time_src	0 = RTC 1 = GPS 2 = NTP Client	Source
sockopt	n	ssh_server_ena	ON, OFF	Enable Secure Shell Server
sockopt	n	telnets	ON, OFF	Enable Telnet over SSL
sockopt	n	https	ON, OFF	Enable Secure Web Server

Configuration – Network > DNS Servers

This section describes the parameters used to configure the DNS server functionality of the router.

Configuration – Network > DNS Servers > DNS Server n

The DNS server selection parameters give the ability to specify a DNS server based on the DNS query. For example, DNS lookups for internal servers can be directed to an internal DNS server and all other DNS requests can be sent direct to an external DNS server managed by the ISP.

For DNS requests matching pattern, send the request to
This text box contains the hostname pattern to match for the specified DNS server. This parameter needs a wildcard to prefix the domain name. For example, to match DNS queries for all digi.com servers, enter *.digi.com.
When using this feature, it is recommended that the last DNS server selection hostname pattern is set to "*" to match all other DNS lookups. This ensures that all the DNS lookup configuration is kept together for ease of troubleshooting. If this is not done, the lookups will use the DNS server configured on the interface of the default route.

DNS Server a.b.c.d
The value in this text box specifies the IP address of the DNS server to use when a DNS request matches the hostname pattern.

Secondary DNS Server a.b.c.d
In the event of the primary DNS server not being available, the IP address in this text box specifies the destination for DNS queries matching the hostname pattern.

Route using

Routing table / Interface x,y
The two radio buttons associated with this text control whether the router should look up the route to the DNS server by using the routing table or should send the DNS query out of a specific interface. When the Interface radio button is selected, the drop-down box and interface instance text box are enabled. The options available for the interface are PPP and Ethernet. The adjacent text box should be filled in with the number of a valid instance of the interface, e.g. Ethernet 3. (Different models of router support different numbers of interfaces).

Use source IP Address of

Sending interface / Interface x,y
The two radio buttons control whether the DNS query should go out having the source address of the sending interface or a different interface. This will be required for routing if the route to the DNS server is via an IPsec tunnel, to ensure the local and remote subnet selectors match.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
dnssel	n	pattern	*.domain.com	For DNS requests matching pattern, send the request to
dnssel	n	svr	Valid IP address	DNS Server a.b.c.d
dnssel	n	secsvr	Valid IP address	Secondary DNS Server a.b.c.d
dnssel	n	ent	PPP,Ethernet	Interface x,y
dnssel	n	add	Valid interface number	Interface x,y
dnssel	n	ipent	PPP,Ethernet	Interface x,y
dnssel	n	ipadd	Valid interface number	Interface x,y

Configuration – Network > DNS Servers > DNS Server Update

"Dynamic DNS" is supported in accordance with RFC2136 and RFC2485. This allows units to update specified DNS servers with their IP addresses when they first connect to the Internet and at regular intervals thereafter. The parameters in this section control how the router updates a specified DNS server with its IP address when it first connects to the Internet and at regular intervals thereafter.

This is not to be confused with the popular dynamic DNS service dyndns.com, there is a separate page for configuring the router to work with dyndns.com

Send an update to DNS Server a.b.c.d for
The IP address in this text box specifies the DNS server that should be sent the updated information. The server must support "DNS Update messages". Dynamic DNS is generally offered as a subscription-based service by ISPs, but for a large number of deployed routers, it may be more appropriate to set up a dedicated DNS server locally.

Name
The value in this text box specifies the member of the DNS zone to update. This name is used in conjunction with the zone parameter (below) to uniquely identify the router. So, for example, if the router has a name of "epos33", the full address of the unit will be "epos33.mycompany.com".

Zone
The value in this text box specifies the DNS zone to update. When using Dynamic DNS it will be necessary to have domain name (this may be purchased from an appropriate vendor). This domain name, e.g. "mycompany.com" is what should be entered into the zone field.

When the default route changes

Interface x,y becomes active

The two radio buttons determine when the update is sent, i.e. when the default route changes or when the specified interface becomes active. The drop-down list offers the options of "PPP" or "Ethernet" and the text box is used to enter the instance number for the specified interface.

Also send an update every h hrs, m mins, s secs

The values in these text boxes specify the interval at which the unit will issue update messages to the DNS server.

The DNS server should delete all previous records

When checked, this checkbox causes the DNS server to delete all records of previous addresses served to the unit.

DNS Server Username

The value in this text box is the username that has been allocated by the Dynamic DNS service provider.

DNS Server Password

The value in this text box is the password that has been allocated by the Dynamic DNS service provider.

Password is Base64 encoded

Some Dynamic DNS servers issue passwords that are Base64 encoded, e.g. Linux Base servers. If this is the case, check this check box to switch on the Base64 decoding of the password before transmission. The password is not actually transmitted as part of the message but is used to create a “signature” that is appended to the message. If the password is issued as a hexadecimal string and not straight text, the password in the password text box must be given the prefix “0x”.

Confirm DNS Server Password

The password should be entered into this text box to confirm it.

Local time offset from GMT

Auto detect

The two radio buttons here control whether or not the offset of the local time from GMT should be auto-detected or specified. This feature is required since a GMT timestamp must be included as part of the authentication message. When set to auto-detect the router will automatically apply the correction. When auto detect is not selected, the correct offset should be selected from the drop-down list.

Required Time Accuracy

The value in this text box specifies the permitted variance between the router’s time and that of the DNS server. If the time difference exceeds this limit, the DNS update will fail.

Allow DNS clients to cache this entry for s seconds

The value in this text box specifies how long a router that resolved the address is allowed to cache that address for.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
dnsupd	0	server	Valid IP address a.b.c.d	Send an update to DNS Server a.b.c.d
dnsupd	0	name	up to 20 characters	Name
dnsupd	0	zone	up to 64 characters	Zone
dnsupd	0	ifent	PPP,ETH	when interface x,y becomes active
dnsupd	0	ifadd	Valid instance number	when interface x,y becomes active
dnsupd	0	upd_int	0 – 2147483648 (seconds)	Also send an update every h hrs, m mins s secs
dnsupd	0	delprevrr	OFF,ON	The DNS server should delete all previous records
dnsupd	0	username	Valid username (up to 20 characters)	DNS Server Username
dnsupd	0	password	Valid password (up to100 characters)	DNS Server Password
dnsupd	0	b64pwd	OFF,ON	Password is Base64 encoded
dnsupd	0	autozone	OFF,ON	Local time offset from GMT auto detect
dnsupd	0	tzone	–2147483648 - 2147483647 (hours)	Local time offset from GMT n
dnsupd	0	fudge	0 – 2157483648 (seconds)	Required Time Accuracy s seconds
dnsupd	0	ttl	0 – 2157483648 (seconds)	Allow DNS clients to cache this entry for s seconds

Configuration – Network > Dynamic DNS

The Dynamic DNS client (DynDNS) is used to update DNS hostnames with the current IP address of a particular interface. It operates in accordance with the specification supplied by dyndns.com (go to http://www.dyndns.com/developers/specs/). When the interface specified by the interface and interface instance number parameters connects, the client checks the current IP address of that interface and if it differs from that obtained from the previous connection, www.dyndns.com is contacted and the hostnames specified in the Hostname parameters are updated with the new address.

Host and Domain Name(s)
These five text boxes specify up to five host/domain names that are to be updated using the service.

Destination port #
The value in this text box specifies the IP port to use as the destination port. The default value is 0 which causes the router to use the default port number which is port 80.

DynDNS User Name
The value in this text box specifies the username to use when updating the hostnames. This will have been supplied by the service provider.

DynDNS Password
The value in this text box specifies the password to use when updating the hostnames. This will have been supplied by the service provider.

Confirm DynDNS Password
Enter the password into this text box to confirm it.

DynDNS DDNS System
The value selected from this drop-down list is used to identify the dynamic DNS system containing the hostnames to be updated. The available options are:

- Dynamic DNS
- Static DNS
- Custom DNS.

When default route/interface x,y becomes active, send DDNS update
The radio buttons select whether or not the router should use the default interface or the interface specified from the drop-down list. If the specified interface option is selected, the required interface is selected from the drop-down list and the interface instance is entered into the adjacent text box. If the default interface is selected, the client will keep track of and use the current default route.

Use Wildcards
This drop-down list selects whether or not wildcard matching on the hostname will be performed. The options are:

- Disable wildcards
- Enable wildcards
- No change to service settings.

When enabled, the Dynamic DNS service will match DNS requests of the form "*.hostname" where "*" matches any text. For example, if Hostname1 was set to "site.dyndns.com" and wildcard matching was enabled, than www.site.dyndns.com would resolve to the interface address.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
dyndns	0	hostname1	Up to 40 characters	Host and Domain Name(s)
dyndns	0	hostname2	Up to 40 characters	Host and Domain Name(s)
dyndns	0	hostname3	Up to 40 characters	Host and Domain Name(s)
dyndns	0	hostname4	Up to 40 characters	Host and Domain Name(s)
dyndns	0	hostname5	Up to 40 characters	Host and Domain Name(s)
dyndns	0	port	0 - 65535	Destination port #
dyndns	0	username	Up to 20 characters	DynDNS User Name
dyndns	0	password	Up to 25 characters	DynDNS Password
dyndns	0	system	Blank, statdns, custom	DynDNS DDNS System
dyndns	0	ifent	Blank,ETH,PPP	When default route/interface x,y becomes active, send DDNS update
dyndns	0	ifadd	0 -2147483647	When default route/interface x,y becomes active, send DDNS update
dyndns	0	wildcard	0,1,2 0 = Disable wildcards 1 = Enable wildcards 2 = No change to service settings	Use Wildcards

Configuration – Network > Dynamic DNS > Advanced

The parameters in this section do not normally need changing from their defaults.

Update interval d days
The value in this text box specifies the number of days between dynamic DNS updates.

Supply the IP address in the update
When checked (the default), this checkbox cause the router to supply the IP address as part of the dynamic DNS update. When unchecked, the IP address is not supplied and the DYNDNS server attempts to determine the correct IP address by other means (IP source address in update packet). This mode would normally only be used if the router is behind a NAT router.

Note:
It may be helpful to visit the www.dyndns.com website before attempting configuration of dynamic DNS.

Only send update when this router is the VRRP master
When checked, this checkbox causes the router NOT to send DDNS updates unless at least one Ethernet interface is a VRRP master.

Enable debug
When checked, this checkbox enables debug tracing of the dynamic DNS transactions.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
dyndns	0	updateint	0 -255	Update interval d days
dyndns	0	noip	OFF,ON	Supply the IP address in the update
dyndns	0	ifvrrpmaster	OFF,ON	Only send update when this router is the VRRP master
dyndns	0	debug	OFF,ON	Enable debug

Configuration – Network > IP Routing / Forwarding - An introduction to TransPort routing

The configuration pages and command line commands that are described in this section control the routing behaviour of the router.

The TransPort's routing table can be viewed by navigating to ***Management - Network Status > IP Routing Table.***

The TransPort's routing table can also be displayed using the CLI command:

```
route print
```

Types of route

TransPort routers support three main types of route:

Dynamic Routes

Static Routes

Default Routes

Dynamic Routes

Dynamic routes are created automatically when an interface is configured or connected.

For example configuring an Ethernet 0 interface with an IP address of 192.168.1.1 and mask of 255.255.255.0 will cause a dynamic route to be created automatically.

Thus any packet with destination IP address in the range 192.168.1.0 to 192.168.1.255 will

automatically be routed through to the Ethernet 0 interface.

Static Routes

Static routes can be added by configuring a route in ***Configuration - Network > IP Routing/Forwarding > Static Routes > Routes 0 – 9 > Route n*** (where n is an instance number).

The minimum configuration required to add a static route is:

IP Address

Mask

Interface

Interface number

If a static route is "pointing" at an Ethernet interface then optionally a gateway IP address can be added. If a gateway IP address is not added then the gateway IP address configured for the Ethernet interface itself will be used automatically.

Default Routes

Default routes can be added by configuring a route in ***Configuration - Network > IP Routing/Forwarding > Static Routes > Default Route n*** (where n is an instance number).

Default routes will match packets with any destination IP address (when in service).

If a default route is configured, packets with destination IP addresses that do not match any of the dynamic or static routes will be sent out the interface specified in the first "in service" default route.

Routing modes

The TransPort has 2 routing modes available, these are:

TransPort routing mode

This is the original routing method and may be seen on existing installations.

CIDR routing mode

Now enabled by default on new TransPort routers.

The CLI command to switch between the 2 modes is:

ip 0 cidr [off|on]

TransPort routing mode

CIDR routing is disabled

When the TransPort receives an IP packet to route, the routing table is used to decide through which interface to send the packet.

Usually the destination IP address of the IP packet is compared with the IP Address and Mask of each entry in the routing table in index order regardless of the order in the routing table or length of mask.

There may be more than one match and in this case the index number of the route is taken into account. The index number is simply the route number in the config, Static Route 0 or 1 is index 0 or 1

Static routes are checked first, then dynamic routes, then default routes.

CLI command: *ip 0 cidr off*

CIDR routing mode

CIDR routing is enabled

When the TransPort receives an IP packet to route, the routing table is used to decide through which interface to send the packet.

Usually the destination IP address of the IP packet is compared with the IP Address and Mask of each entry in the routing table.

There may be more than one match and in this case the most specific route is used to route the packet. Ie, a matching /24 route is used before a matching /16 route.

If multiple routes match the destination and have the same prefix length, the index number of the routes in the routing table is used to determine the route.

CLI command: *ip 0 cidr on*

Route Metrics

Route Metric settings can be set to override the order in which the routes are searched.

Routes with lower metric numbers will always be used in preference to routes with higher metric numbers even if the routes with higher metric numbers appear first in the routing table.

Route metrics can be configured by means of the route parameters:

Connected Metric

Disconnected Metric

Route metrics can be altered automatically according to various circumstances. This is in order to provide automatic backup connection paths.

Routes and interfaces can be put out of service.

Whenever an interface is out of service (oos) any route pointing at the interface will also be out of service.

Whenever a route is out of service, the metric value will be set to 16 in TransPort routing mode and 17 in CIDR mode.

Configuration – Network > IP Routing / Forwarding > IP Routing

Enable CIDR routing
When this checkbox is checked, the following six text boxes are revealed:

Connected Interfaces
The value in this text box specifies the CIDR metric that the router should apply to connected interfaces.

Static Routes
The value in this text box is the CIDR metric that the router should use for static routes. (Default 1)

eBGP Routes
The value in this text box is the CIDR metric that the router should use for eBGP routes. (Default 20).

OSPF Routes
The value in this text box is the CIDR metric that the router should use for OSPF routes. (Default 110)

RIP Routes
The value in this text box is the CIDR metric that the router should use for RIP routing. (Default 120).

iBGP Routes
The value in this text box is the CIDR metric that thae router should use for iBGP routes. (Default 200).

Maximum static route metric
The value in this text box defines the maximum value for the routing metric. The default value is 16.

Route directed IP broadcasts
When checked, this checkbox causes the router to route directed broadcasts. The default state for this parameter is "Off". A directed broadcast is an IP packet with a destination address that is a valid broadcast address for a subnet but does not originate from that subnet. Directed IP broadcasts are used to send a broadcast from one interface to the subnet of another.

Wait s seconds before using an alternative route
The value in this text box specifies the latency to apply before passing traffic on an alternative route in the current route becomes unavailable.

If an interface is configured for "dial on demand" and fails to connect,

Mark a static route as "Out Of Service" for s seconds
The value in this text box specifies the default time that a route should be marked as out of service if the interface it uses fails to establish a connection.

When an "Always On" route becomes "In Service", wait s seconds before using it
The value in this text box specifies the delay that the router should apply to a route before passing traffic on it once it has come into service.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ip	0	cidr	on,off	Enable CIDR routing
ip	0	admin_connected	0 - 2147483647	Connected Interfaces
ip	0	admin_static	0 - 2147483647	Static Routes
ip	0	admin_ebgp	0 - 2147483647	eBGP Routes
ip	0	admin_ospf	0 - 2147483647	OSPF Routes
ip	0	admin_rip	0 - 2147483647	RIP Routes
ip	0	admin_ibgp	0 - 2147483647	iBGP Routes
ip	0	inf_metric	0 - 2147483647	Maximum static route metric
ip	0	route_dbcast	0 - 255	Route directed IP broadcasts
ip	0	route_dly	0 - 2147483647	Wait s seconds before using an alternative route
ip	0	route_dwn	0 - 2147483647	If an interface is configured for "dial on demand" and fails to connect, Mark a static route as "Out Of Service" for s seconds
ip	0	routeup_dly	0 - 2147483647	When an "Always On" route becomes "In Service", wait s seconds before using it

Configuration – Network > IP Routing / Forwarding > Static Routes

The static routing web pages and command line parameters described below control the static routing table used by the router. These allow the setting up of static IP routes for particular IP subnets, networks or addresses.

Configuration – Network > IP Routing / Forwarding > Static Routes > Route n

Each of the static route instances has its own configuration page. These are described below.

Description
The value in this text box is to allow a memorable name for the route to be assigned.

Destination Network a.b.c.d
The value in this text box is the IP address of the destination subnet, network or IP address for the route. If the router receives a packet with a destination IP address that matches the Destination Network/Mask combination it will route the packet through the interface specified below.

Mask a.b.c.d
The value in this text box is the network mask that is used in conjunction with the above destination network address to specify the.

Gateway a.b.c.d
The value in this text box is used to override the default gateway IP address configured for the Ethernet interfaces. Packets matching the route will use the gateway address specified in the route rather than the address specified on the Ethernet interface configuration page. This parameter does NOT apply to routes using PPP interfaces.

Interface x,y
The interface used to route the packets is selected from the drop-down list and the interface instance number is entered into the adjacent text box. The available options are:

- None
- PPP
- Ethernet
- Tunnel

Use PPP sub-configuration
If PPP sub-configs are defined, this text will appear in normal highlighting (i.e. not "greyed out") and text box will accept the number for the desired sub-config to use on this route. This parameter will not appear at all on those models which do not support PPP sub-configurations.

Metric n
The value in this text box is the routing metric to use when the interface is connected. This should have a value between 1 and 16 and is used to select which route should be used when the subnet for a packet matches more than one of the IP route entries.
Each route may be assigned a "connected metric" and a "disconnected metric". The connected metric parameter is used to specify the metric for a route whose interface is active. The disconnected metric is used to specify the metric for a route whose interface is inactive. Normally both values should be the same but in some advanced routing scenarios necessary to use different values.
If a particular route fails it will automatically have its metric set to 16 which means that it is temporarily deemed as being "out of service". The default out of service period is set by the IP route out of service parameter on the .... page. Note however, that this default period may be overwritten in certain situations such as when a firewall stateful inspection rule specifies a different period. When a route is out of service, any alternative routes (with matching subnets) will be used first.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
route	n	descr	Up to 20 characters	Description
route	n	IPaddr	Valid IP address a.b.c.d	Destination Network a.b.c.d
route	n	mask	Valid netmask a.b.c.d	Mask a.b.c.d

Entity	Instance	Parameter	Values	Equivalent Web Parameter
route	n	gateway	Valid IP address a.b.c.d	Gateway
route	n	ll_ent	Blank,PPP,ETH,TUN	Interface x,y
route	n	ll_add	0 – 2147483647	Interface x,y
route	n	upmetric	0 – 2147483647	Metric

Configuration – Network > IP Routing / Forwarding > Static Routes > Route n > Advanced

Use metric n when the interface is not active
The value in this text box specifies the routing metric to use when the interface is not active.

Use this route only if the source IP address of the packet matches
When this checkbox is checked, the following two parameters are enabled.

IP Address a.b.c.d
If necessary, these IP Address and Mask parameters may be used to further qualify the way in which the router routes packets. If the values in this text box and the following Mask parameter are set, the source address of the packet being routed must match these parameters before the packet will be routed through the specified interface.

Mask a.b.c.d
The value in this text box specifies the netmask that is used in conjunction with the IP address as explained above.

Include this route in RIP advertisements
When checked, this checkbox will cause the router to include this static route to be included in RIP advertisements.

Make PPP n interface use the alternative idle timeout when this route becomes available
When checked, this check box, in conjunction with the PPP interface instance number in the text box will cause the router to use the alternative inactivity timeout specified for that interface when this route comes back into service. This feature is useful when it is preferable to close down a backup route quickly when a primary route comes back into service.

Wait for s seconds after power up before allowing this route to activate the interface
The value in this text box specifies the delay that the router should wait after power-up before packets matching this route will initiate a connection of the interface configured in the route. It is typically used on W-WAN routers that have ISDN backup in order to prevent unnecessary ISDN connections from being made whilst a W-WAN connection is first being established.

Mark this route as "Out of Service" in the interface fails to connect after n consecutive attempts

Normally, if an interface is requested to connect by a route and fails to connect, the route metric is set to 16 for the period of time specified by the **Mark a static route as "Out Of Service" for s seconds** parameter on the ***Configuration – Network > IP Routing/Forwarding > IP Routing*** page. If the value in this text box is non-zero, the route metric will not be set to 16 until the number of connection attempts specified by this parameter have been made.

If the interface fails to connect, try again in s seconds
If an interface is requested to connect by this route (due to IP traffic being present) and it fails to connect, the route will be marked as out of service but the router will continue to attempt to connect at the interval specified by the value in this text box. If the interface does connect, the router will clear the out of service status for the route.

Deactivate the interface after it successfully connects
When checked, this check box will cause the router to deactivate an interface once a successful activation attempt has been made. This is used in conjunction with the above retry parameter. If the above retry parameter is not set, this checkbox is "greyed out".

Do not allow this interface to be activated by this route for s seconds after the last activation attempt
The value in this text box is the delay to wait before re-initiating a connection after it has dropped whilst still required.

Only queue one packet whilst waiting for the interface to connect
When checked, this checkbox will cause the router to enqueue only one packet while waiting for the interface to connect. When unchecked, the router will enqueue two packets.

When this route becomes available, deactivate the following interfaces x,y x,y
The interfaces specified by the values in these two pairs of drop-down list and text boxes will be deactivated when this route becomes available again after being out of service. This feature is typically used to deactivate backup interfaces when the primary interface becomes available after being out of service. Select the required interface from the drop-down list and enter the interface instance number into the text box as usual.

When this route becomes unavailable, remove the "Out of Service" state on x,y
This drop-down list and text box are used to specify the interface (available options are "None", "PPP", "Ethernet" and "Tunnel") and instance that should be taken out of the "Out of Service" state when the interface that this route is configured to use is deactivated.

Keep this route in service for s seconds after OOS state is cleared
When this checkbox is checked, the following text box is enabled (i.e. it is no longer "greyed out"), allowing a value to be entered. The value specifies the period that the interface specified above will remain in service even though it is actually unable to pass traffic immediately. This is behaviour useful in situations where a PPP interface is activating and traffic should not try the next interface until this one has been allowed a certain amount of time to come up. When this timer expires, if the interface is unable to pass traffic, it will be marked Out of Service and the next interface will be tried.

Assign this route to recovery group n
The value in this text box is used to assign the route to a "recovery group". This means that if all the routes in a particular recovery group go out of service, the out of service status is cleared for all routes in that group. If one route in a group comes back into service, all routes with a lower priority (metric) also have their out of service status cleared.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
route	n	metric	0 – 2147483647	Use metric n when the interface is not active
route	n	srcip	Valid IP address a.b.c.d	IP Address a.b.c.d
route	n	srcmask	Valid netmask a.b.c.d	Mask a.b.c.d

Entity	Instance	Parameter	Values	Equivalent Web Parameter
route	n	inrip	on,off	Include this route in RIP advertisements
route	n	doinact2	on,off	Make PPP n interface use the alternative idle timeout when this route becomes available
route	n	inact2add	0 – 2147483647	Make PPP n interface use the alternative idle timeout when this route becomes available
route	n	pwr_dly	0 - 255	Wait for s seconds after power up before allowing this route to activate the interface
route	n	actooslim	0 – 2147483647	Mark this route as "Out Of Service" if the interface fails to connect after n consecutive attempts
route	n	chkoos_int	0 – 2147483647	If the interface fails to connect, try again in s seconds
route	n	chkoos_deact	0 - 255	Deactivate the interface after it successfully connects
route	n	dial_int	0 – 255 Default 10	Do not allow this interface to be activated by this route for s seconds after the last activation attempt
route	n	q1	on,off	Only queue one packet whilst waiting for the interface to connect
route	n	deact_ent	Blank,PPP	When this route becomes available, deactivate the following interfaces x,y
route	n	deact_add	0 – 2147483647	When this route becomes available, deactivate the following interfaces x,y
route	n	deact_ent2	Blank,PPP	When this route becomes available, deactivate the following interfaces x,y
route	n	deact_add2	0 – 2147483647	When this route becomes available, deactivate the following interfaces x,y
route	n	unoos_secs	0 – 2147483647	Keep this route in service for s seconds after OOS state is cleared
route	n	rgroup	0 - 255	Assign this route to recovery group n

Configuration – Network > IP Routing / Forwarding > Static Routes > Default Route n

The following two web pages and associated command line commands are used to set up default IP routes that will be used to route non-local IP addresses not specified in a static route. The parameters are identical to those on the static route pages with the exception that there are no IP address or Mask parameters.

Description
The text in this text box is used to assign a convenient and memorable description for the route.

Default route via:

Gateway a.b.c.d
As per equivalent parameter in Routes n.

Interface x,y
As per equivalent parameter in Routes n.

Metric n
As per equivalent parameter in Routes n.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
def_route	n	descr	Up to 20 characters	Description
def_route	n	gateway	Valid IP address a.b.c.d	Gateway a.b.c.d
def_route	n	ll_ent	Blank,PPP,ETH,TUN	Interface x,y
def_route	n	ll_add	0 – 2147483647	Interface x,y
def_route	n	upmetric	1 - 16	Metric

Configuration – Network > IP Routing / Forwarding > Static Routes > Default Route n > Advanced

Use metric n when the interface is not active
As per equivalent parameter in Routes n.

Use this route only if the source IP address of the packet matches
As per equivalent parameter in Routes n.

IP address a.b.c.d
As per equivalent parameter in Routes n.

Mask a.b.c.d
As per equivalent parameter in Routes n.

Include this route in RIP advertisements
As per equivalent parameter in Routes n.

Make PPP x interface use the alternative idle timeout when this route becomes available
As per equivalent parameters in Routes n.

Wait for s seconds after power up before allowing this route to activate the interface
As per equivalent parameter in Routes n.

If the interface is configured for "dial on demand"

Mark this route as "Out Of Service" if the interface fails to connect after n consecutive attempts
As per equivalent parameter in Routes n.

If the interface fails to connect, try again in s seconds
As per equivalent parameter in Routes n.

Deactivate the interface after it successfully connects
As per equivalent parameter in Routes n.

Do not allow this interface to be activated by this route for s seconds after the last activation attempt
As per equivalent parameter in Routes n.

Only queue one packet whilst waiting for the interface to connect
As per equivalent parameter in Routes n.

When this route becomes available, deactivate the following interfaces x,y x,y
As per equivalent parameter in Routes n.

When this route becomes unavailable, remove the "Out Of Service" state on x,y
As per equivalent parameter in Routes n.

Keep this route in service for s seconds after OOS state is cleared
As per equivalent parameter in Routes n.

Assign this route to recovery group n
As per equivalent parameter in Routes n.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
def_route	n	metric	0 – 2147483647	Use metric n when the interface is not active
def_route	n	srcip	Valid IP address a.b.c.d	IP Address a.b.c.d
def_route	n	srcmask	Valid netmask a.b.c.d	Mask a.b.c.d
def_route	n	inrip	on,off	Include this route in RIP advertisements
def_route	n	doinact2	on,off	Make PPP n interface use the alternative idle timeout when this route becomes available
def_route	n	inact2add	0 – 2147483647	Make PPP n interface use the alternative idle timeout when this route becomes available
def_route	n	pwr_dly	0 - 255	Wait for s seconds after power up before allowing this route to activate the interface

Entity	Instance	Parameter	Values	Equivalent Web Parameter
def_route	n	actooslim	0 – 2147483647	Mark this route as "Out Of Service" if the interface fails to connect after n consecutive attempts
def_route	n	chkoos_int	0 – 2147483647	If the interface fails to connect, try again in s seconds
def_route	n	chkoos_deact	0 – 2147483647	Deactivate the interface after it successfully connects
def_route	n	dial_int	0 – 255 Default 10	Do not allow this interface to be activated by this route for s seconds after the last activation attempt
def_route	n	q1	on,off	Only queue one packet whilst waiting for the interface to connect
def_route	n	deact_ent	Blank,PPP	When this route becomes available, deactivate the following interfaces x,y
def_route	n	deact_add	0 – 2147483647	When this route becomes available, deactivate the following interfaces x,y
def_route	n	deact_ent2	Blank,PPP	When this route becomes available, deactivate the following interfaces x,y
def_route	n	deact_add2	0 – 2147483647	When this route becomes available, deactivate the following interfaces x,y
def_route	n	unoos_secs	0 – 2147483647	Keep this route in service for s seconds after OOS state is cleared
def_route	n	rgroup	0 - 255	Assign this route to recovery group n

Configuration – Network > IP Routing / Forwarding > RIP

The web pages and command line commands described in this section control the configuration of the routing Information Protocol (RIP) functionality of the router.

Configuration – Network > IP Routing / Forwarding > RIP > Global RIP Settings

Enable RIP
When checked, this checkbox enables the RIP functionality.

Send RIP advertisements every s seconds
The value in this text box specifies the interval between sending RIP packets. These packets contain the current routes held by the router (e.g. any active PPP routes), static routes and the default route. A value of 0 disables sending.

Mark routes as unusable if we don't get advertisements for s seconds
The value in this text box specifies the time for which an updated metric will apply when a RIP update is received. If no updates are received within this period, the usual metric will take over.

Delete routes after another s seconds
The value in this text box specifies the length of time that the router will continue to advertise this route when a RIP update timeout occurs and the route metric is 16. This behaviour is designed to help propagate the dead route to other routers. The router will no longer use a metric advertised by a RIP update if the route has been set out of service locally.

Allow RIP to update static routes
When checked, this checkbox allows an incoming, matching RIP update to change the metric of the static route. This happens when the update matches a configured static route.

Enable Poison Reverse
When checked, this checkbox enables poison reverse, to notify when a neighbouring router is unavailable.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
rip	n	enable	on,off	Enable RIP
rip	n	interval	0 - 2147483647	Send RIP advertisement every s seconds
rip	n	ripto	0 - 2147483647	Mark routes as unusable if we don't get advertisement for s seconds
rip	n	riplingerto	0 - 2147483647	Delete routes after another s seconds
rip	n	updatestatic	on,off	Allow RIP to update static routes
rip	n	poisonreverse	on,off	Enable Poison Reverse

Configuration – Network > IP Routing / Forwarding > RIP > Global RIP settings > Access Lists

The router has the ability to modify route metrics based upon received RIP responses. Static routes and default routes will have their metric modified if the route fits within one of the routes found within the RIP packet. For Ethernet routes, the gateway for the route will be set to the source address of the RIP packet. The route modifications will be enforced for 180 seconds unless another RIP response is received within that time.

RIP packets must have a source address that is included in the RIP access list.

Adding permitted IP addresses to the access list is controlled using a table with the single parameter described below.

IP Address a.b.c.d
The value in this text box is the IP address to be added to the list of IP addresses that RIP packets must come from if they are to modify route metrics. Up to ten IP addresses may be added. The **Add** and **Delete** buttons work in the usual way for configuration tables.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
riprx	0 - 9	IPaddr	Valid IP address a.b.c.d	IP Address a.b.c.d

Configuration – Network > IP Routing / Forwarding > RIP > Global RIP settings > Authentication Keys

RIP authentication keys are used with the "plain password" and MD5 RIP authentication methods.

Configuration – Network > IP Routing / Forwarding > RIP > Global RIP settings > Authentication Keys > Authentication Key n

Key k
The value in this text box is the RIP authentication key. Enter a string of up to 16 characters long. A current key will not be displayed.

Confirm Key
Re-enter the new key into this text box to allow the router to check that the two are identical.

Key ID (MD5 only)
The value in this text box is the ID for the key. The ID is inserted into the RIP packet when using RIP v2 MD5 authentication and is used to look up the correct key for received packets. The valid range is 0 – 255.

Valid from now/dd,mm,yy
These two radio buttons select, between having the validity period for the key starting immediately of allowing a start date to be defined. The starting date is specified using a drop down list to select the start day, a drop-down list to select the start month and a text box to enter the start year. Selecting the "Disable" option from the day and "None" from the month means that this key should not be used. The year can be specified as either two or four digits (e.g. 11 or 2011).

Expires Never/dd,mm,yy
These two radio buttons select between defining the end date using the drop-down lists and text box or by setting the expiration to "Never". The key end day is selected from the first drop down list, selecting "Disable" means that the key should not be used. The end month is selected from the second drop-down list, selecting "None" means that the key should not be used. The year is entered into the text box and can be in two or four digit format.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ripauth	0 - 9	key	Up to 16 characters	Key k
ripauth	0 – 9	keyid	0 - 255	Key ID
ripauth	0 – 9	sday	0 - 31	Valid from d,m,y
ripauth	0 – 9	smon	0 - 12	Valid from d,m,y
ripauth	0 – 9	syear	0 – 65535	Valid from d,m,y
ripauth	0 – 9	eday	0 - 31	Expires d,m,y
ripauth	0 – 9	emon	0 - 12	Expires d,m,y
ripauth	0 - 9	eyear	0 – 65535	Expires d,m,y

Configuration – Network > IP Routing / Forwarding > RIP > Interfaces > Ethernet / PPP / GRE

The configuration in these three sub-menus is identical.

Send RIP advertisements on this interface
Check this box to enable rip and to reveal further configuration parameters below.

Use RIP:
Select from the values 'v1', 'v2' and 'v1 Compatible' in the dropdown list. When RIP version is set to 'V1' or 'V2', the unit will transmit RIP version 1 or 2 packets respectively (version 2 packets are sent to the "all routers" multicast address 224.0.0.9). When RIP Version is set to "V1 Compat", the unit will transmit RIP version 2 packets to the subnet broadcast address. This allows 'V1' capable routers to act upon these packets.

Send RIP advertisements as:

Broadcasts:
RIP packets are by default sent out on a broadcast basis or to a multi-cast address. Do not change this parameter unless you intend to alter this behaviour.

Multicasts (Only visible when 'v2' is selected in the 'Use RIP' option above):
This is automatically selected for sending to the default RIP v2 multicast address 224.0.0.9.

<BLANK BOX>
This parameter may be used to force RIP packets to be sent to a specified IP or multicast address. It is particularly useful if you need to route the packets via a VPN tunnel. By default Broadcasts/multicasts are selected – depending on your RIP version.

Use Authentication:
This parameter selects the authentication method for RIP packets. Selection is by clickable radio button. Only one option is enabled multiple selections are not possible.

None:
When set to "Off", the interface will send and receive packets without any authentication.

Access list:
When set to "Access List", the interface will send RIP packets without any authentication. When receiving packets, the interface will check the sender's IP address against the list entered on the ***Configuration – Network > IP Routing / Forwarding > RIP > Global RIP settings > Access Lists*** page, and if the IP address is present in the list, the packet will be allowed through.

Plain password:
When set to "Plain password (V1+V2)", the interface will use the first valid key it finds (set on the ***Configuration – Network > IP Routing / Forwarding > RIP > Global RIP settings > Authentication Keys > Authentication Key n*** pages), and use the plaintext RIP authentication method before sending the packet out. If no valid key can be found, the interface will not send any RIP packets. When receiving a RIP packet, a valid plaintext key must be present in the packet before it will be accepted. This method can be used with both RIP v1 and RIP v2.

MD5:
When set to "MD5 (V2 only)", the interface will use the first valid key it finds (set on the ***Configuration – Network > IP Routing / Forwarding > RIP > Global RIP settings > Authentication Keys > Authentication Key n*** pages), and use the MD5 authentication algorithm before sending the packet out. If no valid key can be found, the interface will not send any RIP packets. Received RIP packets must be authenticated using the MD5 authentication algorithm before they will be accepted. This method can be used with RIP v2.

Only send RIP advertisements when this interface is in service:

Select this parameter for RIP advertisements only to be sent when the interface is in the UP state in the routing table.

Use Triggered RIP on this interface:

Enable triggered RIP (RFC2091). When triggered RIP is enabled, RIP timers are disabled.

Include this interface in Rip advertisements:

Select to cause the subnet configured on this interface to not be advertised by RIP.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
tun	n	rip	0,1	Enable RIP = 1 Disable RIP = 0
tun	n	ripip	Valid IP address a.b.c.d	Unicast RIP update address
tun	n	ripauth	0-3	0 = None 1 = Access List 2 = Plain Password 3 = MD5 v2 only
tun	n	ripis	on,off	Turn on to send updates only when in service
tun	n	inrip	on,off	Include interface subnet in RIP advertisements
tun	n	triggeredrip	on,off	Enable RIP RFC2091

Configuration – Network > IP Routing / Forwarding > OSPF

Open Shortest Path First (OSPF) is an Interior Gateway Protocol (IGP) developed for IP networks based on the shortest path first or link-state algorithm.

The router uses link-state algorithms to send routing information to all nodes in a network by calculating the shortest path to each node based on a topography of the network constructed by each node. Each router sends that portion of the routing table that describes the state of its own links and the complete routing structure (network topography).

The advantage of the shortest path first algorithms is that they result in smaller, more frequent update everywhere. They converge quickly, thus preventing such problems as routing loops and Count-to-Infinity (where routers continuously increment the hop count to a particular network). This makes for a stable network.

In order to use OSPF on the router, a valid configuration file must exist in the router's filing system.

Enable OSPF
When checked, this checkbox reveals the following parameters:

OSPF Configuration Filename
The file that contains the configuration data for OSPF is selected from this drop-down list. The file should have a ".conf" extension.

Load Config file
When this button is clicked, the router attempts to load the file specified in the file selection list box into the edit window below the button. The text in the window can be edited as required.

Save Config File
When this button is clicked, the text in the edit window will be saved to the filename specified in the drop-down list above. These three controls allow an OSPF configuration file to be loaded, edited and saved.

Restart OSPF after configuration file is saved
When checked, this checkbox will cause the OSPF functions to restart once the edited configuration file has been saved.

Restart OSPF if a fatal error occurs
When checked this checkbox will cause OSPF functioning to restart after a delay of 5 seconds if a fatal error occurs.

OSPF Tracing
In common with some of the other functionality of the router, OSPF supports some debug functionality. The amount of information in the debug traces is controlled from this drop-down list. The available levels are "Off", "Low", "Med" and "High". Selecting "Off" disables debug tracing.

Ignore MTU indications
All OSPF routers must have the same Maximum Transmitted Unit (MTU) and this value is advertised in the OSPF packets. When checked, this checkbox will cause the router to ignore received packets that have a MTU that differs from that of the router itself.

Use Interface IPsec source IP
When checked, this checkbox will cause OSPF functions to use the source IP address of the interface specified in ***Configuration – Network > Interfaces > Advanced > PPP n*** **:** **Use interface x,y for the source IP address of IPsec packets** on the interface being used. When unchecked, OSPF will use the source IP address of the interface being used for its source address.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ospf	0	Enable	on,off	Enable OSPF
ospf	0	conffile		OSPF Configuration Filename
ospf	0	new_cfg_rest	on,off	Restart OSPF after a configuration file is saved
ospf	0	fatal_rest	on,off	Restart OSPF if a fatal error occurs
ospf	0	debug	0 – 3 0 = Off 1 = Low 2 = Med 3 = High	OSPF Tracing
ospf	0	ignore_mtu	on,off	Ignore MTU indications
ospf	0	useipsecent	on,off	Use Interface IPsec source IP

Configuration – Network > IP Routing / Forwarding > BGP

The Border Gateway Protocol (BGP) routing protocol is supported by TransPort routers. This page contains the configuration parameters used to control the behaviour of BGP. Most of the configuration is controlled by a configuration file (raw text) named bgp.cnf. This file would normally be created in a text editor on a computer and loaded onto the router. The router contains a simple editor that can be used to modify the file. The configuration parameters described here mainly define what action is to be taken when errors occur and specify the configuration file to be used.

Enable BGP
When checked, this checkbox enables BGP routing.

BGP Configuration Filename
The configuration file to use is selected from this drop-down list. The default filename is bgp.cnf. An error message will be displayed if the specified file cannot be found.

Load Config file
Click this button to load the file specified from the drop-down list. The contents of the file will be visible in the edit window which appears below the button.

Save Config File

If the edit functions are used to modify the file, it can be saved back to the filing system by clicking this button.

Restart BGP after configuration file is saved
When checked, this checkbox will cause the router to restart routing using BGP after the file has been saved using the above **Save** button.

Restart BGP if a fatal error occurs
When checked, this checkbox will cause the router to restart routing using BGP if a fatal error occurs.

Advertise non-connected networks
When checked, this checkbox will cause BGP to advertise networks that exist in the BGP configuration file but that are not actually a connected network or interface.

BGP Tracing
As with OSPF, the level of debug tracing information is selected from this drop-down list. The available levels are; “Off”, “Low”, “Med” and High.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
bgp	0	enable	on,off	Enable BGP
bgp	0	conffile		BGP Configuration Filename
bgp	0	new_cfg_rest	on,off	Restart BGP after configuration file is saved
bgp	0	fatal_rest	on,off	Restart BGP if a fatal error occurs
bgp	0	allow_non_nets	on,off Default ON	Advertise non-connected networks
bgp	0	debug	0 - 3	BGP Tracing

Configuration – Network > IP Routing / Forwarding > IP Port Forwarding / Static NAT Mappings

The router supports Network Address Translation (NAT) and Network Address and Port Translation (NAPT). NAT or NAPT may be enabled on a particular interface such as a PPP instance. When operating with NAT enabled, this interface has a single externally visible IP address. When sending IP packets, the local IP addresses (for example on a local area network) are replaced by the single IP address of the interface. The router keeps track of the local IP addresses and port numbers so that if a matching reply packet is received, it is directed to the correct local IP address. With only one externally visible IP address, NAT effectively prevents external computers from addressing specific local hosts, thus providing a very basic level of "firewall" security.

Static NAT mappings allow received packets destined for particular ports to be directed to specific local IP addresses. For example, to have a server, running on a local network, externally accessible, a static NAT mapping would be set up using the local IP address of the server and the port number used to access the required service.

Configuring IP port forwarding and static NAT mapping is done by entering the following configuration values into a table and using the Add button to add them into the NAT configuration for the router.

External Min Port
The value in this text box specifies the lowest port number to be redirected.

External Max Port
The value in this text box specifies the highest port number to be redirected.

Forward to Internal IP Address a.b.c.d
The value in this text box is the IP address to which packets containing the specified destination port number are to be redirected.

Forward to Internal Port
The value in this text box specifies the IP port number to which packets containing the specified port number are to be redirected. When set to "0", no port remapping occurs and the original port number is used. The NAT mode parameter of the appropriate interface must be set to "NAPT" rather than "NAT" or "OFF" for this parameter to take effect.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
nat	0 - 29	minport	0 - 65535	External Min Port
nat	0 - 29	maxport	0 - 65535	External Max Port
nat	0 - 29	IPaddr	Valid IP address a.b.c.d	Forward to Internal IP Address a.b.c.d
nat	0 - 29	mapport	0 - 65535	Forward to Internal Port

Command format:

```
Nat <entry> <parameter> <value>
```

Example commands:

To set the IP address for entry 0 in the table to 10.1.2.10 enter the command:

```
nat 0 IPaddr 10.1.2.10
```

Configuration – Network > IP Routing / Forwarding > Multicast Routes

Digi TransPort routers support multicast routes, allowing them to route packets to multicast group addresses. Up to 20 different static multicast routes may be configured.

Static multicast routes must be used in conjunction with the IGMP parameter on the outbound interface. For example, after configuring a static multicast route for multicast traffic via PPP 1, the **IGMP** parameter in ***Configuration – Network > Interfaces > IGMP*** needs setting to ON. Multicast routing is configured using a table with the following parameters:

Multicast Address a.b.c.d
The value in this text box is used in conjunction with the Mask parameter below, to specify the destination multicast group address for packets that will match this route. So, if a router receives a packet with a destination multicast group address that matches the specified Multicast Address/Mask combination, it will route that packet through the interface specified by the Interface parameters below.

Mask a.b.c.d
The value in this text box is the address mask that is used in conjunction with the Multicast Address parameter as described above.

Interface x,y
These two parameters in the drop-down list and adjacent text box specify the interface and interface instance used to route packets matching the Multicast Address/Mask combination. The options available in the drop-down list are; PPP, Ethernet, Tunnel.

Enable multicast source path checking
When checked, this checkbox

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
mcast	0 - 19	IPaddr	Valid IP address a.b.c.d	Multicast Address a.b.c.d
mcast	0 - 19	mask	Valid IP address a.b.c.d	Mask a.b.c.d
mcast	0 - 19	ll_ent	PPP,ETH,TUN	Interface x,y
mcast	0 - 19	ll_add	Valid interface number 0 - 2147483647	Interface x,y

Configuration – Network > Virtual Private Networking (VPN) > IPsec

IPsec (Internet Protocol security) refers to a group of protocols and standards that may be used to protect data during transmission over the internet (which is inherently insecure). Various levels of support for IPsec can be provided on the router depending on the model. The web pages located under the ***Configuration – Network > Virtual Private Networking (VPN) > IPsec*** are used to set the various parameters and options that are available. You should note however that this is a complex area and you should have a good understanding of user authentication and data encryption techniques before you commence. For further information refer to the “IPsec and VPNs” section in this manual. Also check the Technical Notes section of the Digi International web site at www.digi.com for the latest IPsec application notes.

The first stage in establishing a secure link between two endpoints on an IP network is for those two points to securely exchange a little information about each other. This enables the endpoint responding to the request to decide whether it wishes to enter a secure dialogue with the endpoint requesting it. To achieve this, the two endpoints commonly identify themselves and verify the identity of the other party. They must do this in a secure manner so that the process cannot be “listened in to” by any third party. The IKE protocol is used to perform this “checking” and if everything matches up it creates a Security Association (SA) between the two endpoints, normally one for data being sent TO the remote end and one for data being received FROM it.

Once this initial association exists the two devices can “talk” securely about and exchange information on what kind of security protocols they would like to use to establish a secure data link, i.e. what sort of encryption and/or authentication they can use and what sources/destinations they will accept. When this second stage is complete (and provided that both systems have agreed what they will do), IPSec will have set up its own Security Associations which it uses to test incoming and outgoing data packets for eligibility and perform security operations on before passing them down or relaying them from the “tunnel”.

Configuration – Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec n

Once the IKE parameters have been set-up, the next stage is to define the characteristics of the IPsec tunnels, or encrypted routes. This includes items such as what source and destination addresses will be connected by the tunnel and what type of encryption and authentication procedures will be applied to the packets being tunnelled. For obvious reasons it is essential that parameters such as encryption and authentication are the same at each end of the tunnel. If they are not, then the two systems will not be able to agree on what set of rules or “policy” to adopt for the IPsec tunnel and communication cannot take place.

Description
This parameter allows you to enter a name for IPsec tunnel to make it easier to identify.

The IP address or hostname of the remote unit
The IP address or hostname of the remote IPsec peer that a VPN will be initiated to.

Use a.b.c.d as a backup unit
The IP address or hostname of a backup peer. If the router cannot open a connection to the primary peer, this configuration will be used. Please note that the backup peer device must have an identical IPsec tunnel configuration as the primary peer.

Use these settings for the local LAN
These define the local LAN subnet settings used on the IPsec tunnel.

IP Address
Use this IP address for the local LAN subnet. This is usually the IP address of the router’s Ethernet interface or that of a specific device on the local subnet (such as a PC running a client or host application).

Mask
Use this IP mask for the local LAN subnet. The mask sets the range of IP addresses that will be allowed to use the IPsec tunnel.

Use interface x,y
Use the IP address and mask of the specified interface.

Use these settings for the remote LAN
These define the remote LAN subnet settings used on the IPsec tunnel.

IP Address
Use this IP address for the remote LAN subnet. This is usually the IP address of the peer’s Ethernet interface or that of a specific device on the local subnet (such as a PC running a client or host application).

Mask
Use this IP mask for the remote LAN subnet. The mask sets the range of IP addresses that will be allowed to use the IPsec tunnel.

Remote Subnet ID
Normally used with L2TP/IPsec VPNs. When the router is in server mode and negotiating IPsec from behind a NAT box, this parameter should be configured to the ID sent by the remote Windows client (this is usually the computer name).

Use the following security on this tunnel
These define the security identities used on the IPsec tunnel.

Preshared Keys	Requires that both IPsec peers share a secret key, or password, that can be matched by and verified by both peers. To configure the PSK, a user will need configuring that matches the inbound ID of the remote peer and the PSK is configured using the password parameter. This is done via ***Configuration – Security > Users***. The User configuration serves a dual purpose in that it may contain entries for normal login access (e.g. HTTP, FTP or Telnet) and entries for IPsec tunnels.
XAUTH Init Preshared Keys	Used when the remote peer is a Cisco device using XAUTH and PSK authentication.
RSA Signatures	Select this option when the IPsec authentication will use X.509 certificates.
XAUTH Init RSA	Used when the remote peer is a Cisco device using XAUTH and X.509 certificates for authentication.

Our ID
When Aggressive mode is On, this parameter is a string of up to 20 characters. It is sent to the remote peer to identify the initiator (e.g. the router). The variable **%s** can be used in this parameter which will cause the router’s serial number to be sent. It can be prefixed with other text if required.
When certificates are being used, this parameter should be configured with the “Altname” field in a valid certificate held on the router.

Our ID type

This defines how the remote peer is to process the ***Our ID*** configuration.

IKE ID	The Our ID parameter is a simple key ID (e.g. vpnclient1).
FQDN	The Our ID parameter is a Fully Qualified Domain Name (e.g. vpnclient1.anycompany.com)
User FQDN	The Our ID parameter is a Fully Qualified Domain Name with a user element (e.g. joe.bloggs@anycompany.com)
IPv4 Address	An IPv4 Address in dotted decimal notation.

Remote ID

When Aggressive mode is On, this parameter is a string of up to 20 characters which is used to identify the remote peer. It should contain the same text as the ***Our ID*** parameter in the **remote peer**'s configuration.
When Aggressive mode is Off, this parameter must be the IP address of the remote peer.

RSA Key File

This parameter can be used to override the private key filename in the IKE configuration. It is only used when RSA Signatures (Certificates) are being used for the authentication stage of the IKE negotiation.

Use enc encryption on this tunnel

The ESP encryption protocol to use with this IPsec tunnel. The options are:

- No (None)
- Null
- DES
- 3DES
- AES (128 bit keys)
- AES (192 bit keys)
- AES (256 bit keys)

If the dropdown options only display None and Null, the router will need Encryption enabling. Please speak to your sales contact with regards to getting Encryption enabled.

Use auth authentication on this tunnel

The ESP authentication algorithm to use with this IPsec tunnel. The options are:

- No (None)
- MD5
- SHA1

Use Diffie Hellman group

The Diffie Hellman (DH) group to use when negotiating new IPsec SAs. When used, the IPsec SA keys cannot be predicted from any of the previous keys generated. The options are "No PFS", 1, 2 or 3. The larger values result in "stronger" keys but they take longer to generate.

Use IKE n to negotiate this tunnel

The IKE version to use to negotiate this IPsec tunnel.

Use IKE configuration

The IKE configuration instance to use with this Eroute when the router is configured as an Initiator.

Bring this tunnel up

This controls how the IPsec tunnel is brought up. The options are:

- All the time
- Whenever a route to the destination is available
- On demand

If the tunnel is down and a packet is ready to be sent

Defines the action that is performed when the IPsec tunnel is down and a packet needs to be sent. The options are:

- Bring the tunnel up
- Drop the packet
- Send the packet without encryption and authentication

Bring this tunnel down if it is idle for h hrs m mins s secs

This parameter is used when the IPsec tunnel is configured to come up on demand and defines how long the IPsec tunnel should remain up if there is no traffic is being sent on the tunnel.

Renew the tunnel after

Defines the constraints of when the IPsec tunnel SA has to be renewed.

h hrs m mins s secs
Re-new the IPsec SA after the specified amount of time.

n units of traffic
Re-new the IPsec SA after the specified amount of traffic has been passed over the tunnel.
The units can be Kbytes, Mbytes or Gbytes.
A value of 0 means that this parameter will not be used and SAs will expire and be renewed based time, rather than amount of traffic.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
eroute	n	descr	String	Description
eroute	n	peerip	IP address or hostname	The IP address or hostname of the remote unit
eroute	n	bakpeerip	IP address or hostname	Use n as a backup unit
eroute	n	locip	IP address	IP Address (for Local LAN)
eroute	n	locmsk	IP Mask	IP Mask (for Local LAN)
eroute	n	locipifent	blank, ETH, PPP	Use interface x,y x = Interface type
eroute	n	locipifadd	Integer	Use interface x,y y = interface number

Entity	Instance	Parameter	Values	Equivalent Web Parameter
eroute	n	remip	IP address	IP Address (for Remote LAN)
eroute	n	remmsk	IP Mask	IP Mask (for Remote LAN)
eroute	n	remnetid	String	Remote Subnet ID
eroute	n	authmeth	Off, Preshared, xauthinitpre, rsa, xauthinitrsa	Use the following security on this tunnel
eroute	n	ourid	String	Our ID
eroute	n	ouridtype	0 = IKE ID 1 = FQDN 2 = User FQDN 3 = IPv4 Address	Our ID type
eroute	n	peerid	String	Remote ID
eroute	n	privkey	Filename	RSA Key File
eroute	n	espenc	off, null, des, 3des, aes	Use enc encryption on this tunnel
eroute	n	enckeybits	128, 192, 256	Use enc encryption on this tunnel
eroute	n	espauth	off, md5, sha1	Use auth authentication on this tunnel
eroute	n	dhgroup	0, 1, 2, 3	Use Diffie Hellman group
eroute	n	ikever	1, 2	Use IKE n to negotiate this tunnel
eroute	n	ikecfg	0, 1	Use IKE configuration
eroute	n	autosa	0 = On Demand 1 = When a route to the destination is available 2 = All the time	Bring this tunnel up
eroute	n	nosa	drop, pass, try	If the tunnel is down and a packet is ready to be sent
eroute	n	inact_to	Integer	Bring this tunnel down if it is idle for h hrs m mins s secs This CLI value is entered in seconds only.
eroute	n	ltime	Integer	Renew the tunnel after h hrs m mins s secs This CLI value is entered in seconds only.
eroute	n	lkbytes	Integer	Renew the tunnel after n units of traffic. This CLI value is entered in Kbytes only.

Configuration – Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec n > Tunnel Negotiation

Enable IKE tracing
This will enable the router to write IKE negotiation information in the analyser trace.

Negotiate a different IP address and Mask
The IPsec tunnel can be configured to negotiate a different local LAN IP address and mask. The firewall can then be used to translate the source addresses of the packets to a value that lies within the negotiated range. This is so that a packet can match more than one IPsec tunnel but will use a different source address (from the peer's perspective) depending on which IPsec tunnel gets used.

IP Address
The alternative IP address to negotiate.

Mask
The alternative IP mask to negotiate.

Negotiate a virtual IP address using MODECFG
Used when the remote peer is a Cisco device using MODECFG to assign a specific IP address to this router during SA setup negotiations. This is commonly seen in Remote Access (RA) type VPNs and EasyVPN solutions.

XAuth ID
Extended Authentication ID for use with Cisco XAUTH.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
eroute	n	debug	on, off	Enable IKE tracing
eroute	n	neglocip	IP Address	Negotiate a different IP address and Mask
eroute	n	neglocmsk	IP Mask	Negotiate a different IP address and Mask
eroute	n	vip	on, off	Negotiate a virtual IP address using MODECFG
eroute	n	xauthid	String	XAuth ID

Configuration – Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec n > Advanced

IPsec mode
Selects the IPsec encapsulation type to use on the IPsec tunnel. In Tunnel mode, the entire IP packet (header and payload) is encrypted. In Transport mode, only the IP payload is encrypted.

Use algorithm AH authentication on this tunnel
The AH authentication algorithm to use with this IPsec tunnel. The options are:

- No (None)
- MD5
- SHA1

Use algorithm compression on this tunnel

The compression algorithm to use with this IPsec tunnel. The options are:

- No (None)
- DEFLATE

Delete SAs when this tunnel is down
When selected, all SAs associated with the IPsec tunnel are deleted when the tunnel goes out of service.

Delete SAs when router is not a VRRP master
When selected, at least one Ethernet interface must be set as VRRP Master before the router can create SAs. If the router switches away from VRRP Master state, the SAs will be deleted. When the router switches back to VRRP Master state, the SAs will be created automatically.

Go out of service if automatic establishment fails
The router will take the IPsec tunnel out of service if the automatic establishment fails rather than continually retrying.

Go out of service after n consecutive auto-negotiation failures
The router will take the IPsec tunnel out of service if the auto-negotiation fails for the specified consecutive number of times rather than continually retrying.

This tunnel can only use apn
When enabled, this parameter allows you to choose between using the main APN or the backup APN, as defined in the ***Configuration – Network > Serial > W-WAN Port*** page.

Link tunnel with interface with x,y
When enabled, this parameter can be set so that the IPsec tunnel will only match packets using the specified interface. When this parameter is enabled, the route will take outgoing packets going through this IPsec tunnel and recheck to see if the resultant packet also goes through a tunnel.
If the inner tunnel is an IPsec tunnel (i.e. needs IKE), you can get the inner IKE to use the correct source address (matching the outer tunnel selectors) by enabling the **Use secondary IP address** parameter and the inner IKE will use the IP address configured in the **Secondary IP address** parameter on the ***Configuration – Network > Advanced Network Settings*** page.

Inhibit this IPsec tunnel when IPsec tunnels n are up
This is a list of IPsec tunnels that can inhibit this IPsec tunnel from being used as long as they are up. If this IPsec tunnel has been allowed to come up, and the IPsec tunnel that inhibits it comes back up, this IPsec is taken down and any SAs that may have existed are removed. As soon as an inhibiting IPsec tunnel goes down, the router will check to see if the inhibited IPsec tunnel can now create SAs.

Inhibit this IPsec tunnel unless IPsec tunnel n is up
This IPsec tunnel will be inhibited unless specified IPsec tunnel is also up.

IKE negotiation source IP address is taken from the
This defines which IP address IKE uses as the source IP address during the negotiation.

Interface
Use the IP address of the interface over which the IKE packets will be transmitted.

Secondary IP address
Use the IP address configured in the **Secondary IP address** parameter on the ***Configuration – Network > Advanced Network Settings*** page.

Interface x,y
Use the IP address of the specified interface.

Tunnel this IPsec tunnel inside another IPsec tunnel
It is possible to tunnel packets from an IPsec tunnel within a second (or more) tunnel. When this parameter is enabled.

NAT-Traversal Keepalive timer s seconds
Sets the interval period, in seconds, that the router will use to send regular packets to a NAT device in order to prevent the NAT table entry from expiring.

Allow protocol IP protocol(s) in this tunnel
This restricts the type of IP packets that will be tunnelled through the IPsec tunnel. The options are:

- All
- TCP
- UDP
- GRE

IP packets with ToS values n must use this tunnel
Packets with matching ToS fields will only be tunnelled through this IPsec tunnel and no others. The usual traffic selector matching still takes place as normal. Packets that don't have matching ToS values will get tunnelled as normal.
The ToS values should be entered as a comma separated list. E.g. 2,4

Only tunnel IP packets with
This restricts the IP packets that will be tunnelled to those with matching TCP/UDP port numbers.

local TCP/UDP port n
Allow IP packets with matching source TCP/UDP ports to be tunnelled.

remote TCP/UDP port n
Allow IP packets with matching destination TCP/UDP ports to be tunnelled.

local TCP/UDP port in the range of n1 to n2
Allow IP packets with source TCP/UDP ports in the specified range to be tunnelled. This is only available when IKEv2 is used

remote TCP/UDP port in the range of n1 to n2
Allow IP packets with destination TCP/UDP ports in the specified range to be tunnelled. This is only available when IKEv2 is used

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
eroute	n	mode	tunnel, transport	IPsec Mode
eroute	n	ahauth	off, md5, sha1	Use a AH authentication on this tunnel
eroute	n	ipcompalg	off, deflate	Use c compression on this tunnel
eroute	n	oosdelsa	on, off	Delete SAs when this tunnel is down
eroute	n	ifvrrpmaster	on, off	Delete SAs when router is not a VRRP master
eroute	n	nosaoos	on, off	Go out of service if automatic establishment fails
eroute	n	nosadeactcnt	Integer	Go out of service after n consecutive auto-negotiation failures
eroute	n	check_apnbu	on, off	This tunnel can only use apn
eroute	n	apnbu	0 = Main APN 1 = Backup APN	This tunnel can only use apn
eroute	n	ifent	blank, ETH, PPP	Link tunnel with interface with x,y x = Interface type
eroute	n	ifadd	Integer	Link tunnel with interface with x,y y = Interface number
eroute	n	inhibitno	Comma separated list of Integers	Inhibit this IPsec tunnel when IPsec tunnels n are up
eroute	n	requireno	Integer	Inhibit this IPsec tunnel unless IPsec tunnel n is up
eroute	n	usesecip	on, off	IKE negotiation source IP address is taken from the Secondary IP Address
eroute	n	ipent	blank, ETH, PPP	IKE negotiation source IP address is taken from the Interface x,y x = Interface type
eroute	n	ipadd	Integer	IKE negotiation source IP address is taken from the Interface x,y y = Interface number
eroute	n	intunnel	on, off	Tunnel this IPsec tunnel inside another IPsec tunnel
eroute	n	natkaint	Integer	NAT-Traversal Keepalive timer s seconds
eroute	n	proto	off, tcp, udp, gre	Allow protocol IP protocol(s) in this tunnel
eroute	n	toslist	Comma separated list of Integers	IP packets with ToS values n must use this tunnel
eroute	n	locport	0 - 65535	Only tunnel IP packets with local TCP/UDP port
eroute	n	remport	0 - 65535	Only tunnel IP packets with remote TCP/UDP port
eroute	n	locfirstport	0 - 65535	Only tunnel IP packets with local TCP/UDP port in the range of n1 to n2
eroute	n	loclastport	0 - 65535	Only tunnel IP packets with local TCP/UDP port in the range of n1 to n2
eroute	n	remfirstport	0 - 65535	Only tunnel IP packets with remote TCP/UDP port in the range of n1 to n2
eroute	n	remlastport	0 - 65535	Only tunnel IP packets with remote TCP/UDP port in the range of n1 to n2

Setting up IPsec Tunnels for Multiple Users

For small numbers of users it is usual to set up an individual eroute for each user. However, to ease configuration where large numbers of users are required, the "*" character can be used as a wildcard to match multiple user IDs. For example, setting the **Peer ID** parameter to "Digi*" would match all remote units having an **Our ID** parameter starting with "Digi", e.g. Digi01, Digi02, etc.

Example

To setup multiple users in this way, first set up the **Our ID** parameter on the host unit to a suitable name, e.g. "Host1". Then set the **Peer ID** parameter to "Remote*" for example. In addition, an entry would be made in the user table with "Remote*" for the **Username** and a suitable **Password** value, e.g. "mysecret".

Each of the remote units that required access to the host would then have to be configured with an **Our ID** parameter of "Remote01", "Remote02", etc. and each would have to have an entry in their user table for User Host1 along with its password (i.e. the pre-shared key).

Host Router

Peer ID:	Remote*
Our ID:	Host1
Username:	Remote*
Password:	mysecret

Remote Router 1

Peer ID:	Host1
Our ID:	Remote01
Username:	Host1
Password:	mysecret

Remote Router 2

Peer ID:	Host1
Our ID:	Remote02
Username:	Host1
Password:	mysecret

Remote Router 3

Peer ID:	Host1
Our ID:	Remote03
Username:	Host1
Password:	mysecret

Configuration – Network > Virtual Private Networking (VPN) > IPsec > IPsec Default Action

Like a normal IP routing set-up, IPSec Tunnels have a default configuration that is applied if no specific tunnel can be found. This is useful when, for instance, you wish to have a number of remote users connect via a secure channel (perhaps to access company financial information) but also still allow general remote access to other specific servers on your network or the Internet.

When a packet is received which does not match any IPsec tunnel
How the router will respond if a packet is received when there is no SA.
If “Drop the packet” is selected then only packets that match a specified IPsec tunnel will be routed, all other data will be discarded. This has the effect of enforcing a secure connection to all devices behind the router.
If “Pass the packet” is selected then packets that match an IPsec tunnel will be decrypted and authenticated (depending on the IPsec tunnel’s configuration) but data that does not match will also be allowed to pass.

When a packet is to be transmitted which does not match any IPsec tunnel
How the router will respond if a packet is transmitted when there is no SA.
If “Drop the packet” is selected then only packets that match a specified IPsec tunnel will be routed, all other data will be discarded.
If “Pass the packet” is selected then data that matches an IPsec tunnel will be encrypted and authenticated (depending on the IPsec tunnel configuration) but data that does not match will also be allowed to pass.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
def_eroute	0	nosain	drop, pass	When a packet is received which does not match any IPsec tunnel
def_eroute	0	nosaout	drop, pass	When a packet is to be transmitted which does not match any IPsec tunnel

Configuration – Network > Virtual Private Networking (VPN) > IPsec > IPsec Groups

This mode of operation can be used when the router is terminating tunnels to a large number of remote devices e.g. when being used as a VPN Concentrator. To keep the size of the configuration file in the router small and also to maintain ease of configuration, only the information that is used for all tunnels is stored on the router. All other information that is site specific is stored in a MySQL database. This means the number of sites that can be configured is limited only by the SQL database size and performance. This will be literally millions of sites depending upon the operating system and hardware of the MySQL PC. The number of sites that can be connected to concurrently are much smaller and limited by the model of the router.

Basic Concept

The router with the IPsec Group/MySQL configuration will be the VPN Concentrator. The remote sites will normally not require an IPsec group configuration as they will normally only need to connect to a single peer, the VPN Concentrator. The VPN Concentrator will normally need only a single IPsec group configured. The local and remote subnet parameters need to be set up wide enough to encompass all the local and remote networks. The VPN Concentrator can act as an initiator and/or a responder. In situations where there are more remote sites than the Digi can support concurrent sessions, it will normally be necessary for the VPN Concentrator and the remote sites to be both an initiator and a responder. This is so that both the remote sites and the head-end can initiate the IPsec session when required. Note that it is also important to configure the IPsec tunnels to time out on inactivity to free up sessions for other sites. In the case of the VPN Concentrator acting as an initiator, when it receives a packet that matches the main IPsec tunnel, if no Security Associations already exist it will look up the required parameters in the database. The TransPort will then create a "Dynamic IP Tunnel" containing all the settings from the base IPsec tunnel and all the information retrieved from the database. At this point IKE will create the tunnel (IPsec security associations) as normal. The dynamic IPsec tunnel will continue to exist until all the IPsec Security Associations have been removed. At the point where the maximum supported (or licensed) number of tunnels has been reached by the router, the oldest Dynamic IPsec tunnels (those that have not been used for the longest period of time) and their associated IPsec Security Associations will be dropped to allow new inbound VPNs to connect.

Logic flow - creation of IPSec SAs

VPN Concentrator acting as initiator

The VPN Concentrator will normally act as an initiator when it receives an IP packet for routing with a source address matching the IPsec tunnel local subnet address & mask and a destination address matching the remote subnet address & mask (providing that an IPsec SA does not already exist for this site.)

If an IPsec group is configured to use the matching IPsec tunnel, the router will use a MySQL query to obtain the site specific information in order to create the SA's. The VPN Concentrator will create a SELECT query using the destination IP address of the packet and the mask configured in the IPsec group configuration to determine the remote subnet address. (This means that the remote subnet mask must be the same on all sites using the current IPsec group.) Once the site specific information has been retrieved, the router creates a 'dynamic' IPsec Tunnel which is based upon the base IPSec tunnel configuration plus the site specific information from the MySQL database. The router can then use the completed IPsec tunnel configuration and IKE to create the IPsec SAs. For the pre-shared key, IKE will use the password returned from the MySQL database rather than doing a local look up in the user configuration. Once created, the SAs are linked with the dynamic IPsec tunnel. Replacement SAs are created as the lifetimes start to get low and traffic is still flowing. When all SAs to this remote router are removed, the dynamic IPsec tunnel will also be removed so that IPsec tunnel can then be re-used to create tunnels to other remote sites. When processing outgoing packets, dynamic IPsec Tunnels are searched before base IPsec tunnels. So, if a matching dynamic IPsec tunnel is found, it is used, and the base IPsec tunnel is only matched if no dynamic IPsec tunnel exists. Once the dynamic IPsec tunnel is removed, further outgoing packets will match the base IPsec tunnel and the process is repeated.

VPN Concentrator acting as a responder to a session initiated from the remote site

When a remote site needs to create an IPsec SA with the VPN Concentrator it will send an IKE request to the VPN Concentrator. The VPN Concentrator needs to be able to confirm that the remote device is authorised to create an IPsec tunnel. The remote site will supply its ID to the host during the IKE negotiations. The VPN Concentrator will use this ID and look through the IPsec tunnels configured and dynamic IPsec tunnels to see if the supplied ID matches the configured Peer ID (peerid). If a match is found, the MYSQL database is queried to retrieve the information required to complete the negotiation (e.g. pre-shared key/password). If no matching base IPsec tunnel is found, the local user configuration is used to locate the password, and a normally configured IPsec tunnel must also exist. Once the information is retrieved from the MySQL database, IKE negotiations continue and the created IPsec SAs will be associated with the dynamic IPsec tunnel. As long as the dynamic IPsec tunnel exists, it behaves just like a normal IPsec tunnel. i.e. SAs are replaced/removed as required.

If errors are received from the MySQL database, or not enough fields are returned, the dynamic IPsec tunnel is removed, and IKE negotiations in progress will be terminated. There are a limited number of dynamic IPsec tunnel. If the number of free dynamic IPsec tunnel is less than 10% of the total number of dynamic IPsec tunnel, the Digi router will periodically remove the oldest dynamic IPsec tunnel. This is done to ensure that there will always be some free dynamic IPsec tunnel available for incoming connections from remote routers. It is possible to view the current dynamic tunnels that exist using the WEB server, browse to ***Management - Connections > Virtual Private Networking (VPN) > IPsec***. The table will indicate the base IPsec tunnel and the Remote Peer ID in the status display to help identify which remote sites are currently connected.

Preliminary IP Tunnel configuration

The IPsec tunnel configuration ***Configuration – Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec n*** differs from a normal configuration in the following ways:

- Peer IP/hostname: Because the peer IP address to each peer is unknown and is retrieved from the database, this field is left empty.
- Bakpeerip (CLI only): Because the peer IP address to each peer is unknown and is retrieved from the database, this field is left empty.
- Peer ID: When the host Digi is acting as a responder during IKE negotiations, the router uses the ID supplied by the remote to decide whether or not the MySQL database should be interrogated. So that the Digi can make this decision, the remote router must supply an ID that matches the peerid configured into the IPsec tunnel. Wildcard matching is supported which means that the peerid may contain '*' and '?' characters. If only one IPsec tunnel is configured, the peerid field may contain a '*', indicating that all remote IDs result in a MySQL look up.
- Local subnet IP address / Local subnet mask: Configured as usual.
- Remote subnet IP address / Remote subnet mask: These fields should be configured in such a way that packets to ALL remote sites fall within the configured subnet. e.g. if there are two sites with remote subnets 192.168.0.0/24, and 192.168.1.0/24 respectively, a valid configuration for the host would be 192.168.0.0/23 so that packets to both remote sites match.

All other fields should be configured as usual. It is possible to set up other IPsec groups linked with other IPsec tunnels. This would be done if there is a second group of remote sites that have a different set of local and remote subnets, or perhaps different encryption requirements. The only real requirement is that this second group uses peer IDs that do not match up with those in use by the first IPsec group.

IPsec Group configuration

This configuration holds information relating to the MySQL database, and the names of the fields where the information is held. This configuration is also used to identify which IPsec tunnels are used to create dynamic IPsec tunnels.

Example MySQL schema

```
mysql> describe eroutes;
    +-----------+-------------+------+-----+---------+-------+
    | Field     | Type        | Null | Key | Default | Extra |
    +-----------+-------------+------+-----+---------+-------+
    | peerip    | varchar(20) | YES  |     | NULL    |       |
    | bakpeerip | varchar(20) | YES  |     | NULL    |       |
    | peerid    | varchar(20) | NO   | PRI |         |       |
    | password  | varchar(20) | YES  |     | NULL    |       |
    | ourid     | varchar(20) | YES  |     | NULL    |       |
    | remip     | varchar(20) | YES  | UNI | NULL    |       |
    | remmsk    | varchar(20) | YES  |     | NULL    |       |
    +-----------+-------------+------+-----+---------+-------+
    7 rows in set (0.01 sec)
```

Link this IPsec group with IPsec Tunnel
The base IPsec tunnel number. This parameter allows the router to see that an IPsec tunnel should use the group configuration to retrieve dynamic information from the database.

Remote mask to use for tunnels
This parameter is used in the SQL SELECT query in conjunction with the destination IP address of packets to be tunnelled from the host to the remote peer to identify the correct record to select from the MySQL database.

MySQL Server IP Address or Hostname
The IP address or hostname of the MySQL Server.

MySQL Server Port
The port that the MySQL Server is listening on.

Username
The username to use when logging into the MySQL Server.

Password / Confirm Password
The password to use when logging into the MySQL Server.

Database name
The name of the database to connect to.

Database table
The name of the table when the remote site information is stored.

Remote subnet IP
The name of the field in the table where the ‘remip’ data is stored.

Remote subnet Mask
The name of the field in the table where the ‘remmsk’ data is stored.

Peer IP Address
The name of the field in the table where the ‘peerip’ data is stored.

Backup Peer IP Address
The name of the field in the table where the ‘bakpeerip” data is stored.

Peer ID
The name of the field in the table where the ‘peerid’ data is stored.

Our ID
The name of the field in the table where the ‘ourid’ data is stored.

Password
The name of the field in the table where the password to use in IKE negotiations is stored.

> **Note:**
> The default MySQL field names match the matching IPsec tunnel configuration parameter name. The default field name for the ‘password’ field is ‘password’.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
egroup	n	eroute	Integer	Link this IPsec group with IPsec Tunnel
egroup	n	remmsk	IP Mask	Remote mask to use for tunnels
egroup	n	dbhost	IP Address or Hostname	MySQL Server IP Address or Hostname
egroup	n	dbport	0 - 65535	MySQL Server Port
egroup	n	dbuser	String	Username
egroup	n	dbpwd	String	Password / Confirm Password
egroup	n	dbname	String	Database name
egroup	n	dbtable	String	Database table
egroup	n	fremip	String	Remote subnet IP
egroup	n	fremmsk	String	Remote subnet Mask
egroup	n	fpeerip	String	Peer IP Address

Entity	Instance	Parameter	Values	Equivalent Web Parameter
egroup	n	fbakpeerip	IP Address	Backup Peer IP Address
egroup	n	fpeerid	String	Peer ID
egroup	n	fourid	String	Our ID
egroup	n	fpwd	String	Password

Configuration – Network > Virtual Private Networking (VPN) > IPsec > Dead Peer Detection

When Dead Peer Detection (DPD) is enabled on an IPsec tunnel, the router will send an IKE DPD request at regular intervals. If no response is received to the DPD request, the IPsec tunnel is considered as suspect and the requests are sent at a shorter interval until either the maximum number of outstanding requests allowed is reached or a response is received. If no response is received to the configured maximum requests, the IPSec tunnels are closed.

Note:
IKE DPD requests require that an IKE SA is present. If one is not present, the DPD request will fail.

To help ensure that an IKE SA exists with a lifetime at least as great as the IPsec lifetime, the router creates new IKE SAs whenever the IPsec SA lifetime exceeds the lifetime of an existing IKE SA and attempts to negotiate a lifetime for the IKE SA that is 60 seconds longer than the desired lifetime of the IPsec SA.

Mark the IPsec tunnel as suspect if there is no traffic for n seconds
The period of time of inactivity on a tunnel before it is deemed to be suspect, i.e. if there is no activity on a healthy link for the time period defined, then the tunnel is them deemed to be suspect.

Send a DPD request on a healthy link every n seconds
The interval at which DPD requests are sent on an IPsec tunnel that is deemed to be healthy. A healthy link is one with traffic.

Send a DPD request on a suspect link every n seconds
The interval at which DPD requests are sent on an IPsec tunnel that is deemed to be suspect. A suspect link is one where there has been no traffic for a specified period of time.

Close the IPsec tunnels after no response for n DPD requests
The maximum number of DPD requests that will be sent without receiving a response before the IPsec tunnels are closed.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
dpd	0	inact	Integer	Mark the IPsec tunnel as suspect if there is no traffic for n seconds
dpd	0	okint	Integer	Send a DPD request on a healthy link every n seconds
dpd	0	failint	Integer	Send a DPD request on a suspect link every n seconds
dpd	0	maxfail	Integer	Close the IPsec tunnels after no response for n DPD requests

Configuration – Network > Virtual Private Networking (VPN) > IPsec > IKE

The ***Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKE*** folder opens to list configuration pages for ***IKE 0*** and ***IKE 1*** with a separate page for ***IKE Responder***. The IKE 0 instance can be used as an IKE "initiator" or as an IKE "responder" whereas IKE 1 can only be used as an initiator. The ***IKE 0*** and ***IKE 1*** pages are therefore used to set up the IKE 0 and IKE 1 initiator parameters as required. The ***IKE Responder*** page is used to set up the responder parameters for IKE 0.

Configuration – Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE Debug

Enable IKE Debug
Enables IKE debugging to be displayed on the debug port.

Debug Level
Sets the level of IKE debugging. The options are:

- Low
- Medium
- High
- Very High

Debug IP Address Filter
This parameter is used to filter out IKE packets with particular source or destination IP addresses. The format of this parameter is a comma-separated list of IP addresses. For example, you may wish to exclude the capture of IKE traffic from IP hosts 10.1.2.3 and 10.2.2.2. This can be done by entering "10.1.2.3,10.2.2.2" for this parameter. Conversely, you may wish to only capture traffic to and from particular IP hosts. To do this, use a tilde (~) symbol before the list of IP addresses. For example, to only capture packets to and from IP host 192.168.47.1, enter "~192.168.47.1" for this parameter.

Forward debug to port
When enabled, the IKE debug is sent to debug serial port.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ike	0	deblevel	0 = Off 1 = Low 2 = Medium 3 = High 4 = Very High	Debug Level
ike	0	ipaddfilt	Comma separated list of IP addresses	Debug IP Address Filter
ike	0	debug	on, off	Forward debug to port

Configuration – Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE n

Use the following settings for negotiation
Defines the settings used during the IKE negotiation

Encryption
Defines the encryption algorithm used. The options are:

- None
- DES
- 3DES
- AES (128 bit keys)
- AES (192 bit keys)
- AES (256 bit keys)

Authentication
Defines the authentication algorithm used. The options are:

- None
- MD5
- SHA1

Mode
Defines the negotiation mode. The options are:

- Main
- Aggressive

Historically, fixed IP addresses have been used in setting up IPSec tunnels. Today it is more common, particularly with Internet ISPs, to dynamically allocate the user a temporary IP address as part of the process of connecting to the Internet. In this case, the source IP address of the party trying to initiate the tunnel is variable and cannot be pre-configured.
In Main mode (i.e. non-aggressive), the source IP address must be known i.e. this mode can only be used over the Internet if the ISP provides a fixed IP address to the user or you are using X.509 certificates.

Aggressive mode was developed to allow the host to identify a remote unit (initiator) from an ID string rather than from its IP address. This means that it can be used over the Internet via an ISP that dynamically allocates IP addresses. It also has two other noticeable differences from main mode. Firstly, it uses fewer messages to complete the phase 1 exchange (3 compared to 5) and so will execute a little more quickly, particularly on networks with large turn-around delays such as GPRS. Secondly, as more information is sent unencrypted during the exchange, it is potentially less secure than a normal mode exchange.

> **Note:**
> Main mode can be used without knowing the remote unit's IP address when using certificates. This is because the ID of the remote unit (it's public key) can be retrieved from the certificate file.

MODP Group for Phase 1
Sets the key length used in the IKE Diffie-Hellman exchange to768 bits (group 1) or 1024 bits (group 2). Normally this option is set to group 1 and this is sufficient for normal use. For particularly sensitive applications, you can improve security by selecting group 2 to enable a 1024 bit key length. Note however that this will slow down the process of generating the phase 1 session keys (typically from 1-2 seconds for group 1), to 4-5 seconds.

MODP Group for Phase 2
Sets the minimum width of the numeric field used in the calculations for phase 2 of the security exchange.
With "No PFS" (Perfect Forwarding Security) selected, the data transferred during phase 1 can be reused to generate the keys for the phase 2 SAs (hence speeding up connections). However, in doing this it is possible (though very unlikely), that if the phase 1 keys were compromised (i.e. discovered by a third party), the phase 2 keys might be more easily compromised.
Enabling group 1 (768) or 2 (1024) or 3 (1536), IPSec MODP forces the key calculation for phase 2 to use new data that has no relationship to the phase 1 data and initiates a second Diffie-Hellman exchange. This provides an even greater level of security but of course can take longer to complete.

Renegotiate after h hrs m mins s secs
Determines how long the initial IKE Security Association will stay in force. When it expires any attempt to send packets to the remote system will result in IKE attempting to establish a new SA.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ike	n	encalg	des, 3des, aes	Encryption
ike	n	keybits	0, 128, 192, 256	Encryption (AES Key length)
ike	n	authalg	md5, sha1	Authentication
ike	n	aggressive	on, off	Mode
ike	n	ikegroup	1, 2, 5	MODP Group for Phase 1
ike	n	ipsecgroup	1, 2, 5	MODP Group for Phase 2
ike	n	ltime	1 - 28800	Renegotiate after h hrs m mins s secs This CLI value is entered in seconds only.

Configuration – Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE n > Advanced

Retransmit a frame if no response after n seconds
The amount of time in seconds that IKE will wait for a response from the remote unit before transmitting the negotiation frame.

Stop IKE negotiation after n retransmissions
The maximum number of times that IKE will retransmit a negotiation frame as part of the exchange before failing.

Stop IKE negotiation if no packet received for n seconds
The period of time in seconds after which the unit will stop the IKE negotiation when no response to a negotiation packet has been received.

Enable Dead Peer Detection
Enables Dead Peer Detection. For more information, refer to the ***Configuration – Network > IPsec > Dead Peer Detection (DPD)*** page.

Enable NAT-Traversal
Enables support for NAT Traversal within IKE/IPsec. When one end of an IPsec tunnel is behind a NAT box, some form of NAT traversal may be required before the IPsec tunnel can pass packets. Turning NAT Traversal on enables the IKE protocol to discover whether or not one or both ends of a tunnel is behind a NAT box, and implements a standard NAT traversal protocol if NAT is not being performed.
The version of NAT traversal supported is that described in the IETF draft 'draft-ietf-ipsec-nat-t-ike-03.txt'.

Send INITIAL-CONTACT notifications
Enables INITIAL-CONTACT notifications to be sent.

Retain phase 1 SA after failed phase 2 negotiation
Normally IKE functionality is to remove the phase 1 SA if the phase 2 negotiation fails. Enabling this parameter will cause the router to retain the existing phase 1 SA and retry the phase 2 again.

RSA private key file
The name of a X.509 certificate file holding the router's private part of the public/private key pair used in certificate exchanges. See 'X.509 Certificates' in the 'IPsec and VPNs' section for further explanation.

SA Removal Mode
Determines how IPsec and IKE SAs are removed.
'Normal' operation will not delete the IKE SA when all the IPsec SAs that were created by it are removed and will not remove IPsec SAs when the IKE SA that was used to create them is deleted.
'Remove IKE SA when last IPSec SA removed' will delete the IKE SA when all the IPsec SAs that it created to a particular peer are removed.
'Remove IPSec SAs when IKE SA removed' will delete all IPSec SAs that have been created by the IKE SA that has been removed.
'Both' will remove IPSec SAs when their IKE SA is deleted, and delete IKE SAs when their IPSec SAs are removed.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ike	n	retranint	0 - 255	Retransmit a frame if no response after n seconds
ike	n	retran	0 - 9	Stop IKE negotiation after n retransmissions
ike	n	inactto	0 - 255	Stop IKE negotiation if no packet received for n seconds
ike	n	dpd	on, off	Enable Dead Peer Detection
ike	n	natt	on, off	Enable NAT-Traversal
ike	n	initialcontact	on, off	Send INITIAL-CONTACT notifications
ike	n	keepph1	on, off	Retain phase 1 SA after failed phase 2 negotiation
ike	n	privrsakey	Filename	RSA private key file
ike	n	delmode	0 = Normal 1 = Remove IKE SA when last IPsec SA removed 2 = Remove IPsec SAs when IKE SA remove 3 = Both	SA Removal Mode
ike	n	openswan	on, off	None. This enables support for Openswan IKE implementations.

Configuration – Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE Responder

This page displays the various parameters for IKE 0 when used in Responder mode.

Enable IKE Responder
Allows the router to respond to incoming IKE requests.

Accept IKE Requests with
Defines the settings that the router will accept during the negotiation

Encryption
The acceptable encryption algorithms.

Authentication
The acceptable authentication algorithms.

MODP Group between x and y
The acceptable range for MODP group.

Renegotiate after h hrs m mins s secs
Determines how long the initial IKE Security Association will stay in force. When it expires any attempt to send packets to the remote system will result in IKE attempting to establish a new SA.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ike	0	noresp	on, off	Enable IKE Responder
ike	0	rencalgs	des, 3des, aes Multiple algorithms can specified in a comma separated list	Encryption
ike	0	keybits	0, 128, 192, 256	Encryption (Minimum AES Key length)
ike	0	rauthalgs	md5, sha1 Multiple algorithms can specified in a comma separated list	Authentication
ike	0	rdhmingroup	1, 2, 5	MODP Group between x and y
ike	0	rdhmaxgroup	1, 2, 5	MODP Group between x and y
ike	0	ltime	1 - 28800	Renegotiate after h hrs m mins s secs This CLI value is entered in seconds only.

Configuration – Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE Responder > Advanced

Stop IKE negotiation if no packet received for n seconds
The period of time in seconds after which the unit will stop the IKE negotiation when no response to a negotiation packet has been received.

Enable NAT-Traversal
Enables support for NAT Traversal within IKE/IPsec. When one end of an IPsec tunnel is behind a NAT box, some form of NAT traversal may be required before the IPsec tunnel can pass packets. Turning NAT Traversal on enables the IKE protocol to discover whether or not one or both ends of a tunnel is behind a NAT box, and implements a standard NAT traversal protocol if NAT is not being performed.
The version of NAT traversal supported is that described in the IETF draft 'draft-ietf-ipsec-nat-t-ike-03.txt'.

Send INITIAL-CONTACT notifications
Enables INITIAL-CONTACT notifications to be sent.

Send RESPONDER-LIFETIME notifications
Enables RESPONDER-LIFETIME notifications sent to the initiator. If an initiator requests an IKE lifetime that is greater than the responder, a notification will be sent and the initiator should reduce its lifetime value accordingly.

Retain phase 1 SA after failed phase 2 negotiation
The name of a X.509 certificate file holding the router's private part of the public/private key pair used in certificate exchanges. See 'X.509 Certificates' in the 'IPsec and VPNs' section for further explanation.

RSA private key file
The name of a X.509 certificate file holding the router's private part of the public/private key pair used in certificate exchanges. See 'X.509 Certificates' in the 'IPsec and VPNs' section for further explanation.

SA Removal Mode
Determines how IPsec and IKE SAs are removed.
'Normal' operation will not delete the IKE SA when all the IPsec SAs that were created by it are removed and will not remove IPsec SAs when the IKE SA that was used to create them is deleted.
'Remove IKE SA when last IPSec SA removed' will delete the IKE SA when all the IPsec SAs that it created to a particular peer are removed.
'Remove IPSec SAs when IKE SA removed' will delete all IPSec SAs that have been created by the IKE SA that has been removed.
'Both' will remove IPSec SAs when their IKE SA is deleted, and delete IKE SAs when their IPSec SAs are removed.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ike	0	inactto	0 – 255	Stop IKE negotiation if no packet received for n seconds
ike	0	natt	on, off	Enable NAT-Traversal
ike	0	initialcontact	on, off	Send INITIAL-CONTACT notifications
ike	0	respltime	on, off	Send RESPONDER-LIFETIME notifications
ike	0	keepph1	on, off	Retain phase 1 SA after failed phase 2 negotiation
ike	0	privrsakey	Filename	RSA private key file
ike	0	delmode	0 = Normal 1 = Remove IKE SA when last IPsec SA removed 2 = Remove IPsec SAs when IKE SA remove 3 = Both	SA Removal Mode

Configuration – Network > Virtual Private Networking (VPN) > IPsec > IKE > MODECFG Static NAT mappings

MODECFG is an extra stage built into IKE negotiations that fits between IKE phase 1 and IKE phase 2, and is used to perform operations such as extended authentication (XAUTH) and requesting an IP address from the host. This IP address becomes the source address to use when sending packets through the tunnel from the remote to the host. This mode of operation (receiving one IP address from the remote host) is called "client" mode. Another mode, called "network" mode, allows the unit to send packets with a range of source addresses through the tunnel.

If the unit receives packets from a local interface that need to be routed through the tunnel, it performs address translation so that the source address matches the assigned IP address before encrypting using the negotiated SA. Some state information is retained so that packets coming in the opposite direction with matching addresses/ports can have their destination address set to the source address of the original packet (in the same way as standard NAT).

If the remote end of the tunnel is to be able to access units connected to the local interface, the unit that has been assigned the virtual IP address needs to have some static NAT entries set up. When a packet is received through the tunnel, the unit will first look up existing NAT entries, followed by static NAT entries to see if the destination address/port should be modified, and forwards the packet to the new address. If a static NAT mapping is found, the unit creates a dynamic NAT entry that will be used for the duration of the connection. If no dynamic or stateful entry is found, the packet is directed to the local protocol handlers.

External Port
The lowest destination port number to be matched if the packet is to be redirected.

Forward to Internal IP Address
An IP address to which packets containing the specified destination port number are to be redirected.

Forward to Internal Port
A port number to which packets containing the specified destination port number are to be redirected.

Port Range Count
The number of ports to be matched.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
tunsnat	n	minport	0 - 65535	External Port
tunsnat	n	maxport	0 – 65535	Port Range Count
tunsnat	n	ipaddr	IP Address	Forward to Internal IP Address
tunsnat	n	mapport	0 - 65535	Forward to Internal Port

Configuration – Network > Virtual Private Networking (VPN) > IPsec > IKEv2

When IKE Version 2 is supported, it is possible to specify whether the IKEv1 or IKEv2 protocol should be used to negotiate IKE SAs. By default, IKEv1 is used and routers which have been upgraded to support IKEv2 will not require any changes to their configuration to continue working with IKEv1.

Configuration – Network > Virtual Private Networking (VPN) > IPsec > IKEv2 > IKEv2 n

Use the following settings for negotiation
Defines the settings used during the IKEv2 negotiation

Encryption
Defines the encryption algorithm used. The options are:

- None
- DES
- 3DES
- AES (128 bit keys)
- AES (192 bit keys)
- AES (256 bit keys)

Authentication
Defines the authentication algorithm used. The options are:

- None
- MD5
- SHA1

PRF Algorithm
Defines the PRF (Pseudo Random Function) algorithm used. The options are:

- MD5
- SHA1

MODP Group for Phase 1
Sets the key length used in the IKE Diffie-Hellman exchange to768 bits (group 1) or 1024 bits (group 2). Normally this option is set to group 1 and this is sufficient for normal use. For particularly sensitive applications, you can improve security by selecting group 2 to enable a 1024 bit key length. Note however that this will slow down the process of generating the phase 1 session keys (typically from 1-2 seconds for group 1), to 4-5 seconds.

Renegotiate after h hrs m mins s secs
Determines how long the initial IKEv2 Security Association will stay in force. When it expires any attempt to send packets to the remote system will result in IKE attempting to establish a new SA.

Rekey after h hrs m mins s secs
When the time left until expiry for this SA reaches the value specified by this parameter, the IKEv2 SA will be renegotiated, i.e. a new IKEv2 SA is negotiated and the old SA is removed. Any IPSec "child" SAs that were created are retained and become "children" of the new SA.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ike2	n	iencalg	des, 3des, aes	Encryption
ike2	n	ienkeybits	128, 192, 256	Encryption (AES Key length)
ike2	n	iauthalg	md5, sha1	Authentication
ike2	n	iprfalg	md5, sha1	PRF Algorithm
ike2	n	idhgroup	1, 2, 5	MODP Group for Phase 1
ike2	n	ltime	1 - 28800	Renegotiate after h hrs m mins s secs This CLI value is entered in seconds only.
ike2	n	rekeyltime	1 - 28800	Rekey after h hrs m mins s secs This CLI value is entered in seconds only.

Configuration – Network > Virtual Private Networking (VPN) > IPsec > IKEv2 > IKEv2 n > Advanced

Retransmit a frame if no response after n seconds
The amount of time in seconds that IKEv2 will wait for a response from the remote unit before transmitting the negotiation frame.

Stop IKE negotiation after n retransmissions
The maximum number of times that IKEv2 will retransmit a negotiation frame as part of the exchange before failing.

Stop IKE negotiation if no packet received for n seconds
The period of time in seconds after which the unit will stop the IKE v2 negotiation when no response to a negotiation packet has been received.

Enable NAT-Traversal
Enables support for NAT Traversal within IKE/IPsec. When one end of an IPsec tunnel is behind a NAT box, some form of NAT traversal may be required before the IPsec tunnel can pass packets. Turning NAT Traversal on enables the IKE protocol to discover whether or not one or both ends of a tunnel is behind a NAT box, and implements a standard NAT traversal protocol if NAT is not being performed.
The version of NAT traversal supported is that described in the IETF draft 'draft-ietf-ipsec-nat-t-ike-03.txt'.

NAT traversal keep-alive interval n seconds
The interval in seconds in which the NAT Traversal keepalive packets are sent to a NAT device in order to prevent NAT table entry from expiring.

RSA private key file
The name of a X.509 certificate file holding the router's private part of the public/private key pair used in certificate exchanges. See 'X.509 Certificates' in the 'IPsec and VPNs' section for further explanation.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ike2	n	retranint	0 - 255	Retransmit a frame if no response after n seconds
ike2	n	retran	0 - 9	Stop IKE negotiation after n retransmissions
ike2	n	inactto	0 - 255	Stop IKE negotiation if no packet received for n seconds
ike2	n	natt	on, off	Enable NAT-Traversal
ike2	n	natkaint	Integer	NAT traversal keep-alive interval n seconds
ike2	n	privrsakey	Filename	RSA private key file

Configuration – Network > Virtual Private Networking (VPN) > IPsec > IKEv2 > IKEv2 Responder

This page displays the various parameters for IKEv2 0 when used in Responder mode.

Enable IKEv2 Responder
Allows the router to respond to incoming IKE requests.

Accept IKEv2 Requests with
Defines the settings that the router will accept during the negotiation

Encryption
The acceptable encryption algorithms.

Authentication
The acceptable authentication algorithms.

PRF Algorithm
The acceptable PRF (Pseudo Random Function) algorithms.

MODP Group between x and y
The acceptable range for MODP group.

Renegotiate after h hrs m mins s secs
Determines how long the initial IKE Security Association will stay in force. When it expires any attempt to send packets to the remote system will result in IKE attempting to establish a new SA.

Rekey after h hrs m mins s secs
When the time left until expiry for this SA reaches the value specified by this parameter, the IKEv2 SA will be renegotiated, i.e. a new IKEv2 SA is negotiated and the old SA is removed. Any IPSec "child" SAs that were created are retained and become "children" of the new SA.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ike2	0	rencalgs	des, 3des, aes	Encryption
ike2	0	renckeybits	128, 192, 256	Encryption (Minimum AES key length)
ike2	0	rauthalgs	md5, sha1	Authentication
ike2	0	rprfalgs	md5, sha1	PRF Algorithm
ike2	0	rdhmingroup	1, 2, 5	MODP Group between x and y
ike2	0	rdhmaxgroup	1, 2, 5	MODP Group between x and y
ike2	0	ltime	1 – 28800	Renegotiate after h hrs m mins s secs This CLI value is entered in seconds only.
ike2	0	rekeyltime	1 - 28800	Rekey after h hrs m mins s secs This CLI value is entered in seconds only.

Configuration – Network > Virtual Private Networking (VPN) > IPsec > IKEv2 > IKEv2 Responder > Advanced

Stop IKE negotiation if no packet received for n seconds
The period of time in seconds after which the unit will stop the IKEv2 negotiation when no response to a negotiation packet has been received.

Enable NAT-Traversal
Enables support for NAT Traversal within IKE/IPsec. When one end of an IPsec tunnel is behind a NAT box, some form of NAT traversal may be required before the IPsec tunnel can pass packets. Turning NAT Traversal on enables the IKE protocol to discover whether or not one or both ends of a tunnel is behind a NAT box, and implements a standard NAT traversal protocol if NAT is not being performed.
The version of NAT traversal supported is that described in the IETF draft 'draft-ietf-ipsec-nat-t-ike-03.txt'.

NAT traversal keep-alive interval n seconds
The interval in seconds in which the NAT Traversal keepalive packets are sent to a NAT device in order to prevent NAT table entry from expiring.

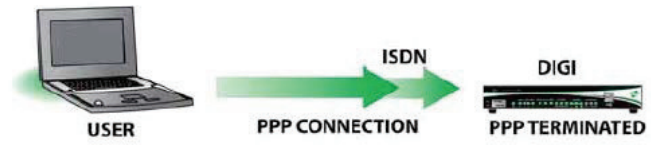
RSA private key file
The name of a X.509 certificate file holding the router's private part of the public/private key pair used in certificate exchanges. See 'X.509 Certificates' in the 'IPsec and VPNs' section for further explanation.

Related CLI Commands

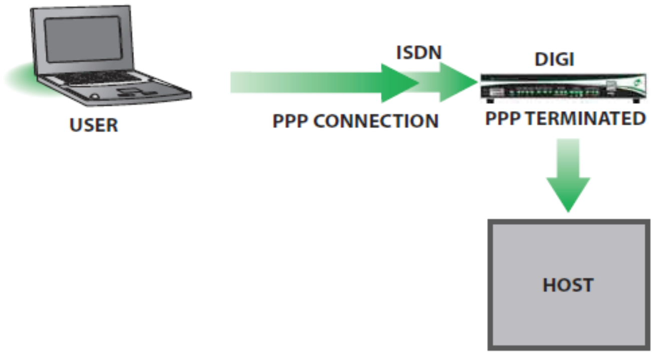
Entity	Instance	Parameter	Values	Equivalent Web Parameter
ike2	0	inactto	0 - 255	Stop IKE negotiation if no packet received for n seconds
ike2	0	natt	on, off	Enable NAT-Traversal
ike2	0	natkaint	Integer	NAT traversal keep-alive interval n seconds
ike2	0	privrsakey	Filename	RSA private key file

Configuration – Network > Virtual Private Networking (VPN) > L2TP

The Layer 2 Tunnelling Protocol (L2TP) provides a means for terminating a logical PPP connection on a device other than the one which terminates the physical connection. Typically, both the physical layer and logical layer PPP connections would be terminated on the same device, a Digi Router for example.



With L2TP answering the call, the router terminates the layer 2 connection only and the PPP frames are passed in an L2TP "tunnel" to another device which terminates the PPP connection. This device is sometimes referred to as a Network Access Server (NAS).



Configuration – Network > Virtual Private Networking (VPN) > L2TP > L2TP n

Act as a listener only
When checked, this checkbox causes the router to NOT actively attempt to establish an L2TP tunnel. In this mode it will only use L2TP if the remote host requests it. When unchecked, the router will actively try to establish an L2TP connection with the remote host.

Enable Server mode
When checked, this checkbox causes the router to act as a L2TP server.

Initiate connections to a.b.c.d
The value in this text box specifies the IP address of the remote host, i.e. the device that will terminate the L2TP connection.

Use a.b.c.d as a backup
It is possible to specify a backup remote L2TP host server using this parameter. The text box contains the IP address of the remote server to use.

Bring this tunnel up All the time/On demand

This parameter only applies to tunnels initiated from this router.

Bring this tunnel down if it is idle for h hrs, m mins, s secs
These radio buttons select whether or not the tunnel is permanently available or not. When set to **On demand**, the tunnel will not activate automatically but will wait until it is triggered by PPP. When set to **On demand** the values in the text boxes determine the timeout after which the L2TP tunnel will closed down after the last L2TP call on that tunnel.

L2TP Window Size
The L2TP window size is selected from this drop down list. Available values are from 1 to 7.

Route UDP packets over interface x,y
These two text boxes specify the interface and its instance number that should be used for L2TP UDP sockets. Specifying these parameters allow the router to raise the interface should it be disconnected.

Source Port Normal/Variable
These radio buttons select the source port for the L2TP tunnel. When set to **Normal** the default port number of 1701 is used. When set to **Variable** a random source port value will be used.

Name
The value in this text box is the name that is used to identify the router during the negotiation phase when establishing an L2TP tunnel.

Authentication Off/Secret
The radio buttons select whether or not to use authentication. This is normally set to **Off** as most host systems require that IPsec be used over L2TP tunnels. If Authentication is set to **On**, authentication is enabled and the **Secret** parameter becomes relevant. The value in the text box contains a passphrase that is shared with the host and which will be used if the remote host requests authentication and **Authentication** is set to **Off** here.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
l2tp	n	listen	OFF,ON	Act as a listener only
l2tp	n	swap_io	OFF,ON	Enable server mode
l2tp	n	remhost	Valid IP address a.b.c.d	Initiate connections to a.b.c.d
l2tp	n	backremhost	Valid IP address a.b.c.d	Use a.b.c.d as a backup
l2tp	n	aot	OFF,ON	Bring this tunnel up All the time/On demand
l2tp	n	nocallto	0 – 4294967296	Bring this tunnel down if it is idle for h hrs, m mins, s secs
l2tp	n	window	1 – 7 Default = 4	L2TP Window Size
l2tp	n	ll_ent	<blank>, PPP, ETH	Route UDP packets over interface x,y
l2tp	n	ll_add	0 - 2147483647	Route UDP packets over

Entity	Instance	Parameter	Values	Equivalent Web Parameter
				interface x,y
l2tp	n	rnd_srcport	OFF, ON	Source Port
l2tp	n	name	Up to 30 characters	Name
l2tp	n	auth	OFF,ON	Authentication Off/Secret
l2tp	n	secret	Up to 80 characters	Authentication Off/Secret

Configuration – Network > Virtual Private Networking (VPN) > L2TP > L2TP n > Advanced

Retransmit interval s milliseconds

The value in this text box specifies the amount of time in milliseconds that the router will wait before retransmitting a Start Control Connection Request (SCCRQ) frame. The default value of 250ms should be changed to a higher value (say 4000ms) if L2TP is running over a GPRS link.

Retransmit count n
When using L2TP over GPRS or satellite networks, the first few packets are sometimes lost. Setting the retransmit count in the text box to a higher value than the default of 5 will increase reliability of the tunnel.

Layer 1 Interface Sync port n/ISDN
These radio buttons select the layer 1 (physical) interface to be used to terminate the L2TP connection. The available options are ISDN or one of the router's synchronous serial ports. When Sync port n is selected, the sync port number is selected from the drop-down list.

Allow this L2TP tunnel to answer incoming ISDN calls
When checked, this checkbox allows the L2TP entity to answer incoming ISDN calls.

MSN
The value in this text box specifies the filter for the ISDN Multiple Subscriber Numbering (MSN). It is blank by default but when the answering facility (above) is enabled, the router will only answer ISDN calls where the trailing digits match this MSN value. For example, setting the MSN value to 123 will prevent the router from answering calls from any calling number that does not end in 123. This parameter is not used when answering is off.

Sub-address
The value in this text box specifies the ISDN sub-address filter to use in conjunction with the ISDN answering function. When answering is set to **On** and there is a valid sub-address in this text box, the router will only answer calls where the trailing digits of the calling sub-address match this sub-address. For example, setting the sub-address value to 123 will prevent the router from answering calls where the sub-address does not end in 123.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
l2tp	n	retxto	0 – 4294967296	Retransmit interval s milliseconds
l2tp	n	retxcnt	0 – 4294967296	Retransmit count
l2tp	n	l1iface	0 – 255	Layer 1 Interface

Entity	Instance	Parameter	Values	Equivalent Web Parameter
l2tp	n	ans	OFF,ON	Allow this L2TP tunnel to answer incoming ISDN calls
l2tp	n	msn	Up to 9 digits	MSN
l2tp	n	sub	Up to 17 digits	Sub-address

Configuration – Network > Virtual Private Networking (VPN) > PPTP

The Point-to-Point tunnelling protocol (PPTP) is a common way of creating a VPN tunnel to a Microsoft Windows™ server.

PPTP works by ending a regular PPP session to the peer encapsulated by the Generic Routing Encapsulation (GRE) protocol. A second session on TCP port 1723 is used to initiate and manage the GRE session. PPTP connections are authenticated with Microsoft MSCHAP-v2 or EAP-TLS. VPN traffic is protected by MPPE encryption. PPTP does not work with GPRS/HSDPA mobile operators that assign a private IP address and then apply NAT to the traffic before it leaves their network. This because the server tries to build a tunnel back to the router on port 1723 but fails when the traffic is blocked by the mobile operators' firewall.

Configuration – Network > Virtual Private Networking (VPN) > PPTP > PPTP n

Description
The text string in this text box is a name to aid the identification of the router.

Remote Host a.b.c.d
The value in this text box specifies the IP address of the remote host, i.e. the device that will terminate the PPTP connection.

Use Interface x,y
The interface to be used for the PPTP tunnel is selected from this drop-down list, the text box next to it is for the interface instance. Specifying these parameters allow the router to raise the interface should it be disconnected. The interface options are:

- Auto
- PPP
- Ethernet.

Accept incoming PPTP connections
When checked, this checkbox allow the router to act as a PPTP server and accept incoming VPN connections.

Enable Server mode
When checked, this checkbox causes the router to send call_out call requests to the remote device. In the default state which is unchecked, the router will send a call_in request to the remote device.

Enable Socket mode
When checked, this checkbox enables the use of a Digi proprietary mode whereby PPP packets are sent via the PPTP control socket rather than in GRE packets.

Encrypt control data using SSL version n
When checked, this checkbox causes the router to encrypt the control data using SSL. This is a Digi proprietary function and is not part of standard PPTP. The drop-down list allows the SSL version to be selected. The available options are:

- Use default

- TLSv1 only
- SSLv3 only
- SSLv2 only.

Enable PPTP debug
When checked, this checkbox enables debug tracing.

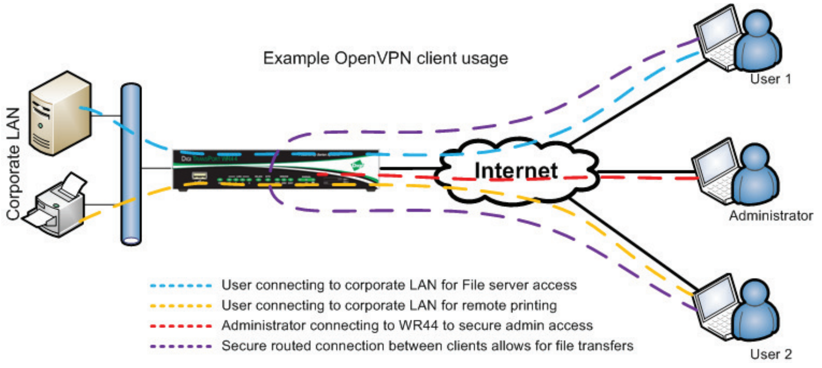
Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
pptp	0 - 9	name	Up to 30 characters	Description
pptp	0 - 9	remhost	Valid IP address a.b.c.d	Remote Host a.b.c.d
pptp	0 - 9	ll_ent	Blank, PPP, ETH Blank means Auto	Use Interface x,y
pptp	0 - 9	ll_add	0 – 4294967296	Use Interface x,y
pptp	0 - 9	listen	OFF,ON	Accept incoming PPTP connections
pptp	0 - 9	swap_io	OFF,ON	Enable Server mode
pptp	0 - 9	usesock	OFF,ON	Enable Socket mode
pptp	0 - 9	sslver	Blank,SSL,TLS1,SSL3,SSL2 Blank is disabled (default) SSL means use default.	Encrypt control data using SSL version n
pptp	0 - 9	debug	OFF,ON	Enable PPTP debug

Configuration – Network > Virtual Private Networking (VPN) > OpenVPN

OpenVPN can be used for connecting to the router for secure management as well as access to services on the LAN side of the TransPort router, such as corporate messaging services, file servers and print servers for example.

OpenVPN is a full-featured SSL VPN which implements OSI layer 2 or 3 secure network extension using the industry standard SSL/TLS protocol, supports flexible client authentication methods based on certificates, smart cards, and/or username/password credentials, and allows user or group-specific access control policies using firewall rules applied to the VPN virtual interface. OpenVPN is not a web application proxy and does not operate through a web browser.


Example OpenVPN client usage
Corporate LAN
Internet
User 1
Administrator
User 2
User connecting to corporate LAN for File server access
User connecting to corporate LAN for remote printing
Administrator connecting to WR44 to secure admin access
Secure routed connection between clients allows for file transfers

The Digi TransPort implementation of OpenVPN can be configured as an OpenVPN server (shown above) or as an OpenVPN client, connecting to an OpenVPN server.

On TransPort firmware, OpenVPN has been implemented as an interface. That means that when an OpenVPN tunnel connects, an interface is added to the routing table. Static routes may be configured to point to an OpenVPN instance, and additionally, OpenVPN may learn routes from the tunnel peer and add these routes to the routing table for the duration of the OpenVPN tunnel. As each tunnel appears just like an interface, support for features like the firewall, NAT, IGMP etc are the same as for other interfaces like PPP and ETH.

Configuration – Network > Virtual Private Networking (VPN) > OpenVPN > OpenVPN n

Description
The text string is a friendly name to help identify this OpenVPN instance.

IP address a.b.c.d
This must be specified correctly. OpenVPN interfaces use a 30 bit mask, the first address is the network address, the 2nd is the server address, the 3rd is the client address, the 4th is the broadcast address. This address must be configured as the 2nd IP address in the block of 4. For example 192.168.0.1 if configured as a server, or 192.168.0.2 if configured as a client.

Destination host a.b.c.d
Only required when configured as an OpenVPN client. This is the IP address of the OpenVPN server.

Link socket interface x,y
If configured, OpenVPN sockets will only be allowed to/from this interface and the routing table will be ignored. When set to Auto, the OpenVPN sockets will use the routing table to identify the best interface to use.

Get link socket source address from this interface x,y
The values in these two text boxes define the interface (Auto,PPP,ETH) and the instance number of the interface to use as a source address for IP sockets when not using the interface that the socket was created on.
Even when this parameter is not configured, the IP address from the interface on which the socket was created will be used. The source address specified in this parameter will only be used if it will cause the traffic to match an Eroute and therefore be sent using IPsec or GRE.

MTU
This parameter is used to set the Maximum Transmit Unit for the OpenVPN instance, in bytes. The default setting is 1400.

Metric
This parameter specifies the connected metric, changing this value will alter the metric of dynamic routes created automatically for this interface.

NAT mode
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.

IP analysis
When enabled, the un-encapsulated IP traffic will be captured into the analyser trace.

Firewall
The Firewall parameter is used to turn Firewall script processing "On" or "Off" for this interface.

IGMP
This IGMP parameter is used to enable or disable the transmission and reception of IGMP packets on this interface. IGMP is used to advertise members of multicast groups. If IGMP is enabled, and a member of a multicast group is discovered on this interface, multicast packets for this group received on other interfaces will be sent out this interface.

Include in RIP advertisements
When checked, this checkbox will cause the router to include this static route to be included in RIP advertisements.

Automatically connect interface
If enabled, this OpenVPN instance will be considered as an always on interface.

Server mode (listener)
This parameter configures the OpenVPN instance to listen for inbound OpenVPN sockets.

Link socket port
The default port used by OpenVPN is 1194. If a different or non-standard port number is used, specify it here.

Link socket protocol
OpenVPN can use TCP or UDP as the transport protocol. Select the required protocol here.

TLS auth password / Confirm TLS auth password
This allows the OpenVPN instance to use an extra level of security by having a TLS password configured.

Push IP address #1/#2/#3
When configured as an OpenVPN server, these parameters can be used to push subnets to the client that need to be routed via the OpenVPN server. Used in conjunction with the Push Mask parameter below.

Push mask #1/#2/#3
Used with the Push IP address parameter above to define subnets that should be routed via the OpenVPN server.

Push DNS server address #1/#2
When configured as an OpenVPN server, these parameters can be used to push DNS server settings to the OpenVPN client.

Pull interface IP address
When configured as an OpenVPN client, this option must be enabled for the router to obtain and use the local IP address supplied from the OpenVPN server.

Pull routes
When configured as an OpenVPN client, this option must be enabled for the router to use routes sent from the OpenVPN server.

Pull DNS server addresses
When configured as an OpenVPN client, this option must be enabled for the router to use DNS servers sent from the OpenVPN server.

Packet replay ID window
When set to a non-zero value, this enables sequence number replay detection. It indicates the number of packet IDs lower than the current highest ID to allow out of sequence.

Packet replay time window (seconds)
Set to a non-zero value to enable time tracking of incoming packets.

OpenVPN TX ping interval (seconds)
Interval between OpenVPN ping transmissions. These are required to detect the operational state of the VPN connection.

OpenVPN RX ping timeout (seconds)
The number of seconds, after which no OpenVPN ping has been received, the VPN will be marked as down.

Include IV
Enabling this option on includes an IV at the head of an encrypted packet. If one peer prepends this IV and the other isn't expecting it, packet decryption will fail.

Key negotiation timeout (seconds)
Maximum time in seconds to allow for a data channel key negotiation.

Key renegotiation interval (seconds)
Interval between key re-negotiations.

Key renegotiation bytes
If non-zero, a key renegotiation will take place after this many bytes have travelled through the data channel (in either direction).

Key renegotiation packets
If non-zero, a key renegotiation will take place after this many packets have travelled through the data channel.

Inactivity timeout (seconds)
The tunnel is disconnected after the tunnel becomes inactive (no IP traffic) for this many seconds. Note that the timer is only restarted with RX traffic, not TX traffic.

Data channel cipher
Sets the cipher used for data channel encryption/decryption. Select from the dropdown list.

Data channel digest
Sets the digest algorithm used for data channel authentication. Select from the dropdown list.

Debug
Enables output of OVPN related debug.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ovpn	n	descr	Up to 30 characters	Description
ovpn	n	IPaddr	Valid IP address a.b.c.d	IP address a.b.c.d
ovpn	n	dest	Valid IP address a.b.c.d	Destination host a.b.c.d
ovpn	n	ll_ent	<blank>, PPP, ETH	Link socket interface x,y x= interface type
ovpn	n	ll_add	0 - 2147483647	Link socket interface x,y y= interface number
ovpn	n	ip_ent	<blank>, PPP, ETH	Get link socket source address from this interface x,y x= interface type
ovpn	n	ip_add	0 - 2147483647	Get link socket source address from this interface x,y y= interface number
ovpn	n	mtu	0 - 2147483647	MTU
ovpn	n	metric	0 - 2147483647	Metric
ovpn	n	do_nat	0,1,2 0 = Off 1 = Address only 2= Address and port	NAT mode
ovpn	n	ipanon	OFF,ON	IP analysis
ovpn	n	firewall	OFF,ON	Firewall
ovpn	n	igmp	OFF,ON	IGMP
ovpn	n	inrip	OFF,ON	Include in RIP advertisements

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ovpn	n	autoup	OFF,ON	Automatically connect interface
ovpn	n	server	OFF,ON	Server mode (listener)
ovpn	n	port	0 - 65535	Link socket port
ovpn	n	proto	TCP,UDP	Link socket protocol
ovpn	n	tls_auth_key	Up to 30 characters	TLS auth password
ovpn	n	etls_auth_key		enciphered version TLS auth password
ovpn	n	puship	Valid subnet a.b.c.d	Push IP address #1 a.b.c.d
ovpn	n	pushmask	Valid netmask a.b.c.d	Push mask #1 a.b.c.d
ovpn	n	puship2	Valid subnet a.b.c.d	Push IP address #2 a.b.c.d
ovpn	n	pushmask2	Valid netmask a.b.c.d	Push mask #2 a.b.c.d
ovpn	n	puship3	Valid subnet a.b.c.d	Push IP address #3 a.b.c.d
ovpn	n	pushmask3	Valid netmask a.b.c.d	Push mask #3 a.b.c.d
ovpn	n	pushdns	Valid IP address a.b.c.d	Push DNS server address #1 a.b.c.d
ovpn	n	pushdns2	Valid IP address a.b.c.d	Push DNS server address #2 a.b.c.d
ovpn	n	pullip	OFF,ON	Pull interface IP address
ovpn	n	pullroute	OFF,ON	Pull routes
ovpn	n	pulldns	OFF,ON	Pull DNS server addresses
ovpn	n	sreplay	0 - 2147483647	Packet replay ID window
ovpn	n	treplay	0 - 2147483647	Packet replay time window (seconds)
ovpn	n	pingint	0 - 2147483647	OpenVPN TX ping interval (seconds)
ovpn	n	pingto	0 - 2147483647	OpenVPN RX ping timeout (seconds)
ovpn	n	inciv	OFF,ON	Include IV
ovpn	n	neg_timeout	0 - 2147483647	Key negotiation timeout (seconds)
ovpn	n	reneg_int	0 - 2147483647	Key renegotiation interval (seconds)

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ovpn	n	reneg_bytes	0 - 2147483647	Key renegotiation bytes
ovpn	n	reneg_packets	0 - 2147483647	Key renegotiation packets
ovpn	n	inact_timeout	0 - 2147483647	Inactivity timeout (seconds)
ovpn	n	cipher	See cipher list below	Data channel cipher
ovpn	n	digest	See digest list below	Data channel digest
ovpn	n	debug	OFF,ON	Debug

Supported Cipher and Digest values for OpenVPN

Cipher values		Digest values
DES-EDE-CBC		md2WithRSAEncryption
AES128		ssl2-md5
DES		MD5
DES-CBC		sha1WithRSAEncryption
AES-128-CBC		ssl3-sha1
AES192		ssl3-md5
AES-192-CBC		SHA1
DES-EDE3-CBC		MD2
AES-256-CBC		RSA-MD2
AES-256		md5WithRSAEncryption
DES3		RSA-SHA1
		RSA-SHA1-2
		RSA-MD5

Configuration – Network > SSL

The secure socket layer (SSL) that provides a secure transport mechanism is supported by Digi's TransPort routers. The configuration of the client-side and server are described in the following pages.

Configuration – Network > SSL > SSL Clients

Some sites require client side authentication when connecting to them. The router's SSL client handles the authentication for SSL connections using certificates signed by a Certificate Authority (CA). For more information regarding certificates and certificate requests, refer to the certificates page ***Administration – X.509 Certificate Management > Certificate Authorities (CAs)***.

Configuring the SSL clients is handled by a table having the columns and parameters listed below:

SSL Client
This column is simply a list of the SSL client numbers supported by the router.

Client Certificate Filename
The name of the required certificate file is selected from those available on the router's filing system from this drop-down list.

Client Private Key Filename
The name of the file that contains the private key that matches the public key stored in the above parameter, is selected from this drop-down list.

Cipher List
The cipher list in this text box is a list of one or more cipher strings separated by colons. Commas or spaces are also accepted as separators but colons are normally used. The actual cipher string can take several different forms. It can consist of a single cipher suite such as RC4-SHA. It can represent a list of cipher suites containing a certain algorithm or cipher suites of a certain type. For example, SHA1 represents all cipher suites using the SHA1 digest algorithm and SSLv3 represents all SSL v3 algorithms. Lists of cipher suites can be combined in a single cipher string using the "+" character. This forms the logical **AND** operation. For example, SHA1+DES represents all cipher suites containing SHA1 and DES algorithms. If left empty, the cipher list is not used.
For more information see: http://www.openssl.org/docs/apps/ciphers.html

Apply to Destination IP Address
The value in this text box allows the configuration of multiple SSL destinations, each having a different certificate/key pair. When set, this parameter will lock the SSL client settings to a specific IP address. If this parameter is left blank, the configured SSL client settings will be used for any connection that requires SSL.

As is usual with the tables on the configuration web pages, the relevant and appropriate parameters are selected and the **Add** button on the right-hand side is clicked to add the entry into the table. Once an entry has been added, it may be removed by clicking the **Delete** button that will appear in the right-hand column.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
sslcli	0 - 4	certfile	Up to 12 characters (DOS 8.3 format)	Client Certificate Filename
sslcli	0 - 4	keyfile	Up to 12 characters (DOS 8.3 format)	Client Private Key Filename
sslcli	0 - 4	cipherlist	Colon-separated list of ciphers	Cipher List
sslcli	0 - 4	IPaddr		Apply to Destination IP Address

Configuration – Network > SSL > SSL Server

This page describes the parameters needed to configure the SSL server.

Server Certificate Filename
The file containing the server certificate is selected from this drop-down list.

Client Private Key Filename
The file containing the private key that matches the above certificate is selected from this drop-down list.

SSL Version
The version of the SSL protocol to use, is selected from this drop-down list. Selecting "Any" allows the use of any version. The available options are:

- Any
- TLSv1 only
- SSLv3 only
- SSLv2 only.

Cipher List
The list of ciphers is the same as described above for the client-side configuration table.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
sslsvr	0	certfile	Up to 12 characters (DOS 8.3 format)	Server Certificate Filename
sslsvr	0	keyfile	Up to 12 characters (DOS 8.3 format)	Server Private Key Filename
sslsvr	0	ver	Blank, TLS1, SSL3, SSL2	SSL Version
sslsvr	0	cipherlist	Colon-separated list	Cipher List
sslsvr	0	debug	OFF,ON	n/a

Configuration – Network > SSH Server

The secure shell (SSH) server allows remote peers to access the router over a secure TCP connection using a suitable SSH client. The SSH server provides a Telnet-like interface and secure file transfer capability.

SSH uses a number of keys during a session. The host keys are used for authentication purposes. Keys unique to each SSH session are also generated and are used for encryption/authentication purposes.

The router supports SSH v1.5 and SSH v2. The host key file format differs for each version but there would normally only be one host key for each version. For this reason the router allows the user to configure two host key files. These keys may be changed from time to time, specifically if it suspected that the key has become compromised. Because the host keys need to be secure, it is highly recommended to store the files on the router's FLASH filing system using filenames prefixed with "priv" which makes it impossible to read the files using any of the normal methods (e.g. FTP). It is possible (using the **genkey** command) to create host keys in either format for use with SSH. Using this utility it is not necessary to have the host key files present on any other storage device (thus providing an additional level of security). Refer to the section of this manual that covers certificates on how to generate a private key file.

Unlike the Telnet server it is possible to configure the number of SSH server sockets that listen for new SSH connections.

Multiple SSH server instances can be configured, each instance can be configured to listen on a separate port number and can use different keys and encryption methods.

It is possible to configure which authentication methods can be used in an SSH session and the preferred selection order. The router currently supports MD5, SHA1, MD5-96 and SHA1-96. If required, a public/private key pair can be used for authentication.

The router currently supports 3DES, 3DES-CBC and AES cipher methods.

DEFLATE compression is also supported. If this is enabled and negotiated, SSH packets are first compressed before being encrypted and delivered to the remote unit via the TCP socket.

Note:
The SSH server supports the SCP file copy protocol but does NOT support filename wildcards.

Enable SSH Servers
When checked, this checkbox enables the SSH servers on the router.

Configuration – Network > SSH Server > SSH Server n

The router supports eight individual SSH servers that are configured independently using the options described below.

Enable SSH Server
When checked, this checkbox enables the SSH server.

Use TCP port p
The value in this text box is the TCP port number (default 22) that the SSH server will use to listen for incoming connections. (Port 22 is the standard SSH port).

Allow up to n connections
The value in this text box specifies the number of sockets listening for new SSH connections (default 1).

Host Key 1 Filename
The value in this text box is the filename of either an SSH V1 or V2 host key. It is highly recommended that the filename be prefixed with "priv" to ensure that the key cannot be easily accessed and compromised. This key may be generated using the facilities described in the Certificates section of this manual.

Host Key 2 Filename
The value in this text box is the filename of either an SSH V1 or V2 key as above.

Note:
The maximum length for these filenames is 12 characters and they must use the DOS 8.3 file naming convention.

Maximum login time s seconds
The value in this text box specifies the maximum length of time (in seconds) that a user is allowed to successfully complete the login procedure once the SSH socket has been opened. The socket is closed if the user has not completed a successful login within this period.

Maximum login attempts n
The value in this text box specifies the maximum number of login attempts allowed in any one session before the SSH socket will be closed.

Use Deflate compression No/Yes, level n
The radio buttons select whether or not DEFLATE compression will be used. If compression is selected, the compression level is chosen from the drop-down list.

Enable Port Forwarding
When checked, this checkbox enables the router to accept traffic on ports other than 23. This functionality is for use with SSH client applications (such as PuTTY) that has port forwarding capability. For example, one the SSH connection is active, traffic for the HTTP port 80 can be sent to the router securely.

Command Session IP Address a.b.c.d Port p
The values in these two text boxes are used to specify the host IP address and port number that the router will use to handle incoming requests for a command session from SSH clients. This is instead of the router's normal command interpreter. For example, if the values are IP address 127.0.0.1, port 4000, the SSH client will make a direct connection to ASY 0 and the device attached to ASY 0 will receive and process the commands from the SSH client.

Enable support for SSH v1.5
When checked, this checkbox allows the server to negotiate SSH V1.5. The router must also have a SSH V1 key present and the filename entered into the SSG configuration.

Server key size
This option applies to V1 SSH. During initialisation of an SSH session, the server sends its host key and a server key (which should be of a different size to the host key). The router generates this key automatically but the length of the server key is determined by this parameter. If when this value is set it is too similar to the length of the host key, the router will automatically adjust the selected value so that the key sizes are significantly different.

Enable support for SSH v2.0
When checked, this checkbox allows the server to negotiate SSH V2. The router must also have a SSH V2 key present and the filename entered into the SSG configuration.

Actively start key exchange
This option applies to V2 SSH. Some SSH clients wait for the server to initiate the key exchange process when a new SSH session is started unless they have data to send to the server, in which case they will initiate the key exchange themselves. When checked, this checkbox will cause the router to automatically initiate a key exchange without waiting for the client.

Rekey Never/After n units of data have been transferred
With SSH V2 it is possible to negotiate new encryption keys after the current ones have been used to encrypt a specified amount of data. The radio buttons select whether this feature should be used. If this feature is to be used the amount of data is entered into the text box and the applicable units (Kbytes, Mbytes, Gbytes) selected from the drop-down list.

Encryption Preferences
The following four configuration options allocate preferences to the encryption method that should be used to encrypt data on the link. A lower value indicates greater preference apart from zero which disables the option.

3DES
The value in this text box is the preference level for the Triple-DES algorithm.

AES (128 bits)
The value in this text box is the preference level for the 128-bit AES algorithm.

AES (192 bits)
The value in this text box is the preference level for the AES algorithm using 192 bits.

AES (256 bits)
The value in this text box is the preference level for the AES algorithm using 256 bits.

Authentication Preferences
The following four configuration options allocate preferences to the authentication methods that should be used. As above, a value of zero disables the particular authentication method and lower values indicated greater preference than higher values. So, for example if MAC SHA1-96 was the preferred method for authentication, this option would be given the value 1 and the other options given a value of 2 or greater. If all these parameters are set to the same value, the router automatically uses them in the following order: SHA1, SHA1-96, MD5, MD5-96.

MAC MD5
The value in this text box is the preference level for MAC MD5.

MAC MD5-96
The value in this text box is the preference level for MAC MD5-96.

MAC SHA1
The value in this text box is the preference level for MAC SHA1.

MAC SHA1-96
The value in this text box is the preference level for MAC SHA1-96.

Enable Debug
The router supports logging and output of debugging information for situations where there are problems establishing a SSH connection. When checked, this checkbox causes the router to trace and output information that should be helpful in diagnosing and resolving the problem.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ssh	0 – 7	port	0 - 65535	Use TCP port p
ssh	0 - 7	nb_listen	0 - 2147483647	Allow up to n connections
ssh	0 - 7	hostkey1	Up to 12 characters (8.3 format)	Host Key 1 Filename
ssh	0 - 7	hostkey2	Up to 12 characters (8.3 format)	Host Key 2 Filename
ssh	0 - 7	loginsecs	0 - 2147483647	Maximum login time s seconds
ssh	0 - 7	logintries	0 - 2147483647	Maximum login attempts n
ssh	0 - 7	comp	0 = disabled	Use Deflate compression , level
ssh	0 - 7	fwd	0 - 2147483647	Enable port forwarding
ssh	0 - 7	cmdhost	Valid IP address a.b.c.d	Command session IP address a.b.c.d
ssh	0 - 7	cmdport	0 - 2147483647	Command session port p
ssh	0 - 7	svrkeybits	0 - 2147483647	Server key size
ssh	0 - 7	initkex	OFF,ON	Actively start key exchange
ssh	0 - 7	rekeybytes	0 - 2147483647 0 = Do not rekey	Rekey After n units of data have been transferred
ssh	0 - 7	enc3descbc	0 - 2147483647 0 = Disabled	3DES
ssh	0 - 7	encaes128cbc	0 - 2147483647	AES (128 bits)
ssh	0 - 7	encaes192cbc	0 - 2147483647	AES (192 bits)
ssh	0 - 7	encaes256cbc	0 - 2147483647	AES (256 bits)
ssh	0 - 7	macmd5	0 - 2147483647	MAC MD5
ssh	0 - 7	macmd596	0 - 2147483647	MAC MD5-96
ssh	0 - 7	macsha1	0 - 2147483647	MAC SHA1
ssh	0 - 7	macsha196	0 - 2147483647	MAC SHA1-96
ssh	0 - 7	debug	0,1 0 = Off 1 = On	Enable Debug

Configuring SSH

In order to fully configure SSH, a version1 SSH key and a version 2 SSH key need to be generated and the router configured to use them. This procedure will be described below.

Note:
SSH version 2 is more secure than version 1 and so is the recommended version to use. However, some SSH clients may only support version 1 keys and so the router supports both version 1 and version 2 SSH.

Configuration using the web interface

Navigate to ***Administration – X.509 Certificate Management > Key Generation*** and select the size of the key file from the drop-down list. The larger the key file, the more secure it will be.

Enter the name for the key file in the **Key filename** box or select from those already present using the drop-down selector. The filename should have a prefix of "priv" and a file extension of ".pem", e.g. "privssh1.pem". (Please note that the 8.3 file name convention applies as mentioned previously).

Check the checkbox marked **Save in SSHv1 format** in order to generate a version 1 SSH key. Click the **Generate Key** button to generate the private key file. The key file will be stored in the router's FLASH filing system.

Repeat steps 1 to 3 in order to generate the second key. This time, however, make sure that the **Save in SSHv1 format** checkbox is unchecked. This key file should be given a different name to the version 1 file previously generated.

On the ***Configuration – Network > SSH Server > SSH Server n*** page, enter the filename generated in step 3 into the **Host Key 1 Filename** text box and the filename generated in step 4 into the **Host Key 2 Filename** text box.

Apply the configuration changes using the Apply button at the bottom of the page and when the "Configuration successfully applied" message appears, click on the highlighted link to save the configuration.

Configuration using the command line interface

Generate the SSH V1 private key using the **genkey** command as follows:

genkey <keybits> <filename> -ssh1 where *<keybits>* is one of the following values; 384, 512, 768, 1024, 1536 or 2048 and *<filename>* is the name for the file, e.g. "privssh1.pem" as described for the web version of this procedure.

Generate the SSH V2 private key using the **genkey** command as per step 1 but this time omit the *-ssh1* switch. For example:

```
genkey 1024 privssh2.pem.
```

Set the first private key as the SSH Host key 1 using the following command:

```
ssh 0 hostkey1 privssh1.pem
```

Set the second private key as SSH Host Key 2 using the following command:

```
ssh 0 hostkey2 privssh2.pem
```

Save the configuration:

```
config 0 save
```

SSH Authentication with a public/private keypair

Once SSH access has been configured and confirmed to be working, RSA key pair authentication can be added and used to replace password authentication.

This process will involve the use of PuTTYgen to create public and private keys. Please see the Technical Notes section on the Digi website for full details on how to perform this procedure.

Configuration – Network > FTP Relay

The FTP Relay agents allow any files to be transferred onto the router by a specified user using the File Transfer Protocol to be temporarily stored in memory and then relayed to a specific FTP host. This is useful when the router is being used to collect data files from a locally attached device such as a webcam which must then be to a host system over a slower data connection such as W-WAN. In effect, the router acts as a temporary data buffer for the files.

The FTP Relay Agent may also be configured to email (as an attachment) any file that it was unable to transfer to the FTP server. To facilitate this, set the Email Template, To, From and Subject parameters as appropriate and also configure the SMTP client (***Configuration – Alarms > SMTP Account***).

Configuration – Network > FTP Relay > FTP Relay n

There are two FTP Relay Agents available, with a separate web page for each. For command line configuration, the instance number can be 0 or 1.

Relay files for user locuser to FTP Server ftphost
The value in the left-hand text box is the name of the local user and should be one of the usernames assigned in the ***Configuration – Security > Users*** web page. This name is then used as the FTP login username when the local device needs to relay a file. The value in the right-hand text box is the name of the FTP host to which the files from the locally attached device are to be relayed.

Server Username
The value in this text box is the username required to log in to the specified FTP host.

Server Password
The value in this text box specifies the password to be used to log in to the host.

Confirm Server Password
The password should be retyped into this text box in order to confirm that it has been entered correctly, given that it is not echoed in clear text.

Remote directory
The value in this text box is the full name of the directory on the FTP host to which the file is to be saved.

Rename file
When checked, this checkbox causes the router to store the uploaded files internally with a filename in the form "relnnnn" where nnnn is a number that is incremented for each new file received. When the file is relayed to the FTP host the original filename is used. When unchecked, the file is stored internally using its original filename. This parameter should be set if it a file having a filename longer than 12 characters is to be uploaded. This is due to the internal file system having the 8.3 filename format (i.e. autoexec.bat).

Transfer Mode ASCII / Binary
These two radio buttons select between the two possible file transfer modes, binary data or ASCII data.

Transfer Command STORE / APPEND
These two radio buttons select between the two possible storage methods, either append to or replace existing file.

Attempt to connect to the FTP Server n times
The value in this text box specifies the number of connection attempts that the router should make if the first attempt is not successful.

Wait s seconds between attempts
The value in this text box specifies the interval (in seconds) that the router should wait in between successive connections attempts.

Remain connected for s seconds after a file has been transferred
The value in this text box specifies how long (in seconds) that the router will maintain the connection to the FTP host after transferring a file.

If unable to relay file Delete File / Retain file
These two radio buttons select the behaviour with respect to storing the file if the router fails to connect to the FTP host (after retrying for the specified number of attempts). Select Delete File if the file should not be stored permanently. If the file is retained, manual intervention will be required to recover it at a later stage.

Note:
If the file is not retained, it will be lost if the power is removed from the router.

Email the file before storing or deleting it
The configuration options following this checkbox are normally disabled (they should appear "greyed out" in the browser). When this checkbox is checked, the parameters are enabled and data can be entered into the text boxes.

Use Email Template File
The value in this text box contains the name of the template file that will be used to form the basis of any email messages generated by the FTP Relay Agent. This would normally be the standard "**EVENT.EML**" template provided with the router but alternative templates may be created if necessary (refer to Email templates elsewhere in this manual).

To
The value in this text box is used to specify the email address of the recipient of email messages generated by the FTP Relay Agent.

From
The value in this text box is used to specify the email address of the router. In order for this to work, an email account must be in place with the Internet Service Provider.

Subject
This text box should contain a brief description of the content of the email.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
frelay	n	locuser	Up to 15 characters	Relay files for user locuser
frelay	n	ftphost	Up to 64 characters	to FTP Server ftphost
frelay	n	ftpuser	Up to 20 characters	Server Username
frelay	n	ftppwd	Up to 20 characters	Server Password
frelay	n	ftpdir	Up to 40 characters	Remote directory

Entity	Instance	Parameter	Values	Equivalent Web Parameter
frelay	n	norename	OFF,ON	Rename file
frelay	n	ascii	OFF,ON	Transfer Mode
frelay	n	appe	OFF,ON	Transfer Command
frelay	n	retries	0 - 2147483647	Attempt to connect to the FTP Server n times
frelay	n	retryint	0 - 2147483647	Wait s seconds between attempts
frelay	n	timeout	0 - 2147483647	Remain connected
frelay	n	savemode	OFF,ON	Delete/Retain file
frelay	n	smtp_temp	Up to 40 characters	Use Email Template File
frelay	n	smtp_to	Up to 100 characters	To
frelay	n	smtp_from	Up to 40 characters	From
frelay	n	smtp_subject	Up to 40 characters	Subject

Configuration – Network > FTP Relay > Advanced

Tx Buffer Size n bytes
The value in this text box specifies the size of the Tx socket buffer.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ftpcli	n	txbuf	0 - 2147483647	Tx Buffer Size

Configuration - Network > IP Passthrough

IP passthrough is a useful feature if a host computer or server on the local area network needs to have access to it from the Internet with a public IP address. With IP passthrough configured, all IP traffic, not just TCP/UDP is forwarded back to the host computer. This feature can be useful for applications that do not function reliably through network address translation.

In this configuration the local PC will share the public IP addressing information with the WAN side of the router.

Enable IP Pass-through
When checked, this checkbox enables IP passthrough mode.

Ethernet interface
The value in this text box specifies the Ethernet interface that the local PC is connected to.

PPP interface
The value in this text box specifies the PPP interface that will share its WAN address with the local PC.

Mode
This drop-down list selects the the mode of operation for the passthrough functionality. The available options are **Normal/28 bit mask** and **Fixed IP Address/32 bit mask**. The default is **Normal/28 bit mask**. When **Fixed IP/32 bit mask** mode of operation is selected, the DHCP server will provide a 32-bit subnet mask to the client and sets the address/subnet mask for the Ethernet interface to 192.168.1.1/32.

Pinhole Configuration
The following parameters are checkboxes that allow specific protocols to be excluded from the IP passthrough feature. An excluded protocol will terminate at the router instead of being forwarded to the local PC.

HTTP
When checked, this checkbox excludes HTTP from passthrough.

HTTPS
When checked, this checkbox excludes HTTPS from passthrough.

Telnet
When checked, this checkbox excludes Telnet from passthrough.

Telnet over SSL
When checked, this checkbox excludes SSL from passthrough.

SSH/SFTP
When checked, this checkbox excludes SSH/SFTP from passthrough.

SNMP
When checked, this checkbox excludes SNMP from passthrough.

iDigi
When checked, this checkbox excludes the iDigi protocol from passthrough.

Note:
This option only appears on models that support the iDigi remote management functionality.

GRE
When checked, this checkbox excludes GRE from passthrough.

Ping
When checked, this checkbox excludes the ICMP echo request from passthrough.

Other Ports
The list of TCP and UDP port numbers in this text box will be added to the list that will not be forwarded to the local PC (comma-separated).

Other Protocols
The list of protocol numbers in this text box will be added to the list that will not be forwarded on to the local PC (comma-separated).

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
passthru	0	enabled	OFF,ON	Enable IP Pass-through
passthru	0	ethadd	0 - 2147483647	Ethernet interface
passthru	0	pppadd	0 - 2147483647	PPP interface
passthru	0	mode	0,1 0 = Normal 1 = 32-bit mask	Mode
passthru	0	http	OFF,ON	HTTP
passthru	0	https	OFF,ON	HTTPS
passthru	0	telnet	OFF,ON	Telnet
passthru	0	telnets	OFF,ON	Telnet over SSL
passthru	0	ssh	OFF,ON	SSH/SFTP
passthru	0	snmp	OFF,ON	SNMP
passthru	0	idigi	OFF,ON	iDigi
passthru	0	gre	OFF,ON	GRE
passthru	0	ping	OFF,ON	Ping
passthru	0	ports	Comma-separated list of ports	Other Ports
passthru	0	protos	Comma-separated list of protocols	Other Protocols

Configuration – Network > UDP Echo

When enabled, the UDP echo client generates UDP packets that contain the router's serial number and ID and transmits them to the IP address specified by the configuration. When the remote router receives a UDP packet on a local port and UDP echo server is configured, it will echo the packet back to the sender. There may be more than one UDP echo instance available on the unit. Instance 0 is used when specifying the local port to listen on.

Configuration – Network > UDP Echo > UDP Echo n

There may be instances of the UDP echo task supported by the router (model-dependent). Each has its own configuration web page, described below. For the command line configuration, valid instance numbers start at 0 as normal.

Enable UDP Echo
This checkbox is unchecked by default – when checked, it reveals the configuration parameters associated with send UDP echo packets.

Send a UDP packet to IP address a.b.c.d port n every s seconds
The values in these three text boxes define the destination IP address for the UDP packets, the port number to which they should be sent and the sending interval. If the destination IP address is left blank, the router will not attempt to send any packets.

Use local port n
The value in this text box specifies which local port the router should listen on for UDP packets. If any UDP packets are sent to this port, the router will send a copy back to the IP address and port they were sent from.

Route via Routing table / Interface x,y
These two radio buttons select whether the router should use its routing table to determine how to send the UDP packets or whether it should use the specified interface. If the specific interface is selected, the interface is selected from the drop-down list. The options available are PPP and Ethernet. The interface instance is specified in the adjacent text box.

Only send packet when the interface is "In Service"
When checked, and the router is using the specified interface, this checkbox will prevent the router from sending UDP packets if the interface is out of service.

Do not send any data with the UDP packet
When checked, this check box causes the router to send only a single null data byte. This is useful to minimise packet size in circumstances where the interface has high data charges (e.g. W-WAN). When unchecked, the router will send packets that contain the router's serial number and ID as text.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
udpecho	n	dstip	Valid IP address a.b.c.d	Send a UDP packet to IP address a.b.c.d port n every s seconds
udpecho	n	dstport	0 - 65535	Send a UDP packet to IP address a.b.c.d port n every s seconds
udpecho	n	interval	0 - 2147483647	Send a UDP packet to IP address a.b.c.d port n every s seconds

Entity	Instance	Parameter	Values	Equivalent Web Parameter
udpecho	n	locport	0 - 65535	Use local port n
udpecho	n	userouting	OFF,ON	Route via Routing table
udpecho	n	ifent	PPP,ETH	Interface x,y
udpecho	n	ifadd	Valid interface instance 0 - 4294967296	Interface x,y
udpecho	n	onlyis	OFF,ON	Only send packet when the interface is "In Service"
udpecho	n	nodata	OFF,ON	Do not send any data with the UDP packet

Configuration – Network > QoS

The Quality of Service (QoS) functionality provides the means of prioritising different types of IP traffic. It is generally used to ensure that low priority applications do not "hog" the available bandwidth to the detriment of those having a higher priority. For example, this might mean that EPOS transactions carried out over XOT will be prioritised over HTTP-type traffic used for Internet access. Without some form of QoS, all IP packets are treated as being equal, i.e. there is no discrimination between applications.

The IP packet Type of Service (TOS) field is used to indicate how a packet should be prioritised. Using the top 6 bits of the TOS field, a router that supports QoS will assign a Differentiated Services Code Point (DSCP) code to the packet. This may take place within the router when it receives the packet or another router closer to the packet source may have already assigned it. Based on the DSCP code, the router will assign the packet to a priority queue. There are currently four such queues for each PPP instance within the router and each queue can be configured to behave a particular way so that packets in that queue are prioritised for routing according to predefined rules.

There are two principal ways in which prioritisation may be effected:

A priority queue can be configured to allow packets to be routed at a specific data rate (providing that queues of a higher priority are not already using the available bandwidth)

Weighted Random Early Dropping (WRED) of packets may be used as queues become busy, in an attempt to get the TCP socket generating the packets to "back off" its transmit timers, thus preventing the queue overflow (which would result in all subsequent packets being dropped).

QoS is a complex subject and can have a significant impact on the performance of the router. For detailed background information on QoS, refer to RFC2472 (Definition of the Differentiated Services Field).

In Digi TransPort routers, the classification of incoming IP packets for the purposes of QoS takes place within the firewall. The firewall allows the system administrator to assign a DSCP code to a packet with any combination of source/destination IP address/port and protocol. Details of how this is done are given in the section on firewall scripts.

When the routing code within the unit receives an incoming packet, it directs it to the interface applicable to that packet at that time (this is the case whether or not QoS is being applied). Just before the packet is sent to the interface, the QoS code intercepts the packet and assigns it to one of the available priority queues (currently 10 per PPP instance) based on its DSCP value.

Each priority queue has a profile assigned to it. This profile specifies parameters such as the minimum transmit rate to attempt, maximum queue length and WRED parameters.

The packet is then processed by the queue management code and either dropped or placed in the queue for later transmission.

There are a couple of configuration web pages associated with QoS functionality:

The ***Configuration – Network > QoS > DSCP Mappings*** page which contains parameters to configure DSCP operation and ***Configuration – Network > Queue Profiles*** page which contains parameters to manage the queue "profiles".

Each ***Configuration – Interfaces > Ethernet*** and ***Configuration – Interfaces > PPP*** instance page contains a QoS sub-page which control how QoS behaves on that particular interface.

When configuring QoS, be aware that the router supports ten queues, numbered from 0 to 9 and that DSCP codes range from 0 to 64.

Configuration – Network > QoS > DSCP Mappings

Each DSCP value must be mapped to a queue. These mappings are set up using this page.

Default
This drop-down list selects the default queue. When this is changed, any DSCP codes that are set to use the default will have their queue number changed.

DSCP
This column is simply a list of valid DSCP codes with an associated drop-down list box to the right.

Queue
Each of the DSCP codes in the left-hand column has a queue associated with it. To change the value from what is shown, select the desired value from the drop-down list.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
dscp	n	q	0 – 63 Default 4	Queue

Example command line commands.

To display a DSCP mapping from the command line, type the following:

```
dscp <code> ?
```

Where *<code>* is a valid DSCP code from 0 to 63, or 64 (but see note below).

To change the value of a parameter, use the following command:

```
dscp <code> q <value>
```

Where *<code>* is a valid DSCP code and *<value>* is from 0 to 9.

To set the default mapping value, enter the command:

```
dscp 64 q <value>
```

Where *<value>* is the default queue number required and has a value from 0 to 9.

Note:
DSCP code 64 is not actually a valid code but is used to set up the default priority.

Configuration – Network > QoS > Queue Profiles

Up to 12 distinct queue "profiles" may be defined using this page that may then be assigned to QoS queues as required. The queue profile determines how QoS queues with that profile assigned to them will behave.

Queue
This is the queue number that relates to the queues defined in the DCSP mappings page.

Minimum kbps
The value in this text box sets the minimum data transfer rate in kilobits/second that the router will try to attain for the queue.

Maximum kbps
The value in this text box sets the maximum data transfer rate in kilobits/second that the router will try to attain for this queue. This means that if the router determines that bandwidth is available to send more packets from a queue that has reached its Minimum kbps setting, it will send more packets from that queue until the Maximum kbps setting is reached.
Note that if the bandwidth on a queue should be restricted, setting the **Maximum kbps** value to the same as, or lower than the **Minimum kbps** value ensures that only the **Minimum kbps** setting will be achieved.

Maximum Packet Queue Length
The value in this text box specifies the maximum length of a queue in terms of the number of packets in the queue. Any packets received by the router that would cause the maximum length to be exceeded, are dropped.

WRED Minimum Threshold
The value in this text box specifies the minimum queue length threshold for using the WRED algorithm to drop packets. Once the queue length exceeds this value, the WRED algorithm may cause packets to be dropped.

WRED Maximum Threshold
The value in this text box specifies the maximum queue length threshold for using the WRED algorithm to drop packets. Once the queue length exceeds this value, the WRED algorithm will cause all packets to be dropped.

WRED Maximum Drop Probability (%)
The value in this text box sets the maximum percentage probability used by the WRED algorithm to determine whether or not a packet should be dropped when the queue length is approaching the WRED maximum threshold value.

Note:
If the length of a queue is less than the WRED minimum threshold value there is a 0% chance that a packet will be dropped. When the queue length is between the WRED minimum and maximum values, the % probability of a packet being dropped increases linearly up to the WRED maximum drop probability.

WRED Queue Length Weight factor
The value in this text box specifies a weighting factor to be used in the WRED algorithm when calculating the weighted queue length. The weighted queue length is based on the previous queue length and has a weighting factor that may be adjusted to provide different transmit characteristics. The actual formula used is:

new_length = (old_length * (1-1/2^n)) + (current_length * 1/2^n)
Small weighting factor values result in a weighted queue length that moves quickly and more closely matches the actual queue length. Larger weighting factor values result in a queue length that adjusts more slowly. If a weighted queue length moves too quickly (small weighting factor), it may result in dropped packets if the transmit rate rises quickly but will also recover quickly after the transmit rate tails off. If a weighted queue length moves too slowly (large weighting factor), it will allow a burst of traffic through without dropping packets, but may result in dropped packets for some time after the actual transmit rate drops off. The weighting factor should be selected carefully to suit the type of traffic using the queue.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
qprof	n	minkbps	0 - 2147483647	Minimum kbps
qprof	n	maxkbps	0 - 2147483647	Maximum kbps
qprof	n	qlen	0 - 2147483647	Maximum Packet Queue Length
qprof	n	minth	0 - 2147483647	WRED Minimum Threshold
qprof	n	maxth	0 - 2147483647	WRED Maximum Threshold
qprof	n	mprob	0 - 100	WRED Maximum Drop Probability (%)
qprof	n	wfact	0 - 2147483647	WRED Queue Length Weight factor

Command line examples.

To display a queue profile, enter the following command:

```
gqprof <instance> ?
```

Where *<instance>* is the number of the queue profile to be displayed.

To change the value of a parameter, use the following command:

```
qprof <instance> <parameter> <value>
```

To set the maximum throughput for queue profile 5 to 10kbps, enter the following command:

```
qprof 5  maxkbps 10
```

Configuration – Network > Timebands

Digi TransPort routers support "Time Bands" which are used to determine periods of time during which PPP interfaces allowed or prevented from activating. For example, a router in an office could be configured so that the ADSL PPP interface is only raised on weekdays. Time Bands may only be applied to PPP instances.

Time Bands are specified by a series of "transition" times. At each of these times routing is either enabled or disabled. The default state for a Time Band is **On** which means that PPP instances that are associated with unconfigured Time Bands will operate normally. The router supports four Time Band configurations.

Note:
An entry is made in the event log whenever a Time Band transition occurs.

Whether or not Time Bands are enabled for a particular PPP instance is controlled by the settings in a table having the following columns:

Interface
This column simply lists the available PPP instances.

Enable
This column contains checkboxes, each checkbox controls whether or not Time Bands are enabled for the PPP instance in the left-hand column of the row. Check the checkbox to enable Time Bands for the associated PPP instance.

Timeband
This drop-down list selects which of the four available Time Band instances should be associated with the PPP instance.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	tband	0 - 3	Timeband

The default state of this parameter is blank.

Configuration – Network > Timebands > Timeband n

These four pages each control the configuration of one Time Band instance. Configuration is controlled by a table, having the parameters described below. Up to ten transitions may be configured.

Days
There is a selection of checkboxes in this column which are used to select which days of the week the Time Band transitions apply to. Days may be selected individually or in groups for convenience. So, for instance, to select all the days of the week, check the "**All**" checkbox. To select the weekend only, check the "**Sat->Sun**" checkbox. To select weekdays only, check the "**Mon->Fri**" checkbox.

Time
The value in this text box is the transition time. This is specified in 24-hour format with a colon separator between the hours and minutes.

State
This drop-down list selects the routing state which can be **On** or **Off**. (For convenience, the state of this parameter toggles for each new addition so if an on transition is configured, the default state for the next addition will be **Off**).