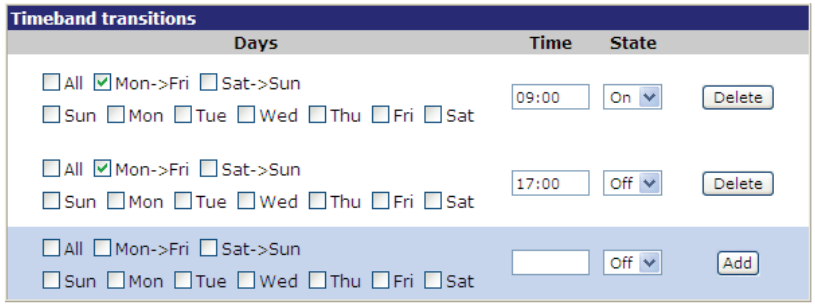
The following screenshot shows a PPP instance configured so that routing is allowed on weekday from 09:00 to 17:00. Clicking the **Add** button adds the entry into the table. Once an entry has been added to the table, it may be removed by clicking the associated **Delete** button. As mentioned previously, this Time Band instance is activated by navigating to the associated PPP Time Band (previous page) configuration page and clicking the Enable checkbox, or by entering the equivalent command line command.



Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
tband	0 - 3	days	ALL,MF,Mon, Tue,Wed,Thu,Fri,S at,Sun	Days
tband	0 - 3	time	HH:MM	Time
tband	0 - 3	state	OFF,ON	State

Command format:

tband <instance> <days#> <days>

tband <instance> <time#> <time>

tband <instance> <state#> <on|off>

To specify multiple days, separate the days with a comma, e.g. **Mon**,**Wed**,**Fri**. The abbreviation "**MF**" is used to specify Monday to Friday.

Example commands.

To allow PPP routing only on weekdays between 9:00 a.m. and 5:30 p.m. enter the following commands:

tband 0 days 0 mf

tband 0 time0 9

tband 0 state0 on

tband 0 days1 mf

tband 0 time1 5:30

tband 0 state1 off

Configuration – Network > Advanced Network Settings

The settings described in this web page are "advanced" in the sense that in the vast majority of configurations and implementations they should not require changing.

Secondary IP Address a.b.c.d
The value in this text box assigns an additional IP address to the router that is not associated with any particular interface. The router will respond directly to incoming traffic for this address, i.e. it will not attempt to onward route any IP packets for this address.

When connected to a Serial interface using TCP

Advertise an MSS of n bytes
The value in this text box sets the maximum segment size used/advertised by an asynchronous serial port connected to TCP sockets.

Use a Rx Window size of n bytes

The value in this text box sets the Rx window size used/advertised by an asynchronous serial port connected to TCP sockets.

Default SSL version for outgoing connections
This drop-down menu box selects which version of the SSL protocol to use in the "tcpdial" command. The options are:

- Auto, which allows the server to select the version.
- TLSv1 only
- SSLv2 only
- SSLv3 only.

Some servers are configured to work with a particular version, and unless this version is specifically requested, the connection attempt will fail.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
cmd	n	sec_ip	Valid IP address	Secondary IP address a.b.c.d
sockopt	n	asymss	0 - 2147483648	When connected to a serial interface using TCP Advertise an MSS of n bytes
sockopt	n	asyrxwin	0 - 2147483648	Use a Rx Window size of n bytes
sockopt	n	sslver	0 – 3 0 = Auto 1 = TLSv1 2 = SSLv2 3 = SSLv3	Default SSL version for outgoing connections

Configuration - Network > Advanced Network Settings > Socket Settings

Default source IP address interface x,y
The values in these two text boxes define the interface (None,PPP,ETH) and the instance number of the interface to use as a source address for IP when not using the interface that the socket was created on.
The router creates general-purpose sockets automatically when the controlling application requests them. As, for example, when TPAD calls are made over IP or XOT. Normally, the source address used by the socket will be that of the outgoing interface (usually PPP). However, for some applications such as when setting up a VPN, it may be necessary to specify that the socket uses a different source address such as that of the local Ethernet port. This parameter is used to specify the interface from which the source address should be derived.

Note:
Even when this parameter is not configured, the IP address from the interface on which the socket was created 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.

Connect Timeout s seconds
The value in this text box is used to specify the amount of time after which a TCP socket may remain idle before being closed. If the value is set to 0 the socket may remain open indefinitely.

TCP socket inactivity timer s seconds
The value in this text box specifies the maximum period of inactivity (in seconds) that may occur before and open TCP/IP socket is closed. The default value is 300 seconds (five minutes) and should not normally require altering.

TCP socket keep-alive s seconds
The value in this text box specifies the amount of time (in seconds) between sending "keep-alive" messages over open TCP connections. The purpose of these messages is to prevent a connection from closing even when no data is being transmitted or received. The default value of this parameter is zero which disables keep-alive messages.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
sockopt	n	gp_ipent	0,PPP,ETH	Default source IP address interface x,y
sockopt	n	gp_ipadd	Valid interface number	Default source IP address interface x,y
sockopt	n	sock_connto	0 - 2147483648	Connect Timeout s seconds
sockopt	n	sock_inact	0 - 2147483648	TCP socket inactivity timer s seconds
sockopt	n	sock_keepact	0 - 2147483648	TCP socket keep-alive s seconds

Configuration – Network > Advanced Network Settings > XOT Settings

Default source IP address interface x,y
The values in these two text boxes specify the interface (None,PPP,ETH) and instance number of that interface that IP address that XOT sockets should use instead of the interface that the socket was created on.

Note:
Even when this parameter is not configured, the IP address from the interface on which the socket was created will be used. The source address specified in this parameter will only be used if it will cause the traffic to match an Eroute and therefore be sent using IPsec or GRE.

NB of XOT listening sockets
The value in this text box specifies the maximum number of XOT sockets available. This may be used to reduce the number of XOT sockets in order to free up more general-purpose sockets for other purposes. The default value of 0 enables the maximum number of XOT sockets available.

Maximum ACK time for XOT data
The value in this text box sets the maximum time allowance for a remote unit to acknowledge TCP data transmitted by a unit's socket. If this timer expires, the socket is aborted. The default value of 0 disables the timer.

Note:
There is no requirement for the remote unit to acknowledge received data immediately, therefore setting this parameter to too small a value is not recommended. Some stacks delay sending TCP ACKs in order that they can be incorporated with data sent by the application.

Do not deactivate outgoing XOT sockets when interface disconnects
When checked, this checkbox sets outgoing XOT sockets not to close when the interface they are using disconnects.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
sockopt	n	xot_ipent	Valid interface type, ETH, PPP	Default source IP address interface x,y
sockopt	n	xot_ipadd	Valid interface number	Default source IP address interface x,y
sockopt	n	xot_listens	0 - 2147483648	NB of XOT listening sockets
sockopt	n	xot_maxack	0 - 2147483648	Maximum ACK time for XOT data

Configuration – Network > Advanced Network Settings > Backup IP Addresses

This page contains a table that is used to specify alternative IP addresses to use when the router fails in an attempt to open a socket. These addresses are used only for socket connections that originate from the router and are typically used to provide back-up for XOT connections, TANS (TPAD answering) connections or any application in which the unit is making outgoing socket connections.

When a backup address is in use, the original IP address that failed to open is tested at intervals to check if it has become available again. Additionally, at the end of a session, the unit will remember when an IP address has failed and use the backup address immediately for future connections. When the original IP address becomes available again, the router will automatically detect this and revert to using it.

The table has the following four column headings:

IP Address a.b.c.d
This text box should contain the original IP address to which the back-up address relates.

Backup IP address a.b.c.d
This text box should contain the backup address to try when the router fails to open a connection to the previous IP address.

Retry Time s (seconds)
This text box contains the length of time (in seconds) that the router will wait between checks to see if a connection can be made to **IP Address**.

Try Next
In the case that a connection to the primary IP address has just failed, this text box determines whether a connection to the backup IP address should be attempted immediately or when the application next attempts to open a connection. When checked, the socket will attempt to connect to the backup IP address immediately after the connection to the primary IP address failed and **before** reporting this failure to the calling application, e.g. TPAD. If the backup is successful this means that the application will not experience any kind of failure even though the router has connected to the backup IP address.
When unchecked, the socket will report the failure to connect back to the calling application immediately after the connection to the primary IP address has failed. The router will not try to connect to the backup IP address at this stage. The next time that the application attempts to connect to the same IP address, the router will instead, automatically connect to the backup IP address.

As is usual for these tables, the Add button and Delete button are used to add and delete entries to and from the table respectively.

Send "Backup IP" system messages to IP Address: a.b.c.d
The IP address in this text box specifies the destination to which system messages notifying of the unavailability of an IP address should be sent. This allows the router to send UDP messages to other routers to notify them that an IP address has become available/unavailable. Devices that receive the IP address available/unavailable messages Will search their own backup IP address tables for the IP addresses indicated and tag those addresses as available/unavailable as appropriate.

Chaining IP Addresses
It is possible to chain backup IP addresses by making multiple entries in the table.
For example, if the backup IP address for the original IP address appears as the IP address in the next row, along with a new backup IP address for that IP address, then when, the original IP address becomes unavailable, the router will try the backup IP address and if that is unavailable, the router will try its backup IP address and so on. To make this example more concrete, say the original IP address is 192.168.0.1 with a backup IP address of 192.168.0.2, then setting the IP address in the next row to 192.168.0.2 with a backup IP address of 192.168.0.3 will cause the router to try all these IP addresses in succession.

Note:
The length of time that it takes for a connection to an IP address to fail is determined by the Connect timeout parameter on the ***Configuration – Network > Advanced Network Settings > Socket Settings*** web page.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ipbu	n	IPaddr	Valid IP address a.b.c.d	IP Address a.b.c.d
ipbu	n	BUIPaddr	Valid IP address a.b.c.d	Backup IP Address a.b.c.d
ipbu	n	retrysec	0 - 2147483648	Retry Time s (seconds)
ipbu	n	donext	OFF,ON	Try Next
sarsys	0	dest	Valid IP address a.b.c.d	Send "Backup IP" system messages to IP address a.b.c.d

Configuration - Network > Legacy Protocols

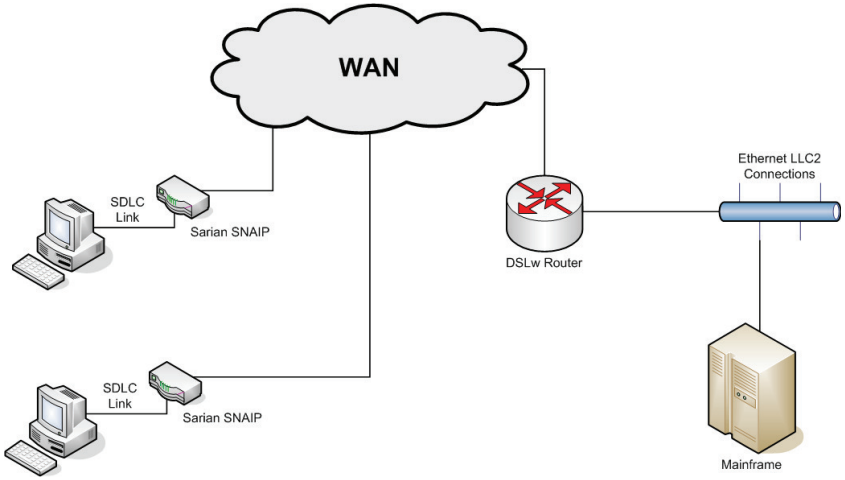
Older protocols that existed before TCP/IP became dominant are often referred to as legacy protocols. Examples of legacy protocols are X.25, SNA and LAPB.

Digi TransPort routers are capable of connecting to legacy networks such as X.25. They are also capable of simulating a legacy network so that equipment that in the past would have connected to a legacy network can connect to the Digi TransPort router instead. Thus old equipment can be connected to modern networks such as HSUPA.

Configuration - Network > Legacy Protocols > SNA over IP

The unit is capable of sending Systems Network Architecture (SNA) traffic over TCP/IP, using the DLSw protocol, this is often called SNAIP. The unit is also capable of sending HDLC traffic over TCP/IP.

SNA uses Synchronous Data Link Control (SDLC) which is an unbalanced mode in which there is one master station and 1 or more secondary stations. Each secondary station owns a station address and can only respond when this address has just been polled by the master. A typical scenario is shown in the diagram below:



Configuration - Network > Legacy Protocols > SNA over IP > SNAIP 0

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

Send SNAIP traffic over interface
This setting determines which physical interface is to be used for carrying SNAIP data. This can be set to either "ISDN", "Serial Port" or "SharedPort". If "ISDN" is selected then SNAIP data is carried over the ISDN BRI physical interface. By selecting "Serial Port", SNAIP data can be routed to either serial "Port 0" or serial "Port 1" (operating in synchronous mode). To configure Port 0 or Port 1 for synchronous operation refer to the ***Configuration - Network > Interfaces > Serial > Serial Port x > Sync Port x***.

If "Shared Port" is selected, the drop down list next to "Shared Port" specifies the SNAIP instance that has sync port configured. When sync port sharing is enabled only one SNAIP instance can currently own the sync port. Other SNAIP instances however can share this sync port in the event that there is more than one terminal residing on a multi-drop sync line In this situation with multiple terminals, each terminal station will operate a DLSw state independently of all other stations.

The SNAIP parameter "Priority" is used to select the SNAIP instance to use when more than one is available; the highest number being given preference.

As an example consider that 4 SNAIP instances to all share sync port 0. To do this, configure SNAIP 0 in the usual way on "PORT 0" and then configure SNAIP instances 1,2 & 3 to use "SharedPort" and "Sync Port from SNAIP 0"

Use protocol
This parameter sets the appropriate protocol for the interface. Choose "LAPB", "SNA" for SDLC or "RAW" for raw mode in which all L2 frames are transmitted and received. You can also choose "RAW_NOHDR" for raw mode with no DLSw headers.

Allow this unit to answer calls
If this parameter is set to "On", the unit will answer incoming calls on the relevant LAPB session. To prevent the unit from answering incoming calls on this LAPB session set the option to "Off". This setting is only relevant when the interface is set to ISDN.

Only accept calls with MSN ending with
This parameter provides the filter for the ISDN Multiple Subscriber Numbering facility. It is blank by default but when set to an appropriate value with answering calls parameter above enabled, it will cause the unit to answer incoming calls only to ISDN numbers where the trailing digits of the called number match the MSN value. For example, setting the MSN parameter to 123 will prevent the unit from answering any calls to numbers that do not end in 123. This setting is only relevant when the interface is set to ISDN.

Only accept calls with sub-address ending with
This parameter provides the filter for the ISDN sub-addressing facility. It is blank by default but when set to an appropriate value, with answering calls parameter above enabled, it will cause the unit to answer incoming ISDN calls only where the trailing digits of the sub address called match the Sub-address value. For example, setting the Sub-address to 123 will prevent the unit from answering any calls where the sub-address called does not end in 123. This setting is only relevant when the interface is set to ISDN.

Assume station exists (Do not send TEST frames)
When this parameter is enabled TEST frames are not transmitted and the TEST response is not expected. Instead the unit assumes the station exists and proceeds with the protocol as if the DLSw has received the TEST response.

Toggle DCD output each time the DLSw protocol enters the DISCONNECTED state
When this parameter is set to "On", the DCD (Data Carrier Detect) output will turn off briefly each time the DLSw protocol enters the DISCONNECTED state. Thus any attached equipment that needs to will see signals changing state.

Sync port should not send or receive data when WAN link is down
This parameter causes the Sync port to be deaf and dumb (and have DCD low) while the connection with the WAN is down. This is so that some terminals don't get too excited just because L2 is up and think everything else should be working (and go into a management error state).

Configuration - Network > Legacy Protocols > SNA over IP > SNAIP 0 > SNA Parameters

Router to be Master on an unbalanced link
Enable this parameter if this unit is to be the Master in an unbalanced link, or "Off" if the unit is to be a secondary station.

Polling Response Time
The poll time in milliseconds (if the unit is the master in an unbalanced link).

Polling Stations Addresses
This parameter lists the station addresses on the data link as a comma-separated list of hex values (e.g. "c1,d1" for station addresses 0xc1 & 0xd1). This parameter is only applicable in SNA mode.

SAPs
This parameter contains a list of SAP values which correspond to the station addresses.

DSAPs(blank=default)
This is the Destination SAP value, if left blank the SAP value above is used.

Send Null XID (XID with no Data)
When this parameter is set to "On" a null XID SSP message will be sent when the unit has just received or sent a REACH ACK SSP message.

Send XID with Data
This parameter is a hex string to define binary data and defines an XID SSP message that would be sent in response to a XIDFRAME SSP message being received.

Tx Turn Around Time
This parameter specifies the time in milliseconds between receiving a frame from an outstation and transmission back to the same station. If this parameter is set to "0" this is disabled and the Digi can respond immediately. The minimum non-zero value is 10ms.

Mode
This parameter is used to define the mode in balanced links. In unbalanced links (like SNA/SDLC) the mode is defined by being master or the station, but for balanced links (like HDLC).

N400 counter
This is the standard LAPB retry counter. The default value is 3 and it should not normally be necessary to change this.

RR Timer
This is a standard LAPB/LAPD "Receiver Ready" timer. The default value is 10,000ms (10 seconds) and it should not normally be necessary to change this.

T1 timer
This is a standard LAPB timer. The default value is 1000 milliseconds (1 second) and under normal circumstances, it should not be necessary to change it.

T200 timer
This is the standard LAPB re-transmit timer. The default value is 1000 milliseconds (1 second) and under normal circumstances, it should not be necessary to change it.

Window Size
This parameter is used to set the X.25 window size. The value range is from 1 to 7 with the default being 7.

Disconnect link if there has been no activity for x seconds
This parameter may be used to specify the length of time (in seconds) before the link is disconnected if there has been no activity. If this parameter is zero or not specified, then the inactivity timer is disabled. It is useful to set this to a short period of time (say 120 seconds) when an LAPB instance is being used over ISDN. This timer can be used as a backup hang-up timer thus saving ISDN call charges. When LAPB is being used on a synchronous port, this parameter should normally be set to 0.

Configuration - Network > Legacy Protocols > SNA over IP > SNAIP 0 > SSP (WAN) Parameters

Virtual MAC Address
Virtual MAC address. The host uses MAC addresses and SAP values as the addressing values to discriminate between circuits (in much the same way as an IP address & TCP port define an addressing point for a TCP socket). This is the MAC address that is reported as part of the DLSw protocol.

Virtual MAC Address of Peer
The Virtual MAC address of the peer.

IP address of the Peer DLSw unit
The IP address of the peer DLSw unit.

Listen on Port
The read IP port. The TCP socket SNAIP listens on.

Use Port x if this unit starts the DLSw protocol
The write IP port. This TCP socket will be opened by the unit if it needs to start the DLSw protocol.

Use interface for source IP address
Setting this parameter to a "PPP" or "ETH" instance will cause the source address used by this SNAIP instance to match that of the Ethernet or PPP interface specified.

Close TCP connection if it is idle for x secs
This specifies the maximum period of inactivity (in seconds) that may occur before an open TCP/ IP socket is closed. The default value is 300 seconds (5 minutes) and should not normally require altering.

DLSw Ver
This parameter controls the DLSw version to be used. Set to 0 (default) for version 1, set to 2 for version 2.

DLSw Role
When this parameter is set to "Active", and the unit is in SNA mode, then this DLSw switch will actively connect to the remote DLSw switch.

DLSw Window
This parameter is used to set the DLSw window size. The value range is from 10 to 100 with the default being 20.

UDP Capable
This controls the UDP transmission of DLSw SSP packets. Reception is always enabled for version 2 support. If set to "OFF", the state transitions occur just like DLSw version 1 but the Digi will indicate it is version 2 capable.

Use 1 socket
When this parameter is set to "On" then only one socket is used for both read and write data. This is useful if the unit is behind a NAT box and incoming connections are not possible. This parameter can also be set to "Compatible", in which mode both sockets are open to start with and then after a negotiation one of the sockets is dropped.

Include MAC Exclusivity Capability
On or Off. Set this parameter to "On" in order to include the MAC exclusivity value in the capabilities exchange message.

MAC Exclusivity Value
See above.

Ignore unsolicited response frames
When this parameter is enabled, the unit will ignore unsolicited response frames.

Wait for Contact before progressing to CONNECT PENDING state
During the DLSw negotiation phase and when XID messages are being exchanged this parameter controls which end sends the "CONTACT" message. Normally this would be off in which case this unit would send the "CONTACT" message, but if this parameter is set we would not send this message but instead wait for it to be sent to us before progressing in the DLSw state machine.

Make immediate connection attempts before backing off
This parameter defines the number of successive connection attempts before backing off for the number of seconds (default 30) defined in the "Backoff for x seconds" parameter. This backoff might be necessary in the case where a servers is behind a firewalls that detects too many successive connection attempts in a certain time frame.

Backoff for x seconds before attempting to connect again
When backing off because of too many failed consecutive connection attempts this parameter defines the time in seconds that we should remain idle for before attempting another connection.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
snaip	x	l1iface	ISDN, Port, SharedPort	Send SNAIP traffic over interface
snaip	x	l1nb	0 – 255 (Select LAPB, Port or SharePort instance)	Send SNAIP traffic over interface
snaip	x	protocol	LAPB, SNA, RAW,	Use protocol

Entity	Instance	Parameter	Values	Equivalent Web Parameter
			RAW_NOHDR	
snaip	x	ans	1 = enabled, 0 = disabled	Allow this unit to answer calls
snaip	x	msn	text	Only accept calls with MSN ending with
snaip	x	sub	text	Only accept calls with sub-address ending with
snaip	x	autocontact	1 = enabled, 0 = disabled	Assume station exists (Do not send TEST frames)
snaip	x	dcd_toggle	1 = enabled, 0 = disabled	Toggle DCD output each time the DLSw protocol enters the DISCONNECTED state
snaip	x	l1oos	1 = enabled, 0 = disabled	Sync port should not send or receive data when WAN link is down
snaip	x	master	1 = enabled, 0 = disabled	Router to be Master on an unbalanced link
snaip	x	pollresp	0 - 2147483647	Polling Response Time
snaip	x	stations	text	Polling Stations Addresses
snaip	x	saps	text	SAPs
snaip	x	dsaps	text	DSAPs(blank=default)
snaip	x	send_xid_null	1 = enabled, 0 = disabled	Send Null XID (XID with no Data)
snaip	x	xid_data	text	Send XID with Data
snaip	x	turntxtim	0 - 2147483647	Tx Turn Around Time
snaip	x	dtemode	1 = DTE, 0 = DCD	Mode
snaip	x	n400	0 - 255	N400 counter
snaip	x	tnoact	1000 - 60000	RR Timer
snaip	x	t1time	1 - 60000	T1 timer
snaip	x	t200	1 - 60000	T200 timer
snaip	x	window	1 - 7	Window Size
snaip	x	tinact	0 - 3000	Disconnect link if there has been no activity for x seconds
snaip	x	vmac	Text (valid MAC address)	Virtual MAC Address
snaip	x	peervmac	Text (valid MAC address)	Virtual MAC Address of Peer
snaip	x	IPaddr	Text (valid IP address)	IP address of the Peer DLSw unit
snaip	x	r_IPport	0 - 65535	Listen on Port
snaip	x	w_IPport	0 - 65535	Use Port x if this unit starts the DLSw protocol

Entity	Instance	Parameter	Values	Equivalent Web Parameter
snaip	X	srcipent	auto, eth, ppp	Use interface for source IP address
snaip	x	srcipadd	0 - 255	Use interface for source IP address
snaip	x	sock_inact	0 - 2147483647	Close TCP connection if it is idle for x secs
snaip	x	ver	0 - 2	DLSw Ver
snaip	x	passive	0 = active, 1 = passive	DLSw Role
snaip	x	dlswwindow	1 - 100	DLSw Window
snaip	x	udp_cap	1 = enabled, 0 = disabled	UDP Capable
snaip	x	use1sock	On, Off, Compatible	Use 1 socket
snaip	x	inc_mac_exc	1 = enabled, 0 = disabled	Include MAC Exclusivity Capability
snaip	x	mac_exc_val	0 - 1	Mac Exclusivity Value
snaip	x	iunsolresp	1 = enabled, 0 = disabled	Ignore unsolicited response frames
snaip	x	waitforcontact	1 = enabled, 0 = disabled	Wait for Contact before progressing to CONNECT PENDING state
snaip	x	con_attempts	0 - 2147483647	Make immediate connection attempts before backing off
snaip	x	con_boff_time	0 - 2147483647	Backoff for x seconds before attempting to connect again

Forcing SNAIP to use a specific instance

If several SNAIP instances are sharing an ASY port, a switchover to a specific instance can be initiated by issuing "**`snasw x`**". Where x is the SNAIP instance number, this instance must be available to go online or this command will fail.

To revert back and use the default instance, issue the "**`snadis x`**" command. Normal priorities will be used to determine which SNAIP instance gets to use the SYNC port.

Configuration - Network > Legacy Protocols TPAD

TPAD is a simplified version of the X.25 PAD specification that is commonly used for carrying out credit-card clearance transactions. Digi units support the use of TPAD over:

ISDN B and D-channels

TCP

UDP

SSL

XoT

Automatic back-up between any two of these "layer 2 interfaces" or "transport protocols" is supported.

For further information on using TPAD please refer to Digi technical support and ask for a copy of "TG2 - Introduction to TPAD and X.25".

Configuration - Network > Legacy Protocols TPAD n

Use TPAD over interface
This section is used to select whether the TPAD instance will use ISDN B-channel X.25, ISDN D-channel X.25, TCP, VXN or SSL as the transport protocol. For ISDN D-channel operation, ensure that the "LAPD" option is selected. For ISDN B-channel operation or operation through a synchronous port, select "LAPB". In the case of LAPB and LAPD it is also possible to specify an interface number. This parameter specifies which LAPB or LAPD instance to use for the relevant TPAD instance. Select "0" or "1" for LAPB or "0" or "1" for LAPD. When using LAPB with ISDN this parameter may be set to "255", which means use any free LAPB instance. This is useful when more than 2 POS terminals are connected to the router and the acquirer does not support multiple Switched Virtual Circuits (SVCs) on a single B-Channel. A value of 254 will use an available LAPB instance but will use the same ISDN B channel if two calls are attempted to the same ISDN number at the same time. (All services that the POS terminals may dial must support multiple SVCs if using the setting 254.)

Use backup interface
This section is used to specify a backup interface that will be used automatically if the call to the primary interface fails. Note that the primary interface will be tried first for every new call attempt.

Configuration - Network > Legacy Protocols TPAD n > ISDN settings

Use number x to make outgoing ISDN calls
This parameter may be used to specify an ISDN number. This is used in cases where no ISDN number is provided with the ATD command when making an outgoing call.

Use prefix x
This parameter is used to specify a dialling code that the unit will place in front of the telephonenumber that is issued by the terminal in the ATD command. For example, if the Prefix # was set to 0800 and the number specified by the terminal in the ATD command was 123456, the actual number dialled by the unit would be 0800123456.

Remove prefix x from number in ATD command
This parameter is used to specify a dialling prefix that is normally inserted by the terminal in the ATD command that is removed by the unit before dialling takes place. For example, if the Prefix removal # was set to 0800 and the terminal issued an ATD command containing 0800123456 then the actual number dialled by the unit would be 123456.

Use suffix x
The Suffix # parameter may be set to contain additional numbers that are dialled after the number specified by B-channel ISDN #. For example, if B-channel ISDN # was set to 123456 and Suffix # was set to 789, the actual number dialled would be 123456789.

On the main interface Deactivate LAPB session x seconds after TPAD X.25 call has been cleared
Once a TPAD X.25 call has been cleared, the unit will keep a LAPB instance active for the length of time set by this parameter. This is to allow further TPAD transactions to take place without having to make another ISDN call. The default value of 10 seconds should be acceptable for most applications. The value of 1 is a special value which means terminate layer 2 immediately the transaction is finished. (When the X.25 call is cleared.)

If you select LAPD as the TPAD layer-2 interface, this value will automatically be set to 0 to disable layer-2 deactivation. You may still override the 0 setting by entering a new value but note that most network service providers prefer that LAPD connections are not repeatedly deactivated.

On the backup interface Deactivate LAPB session x seconds after TPAD X.25 call has been cleared.
This is equivalent to the deactivation timer above but applies only to backup calls.

With X.25 over ISDN D-channel mode

Send X.25 RESTART packets
d

Delay the X.25 RESTART packets by x milliseconds
d

Configuration - Network > Legacy Protocols TPAD n > X.25 settings

Default X.25 Packet Size
This parameter specifies the default X.25 packet size to be used for TPAD transactions.

Use NUA
This parameter specifies the X.25 Network User Address to be used for outgoing X.25 calls if no NUA is specified in the call string.

Use NUI
This specifies the X.25 Network User Identifier to be used for outgoing X.25 calls if no NUI is specified in the call string.

LCN
The unit supports up to eight logical X.25/TPAD channels. In practice, the operational limit is determined by the particular service to which you subscribe (usually 4).
Each logical channel must be assigned a valid Logical Channel Number (LCN). The LCN parameter is the value of the first LCN that will be assigned for outgoing X.25 CALLs. The default is 1027. For incoming calls, the unit accepts the LCN specified by the caller.

LCN direction
This parameter determines whether the X.25 LCN used for outgoing TPAD calls is incremented or decremented from the starting value when multiple TPAD instances share one layer 2 (LAPB or LAPD), connection. The default is "DOWN" and LCNs are decremented, i.e. if the first CALL uses 1024, the next will use 1023, etc. Setting the parameter to "UP" will cause the LCN to be incremented from the start value.

On the backup interface

Use NUA
The LCN parameter is used to set the first LCN that will be used for the backup interface.

Use NUI
This specifies the X.25 Network User Identifier to be used for outgoing X.25 calls if no NUI is specified in the call string for the backup interface.

LCN
The LCN parameter is used to set the first LCN that will be used for the backup interface.

LCN direction
This parameter determines whether the LCN used for the backup X.25 interface is incremented or decremented from the starting value when multiple X.25 instances share a single layer 2 connection.

Report our NUA as n to the X.25 network
This is the NUA that the unit will report to the X.25 network as its own NUA when making a call. It is also known as the calling NUA. Often the X.25 network will override this NUA.

Call User Data
This specifies a text string that will be placed in the Call User Data field of an outgoing X.25 call request packet. Whether or not this information is required will depend on the X.25 host that you are connecting to. In most cases the information is not required.

X.25 calls

These setting controls how transactions are sent to the host when TPAD is running in "direct mode".

One per transaction
Only one transaction is allowed per call.

Allow consecutive transactions
Multiple transactions are allowed per X.25 call, but not until a response has been received from the host.

Allow concurrent transactions
Multiple transactions per X.25 call are allowed irrespective of whether a response has been received from the host.

Use ASCII character x as the delimiter character
This parameter specifies the character used to separate a main NUA from a backup NUA, and a main NUI from a backup NUI in an ATD command. The default value is the ASCII "!" character (decimal 33).

Forward mode time x milliseconds
If not framed with STX and ETX characters, can still have data formatted after this period.

Create an event when reply from X.25 host matches
This parameter can be used to generate a "Data Trigger" event (code 47) when the reply from the X.25 host contains the string specified in this parameter. It is possible to configure the unit to generate an email alert message when this event occurs. See "LOGCODES.TXT" for a complete list of events.

Configuration - Network > Legacy Protocols TPAD n > XoT/TCP settings

Connect to remote IP address
When the unit is configured for XOT or TCP socket mode, this parameter is used to specify the IP address of the host to which the TCP/XOT connection is made. Note that the transport protocol must be set to TCP.

Port
When making a TCP socket connection (i.e. the transport protocol has been set to TCP not XoT), this parameter must be used to specify the TCP port number to use.

IP length header
When making a TCP socket connection (i.e. the transport protocol has been set to TCP), setting this parameter to "On" will pre-pend the data sent to the host with a 2 byte length header. The 2 byte length header will not be included in the length calculation. When set to "8583 Ascii 4 byte", the IP length header will conform to the ISO 8583 format. When set to "On Inclusive" it will pre-pend a 2 byte length header and the calculation of the length will include the 2 bytes of the length header.

Configuration - Network > Legacy Protocols TPAD n > TPAD Settings

Use Terminal ID (TID)
The Terminal ID parameter can be used to insert or replace a Terminal ID in the APACS 30 string.

> **Replace TID provided by connected terminal with configured TID**
> When this check box is ticked, any Terminal ID provided by a connected terminal will be replaced by the ID set in the Use Terminal ID field above.

The TID will be become inactive in n seconds.
This specifies the time in seconds before the Terminal ID is considered inactive. Local authorisations may be configured to occur on active TIDs (terminal Ids), so this parameter defines how long a time (without transactions) must pass for a TID to change from active to inactive.

Use TID xxxxxxxxx with incoming APACS 50 polling calls
This parameter specifies the terminal ID to associate with this TPAD instance when answering an incoming APACS 50 polling call.

Use merchant Number
This parameter can be used to insert a merchant number into the APACS 30 string when the locally connected equipment does not transmit a merchant number.

Use Connect String
This parameter specifies a string to be sent to the user's terminal when an outgoing TPAD call has been connected, instead of the normal ENQ character. For example, this might be used to make a TPAD connection look like a PAD connection by specifying "CON COM" as the connect string.

The polling character set is c
This parameter is a string that specifies a character or set of characters to be treated as polling characters. The unit will respond to any of these characters using ACK. This parameter should normally be left blank.

Enable Message Numbering
When this check box is ticked the unit will override the message numbering of the local equipment and substitute its own message numbering in the APACS 30 data. This is useful when the locally connected equipment does not automatically increment the APACS 30 message number.

Disable Direct Mode
Enabling this setting will prevent the unit from automatically using Direct Mode (see below) when it receives an APACS 30 packet without any call set-up.

Boot to Direct Mode
Direct mode is a mode of operation whereby the unit automatically routes APACS 30 packets to their destination without the terminal having to perform any call control. If this parameter is set to "Yes", then the next time the unit is rebooted it will operate in direct mode. For Direct Mode to work you must set up the appropriate addressing information (e.g. Transport protocol, NUA, NUI, IP address etc). If this parameter is not enabled the unit will still try to use direct mode if it detects that it is required (due to the absence of call control information). This parameter can be used in certain cases where for some reason the unit cannot automatically determine whether or not to use direct mode.

> **Use response code n in "unable to authorise" message**
> This parameter only applies when the unit is operating in direct mode. In cases where the unit is unable to send the APACS 30 packet to the remote host, it replies to the terminal with an "unable to authorise" message. By default, this message contains a response code 05 which means declined. Entering a number for this parameter causes the unit to use that number in place of the default response code. A value of zero for this parameter prevents the unit from replying.
>
> **Clearing time n milliseconds**
> This parameter defines the clearing time in milliseconds that an X.25 call will be left "open" after receiving a response from the host. Each response from the host resets this timer.

Delay transmitting the APACS 30 string for x milliseconds after connecting to X.25 host
Setting this parameter will cause the unit to pause for the specified number of milliseconds in between successfully connecting to the remote X.25 host and transmitting the APACS 30 string.

Retransmit APACS 30 string if error detected
Ticking this check box will cause the unit to retransmit the APACS 30 string to the terminal if an error is detected. (e.g. no ACK received from terminal)

STX/ETX removal
Enabling "Del STX&ETX" will cause the unit to strip off the STX and ETX characters that normally surround the APACS 30 string before sending it to the host. Enabling "Del STX only" will cause it to strip of the STX character only.

Do not transmit ENQ characters
Under the TPAD protocol the ENQ character is normally used to indicate that a call has connected and that the TPAD terminal may proceed with the transaction. Enabling this parameter will prevent the router from transmitting ENQ characters to the TPAD terminal when a connection is made.

Delay sending ENQ characters to TPAD terminal for x milliseconds when a call has been connected
This parameter may be used to set the delay in ms from when the router first connects the call to when it transmits the ENQ to the terminal. By default there is no delay.

Wait for x milliseconds for an ACK before retransmitting the data
This parameter defines the time period the unit will wait for an ACK character to be received after sending data to the terminal. If an ACK character is not received within this time the data will be retransmitted. A value of "0" entered here will default to a delay of 1 second.

Transmit TPAD transactions directly in a Synchronous frame
When this check box is ticked TPAD transactions are transmitted without any "outer" protocol such as X.25, i.e. they are placed directly in a synchronous frame on ISDN. This sometimes referred to as HDLC by certain card acquirers.

Include LRC
The LRC (Longitudinal Redundancy Check) is a form of error checking that may be required by some TPAD terminals. When the Include LRC option is enabled the unit will check the LRC sent by the terminal and if it indicates a problem has occurred NAK the message. If this parameter is enabled but no LRC is sent by the terminal, the transaction will not be forwarded to the host.

Include LRC line
This parameter is normally disabled so that any LRCs received from a TPAD terminal will be removed before the transaction data is transmitted to the remote host. In most cases this is acceptable because the network will provide error correction and so the LRC is redundant. In some circumstances it may be necessary to enable this parameter so that the unit transmits the LRC to the remote host along with the transaction data.

Force parity when sending data to the terminal
When this parameter is enabled the unit will always use even parity when relaying data from a remote host to a locally connected TPAD terminal. To allow data to pass through without the parity being changed disable this setting.

Strip parity when sending data to the host
Enabling this parameter will cause the unit to remove any parity before sending the data to the host.

Force parity when sending data to the host
When this parameter is enabled the unit will always use EVEN parity when relaying data from the locally connected TPAD terminal to the remote host. To allow data to pass through without the parity being changed disable this setting.

Strip Trailing Spaces
When this parameter is enabled the TPAD instance will look at responses coming from the host and remove any trailing space characters from the end of the packet before relaying the data to the terminal. This may be necessary if the host system "pads out" responses with unnecessary spaces which can cause abnormal behaviour in some terminals.

Acknowledge TPAD data packets
This parameter causes the unit to acknowledge TPAD data packets from the terminal. This parameter should normally be enabled. Note that this parameter is only used if no polling characters (see above) are defined.

Convert leading STX character to SOH
Enabling this parameter will cause the unit to convert the leading STX character in a transaction to an SOH character.

Terminate TPAD call is EOT only
A TPAD call is normally terminated with a DLE EOT sequence. Some terminals only require the EOT character on its own. If this is the case then enable this parameter.

Clear TPAD call if there is no response to a TPAD transaction request for x seconds
This is the length of time in seconds that the unit will wait for a response to a TPAD transaction request before clearing the TPAD call.

Generate an event when a TPAD transaction takes longer than x seconds
Setting this parameter to a non-zero value causes the unit to generate an "Excessive Transaction Time" event (code 56) each time a TPAD transaction takes longer that the specified number of seconds. This could be used in conjunction with an appropriate Event Handler configuration to generate email alert messages or SNMP traps when TPAD transactions take longer than expected. See ***Configuration - Alarms > Event Logcodes*** for a complete list of events.

When the transaction time exceeds x milliseconds, increment the "SLA Exceptions" statistic
When the total transaction time exceeds the value (in ms) set in this parameter, the NB SLA exceptions statistic on the Diagnostics - Statistics > TPAD page is incremented. This statistic can be viewed on the CLI interface by entering the at\mibs=tpad.n.stats command, where n is the TPAD instance.

Clear the call x seconds after receiving a response
This parameter defines the time period for which the socket closing or the X.25 call clearing is delayed by after the TPAD session has finished. For example, if this parameter is set to 10 then 10 seconds after the TPAD session is finished (NO CARRIER is seen on the ASY TPAD port) the network call (X25 or TCP socket) is cleared. The number "1" is a special value. If set to the number "1" the call will be cleared immediately (not after 1 second).

If the terminal dial command specifies V.120 use PANS context x
This parameter is for advanced users only. It enables TPAD transactions to be carried out using the V.120 protocol ("ATDV" command). The parameter is used in conjunction with the Polling Answering Service (PANS), and identifies which PANS instance is to be used for an outgoing V.120 call. For this to work, the PANS instance must be bound to a Rate Adaption instance.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
tpad	n	l2iface	lapb, lapd, tcp, ssl, vxn	Use TPAD over interface
tpad	n	l2nb	0 – 255	Use TPAD over interface
tpad	n	ipmode	0=XOT, 1=raw TCP	Use TPAD over interface
tpad	n	bakl2iface	lapb, lapd, tcp, ssl, vxn	Use backup interface
tpad	n	bakl2nb	0 - 255	Use backup interface

Entity	Instance	Parameter	Values	Equivalent Web Parameter
tpad	n	bnumber	text (valid ISDN number)	Use number x to make outgoing ISDN calls
tpad	n	prefix	text (numeric)	Use prefix x
tpad	n	prefix_rem	text (numeric)	Remove prefix x from number in ATD command
tpad	n	suffix	text (numeric)	Use suffix x
tpad	n	tl2deact	0 - 10000	On the main interface Deactivate LAPB session x seconds after TPAD X.25 call has been cleared
tpad	n	baktl2deact	0 – 10000	On the backup interface Deactivate LAPB session x seconds after TPAD X.25 call has been cleared.
tpad	n	defpak	16,32,64,128,256,512,1024	Default X.25 Packet Size
tpad	n	nua	text	Use NUA
tpad	n	nui	text	Use NUI
tpad	n	lcn	1 - 4095	LCN
tpad	n	lcnup	1 = up, 0 = down	LCN direction
tpad	n	baknua	text	(Backup) Use NUA
tpad	n	baknui	numeric text	(Backup) Use NUI
tpad	n	baklcn	1 - 4095	(Backup) LCN
tpad	n	baklcnup	1 = up, 0 = down	(Backup) LCN direction
tpad	n	cingnua	numeric text	Report our NUA as n to the X.25 network
tpad	n	cud	text	Call User Data
tpad	n	samecall	0	One per transaction
tpad	n	samecall	1	Allow consecutive transactions
tpad	n	samecall	2	Allow concurrent transactions
tpad	n	delimchar	32 - 127	Use ASCII character x as the delimiter character
tpad	n	ftime	0 - 20000	Forward mode time x milliseconds
tpad	n	trig_str	text	Create an event when reply from X.25 host matches

Entity	Instance	Parameter	Values	Equivalent Web Parameter
tpad	n	IPaddr	IP address	Connect to remote IP address
tpad	n	iphdr	0=Off 1=On 2=8583 Ascii 4 byte	IP length header
tpad	n	termid	text	Use Terminal ID (TID)
tpad	n	dotermid	1 = enabled, 0 = disabled	Replace TID provided by connected terminal with configured TID
tpad	n	tid	text	Use TID xxxxxxxxx with incoming APACS 50 polling calls
tpad	n	merchnum	text	Use merchant Number
tpad	n	useconstr	1 = enabled, 0 = disabled	Use Connect String
tpad	n	constr	text	Use Connect String
tpad	n	pollchars	text	The polling character set is c
tpad	n	domsgnb	1 = enabled, 0 = disabled	Enable Message Numbering
tpad	n	disdir	1 = enabled, 0 = disabled	Disable Direct Mode
tpad	n	bdir	1 = enabled, 0 = disabled	Boot to Direct Mode
tpad	n	uaarc	0 - 99	Use response code n in "unable to authorise" message
tpad	n	clear_dirtime	0 - 60000	Clearing time n milliseconds
tpad	n	trandel	0 - 5000	Delay transmitting the APACS 30 string for x milliseconds after connecting to X.25 host
tpad	n	teretran	1 = enabled, 0 = disabled	Retransmit APACS 30 string if error detected
tpad	n	delstx	1 = enabled, 0 = disabled	STX/ETX removal
tpad	n	no_enq	1 = enabled, 0 = disabled	Do not transmit ENQ characters
tpad	n	tenqdel	0 - 5000	Delay sending ENQ characters to TPAD terminal for x milliseconds when a call has been connected

Entity	Instance	Parameter	Values	Equivalent Web Parameter
tpad	n	tackdel	0 – 10000	Wait for x milliseconds for an ACK before retransmitting the data
tpad	n	dsync	1 = enabled, 0 = disabled	Transmit TPAD transactions directly in a Synchronous frame
tpad	n	inclrc	1 = enabled, 0 = disabled	Include LRC
tpad	n	incllrc	1 = enabled, 0 = disabled	Include LRC line
tpad	n	fpar	1 = enabled, 0 = disabled	Force parity when sending data to the terminal
tpad	n	lrpar	1 = enabled, 0 = disabled	Strip parity when sending data to the host
tpad	n	lfpar	1 = enabled, 0 = disabled	Force parity when sending data to the host
tpad	n	strip_tspaces	1 = enabled, 0 = disabled	Strip Trailing Spaces
tpad	n	ackdat	1 = enabled, 0 = disabled	Acknowledge TPAD data packets
tpad	n	stx_2_soh	1 = enabled, 0 = disabled	Convert leading STX character to SOH
tpad	n	eot_only	1 = enabled, 0 = disabled	Terminate TPAD call is EOT only
tpad	n	tresp	0 – 1000	Clear TPAD call if there is no response to a TPAD transaction request for x seconds
tpad	n	texcess	0 – 100	Generate an event when a TPAD transaction takes longer than x seconds
tpad	n	tsla	0 – 3000	When the transaction time exceeds x milliseconds, increment the "SLA Exceptions" statistic
tpad	n	clear_time	0 - 2147483647	Clear the call x seconds after receiving a response
tpad	n	dialctx	0 - 255	If the terminal dial command specifies V.120 use PANS context x

Configuration - Network > Legacy Protocols > X.25 > General

This section contains some global X.25 settings.

When answering a X.25 call, use the addresses from CALL packet in the CALL CNF packet
When this setting is enabled when answering a call the called and calling addresses from the CALL packet are used in the X25 CALL CNF (call confirm packet) that the unit sends to answer the call. This setting can be enabled on a per "interface type" basis, (LAPD, LAPB or XoT)

Reset XOT PVC if the router is the Initiator
When this parameter is enabled the unit is responsible for resetting the links when an XOT PVC comes up. This parameter should only be set to "Off" when it is known that the responder will reset the links.

Reset XOT PVC if the router is the Responder
When this parameter is set to "On" the unit is responsible for resetting the links on XOT PVC links when it is the responder. The default for this parameter is "Off".

Include length of header in IP length header

For all X.25 calls which include an IP header length indication (i.e. IP Length Header is set to "On" a TPAD or PAD, etc.) this parameter specifies whether the length indicated includes or excludes the length of the header itself.

By default it is "Off", in which case the length of the header is NOT included in the value. For example, say we had one byte of data of value 67 to encode. Then "00 01 67" is the encoding if this parameter is set to "Off" as the length (00 01) is 1 because the length does not include the length of the header. When set to "On" the length of the IP header is included in the value, i.e. "00 03 67" is the encoding as the header bytes are included.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
X25gen	0	lapd_cnf_addr	1 = enabled, 0 = disabled	When answering a X.25 call, use the addresses from CALL packet in the CALL CNF packet. LAPD setting
X25gen	0	lapd_cnf_addr	1 = enabled, 0 = disabled	When answering a X.25 call, use the addresses from CALL packet in the CALL CNF packet LAPB setting
X25gen	0	xot_cnf_addr	1 = enabled, 0 = disabled	When answering a X.25 call, use the addresses from CALL packet in the CALL CNF packet XoT setting
X25gen	0	reset_xotpvc_ini	1 = enabled, 0 = disabled	Reset XOT PVC if the router is the Initiator
X25gen	0	reset_xotpvc_resp	1 = enabled, 0 = disabled	Reset XOT PVC if the router is the Responder
X25gen	0	en_incl_iphdr	1 = enabled, 0 = disabled	Include length of header in IP length header

Configuration - Network > Legacy Protocols > X.25 > LAPB

LAPB (Link Access Procedure Balanced) is a standard subset of the High-Level Data Link Control (HDLC) protocol. It is a bit-oriented, synchronous, link-layer protocol that provides data framing, flow control and error detection and correction. LAPB is the link layer used by X.25 applications.

On Digi TransPort routers LAPB can be used over ISDN or over a synchronous serial port.

Configuration - Network > Legacy Protocols > X.25 > LAPB n

Use: Serial port Port x (in Synchronous Mode)
To use the LAPB instance over a synchronous serial port enable this setting and select a serial port number. To configure settings of the synchronous port such as speed and clock source navigate to ***Configuration - Network > Interfaces > Serial > Serial Port n > Sync Port n.***

Use: ISDN
Enable this setting to use LAPB over ISDN.

Mode DTE or DCE
Determines whether LAPB will behave as DTE (Data Terminal Equipment) or DCE (Data Circuit-terminating Equipment) in an X.25 protocol sense. (Physical DTE vs. DCE wiring cannot be changed by configuration.)

N400 Counter x
This is the standard LAPB retry counter. The default value is 3 and it should not normally be necessary to change this.

RR Timer x milliseconds
This is a standard LAPB "Receiver Ready" timer. The default value is 10,000ms (10 seconds) and it should not normally be necessary to change this.

T1 Timer x milliseconds
This is a standard LAPB timer. The default value is 1000 milliseconds (1 second) and under normal circumstances, it should not be necessary to change it.

T200 Timer x milliseconds
This is the standard LAPB re-transmit timer. The default value is 1000 milliseconds (1 second) and under normal circumstances, it should not be necessary to change it.

X.25 Window Size
This parameter is used to set the X.25 window size. The value range is from 1 to 7 with the default being 7.

Disconnect link if there has been no X.25 activity for x seconds
This parameter may be used to specify the length of time (in seconds) before the link is disconnected if there has been no X.25 activity. If this parameter is zero or not specified, then the inactivity timer is disabled.

Disconnect link if there has been no activity for x seconds
This parameter may be used to specify the length of time (in seconds) before the link is disconnected if there has been no activity. If this parameter is zero or not specified, then the inactivity timer is disabled. It is useful to set this to a short period of time (say 120 seconds) when a LAPB instance is being used over ISDN for example with TPAD. Should the POS device fail to instruct TPAD to hang up then this timer can be used as a backup hang-up timer thus saving ISDN call charges. When LAPB is being used on a synchronous port, this parameter should normally be set to 0.

Send X.25 Restart packet on receipt of SABM frame
This parameter can be set to "No" or "Immediate". When set to "Immediate", the LAPB instance will send an X.25 restart packet immediately on receipt of an SABM (Set Asynchronous Balanced Mode) frame. If the parameter is set to "No", then no X.25 restart is sent.

Configuration - Network > Legacy Protocols > X.25 > LAPB n > ISDN Parameters

Allow this unit to answer calls
When this parameter is enabled this instance of LAPB will answer incoming ISDN calls.

Only accept calls from calling number ending with
This parameter provides the filter for the ISDN Multiple Subscriber Numbering facility. It is blank by default but when set to an appropriate value with "Allow this unit to answer calls" enabled it will cause the unit to answer incoming calls only to ISDN numbers where the trailing digits match the MSN value. For example, setting the MSN parameter to 123 will prevent the unit from answering any calls to numbers that do not end in 123.

Only accept calls with sub-address ending with
This parameter provides the filter for the ISDN sub-addressing facility. It is blank by default but when set to an appropriate value, with "Allow this unit to answer calls" enabled it will cause the unit to answer incoming ISDN calls only where the trailing digits of the sub address called match the Sub-address value. For example, setting the Sub-address to 123 will prevent the unit from answering any calls where the sub-address called does not end in 123.

Keep ISDN LAPB link activated when user sends a DISC or X.25 PAD session terminated
When this parameter is enabled

Wait x milliseconds before attempting to establish the LAPB link after B-channel becoming active
This parameter sets the length of time (in milliseconds), that the LAPB instance will wait from an ISDN B-channel becoming active before attempting to establish a LAPB connection, i.e. the length of time for which the LAPB instance stays passive. The default is 0 as most ISDN networks allow CPE devices to initiate a LAPB link. If your ISDN network does not permit CPE devices to initiate the LAPB link you should set this parameter to a value that allows the network sufficient time to establish the LAPB link.

Use as x a calling party number when making ISDN calls
This is "Calling Line Identification". The unit will only answer calls from numbers whose trailing digits match what is entered in this field. The line the unit is connected to must have CLI enabled by the telecoms provider, and the calling number cannot be withheld.

Configuration - Network > Legacy Protocols > X.25 > LAPB n > Async Mux 0710 Parameters

For certain W-WAN modules LAPB is used to perform multiplexing of serial channels. If using LAPB for X.25 over ISDN or serial then these settings should be ignored. These settings should not be changed unless under the instruction of technical support.

Mux 0710 mode
When enabled configures the LAPB instance to be used for multiplexing of serial channels instead of X.25.

Mux mode
This setting controls the multiplexing mode.

DLC #
The data link channel number to use for this virtual ASY port.

ASY port
This is the physical ASY port over which to multiplex.

Virtual ASY port
This is the virtual ASY port number that this LAPB instance will multiplex over the physical port.

Entity	Instance	Parameter	Values	Equivalent Web Parameter
lapb	n	l1iface	port, isdn (use "port" for sync port)	Use: Serial port Port x (in Synchronous Mode)
lapb	n	l1nb	0,1	Use: Serial port Port x (in Synchronous Mode) 0 for "Port 0", 1 for "Port 1"
lapb	n	l1iface	port, isdn (use "isdn" for ISDN)	Use: ISDN
lapb	n	dtemode	DTE/DCE mode: 0=DTE 1=DCE	Mode DTE or DCE
lapb	n	N400	1 - 255	N400 Counter x
lapb	n	tnoact	1000 - 60000	RR Timer x milliseconds
lapb	n	t1time	1 - 60000	T1 Timer x milliseconds
lapb	n	t200	1 - 60000	T200 Timer x milliseconds
lapb	n	Window	1 - 7	X.25 Window Size
lapb	n	tinactx25	0 - 3000	Disconnect link if there has been no X.25 activity for x seconds
lapb	n	tinact	0 - 3000	Disconnect link if there has been no activity for x seconds
lapb	n	restartact	1 = enabled, 0 = disabled	Send X.25 Restart packet on receipt of SABM frame
lapb	n	ans	1 = enabled, 0 =	Allow this unit to answer calls

Entity	Instance	Parameter	Values	Equivalent Web Parameter
			disabled	
lapb	n	msn	text	Only accept calls from calling number ending with
lapb	n	sub	text	Only accept calls with sub-address ending with
lapb	n	ptime	0 - 60000	Wait x milliseconds before attempting to establish the LAPB link after B-channel becoming active
lapb	n	cli	text	Only answer calls from numbers whose trailing digits match
lapb	n	mux_0710	1 = enabled, 0 = disabled	Mux 0710 mode
lapb	n	mux_mode	0 = Basic, 1 = Error Recovery	Mux mode
lapb	n	dlc	0 - 63	DLC #
lapb	n	asyport	0 - 255	ASY port
lapb	n	virt_async	0 - 255	Virtual ASY port

Configuration - Network > Legacy Protocols > X.25 > NUI Mappings

When a TPAD call is taking place the attached terminal sometimes only specifies an "NUI" (Network User ID) to call. If the X.25 network requires an NUA instead of an NUI to determine the destination of a call then the NUI Mappings table can be used to convert an NUI to an NUA.

If a TPAD call specifies a call in which the NUI matches an entry the call actually placed on the network will contain the respective NUA and no NUI.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
nuimap	n	nua	text	Maps to NUA
nuimap	n	nui	text	NUI

Configuration - Network > Legacy Protocols > X.25 > NUA / NUI Interface Mappings

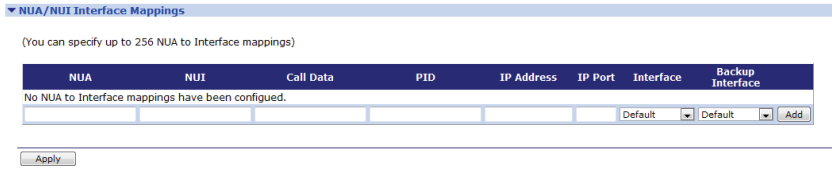
For PAD and TPAD instances, this table can be used to override the following:

- Interface
- Backup interface
- IP address
- TCP/UDP port number

Based upon data in the call request matching the following comparison fields:

- NUA called
- NUI called
- X.25 Call Data
- PID

All the comparison fields, NUA, NUI, Call Data and PID can use the wildcard matching characters "?" and "*".



NUA
Network User Address

NUI
Network User Identifier

Call Data
X.25 Call Data

PID
Protocol Identifier

IP address
IP address

IP Port
IP port number

Interface
Primary interface

Backup Interface
Backup interface

Note that this table is duplicated in the ***Configuration - Network > Protocol Switch > NUA to Interface Mappings*** section as it can also be used by the Protocol Switch. Not all of the fields are visible in the Protocol Switch section as they do not all apply to the Protocol Switch.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
nuaip	N	nua	text	NUA
nuaip	N	nui	text	NUI
nuaip	N	cud	text	Call Data
nuaip	n	pid	text	PID
nuaip	n	IPaddr	IP address	IP Address
nuaip	n	ip_port	0 - 65535	IP Port
nuaip	n	swto	0 -15	Interface
nuaip	n	buswto	0 -15	Backup Interface

The interface and backup interface values are as follows:

Parameter Value	Interface Type
0	Default
1	LAPD
2	LAPB 0
3	LAPB 1
4	XOT
5	LAPD x (instance determined by NUA)
6	LAPB 0 PVC
7	LAPB 1 PVC
8	XOT PVC
9	TCP Stream
10	UDP Stream
12	LAPB 2
13	LAPB 2 PVC
14	VXN
15	SSL

Configuration - Network > Legacy Protocols > X.25> Calls Macros

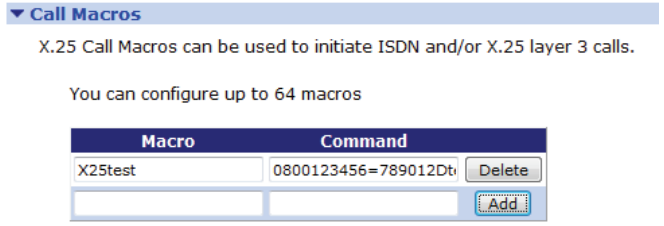
This page allows you to define up to 64 X.25 CALL "macros" that can be used to initiate ISDN and/or X.25 layer 3 calls. These simple English-like names are mapped to full command strings. For example, the call string:

```
0800123456=789012Dtest data
```

could be given the name "X25test" and then executed simply by entering:

```
CALL X25test
```

To create a macro, enter a name for the macro in the left column of the Call Macros table and in the right column enter the appropriate command string (excluding the ATD). Then click Add.



Macro
The name of the macro, this can be any text.

Command
The X.25 call command.

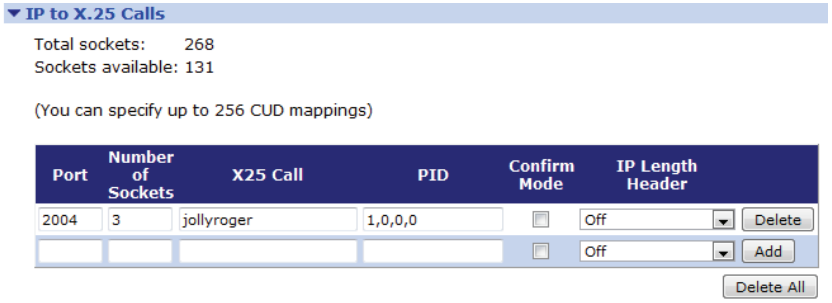
Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
macro	n	name	text	Macro
macro	n	cmd	text	Command

Configuration - Network > Legacy Protocols > X.25 > IP to X.25 Calls

This page contains a table that allows you to enter a series of IP Port numbers and X.25 Call strings as shown below. It is used to configure the unit so that IP data can be switched over X.25. For example data that is received on a TCP connection can be answered by a PAD as if it is an X.25 call.

This table is duplicated in the ***Configuration - Network > Protocol Switch > IP Sockets to Protocol Switch*** section as it is also used by the protocol switch. It is included at this point in the web user interface as a convenience in case the table is being used in conjunction with PAD and not the protocol switch.



IP Port
The IP Port field is used to setup the port numbers for those IP ports that will "listen" for incoming connections that are to be switched over X.25 or other protocol. In the case of switching to X.25, when such a connection is made the unit will make an X.25 Call to the address specified in the X.25 Call field. Once this call has been connected, data from the port will be switched over the X.25 session.

Number of Sockets
The Number of Sockets field is used to select how many IP sockets should simultaneously listen for data on the specified port. The number of available IP sockets will depend on the model you are using and how many are already in use (see note below).

X25 Call
The X.25 call field may contain an X.25 NUA or NUI or one of the X.25 Call Macros defined on the ***Configuration - Advanced applications > X25 > Macros page***.

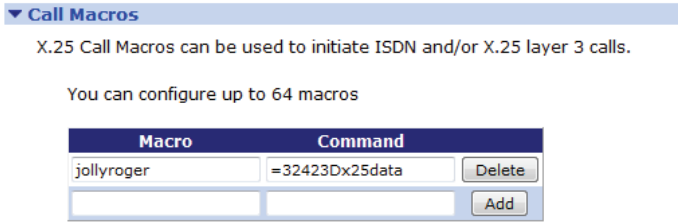
PID
The PID (Protocol Identifier), field specifies the PID to use when the unit switches an IP connection to X.25. The PID (protocol ID) field takes the format of four hexadecimal digits separated by commas, e.g. 1,0,0,0, at the start of the Call User Data field in the X.25 call.

Confirm Mode
When confirm mode is set to "On" then the incoming TCP socket will not be successfully connected until the corresponding outgoing call has been connected. The incoming TCP socket will trigger the corresponding outgoing call either to a local PAD instance or to whatever is configured. The effect of this mode is that the socket will fail if the outbound call fails and so may be useful in backup scenarios. In addition it will ensure that no data is sent into a "black hole". (When this setting is not enabled data that is sent on the inbound TCP connection before the outbound connection has been successful can be lost.)

RFC 1086 Mode:
RFC 1086 specifies a mode of operation in which the IP socket answers and then with a simple protocol in the socket identifies the X.25 address and other X.25 call setup parameters to be used. Then when the X.25 call parameters have been identified the X.25 call is made and if successful then data is then switched between the X.25 call and the IP socket. The protocol will select whether incoming or outgoing support is required.

IP length header
When IP length header is "On", the IP length indicator field is inserted at the start of each packet. When set to "8583 Ascii 4 byte", the IP length header will conform to the ISO 8583 format.

In the example above, 3 IP sockets will "listen" for an incoming connection on IP Port 2004. Once connected they will each will make an X.25 Call to "jollyroger". The unit will recognise that "jollyroger" is a pre-defined macro (as illustrated below), and will translate it into an X.25 Call to address 32423 with the string "x25 data" included as data in the call. The outgoing X.25 call(s) will be made over whichever interface is specified by the Switch from XOT(TCP) to parameter on the ***Configuration - Network > Protocol Switch*** page.



Note:
At the top of the page the total number of sockets available and the number currently free is shown. Care should be take not to allocate too many of the free sockets unless you are confident that they are not required for other applications.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ipx25	n	ip_port	0 - 65535	IP Port
ipx25	n	nb_listens	0 – software dependant max	Number of Sockets
ipx25	n	x25call	NUA, NUI or X.25 macro name	X25 Call
ipx25	n	pid	hex numbers	PID
ipx25	n	cnf_mode	1 = enabled, 0 = disabled	Confirm Mode
ipx25	n	rfc1086_mode	1 = enabled, 0 = disabled	RFC 1086 Mode
ipx25	n	iphdr	0=Off 1=On 2=8583 Ascii 4 byte	IP length header

Configuration - Network > Legacy Protocols > X.25 > PADS n

PAD which stands for **P**acket **A**ssembler **D**issembler is used to interface between a character based serial connection and an X.25 synchronous packet switched network.

There are two main elements to the configuration procedure for accessing X.25 networks:

General and service related parameters

PAD parameters (X.3)

Each X.25 PAD configuration page also includes a sub-page detailing the X.3 PAD parameters. Collectively this set of values is known as a PAD profile. Your unit contains four pre-defined standard PAD profiles numbered 50, 51, 90 and 91. You may also create up to four custom PAD profiles numbered 1 to 4 for each PAD instance.

Use PAD over interface
This section is used to select whether the PAD instance will use ISDN B-channel X.25, ISDN D-channel X.25, TCP, UDP, VXN, SSL TCP or SSL XoT as the transport protocol. For ISDN D-channel operation, ensure that the "LAPD" option is selected. For ISDN B-channel operation or operation through a synchronous port, select "LAPB". In the case of LAPB and LAPD it is also possible to specify an interface number. This parameter specifies which LAPB or LAPD instance to use for the relevant TPAD instance. Select "0" or "1" for LAPB or "0" or "1" for LAPD.

Use backup interface
This section is used to specify a backup interface that will be used automatically if the call to the primary interface fails. Note that the primary interface will be tried first for every new call attempt.

X.25 Settings

Default X.25 packet size
This parameter determines the default X.25 packet size. This may be set to "16", "32", "64", "128", "256", "512" or "1024", but the actual values permitted will normally be constrained by your service provider.

Answer incoming calls from NUA
This is the NUA that the unit responds to for incoming X.25 calls.

Only answer calls with CUG
The PAD will only answer calls with this Call User Group (CUG) specified.

Use X.25 Call Macro macroname to an ATD command
This parameter specifies the name of an X.25 call macro that is used when an ATD command is received by the unit. The ATD command is ignored, and a PAD CALL command using the macro replaces it. The purpose of this feature is to allow non-PAD terminals to use an X.25 PAD network connection. X.25 call macros are set up in the ***Configuration - Network > Legacy Protocols > X.25 > Call Macros*** web page, or by using the macro text command.

Use NUA
This NUA will be used as the calling NUA when an outgoing X.25 call is made.

LCN

The unit supports up to eight logical X.25 channels. In practice, the operational limit is determined by the particular service to which you subscribe (usually 4).

Each logical channel must be assigned a valid Logical Channel Number (LCN). The LCN parameter is the value of the first LCN that will be assigned for outgoing X.25 CALLs. The default is 1027.

For incoming calls, the unit accepts the LCN specified by the caller.

LCN Direction

This parameter determines whether the LCN used for outgoing X.25 calls is incremented or decremented from the starting value when multiple X.25 instances share one layer 2 (LAPB or LAPD), connection. The default is "Down" and LCNs are decremented, i.e. if the first CALL uses 1024, the next will use 1023, etc. Setting the parameter to "Up" will cause the LCN to be incremented from the start value.

NUI/NUA selection
If both an NUI and an NUA are included in the call string, this parameter allows the unit to filter one of these out of the X.25 call request. This can be extremely useful in backup scenarios. Consider the following example; the unit is configured to do online authorisations via the ISDN D channel and to fall back to B-channel (if the D-channel host did not respond for any reason). Using this parameter in conjunction with the backup equivalent, it is possible to configure the unit to use the supplied NUA to connect over D-channel and the supplied NUI to connect over B channel (for backup).

On the backup interface LCN
The LCN parameter is used to set the first LCN that will be used for the backup interface.

On the backup interface LCN Direction
This parameter determines whether the LCN used for the backup X.25 interface is incremented or decremented from the starting value when multiple X.25 instances share a single layer 2 connection.

On the backup interface NUI/NUA selection
If both an NUI and an NUA are included in the call string, this parameter allows the unit to filter one of these out of the X.25 call request.

Enable X.25 Restart Packets
It is normally possible to make X.25 CALLs immediately following the initial SABM-UA exchange. In some cases however, the X.25 network may require an X.25 Restart before it will accept X.25 CALLs. The correct mode to select depends upon the particular X.25 service to which you subscribe. The default value is "On". This means that the unit WILL issue X.25 Restart packets. To prevent the unit from issuing Restart packets set this parameter to "Off".

Restart delay
When the Restarts parameter is "On" the Restart Delay value determines the length of time in milliseconds that the unit will wait before issuing a Restart packet. The default value is 2000 giving a delay of 2 seconds.

IP Settings

Remote IP address
This field indicates the destination host that will answer the XOT, TCP, SSL, UDP call.

Remote IP Address when using the backup interface
This field indicates the destination host that will answer the XOT, TCP, SSL, UDP call if a connection via the primary interface has failed and the PAD is configured to backup to a secondary interface that is using an IP based protocol.

IP Stream port
This is the TCP or UDP port number to use for IP (but not XoT) connections.

IP length header
When set to "On", and in IP Stream mode, the length of a data sequence is inserted before the data. For the receive direction it is assumed the length of the data is in the data stream. When set to "8583 Ascii 4 byte", the IP length header will conform to the ISO 8583 format.

PAD Settings

PAD prompt
This parameter allows you to redefine the standard "PAD>" prompt. To change the prompt enter a new string of up to 15 characters into the text box.

PAD mode
The PAD Mode parameter can be set to "Normal" or "Prompt Always On". In Prompt Always On mode, the ASY port attached to the PAD behaves as if it were permanently connected at layer 2, i.e. it always displays a "PAD>" prompt. AT commands may still be entered but the normal result codes are suppressed. To disable this mode set the parameter to "Normal".

Use PAD Profile
The PAD profile # allows you to select the PAD profile to use for this PAD instance. There are four pre-defined profiles numbered "50", "51", "90" and "91". In addition to the pre-defined profiles you can also create up to four user-defined profiles numbered "1", "2", "3" and "4". To assign a particular profile to the PAD select the appropriate number from the list.

Strip Trailing Spaces
When this parameter is turned on any spaces received at the end of a sequence of data from the network will be removed before being relayed to the PAD port.

Enable Leased Line Mode
When this parameter is set to "On", it causes the PAD to always attempt to be connected using the Auto macro setting as the call command.

Send ENQ on Connect
When this parameter is set to "On" the PAD will send an ENQ character on the ASY link when an outgoing call has been answered.

Enable STX / ETX Filtering
When this parameter is "On", the PAD will ignore data that is not encapsulated between ASCII characters STX (Ctrl+B) and ETX (Ctrl+C). To disable this feature select the "Off" option.

Delay connect message n x 10 milliseconds
Delay the Connect message by the number of milliseconds specified. (Useful when working with equipment that previously connected to slower networks and is upset by the quicker "Connect" when used with modern networks.)

Delay data transfer after connection by n x 10 milliseconds
Delays the data delivered from the X.25 or other type of connection to the terminal upon initial connection.

Terminate the PAD call after x seconds if there has been no data transmission
This parameter specifies the length of time in seconds after which the PAD will terminate an X.25 call if there has been no data transmission.

Disconnect the layer 2 call if there is no layer 3 call in progress for x seconds
This parameter specifies the length of time in seconds after which the unit will disconnect a layer 2 link if there are no layer 3 calls in progress. For LAPB sessions this will also terminate the ISDN call.

Create an event when the following data is on the PAD
This parameter specifies a string, which if it appears in the received data causes a "Data Trigger" (47) event to be generated and recorded in the event log.

Create an event when there has been no activity on the PAD for x seconds
This specifies the time in seconds in which if there is no activity on the PAD an event in the event log will be posted. This can be used to trigger email exceptions.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
pad	n	l2iface	lapb, lapd, TCP, SSL	Use PAD over interface
pad	n	l2nb	0 – 255 (instance of LAPB or LAPD)	Use PAD over interface
pad	n	ip_stream	0 = off (for XoT), 1 = TCP, 2 = UDP	Use PAD over interface
pad	n	defpak	16,32,64,128,256,512 or 1024	Default X.25 packet size
pad	n	ansnua	text (valid NUA)	Answer incoming calls from NUA
pad	n	anscug	text (valid CUG)	Only answer calls with CUG

Entity	Instance	Parameter	Values	Equivalent Web Parameter
pad	n	amacro	text	Use X.25 Call Macro macroname to an ATD command
pad	n	cingnua	text (valid NUA)	Use NUA
pad	n	lcn	1 - 4095	LCN
pad	n	lcnup	1 = up, 0 = down	LCN Direction
pad	n	nuaimode	0 = NUI and NUA, 1 = NUA only, 2 = NUI only	NUI/NUA selection
pad	n	dorest	1 = enabled, 0 = disabled	Enable X.25 Restart Packets
pad	n	restdel	0 - 60000 (ms)	Restart delay
pad	n	IPaddr	text	Remote IP address
pad	n	buipaddr	text	Remote IP Address when using the backup interface
pad	n	ip_port	0 - 65535	IP Stream port
pad	n	iphdr	0=Off, 1=On, 2=8583 Ascii 4 byte	IP length header
pad	n	prompt	text	PAD prompt
pad	n	padmode	0 = Normal, 1 = Prompt Always On	PAD mode
pad	n	profile	1-4, 50, 51,90,91	Use PAD Profile
pad	n	strip_tspaces	1 = enabled, 0 = disabled	Strip Trailing Spaces
pad	n	llmode	1 = enabled, 0 = disabled	Enable Leased Line Mode
pad	n	enqcon	1 = enabled, 0 = disabled	Send ENQ on Connect
pad	n	stxmode	1 = enabled, 0 = disabled	Enable STX / ETX Filtering
pad	n	delconmsg	0 - 10	Delay connect message n x 10 millisecondss
pad	n	data_del	0 - 2147483647	Delay data transfer after connection by n x 10 milliseconds
pad	n	inacttim	0 - 1000	Terminate the PAD call after x seconds if there has been no data transmission
pad	n	nocalltim	0 - 60000	Disconnect the layer 2 call if there is no layer 3 call in progress for x seconds
pad	n	trig_str	text	Create an event when the following data is on the

Entity	Instance	Parameter	Values	Equivalent Web Parameter
				PAD
pad	n	inactevent	0 - 2147483647	Create an event when there has been no activity on the PAD for x seconds

Stopping and starting PADs

PAD instances can be stopped and started using the following CLI commands:

stoppads

gopads

The stoppads command stops all PAD instances from accepting and performing any PAD commands.

The gopads command resumes processing of PAD commands.

The stoppads and gopads commands can have the PAD number specified in the syntax to stop and start individual PAD instances.

For example:

To stop PAD 1 from processing PAD commands:

stoppads 1

and to re-enable PAD 1:

gopads 1

Configuration - Network > Legacy Protocols > X.25 > PADs 0-9 > PAD 0 > X3 Parameters

Each PAD configuration page has an attached sub-page that allows you to edit the X.3 PAD parameters. These pages allow you to load one of the standard profiles or edit the individual parameters to suit your application requirements and save the resulting customised "user" profile to non-volatile memory.

Loading and Saving PAD Profiles

To create your own PAD profiles, edit the appropriate parameters and then select user profile 1, 2, 3 or 4 as required from the list and click the "Save Profile" button.

Each PAD profile page includes two list boxes that allow you to load and save PAD profiles. To load a particular profile, select the profile from the list and click the "Load Profile" button. The parameter table will be updated with the values from the selected profile.

1 PAD Recall Character
This parameter determines whether PAD recall is enabled. When this facility is enabled, typing the PAD recall character temporarily interrupts the call and returns you to the PAD> prompt where you may enter normal PAD commands as required. To resume the interrupted call, use the CALL command without a parameter.

The default PAD recall character is [Ctrl-P]. This may be changed to any ASCII value in the range 32-125 or disabled by setting it to 0.

When a call is in progress and you need to actually transmit the character that is currently defined as the PAD recall character, simply enter it twice. The first instance returns you to the PAD> prompt; the second resumes the call and transmits the character to the remote system.

Option	Description
0	Disabled
1	PAD recall character is CTRL-P (ASCII 16, DEL)
32 - 126	PAD recall character is user defined as specified

2 Echo
This parameter enables or disables local echo of data transmitted during a call. When echo is enabled, X.3 parameter 20 may be used to inhibit the echo of certain characters.

Option	Description
0	Echo off
1	Echo on

3 Data Forwarding Characters
This parameter defines which characters cause data to be assembled into a packet and forwarded to the network.

Option	Description
0	No data forwarding character
1	Alphanumeric characters (A-Z, a-z, 0-9)
2	CR
4	ESC, BEL, ENQ, ACK
8	DEL, CAN, DC2
16	EXT, EOT
32	HT, LF, VT, FF
64	Characters of decimal value less than 32

Combinations of the above sets of characters are possible by adding the respective values together. For example, to define CR, EXT and EOT as data forwarding characters, set this parameter to 18 (2 + 16).

If no forwarding characters are defined the Idle timer delay (parameter 4) should be set to a suitable value, typically 0.2 seconds.

4 Idle Timer Delay
This parameter defines a time-out period after which data received from the DTE is assembled into a packet and forwarded to the network. If the forwarding time-out is disabled, one or more characters should be selected as "data forwarding characters" using parameter 3.

Option	Description
0	No data forwarding time-out
1	Data forwarding time-out in 20ths of a second.

5 Ancillary Device Control
This parameter determines method of flow control used by the PAD to temporarily halt and restart the flow of data from the DTE during a call.

Option	Description
0	No flow control
1	XON/XOFF flow control
3	RTS/CTS flow control (not a standard X.3 parameter)

6 Suppression of PAD Service Signals
This parameter determines whether or not the "PAD>" prompt and/or Service/Command signals are issued to the DTE.

Option	Description
0	PAD prompt and signals disabled
1	PAD prompt disabled, signals enabled
4	PAD prompt enabled, signals disabled
5	PAD prompt enabled, signals disabled

7 Action on Break (from DTE)
This parameter determines the action taken by the PAD on receipt of a break signal from the DTE.

Option	Description
0	No action
1	Send an X.25 interrupt packet
2	Send an X.25 reset packet to the remote system
4	Send an X.29 indication of break
8	Escape to PAD command state
16	Set PAD parameter 8 to 1 to discard output

Multiple actions on receipt of break are possible by setting this parameter to the sum of the appropriate values for each action required.

For example, when parameter 7 is set to 21 (16 + 4 + 1), an X.25 interrupt packet is sent followed by an X.29 indication of break and then parameter 8 is set to 1.

You should NOT set this parameter to 16 because the remote system would receive no indication that a break had been issued and output to the DTE would therefore remain permanently discarded. If you need to use the discard output option, use it in conjunction with the X.29 break option so that on receipt of the X.29 break the remote system can re-enable output to your DTE using parameter 8.

8 Discard Output
This parameter determines whether data received during a call is passed to the DTE or discarded. It can only be directly set by the remote system and may be used in a variety of circumstances when the remote DTE is not able to handle a continuous flow of data at high speed.

Option	Description
0	Normal data delivery to DTE
1	Output to DTE discarded

9 Padding after CR
Slower terminal devices, such as printers, may require a delay after each Carriage Return before they can continue to process data. This parameter controls the number of pad characters (NUL - ASCII 0) that are sent after each CR to create such a delay.

Option	Description
0	No padding characters after CR
1 - 255	Number of padding characters (NUL) sent after CR

10 Line Folding
Controls the automatic generation of a [CR],[LF] sequence after a certain line width has been reached.

Option	Description
0	No line folding
1 - 255	Width of line before the PAD generates [CR],[LF]

11 Port Speed
This is a "read only" parameter, set automatically by the PAD and accessed by the remote system.

Option	Description
15	19,200 bps
14	9,600 bps
12	2,400 bps
3	2,400 bps

12 Flow Control of PAD (by DTE)
Determines the flow control setting of the PAD by the DTE in the on-line data state.

Option	Description
0	No flow control
1	XON/XOFF flow control
3	RTS/CTS flow control (not a standard X.3 parameter)

13 LF Insertion (after CR)
Controls the automatic generation of a Line Feed by the PAD.

Option	Description
0	No line feed insertion
1	Line Feeds inserted in data passed TO the DTE
2	Line Feeds inserted in data received FROM the DTE
4	Line Feeds inserted after CRs echoed to DTE

The line feed values can be added together to select Line Feed insertion to any desired combination.

14 LF Padding
Some terminal devices such as printers require a delay after each Line Feed before they can continue to process data. This parameter controls the number of padding characters (NUL - ASCII 0) that are sent after each [LF] to create such a delay.

Option	Description
0	No line feed padding.
1 - 255	Number of NUL characters inserted after LF

15 Editing
Enables (1) or disables (0) local editing of data input fields by the PAD before data is sent. The three basic editing functions provided are character delete, line delete and line re-display.

The editing characters are defined by parameters 16, 17 and 18. In addition, parameter 19 determines which messages are issued to the DTE during editing.

When editing is enabled, the idle timer delay (parameter 4) is disabled and parameter 3 must be used to select the desired data forwarding condition.

16 Character Delete Character
This parameter defines the edit mode delete character (ASCII 0-127). The default is backspace (ASCII 08).

17 Line Delete Character
This parameter defines the edit mode line buffer delete character (ASCII 0-127). The default is CTRL-X (ASCII 24).

18 Line Redisplay Character
Specifies the character that re-displays the current input field when in editing mode (ASCII 0-127). The default is CTRL-R (ASCII 18).

19 Editing PAD Service Signals
Specifies the type of service signal sent to the DTE when editing input fields.

Option	Description
0	No editing PAD service signals
1	PAD editing service signals for printers
2	PAD editing service signals for terminals

20 Echo Mask
This parameter defines characters that are NOT echoed when echo mode has been enabled using parameter 2.

Option	Description
0	No echo mask (all characters are echoed)
1	CR
2	LF
4	VT, HT or FF
8	BEL, BS
16	ESC,ENQ
32	ACK,NAK,STX,SOH,EOT,ETB,ETX
64	No echo of characters set by parameters 16, 17 & 18
128	No echo of characters set by parameters 16, 17 & 18

Combinations of the above sets of characters are possible by adding the respective values together.

21 Parity Treatment
This parameter determines whether parity generation/checking is used.

Option	Description
0	No parity generation or checking
1	Parity checking on
2	Parity generation on
3	Parity checking and generation on

22 Page Wait
This parameter determines how many line feeds are sent to the terminal before output is halted on a page wait condition. In other words, it defines the page length for paged mode output. A page wait condition is cleared when the PAD receives a character from the terminal.

Option	Description
0	Page wait feature disabled
1	Number of line feeds sent before halting output

Related CLI Commands

The X.3 PAD parameters can be edited from the command line using the **`set`** command described under the X.28 Commands section.

Configuration - Network > Legacy Protocols > X.25 > X.25 PVCs

A Permanent Virtual Circuit (PVC) provides the X.25 equivalent of a leased line service. With a PVC there is no call setup or disconnect process; you can just start sending and receiving X.25 data on a specified LCN. For each X.25 service connection you may setup up multiple PVCs each of which uses a different LCN (or a mixture of PVCs and SVCs). Digi routers support up to four PVCs numbered 0-3.

Configuration - Network > Legacy Protocols > X.25 > X.25 PVC n

Enable this PVC
Enables or disables the PVC.

LCN
This is the LCN value to be used for this PVC. In the case of an XOT PVC, this parameter defines the Responder LCN field in the PVC setup packet (though an LCN of 1 is always used in the XOT PVC connection). So for an XOT PVC this field should contain the remote connections LCN.

PVC Mode
This parameter defines the lower layer interface to be used for the PVC and can be set to "LAPB", "LAPD" or "TCP" (for XOT mode).

Connect this PVC to PAD x
This parameter defines what type of upper layer interface is connected to this PVC and can be set to "PAD" (for an X.25 PAD), "TPAD" (for a TPAD instance) or "XSW" (for X.25 switching). Note that if set to "XSW" (for the X.25 switch) then the X.25 switch will need to also be configured regarding the interfaces to switch this PVC to/from. For example, if this is an incoming XOT PVC we are configuring then the Switch from XOT PVC parameter needs to be set to the desired destination interface.

Use packet size
This parameter defines the packet size to be used for the PVC. Select the appropriate value from the drop down list.

Use window size
This parameter defines the layer 3 window size to be used for the PVC. Select the appropriate value from the drop down list.

Remote IP address
This is the IP address to be used for outgoing XOT calls.

Use the source IP address from interface x,y
This parameter defines which Ethernet or PPP interface to use for the source IP address.

Initiator interface
This parameter may be set to the name of the interface from which the PVC was initiated, e.g. Serial 1. The initiator and responder strings are used to identify the circuit when PVCs are being set up. They must match the names in the remote unit that terminates the XOT PVC connection. If the unit terminating the PVC XOT connection is not another Digi unit then you need to refer to the documentation or the configuration files of the other unit to determine the names of the interfaces.

Responder interface
This parameter may be set to the name of the interface to which a PVC initiator is connected, e.g. Serial 2.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
pvc	n	l2iface	Blank or lapb, lapd, tcp	Enable this PVC
pvc	n	lcn	0 - 4096	LCN
pvc	n	uliface	pad, tpad, xsw	Connect this PVC to PAD x
pvc	n	psize	0=default 4=16 5=32 6=64 7=128 8=256 9=512 10=1024	Use packet size
pvc	n	window	1 - 7	Use window size
pvc	n	ipaddr	IP address	Remote IP address
pvc	n	srcipent	auto, eth, ppp	Use the source IP address from interface x,y
pvc	n	srcipadd	0 - 255	Use the source IP address from interface x,y
pvc	n	iniface	text	Initiator interface
pvc	n	respiface	text	Responder interface

Configuration - Network > Legacy Protocols > MODBUS

Digi TransPort routers support conversion from MODBUS serial to MODBUS TCP.

When converting from MODBUS serial to MODBUS TCP over a WAN link it is necessary to have intelligence in the gateway\router to minimise the effect of the higher latency.

Digi TransPort supports being a MODBUS server only. Clients (e.g. remote PCs) can send overlapping requests and the Digi TransPort will create a queue of info requests and deal with them appropriately sending them out over the serial port and relaying the responses back. Overlapping polls from multiple clients are supported.

Enable MODBUS Gateway
Enables or disables MODBUS gateway instance.

Async Port
Configure the local serial port number (asynchronous port) for the MODBUS serial interface.

Async Mode
Configures the serial driver for RS232 or RS485 on supported hardware.

Duplex Mode
Sets the duplex mode to half or full. Full would be for 4-wire installations otherwise half is required.

Idle Gap

When receiving an modbus response from a station when this idle gap (pause with no reception of characters) is detected the message (currently received from the station) is at that staged forwarded on as the complete response.

Fix slave address

The address of the slave is fixed at this value. An address conversion will take place if a message that does not contain this address is received from the TCP master. If not used the TCP master must use the correct slave address.

Adjust slave address

The address of the slave is adjusted by this value. If left to zero then the slave address is not adjusted at all.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
modbus	n	enabled	1 = enabled, 0 = disabled	Enable MODBUS Gateway
modbus	n	asy_add	0 - 255	Async Port
modbus	n	async_mode	RS322 or RS422	Async Mode
modbus	n	duplex	0 = full, 1 = half	Duplex Mode
modbus	n	idle_gap	0 - 2147483647	Idle Gap
modbus	n	fix_slave_address	0 - 255	Fix slave address
modbus	n	adj_slave_address	0 - 255	Adjust slave address
modbus	n	ipport0	0 - 65535	IP Port (row 1)
modbus	n	nbsocks0	0 - "currently available"	Number of sockets (row 1)
modbus	n	ipmode0	0 = TCP, 1 = UDP	IP Mode (row 1)
modbus	n	rawmode0	1 = enabled, 0 = disabled	Raw Mode (row 1)
modbus	n	Ipport1	0 - 65535	IP Port (row 2)
modbus	n	nbsocks1	0 - "currently available"	Number of sockets (row 2)
modbus	n	ipmode1	0 = TCP, 1 = UDP	IP Mode (row 2)
modbus	n	rawmode1	1 = enabled, 0 = disabled	Raw Mode (row 2)

Configuration - Network > Protocol Switch

The Protocol Switch software available on some models provides X.25 call switching between the various protocols and interfaces that may be available including:

Interface / Protocol	Description
Off/None	Data will not be switched from / backed-up to this protocol
LAPD	Data will be switched from / backed-up to LAPD using the X.25 service.
LAPD X	As above but the actual LAPD instance used will be determined by the NUA.
LAPB 0	Data will be switched from / backed-up to LAPB 0.
LAPB 1	Data will be switched from / backed-up to LAPB 1.
LAPB 2	Data will be switched from / backed-up to LAPB 2.
LAPB 0 PVC	Data will be switched from / backed-up to an X.25 PVC on LAPB 0.
LAPB 1 PVC	Data will be switched from / backed-up to an X.25 PVC on LAPB 1.
LAPB 2 PVC	Data will be switched from / backed-up to an X.25 PVC on LAPB 2.
XoT	Data will be switched from / backed-up to an XOT (X.25 over TCP/IP) connection.
XoT PVC	Data will be switched from / backed-up to an XOT PVC connection.
TCP stream	Data will be switched from / backed-up to a TCP socket. The socket's IP address will be determined from the IP stream port setting.
UDP stream	This is similar to the TCP stream setting but instead of switching onto a TCP socket, data is switched onto a UDP socket. In the case of switching from X.25. the effect is that a UDP frame will be sent for each packet of X.25 data being switched.
VXN	Data will be switched / backed-up to Datawire's VXN protocol
SSL	Data will be switched / backed-up to SSL
DialServ	Data will be switched backed-up to an analogue modem via the built in DiaslServ daughter card.

When this optional feature is included, the unit may be configured to pass X.25 calls or data received in a TCP connection to another protocol or interface.

In addition, it is possible to specify a backup protocol or interface so that if an outgoing call on one interface fails, then the backup interface is automatically tried. LAPB can be used to switch to either ISDN or X.25 over serial depending on the configuration of the LAPB instance chosen.

The logic used in the switching software is outlined in the flowchart below. The following notes provide a more in-depth explanation of the actions taken in each of the numbered boxes.

The unit will first look up the Called NUA/NUI in the Configuration - Network > Protocol Switch > NUA to Interface Mappings mapping table to determine the IP address to use in the event that the call ends up being switched to a TCP or XOT interface. If a match is found on the Called NUA/NUI the unit assigns the matching IP address from the table to the call. If IP address mapping table does not contain an entry for the Called NUA/NUI and the call is eventually switched to a TCP or XOT channel then the default IP address (IP Stream or XOT Remote IP Address) is used.

The unit then determines from the source interface of the incoming call which interface type it should be switched to (from the Switch from parameters on the Protocol Switch page). For example, if the call arrived via a LAPB 0 interface and the Switch from LAPB 0 to parameter was set to LAPD, then the outgoing interface would LAPD.

If the outgoing interface is LAPD the unit changes the Calling NUA field of the incoming call to the D-Channel NUA value (as defined on the Protocol Switch page). If the outgoing interface is NOT LAPD processing proceeds as at step 6.

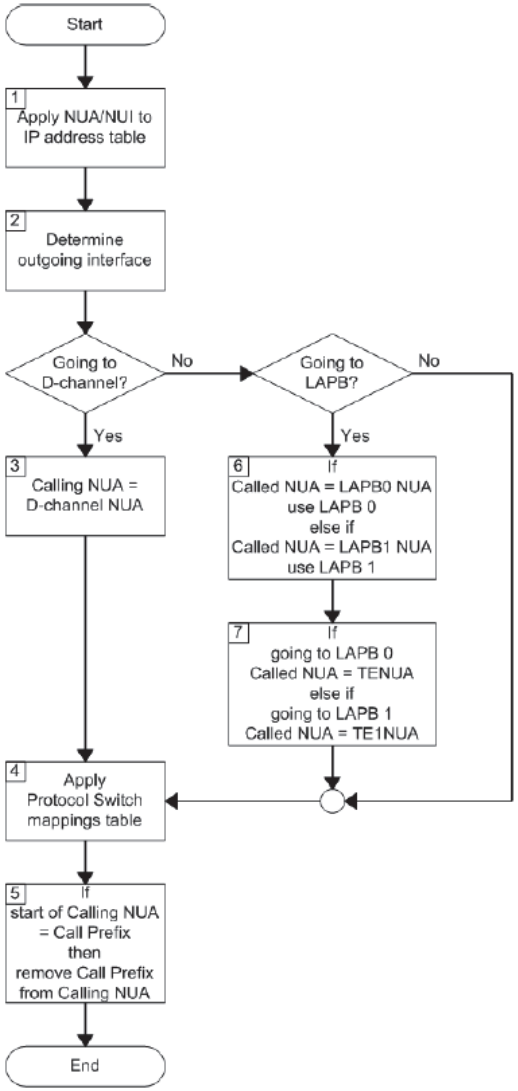
The unit then searches the Configuration - Network > Protocol Switch > NUA Mappings table to see if there are any matches for the Called or Calling NUA values on the specified interface. In cases where there Interface Description Off/None Data will not be switched from / backed-up from this protocol is a match, the NUA In value is substituted by the NUA out value, i.e. the mapping is applied individually to both the Calling NUA and Called NUA for the packet.

The unit then checks the leading characters of the Calling NUA to see if there is a match with the Call Prefix parameter. If there is a match then the prefix digits are removed before the outgoing X.25 call is made. Otherwise the call is made anyway and the switching process is complete for this call.

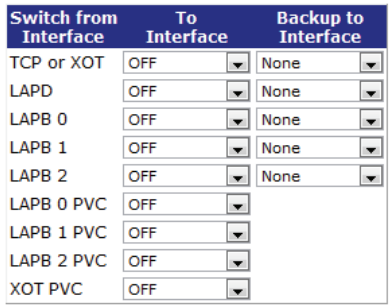
If after step 3, the unit has determined that the outgoing interface is not LAPD, it checks if the outgoing interface is LAPB. If it is, it then checks to see if the Called NUA field in the call packet matches the LAPB 0 NUA parameter and if it does, selects LAPB 0 as the outgoing interface. If the Called NUA field does not match LAPB 0 NUA, it checks for a match with LAPB 1 NUA and if there is a match, sets the outgoing interface to LAPB 1.

If the Called NUA field in the calling packet matches neither the LAPB 0 NUA or LAPB 1 NUA parameters then the outgoing interface is set to the interface specified by the relevant Switch from parameter.

If the call is being switched over LAPB 0 the unit then sets the Called NUA to the TE NUA (LAPB 0) value. If the call is being switched over LAPB 1 the unit then sets the Called NUA to the TE NUA (LAPB 1) value.



Parameters



TCP or XoT
This parameter controls the switching of incoming X.25 calls received via TCP or XOT. Select the interface to which data should be switched from the drop down list, or select "Off" and the protocol switch will not respond to any incoming XOT or TCP connections.

LAPD
This parameter controls the switching of incoming X.25 calls received via ISDN LAPD. Select the interface to which data should be switched from the drop down list, or select "Off" and the protocol switch will not respond to any incoming LAPD calls.

LAPB X
This parameter controls the switching of incoming X.25 calls received via LAPB X. Select the interface to which data should be switched from the drop down list, or select "Off" and the protocol switch will not respond to any incoming LAPB X calls.

LAPB X PVC
This parameter controls the switching of incoming X.25 calls received via an LAPB X PVC. Select the interface to which data should be switched from the drop down list, or select "Off" and the protocol switch will not respond to any incoming PVC calls on LAPB X.

XOT PVC
This parameter controls the switching of incoming X.25 calls received via an XOT PVC. Select the interface to which data should be switched from the drop down list, or select "Off" and the protocol switch will not respond to any incoming XOT PVC calls.

TCP XOT backup to interface
If any of the Switch from parameters has been set to XOT, and XOT is unavailable, this parameter may be used to specify an alternative interface to switch the X.25 call to. Any of the other interfaces may be chosen, or "None". If "None" is chosen, then no backup call will be attempted.

LAPD backup to interface
If any of the Switch from parameters has been set to LAPD, and LAPD is unavailable, this parameter may be used to specify an alternative interface to switch the X.25 call to. Any of the other interfaces may be chosen, or "None". If "None" is chosen, then no backup call will be attempted.

LAPB X backup to interface
If any of the Switch from parameters has been set to LAPB X, and LAPB X is unavailable, this parameter may be used to specify an alternative interface to switch the X.25 call to. Any of the other interfaces may be chosen, or "None". If "None" is chosen, then no backup call will be attempted.

VXN backup to interface
If any of the Switch from parameters has been set to VXN, and VXN is unavailable, this parameter may be used to specify an alternative interface to switch the X.25 call to. Any of the other interfaces may be chosen, or "None". If "None" is chosen, then no backup call will be attempted.

LAPD Parameters

Calling Prefix
This parameter specifies the call prefix to inserted in front of the NUA in calls being switched to LAPD. For example, if the called NUA in the call being received by the LAPB 0 interface is 56565 and the call prefix is 0242 then the call placed on the LAPD interface is to NUA 024256565. Also, for calls in the reverse direction, if the prefix in the calling NUA matches this parameter then it is removed from the calling NUA field.

D-Channel LCN
This is the value of the first LCN that will be assigned for outgoing X25 calls on LAPD.D-Channel LCN Direction

Max VCs: Unlimited
This parameter sets the maximum number of Virtual Circuits (VCs) to be used on an LAPD interface. When the maximum has been reached, then the backup call will take place immediately (or the call will clear if there is no backup call). If this parameter is set to "0", there is no limit.

Default Packet Size
This is the default packet size for X.25 calls being switched onto LAPD. The default packet size is 128, other possible values are 256, 512 or 1024 bytes.

Default Window Size
This is the default window size for calls being switched onto LAPD. The default window size is 2, the valid range is 1 to 7.

LAPB Parameters

LCN
This is the value of the first LCN that will be assigned for outgoing X25 calls on LAPB.

LCN direction: Up Down
This parameter determines whether the LCN used for outgoing X.25 calls on LAPB is incremented or decremented from the starting value.

Max VCs: Unlimited
This parameter sets the maximum number of Virtual Circuits (VCs) to be used on an LAPB interface. When the maximum has been reached, then the backup call will take place immediately (or the call will clear if there is no backup call). If this parameter is set to "0", there is no limit.

B-Channel Number:
This parameter specifies an ISDN number to be used for calls being switched in the direction of LAPB 0 or LAPB 1.

Enable ENQ Char:
When this parameter is set to "On", when an incoming call on LAPB is switched and the unit connects to it, the X.25 switch sends a data packet on the LAPB X.25 SVC containing the ENQ character.

LAPB 0 Default Packet Size: 128 256 512 1024
This is the default packet size for calls being switched onto LAPB 0. The default packet size is 128, other possible values are 256, 512 or 1024 bytes.

LAPB 0 Default Window Size: 2 1 3 4 5 6 7
This is the default window size for calls being switched onto LAPB 0. The default window size is 2, the valid range is 1 to 7.

LAPB 1 Default Packet Size: 128 256 512 1024
This is the default packet size for calls being switched onto LAPB 1. The default packet size is 128, other possible values are 256, 512 or 1024 bytes.

LAPB 1 Default Window Size: 2 1 3 4 5 6 7
This is the default window size for calls being switched onto LAPB 1. The default window size is 2, the valid range is 1 to 7.

LAPB 2 Default Packet Size: 128 256 512 1024
This is the default packet size for calls being switched onto LAPB 2. The default packet size is 128, other possible values are 256, 512 or 1024 bytes.

LAPB 2 Default Window Size: 2 1 3 4 5 6 7
This is the default window size for calls being switched onto LAPB 2. The default window size is 2, the valid range is 1 to 7.

IP Stream / XOT Parameters

IP Stream or XOT Remote IP Address:
For calls being switched in the direction of XOT, this parameter specifies the destination IP address to be used for the outgoing XOT call. This is also used as the destination IP address in the IP/UDP stream modes.

IP Stream or XOT Backup IP Address:
If the Switch from XOT to parameter is set to "XOT", this is the IP address that the XOT call will be switched to, in the event the original XOT IP address is unavailable.

IP Stream Port:
This parameter determines the IP port number used when IP stream or UDP stream are selected as the parameter for any of the Switch from or Backup from parameters.

Note:
The XOT remote IP address and IP stream port parameters will be overridden by the values in the NUA/NUI to IP addresses table if the call matches any entry in that table.

IP Length Header: Off On 8583 Ascii 4 byte On(inclusive)
When IP length header is "On", a length indicator field is inserted at the start of each packet. When set to "8583 Ascii 4 byte", the IP length header will conform to the ISO 8583 format.

Source IP address interface: Auto Ethernet PPP
The default value for this parameter is "Auto", which means that the source IP address of an outgoing XOT connection on an un-NATed W-WAN link is the address of the PPP interface assigned to W-WAN. This is because the XOT connection is initiated (automatically) within the router and so does not originate from the local subnet (LAN segment to which the unit is attached via the Ethernet interface).

However, this means that if you are routing traffic from the local subnet across a VPN tunnel you would have to set up two Eroutes; one to match the local subnet address and one to match the XOT source address (i.e. the address of the PPP interface associated with to the wireless network).
By setting this parameter to "Ethernet" the unit will use the IP address of the Ethernet port instead of that of the PPP interface so that you need only set up on Eroute.

X.25 Parameters

Don't switch facilities:
If this parameter is set to "Off", the packet size and window size are only switched if they need to, i.e. they specify a value different from what is currently being negotiated. If this parameter is set to "On", the facilities shall not be switched.

Don't strip facilities:
When set to "On" this parameter stops the X.25 switch from stripping packet size and window size facilities as it switches an X.25 call. When set to "Off", the X.25 switch will strip facilities if the requested facilities match the defined defaults for that interface.

L2 Deactivation Clear Cause:
When one side of a switch call fails because layer 2 drops, the other side is usually cleared with a clear cause 9 "out of order". This parameter allows you to set this code to any value.

X25 Version: 84 88
This parameter allows you to switch between X.25 version 88, and X.25 version 84, in which clear causes are always "0" when issued if the unit is the DTE.

Interpret no facilities on Call Accept as P7W2:
When this parameter is set to "On", the X.25 switch will interpret any call accept packets that do not include the window size ('W') or packet size ('P') as if the call accept has 'P7W2' (i.e. a packet size of 128 bytes and a windows size of 2).

Notes on PAD Answering
Because the other interfaces can operate as normal, even when the switch is operating, special care needs to be taken with regard to answering NUAs programmed on active PADs. For example when a call is being received on a LAPD or LAPB interface, a PAD instance (or remote configuration session) is capable of answering and terminating the call in preference to the call being switched. This means that the PADs "Answering NUA" parameters should be left blank to ensure that the unit's PADs are not answering calls that need to be switched. If you do want a PAD instance to answer a call then program the "Answering NUA" field with as many digits as you can to ensure it only answers calls destined for that PAD. The same precautions apply to the **Allow CLI access from X.25 address** parameter on the ***Configuration - System > General*** page.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
X25sw	0	swfrlapb0	0,1,3- 10,12-15 (see below)	Switch from LAPB 0 to
X25sw	0	swfrlapb0pvc	0-5,7-10,12-15 (see below)	Switch from LAPB 0 PVC to
X25sw	0	swfrlapb1	0-2,4-10,12-15 (see below)	Switch from LAPB 1 to
X25sw	0	swfrlapb1pvc	0-6,8-10,12-15 (see below)	Switch from LAPB 1 PVC to

Entity	Instance	Parameter	Values	Equivalent Web Parameter
X25sw	0	swfrlapb2	0-10,13-15 (see below)	Switch from LAPB 2 to
X25sw	0	swfrlapb2pvc	0-10,12, 14, 15 (see below)	Switch from LAPB 2 PVC to
X25sw	0	swfrlapd	0, 2-10,12-15 (see below)	Switch from LAPD to
X25sw	0	swfrxot	0-3,5-10,12-15 (see below)	Switch from XOT (TCP) to
X25sw	0	swfrxotpvc	0-7,9,10,12-15 (see below)	Switch from XOT PVC to
X25sw	0	callprefix	<NUA>	Calling Prefix
X25sw	0	dlcn	0-65535	D-Channel LCN
X25sw	0	dlcnup	off, on Off = Down On = Up	D-Channel LCN Direction
X25sw	0	dmaxvc	0-65535	Max VCs
X25sw	0	lapb0ppar	7,8,9,10 7=128 8=256 9=512 10=1024	Default Packet Size
X25sw	0	lapb0wpar	1-7	Default Window Size
X25sw	0	blcn	0-65535	LCN
X25sw	0	blcnup	off, on Off = Down On = Up	LCN direction
X25sw	0	bmaxvc	0-65535	Max VCs
X25sw	0	bnumber	ISDN number	B-Channel Number
X25sw	0	benqcon	off, on	Enable ENQ Char
X25sw	0	lapdppar	7,8,9,10 7=128 8=256 9=512 10=1024	LAPB 0 Default Packet Size
X25sw	0	lapdwpar	1-7	LAPB 0 Default Window Size
X25sw	0	lapb1ppar	7,8,9,10 7=128 8=256 9=512 10=1024	LAPB 1 Default Packet Size
X25sw	0	lapb1wpar	1-7	LAPB 1 Default Window Size

Entity	Instance	Parameter	Values	Equivalent Web Parameter
X25sw	0	lapb2ppar	7,8,9,10 7=128 8=256 9=512 10=1024	LAPB 2 Default Packet Size
X25sw	0	lapb2wpar	1-7	LAPB 2 Default Window Size
X25sw	0	ipaddr	IP address	IP Stream or XOT Remote IP Address
X25sw	0	buipaddr	IP address	IP Stream or XOT Backup IP Address
X25sw	0	ip_port	0-65535	IP Stream Port
X25sw	0	iphdr	0,1,2 0=Off 1=On 2=8583 Ascii 4 byte	IP Length Header
X25sw	0	srcipadd	Interface number 0-65535	Source IP address interface
X25sw	0	srcipent	<blank>, PPP, ETH	Source IP address interface
X25sw	0	noswfac	off, on	Don't switch facilities
X25sw	0	nostripfac	off, on	Don't strip facilities
X25sw	0	l2deactcc	0-65535	L2 Deactivation Clear Cause
X25sw	0	x25ver84	off, on Off=88 On=84	X25 Version
X25sw	0	accdefp7w2	off, on	Interpret no facilities on Call Accept as P7W2

Interfaces are coded as follows:

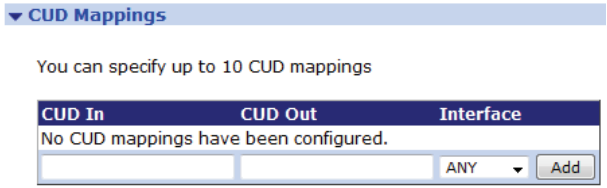
Parameter value	Interface type
0	None
1	LAPD
2	LAPB 0
3	LAPB 1
4	XOT
5	LAPD X (actual instance is determined by NUA)
6	LAPB 0 PVC
7	LAPB 1 PVC
8	XOT PVC
9	TCP stream

Parameter value	Interface type
10	UDP stream
12	LAPB 2
13	LAPB 2 PVC
14	VXN
15	SSL

Configuration - Network > Protocol Switch > CUD Mappings

Protocol Switch CUD mappings allow you to map an incoming call's CUD (call user data) from one value to another. The PID (protocol identifier) portion of the CUD (if present) is maintained from input to output and is not involved in the comparison.

The ***Configuration - Network > Protocol Switch > CUD Mappings*** web page displays a table with four columns in which you can specify the CUD In values, corresponding CUD Out values and to which interfaces the mappings should be applied. The "interface" field defines which output interfaces this mapping applies to. Wildcard characters are allowed, and In each case the interface type to which the mapping applies can be selected from "ANY", "LAPD", "LAPB0", "LAPB1" "LAPB2" or "XOT".



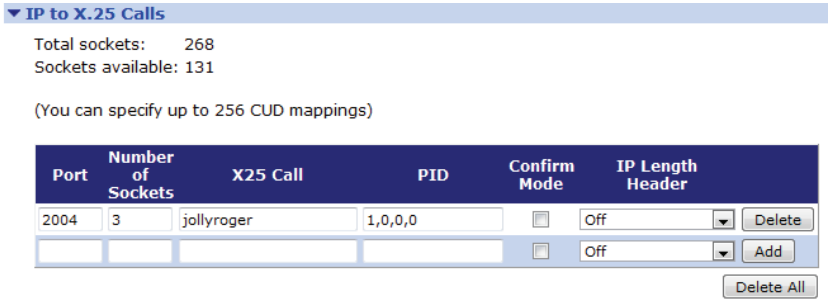
Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
cudmap	0-9	cudfrom	0-65536	CUD In
cudmap	0-9	cudto	0-65536	CUD Out
cudmap	0-9	Interface	0,1,2,3,4,12 0=Any 1=LAPD 2=LAPB 0 3=LAPB 1 4=XOT 12=LAPB 2	Interface

Configuration - Network > Protocol Switch > IP Sockets to Protocol Switch

This page contains a table that allows you to enter a series of IP Port numbers and X.25 Call strings as shown below. It is used to configure the unit so that IP data can be switched to any of the protocols support by the protocol switch includingX.25. For example data that is received on a TCP connection can be forwarded over SSL, XoT or a UDP stream. The only columns that must be filled out are "Port" and "Number of Sockets".

This table is duplicated in the ***Configuration - Network > Legacy Protocols > X.25 > IP to X.25 Call*** section as it can also be used to convert an incoming TCP connection to an X.25 session to be answered by PAD without using the protocol switch. It is included at this point in the web user interface as a convenience in case the table is being used in conjunction with PAD and not the protocol switch.



IP Port
The IP Port field is used to setup the port numbers for those IP ports that will "listen" for incoming connections that are to be switched over X.25 or other protocol. In the case of switching to X.25, when such a connection is made the unit will make an X.25 Call to the address specified in the X.25 Call field. Once this call has been connected, data from the port will be switched over the X.25 session.

Number of Sockets
The Number of Sockets field is used to select how many IP sockets should simultaneously listen for data on the specified port. The number of available IP sockets will depend on the model you are using and how many are already in use (see note below).

X25 Call
The X.25 call field may contain an X.25 NUA or NUI or one of the X.25 Call Macros defined on the ***Configuration - Advanced applications > X25 > Macros page***.

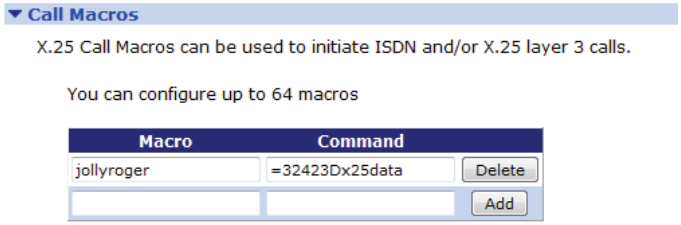
PID
The PID (Protocol Identifier), field specifies the PID to use when the unit switches an IP connection to X.25. The PID (protocol ID) field takes the format of four hexadecimal digits separated by commas, e.g. 1,0,0,0, at the start of the Call User Data field in the X.25 call.

Confirm Mode
When confirm mode is set to "On" then the incoming TCP socket will not be successfully connected until the corresponding outgoing call has been connected. The incoming TCP socket will trigger the corresponding outgoing call either to a local PAD instance or to whatever is configured. The effect of this mode is that the socket will fail if the outbound call fails and so may be useful in backup scenarios. In addition it will ensure that no data is sent into a "black hole". (When this setting is not enabled data that is sent on the inbound TCP connection before the outbound connection has been successful can be lost.)

RFC 1086 Mode:
RFC 1086 specifies a mode of operation in which the IP socket answers and then with a simple protocol in the socket identifies the X.25 address and other X.25 call setup parameters to be used. Then when the X.25 call parameters have been identified the X.25 call is made and if successful then data is then switched between the X.25 call and the IP socket. The protocol will select whether incoming or outgoing support is required.

IP length header
When IP length header is "On", the IP length indicator field is inserted at the start of each packet. When set to "8583 Ascii 4 byte", the IP length header will conform to the ISO 8583 format.

In the example above, 3 IP sockets will "listen" for an incoming connection on IP Port 2004. Once connected they will each will make an X.25 Call to "jollyroger". The unit will recognise that "jollyroger" is a pre-defined macro (as illustrated below), and will translate it into an X.25 Call to address 32423 with the string "x25 data" included as data in the call. The outgoing X.25 call(s) will be made over whichever interface is specified by the Switch from XOT(TCP) to parameter on the ***Configuration - Network > Protocol Switch*** page.



Note:
At the top of the page the total number of sockets available and the number currently free is shown. Care should be take not to allocate too many of the free sockets unless you are confident that they are not required for other applications.

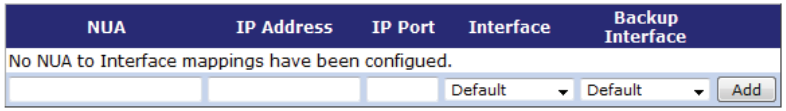
Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ipx25	n	ip_port	0 - 65535	IP Port
ipx25	n	nb_listens	0 – software dependant max	Number of Sockets
ipx25	n	x25call	NUA, NUI or X.25 macro name	X25 Call
ipx25	n	pid	hex numbers	PID
ipx25	n	cnf_mode	1 = enabled, 0 = disabled	Confirm Mode
ipx25	n	rfc1086_mode	1 = enabled, 0 = disabled	RFC 1086 Mode
ipx25	n	iphdr	0=Off 1=On 2=8583 Ascii 4 byte	IP length header

Configuration - Network > Protocol Switch > NUA to Interface Mappings

This page contains a table that allows you to enter a series of X.25 NUA or NUI values along with IP addresses/Ports to which they should be mapped if you need to override the default settings in the Configuration - Network > Legacy Protocols > X.25 > NUA/NUI Interface Mappings page.

(You can specify up to 256 NUA to Interface mappings)



So, if in the Protocol Switch configuration you had configured the unit to switch from LABP 0 to TCP, the IP Address and Port values would normally be determined from the XOT Remote IP address and IP stream port parameters. However, having set up the NUA/NUI to IP addresses table as shown in the example above, if an X.25 call with NUA of value "222" is received on LAPB 0 it will be switched onto a TCP socket using IP address "1.2.3.4" on port 45 instead of those settings configured on the Configuration - Network > Legacy Protocols > X.25 > NUA/NUI Interface Mappings page.

Similarly, NUIs can also be matched and in this example a call with NUI of value "test" will be switched onto a TCP socket using IP address "100.100.100.1" on port 678.

All 3 comparison fields, NUA, NUI and Call Data, can use the wildcard matching characters "?" and "*". In the example shown above when an X.25 call is received with either the NUA having "1234" followed by any 2 digits or a call being received with call user data with any 4 characters followed by "aa" then the call is switched to a TCP socket on address 100.100.100.52 on port 4001.

When a connection has been successfully established and data is being switched from the X.25 call to the socket and from the socket to the X.25 connection, it can be terminated by either the socket closing or the X.25 call clearing.

If the connection terminates because of an incoming X25 Call Clear packet then the switch will terminate the socket connection. If the connection terminates because the socket is closed then the switch will clear the X.25 call by transmitting a CALL CLEAR packet.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
nuaip	0-255	nua	0-65536	NUA
nuaip	0-255	ipaddr	IP address	IP Address
nuaip	0-255	ip_port	0-65536	IP Port
nuaip	0-255	swto	0-10, 12-15 (see table below)	Interface
nuaip	0-255	buswto	0-10, 12-15 (see table below)	Backup Interface

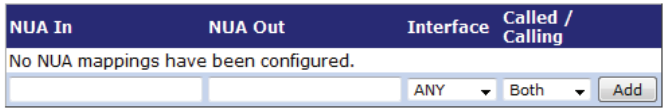
Interfaces are coded as follows:

Parameter Value	Interface Type
0	Default
1	LAPD
2	LAPB 0
3	LAPB 1
4	XOT
5	LAPD X (actual instance determined by NUA)
6	LAPB 0 PVC
7	LAPB 1 PVC
8	XOT PVC
9	TCP stream
10	UDP stream
12	LAPB 2
13	LAPB 2 PVC
14	VXN
15	SSL

Configuration - Network > Protocol Switch > NUA Mappings

Protocol switch NUA mappings allow you to redirect specified NUAs to alternative NUAs for switched X.25 calls. Up to twenty "NUA In" to "NUA Out" mappings are available. These mappings alter the called NUA field in any X.25 call. The comparison uses "tail" matching, so that only the rightmost digits in the NUA are compared with the table entry.

You may specify up to 20 NUA mappings



This page displays a table with four columns in which you can specify the NUA In values, corresponding NUA Out values, to which interfaces the mappings should be applied, and whether the mapping should apply if the unit is making the call, receiving the call, or both. For example, if the called NUA is 123456789345 and there is an NUA In table entry of 9345, with Called/Calling set to either "Both" or "Called", then this will match, and the entire called NUA will be replaced with the corresponding NUA Out entry. In each case the interface type to which the mapping applies can be selected from "ANY", "LAPD", "LAPB0", "LAPB1" "LAPB2" or "XOT".

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
X25map	0-19	nuafrom	0-65536	NUA In
X25map	0-19	nuato	0-65536	NUA Out
X25map	0-19	interface	0,1,2,3,4,12 0=Any 1=LAPD 2=LAPB 0 3=LAPB 1 4=XOT 12=LAPB 2	Interface
X25map	0-19	ca_or_ci	0,1,2 0=Both 1=Called 2=Calling	Called / Calling

Configuration – Alarms > Event Settings

The router maintains a log of events in the "LOGCODES.TXT" pseudo file. When an event of a specified (or lower priority) level occurs, a syslog message, an email alert or SMS alert (on W-WAN models) can be sent to a pre-defined address.

The ***Configuration > Alarms > Event Settings*** folder opens to show the following parameters:-

Only log events with a log priority of at least n
This parameter enables a filter that ensures that only events having a specified severity or lower level are logged.

Do not log the following events
This is a numerical list of comma-separated values specifying events to be excluded from the log. These numerical values can be found in the eventlog.txt file on the router.

After power up, wait s seconds before sending Emails, SNMP traps, SMS or Syslog messages
This parameter specifies the delay, in seconds, after power-up that the router should wait before sending any alert messages. This is useful in circumstances where the sending of those items would fail if sent too soon after the unit powers up because the underlying interface that would be used has not completed initialisation.

Include event number in the event log and Email, SNMP traps or Syslog messages
When this option is enabled, event numbers from the "logcodes.txt" file will be included.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
event	n	loglevel	0 – 9 0 none 1 low 9 high	Only log events with a log priority of at least n
event	n	ev_filter	Comma separated list of event numbers	Do not log the following events
event	n	action_dly	Number of seconds (e.g. 60)	After power up, wait s seconds before sending Email, SNMP traps, SMS or Syslog messages
event	n	incevnums	0,1	Include event number

Configuration – Alarms > Event Settings > Email Notifications

To use the email alert facility, you must first ensure that a valid Dial-out number, Username and Password have been specified and that the SMTP parameters have been set correctly. The Dial-out number, Username and Password parameters are to be found in the ***Configuration – Network > Interfaces > Advanced > PPP n*** pages where n is the relevant interface number.

The SMTP parameters are to be found under ***Configuration – Alarms > SMTP Account***.

Send email notifications
This checkbox simply enables the display of the configurable parameters when checked.

Send an email notification when the event priority is at least n
This is the lowest priority event that will generate an email alert message. For example, if this value is set to 6, only events with a priority of 6 or lower (7, 8 or 9) will trigger an automated email alert message. To disable email alarms, set this value to 0.

Send a maximum of n emails per day
This parameter sets the limit on the number of emails that may be sent during any 24 hour period. The intention is to prevent excessive alerts being sent when the event trigger value is set to a high priority / low value (1, 2 or 3 for example), i.e. a value that results in a large number of automated email alert messages being generated.

n emails have been sent today
This is a status message, indicating how many emails have been sent during the last 24 hour period.

Use email template file
This field contains the name of a template file that will be used to form the basis of any email alert messages generated by the event logger. The default template is a file called "EVENT.EML" that is stored within the compressed .web file. Alternative templates may be created, but in order to be valid, these must have the ".EML" file extension and be stored in the normal file directory. A new template having the name "EVENT.EML" will take precedence over the predefined "EVENT.EML" template but it is recommended that a new name is used, such as "event1.eml".

Email To
This text field is the standard email address format for the intended recipient of the alert.

Email From
This text field should contain a valid email address that will be accepted by the SMTP server as being authorised to send email.

Email Subject
This text field should contain a short description of the email content.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
event	n	etrig	0 – 9 0 disables sending alerts	Send an email notification when the event priority is at least n
event	n	emax	0 – 255	Send a maximum of n emails per day
event	n	etemp	The name of a template file. Default is EVENT.EML	Use email template file
event	n	to	A valid email address, e.g. you@yourdomain.com	Email To
event	n	from	A valid email address	Email From
event	n	subject	A brief description of the content of the email	Email Subject

Configuration – Alarms > Event Settings > SNMP Traps

The router firmware supports the use of SNMP, with the ability to generate traps. In order for this facility to function, a SNMP trap server will need to be configured. SNMP trap server configuration is to be found under ***Configuration – Remote Management > SNMP > SNMP Traps***.

Send SNMP Traps
This checkbox, when checked enables the display of the following parameters:

Send a SNMP Trap when the event priority is at least n
This is the lowest priority event that will generate an SNMP trap message. For example, if this value is set to 6, only events with a priority of 6 or lower (7, 8 or 9) will trigger an automated SNMP trap message. To disable SNMP traps, set this value to 0.

Send a maximum of n SNMP taps per day
This parameter sets the limit on the number of emails that may be sent during any 24 hour period. The intention is to prevent excessive alerts being sent when the event trigger value is set to a high priority / low value (1, 2 or 3 for example), i.e. a value that results in a large number of SNMP trap messages being generated.

n SNMP traps have been sent today
This is a status message, indicating how many SNMP trap messages have been sent during the last 24 hour period.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
event	n	trap_trig	0 – 9 0 disables sending alerts	Send a SNMP Trap when the event priority is at least n
event	n	trap_max	0 – 255	Send a maximum of n SNMP traps per day

Configuration – Alarms > Event Settings > SMS Messages

Note:
This option is only available on routers with W-WAN capability.

This section has three identical rows, each of which controls the setting of the SMS alert messages.

Send SMS messages to
This field should contain the destination telephone number (MSISDN) for SMS alert messages. The format for this field is the international dialling code followed by the number, but should not contain a '+' prefix. For example, UK mobile 07871 445677 would be 447871445677

If the event priority is at least n
This numeric input field sets the trigger level for the alert message. If, for example, this field is set to the value 6, only events having a priority of 6 or higher will trigger an automated SMS alert. Setting this field to 0 disables the sending of SMS alerts.

Use SMS template
This field contains the name of the template file that will be used to form the basis of any alarm messages generated by the event logger. The default template file is a test file called "EVENT.SMS" that is stored in the compressed .web file. A new template may be created, and if named "EVENT.SMS" will take precedence over the pre-defined "EVENT.SMS" template but it is recommended that a new name is used, such as "event1.sms". Templates should use the ".SMS" file extension.

Send a maximum of n SMS messages per day
This parameter limits the number of SMS alert messages sent by the router in any one day.

n SMS messages have been sent today
This is a status message, indicating how many SMS alert messages have been sent during the last 24-hour period.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
event	n	sms_to	A valid mobile number e.g. 447871445677	Send SMS messages to
event	n	sms_trig	0 – 9	If the event priority is at least n
event	n	sms_to2	A valid mobile number e.g. 447871445677	Send SMS messages to
event	n	sms_trig2	0 – 9	If the event priority is at least n
event	n	sms_to3	A valid mobile number	Send SMS messages to

Entity	Instance	Parameter	Values	Equivalent Web Parameter
			e.g. 447871445677	
event	n	sms_trig3	0 – 9	If the event priority is at least n
event	n	sms_temp	A valid mobile number e.g. 447871445677	Use SMS template
event	n	sms_max	0 – 255	Send a maximum of n SMS messages per day

Configuration – Alarms > Event Settings > Local Logging

A secondary log file can be created on a USB flash drive and events will be appended to this log file. This facility is useful if an extended logging period is required where, the normal eventlog.txt file would overwrite early events before the operator has had a chance to view them. The secondary log file can be limited in size or allowed to fill the USB flash drive. Once the log file is full, earlier events will be pruned from the end of the file to allow new events to be added.

Local Drive to log to
This parameter determines the drive letter where the USB flash drive is located. This is designated "u" for a USB drive.

Log filename
This specifies the name of the file for the secondary event log.

Log size
This field specifies the maximum size of the log file in kilobytes.

XML logs
On platforms that support it, event logs can be saved in XML format. This field specifies the size of the XML log file in kilobytes. The files created will be named EVXML1.XML, EVXML2.XML etc.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
event	n	logdrive	Drive letter, e.g. "**u**" for USB flash drive	Local drive to log to
event	n	logfile	Name of the file e.g. mylog.txt	Log filename
event	n	logsizek	Size of log in kilobytes e.g. 1048576 Which is 1MB	Log size
event	n	xmllogs		None

Configuration – Alarms > Event Settings > Syslog Messages

As well as logging events to an internal log file and to a file on a USB flash drive, the router can log events to a Syslog server.

This section describes how to configure the router to send Syslog messages to a Syslog server.

Send Syslog messages
When this checkbox is checked, the following options are displayed:

Send a Syslog message when the event priority is at least n
This is the lowest priority event that will generate a syslog message. For example, if this value is set to 6, only events with a priority of 6 or lower (7,8 or 9) will trigger an automated syslog message. To disable syslog messages, set this value to 0.

Send a maximum of n Syslog messages per day
This parameter sets the limit on the number of syslog messages that may be sent during any 24 hour period. The intention is to prevent excessive alerts being sent when the event trigger value is set to a high priority / low value (1, 2 or 3 for example), i.e. a value that results in a large number of syslog messages being generated.

n Syslog messages have been sent today
This is a status message that indicates how many Syslog messages have been sent in the last 24 hour period.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
event	n	syslog_trig	0 – 9	Send a Syslog message when the event priority is at least n
event	n	syslog_max	0 - 255	Send a maximum of n Syslog messages per day

Configuration – Alarms > Event Settings > Syslog Server n

This section describes the configuration of the router for defining the Syslog server to send messages to.

Syslog server IP address
This parameter sets the IP address of the server.

Port
This parameter sets the port to use.

Note:
The following three items (Mode, TCP timeout and Route) only appear on routers that have the TCP logging software option enabled. This is not a commonly used option.

Mode
There are currently three supported communication modes, these are selected from a drop-down list and are TCP, UDP and a protocol described in RFC 3195.

TCP timeout s seconds
For TCP communications, this parameter sets the timeout on the socket.

Route using

These radio buttons selects which method of establishing a route to the server should be used.

Routing table
When this radio button is selected, the routing table is used to determine the interface that will be used to transmit the syslog message.

Interface x,y
If the routing table is not to be used, an interface type (PPP or Ethernet) may be selected from the drop-down selection box and the interface instance number may be typed into the adjoining text entry box. The route is then determined by that interface.

Priority
The checkboxes listed in this section select the event priorities that should cause the event to be logged.

Facility
The checkboxes listed in this section select which of the router facilities should be logged.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
syslog	n	server	IP address	Syslog server IP address
syslog	n	port	IP port number	Port
syslog	n	mode	UDP, TCP, RFC3195	Mode
syslog	n	tcp_to	Timeout in seconds, e.g. 86400	TCP timeout s seconds
syslog	n	source_ent	PPP, ETH	Interface x,y x = Interface type
syslog	n	source_add	0 - 4	Interface x,y y = interface number
syslog	n	priority	Hyphen separated 0 – 7 Comma separated 0,3,5 or 'all'	Priority checkboxes
syslog	n	facility	Hyphen separated 0 – 23 Comma separated 4,3,5,10,15,22 or 'all'	Facility checkboxes

Configuration – Alarms > Event Logcodes

This page allows you to edit the logcodes used to describe events entered in the "EVENTLOG.TXT" pseudo file. If a change is made to the logcodes.txt file, the changes will be saved in the file logcodes.dif so when a firmware upgrade is performed the changes to the logcodes are retained.

The page that appears under the blue bar initially shows a table containing the Event descriptions and reason. Clicking on an item shown in bright blue (an HTML link) causes a configuration page associated with that item to be opened. The newly-opened page allows that item to be configured. The configuration options shown on that page are described below.

Event
This is not a configurable parameter; it is simply the event number, displayed for information only. This is the number to refer to when filtering events in the event log settings ***Configuration – Alarms > Event Settings***.

Description
This field is a description of the event code. Clicking on a link in this field brings up the configuration page associated with that event.

Filter
This parameter is for information only. If event filtering is applied to an event, the associated filter is shown as "On". This is a result of enabling the parameter 'Do not log this event' as described below.

Event Priority
This parameter controls the priority of the event and is used to determine whether an event will trigger email, SMS messages or SNMP traps.

Reasons
The reason why the event occurred. Not every event has a list of reasons.

Reason Priority
This parameter is for information only.

Attachment List ID
This is just a fixed list of values that may be used to conveniently refer to the associated list of files to attach to an email.

Files
This text entry box allows the user to type in a comma-separated list of names for the files that should be attached to an email.

Configuration – Alarms > Event Logcodes > Configuring Events

This page controls the configuration of the event that is displayed in bold font at the top of the page, just below the blue title bar.

Do not log this event
When checked, this checkbox disables logging of the event.

Note:
This parameter is **not** saved in the logcodes.txt file but in the config.dan file. This means that after changing this parameter, the changes must be saved by clicking the save changes link when prompted (this appears after clicking the "Apply" button). Clicking the Save All Event Code Changes will not have the desired effect.

Log Priority
This parameter sets the priority of the event to determine whether the event will trigger emails, SMS messages or SNMP traps. 0 = disabled, 1 = highest priority, 9 = lowest priority

Alarm Priority
If the above "Inherit alarm priority from event" checkbox is **not** checked, this parameter selects the priority of the reason. Valid values are 0 to 9.

Alarm Priority is dependent on the event being logged by Entity
Selecting this checkbox makes the priority conditional on which system entity triggered the event (e.g. ethernet) and enables the following two configuration options:

Entity
This drop-down selection box contains a list of the system entities.

All
Selecting this radio button causes all of the system entities

Instance
Selecting this radio button enable a text entry box that allows the user to enter the instance of the selected entity.

Priority only applies to
This configuration section comprises a set of checkboxes, each checkbox controlling whether the priority is applied to that interface instance. So for example, to apply the priority to PPP interface 1, click on the checkbox labelled PPP 1.

Store a snapshot of the Traffic Analyser trace on the log drive
Selecting this checkbox causes a snapshot of the analyser trace to be stored on the USB flash drive

If this event creates an Email alarm

Attach a snapshot of the Traffic Analyser trace
Checking this checkbox will cause a snapshot of the analyser trace to be attached to the email.

After this event

Leave the Analyser trace
This option will leave the analyser trace unchanged.

Freeze the Analyser trace
This selection will cause the analyser to be "frozen", i.e. no more logging will take place until the email has been sent.

Delete the Analyser trace
This selection will cause the analyser trace to be deleted once the email has been sent.

Attach a snapshot of the Event Log
Selecting this checkbox will cause the eventlog to be attached to the email.

After this event

Leave the Event Log
Selecting this radio button will leave the event log unchanged.

Delete the Event Log
Selecting this radio button will cause the event log to be deleted after the email has been sent.

Attachment List ID
This text entry box allows the user to specify which files to attach to the email. The ID refers to the table of files.

Syslog Priority
This drop-down selection box contains the following options:
Emergency, Alert, Critical, Error, Warning, Info, Debug

Syslog Facility
This drop-down selection box contains the following options:
Kernel, User, Mail, System, Auth, Syslog

Configuration - Alarms > Event Logcodes > Configuring Reasons

The page invoked by selecting a reason link in the event logcodes table is very similar to the Configuring Events page but with the following differences.

There is no "Do not log this event" checkbox. There is the following additional parameter:

Inherit alarm priority from event
Selecting this checkbox causes the following "Alarm Priority" parameter to be disabled and cause the priority to be the same as the event that triggered it. The "Alarm Priority" parameter is the same as in the "Configuring Events" page.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
event	n	ev_filter	Comma separated list of event codes	Do not log this event

There are no CLI commands for editing Event logcodes. However, it is possible to edit the "LOGCODES.TXT" file which holds all the logcode information. For details on how to do this, refer to the "Event Log" section of this manual.

Configuration - Alarms > SMTP Account

In order for the router to successfully send emails, an email account (SMTP) must be available. This section describes the configuration of the router in order to use the email account that has been set up for it.

Hostname or IP address of your SMTP server

This parameter sets the IP address or hostname of the SMTP mail server, e.g. smtp.myisp.com. Sending email requires a connection to the Internet so depending upon how the router is configured, it may be necessary to check that the PPP configuration allows a connection to the ISP or external SMTP mail server.

Port

The Simple Mail Transfer Protocol (SMTP) uses TCP port 25, which is the default for this parameter. If the mail server uses a different TCP port, enter it here.

Username

Email accounts are controlled by requiring a username and password in order to send and receive mail. This field is where the account username is set. This information will be provided by the administrator of the email server.

Password

This field is where the account password is set.

Confirm Password

This field is used to re-enter the password. The two passwords are compared to check that they are the same and that there hasn't been a typographical error when entering them. This check is used since the password characters are not echoed and so the usual visual feedback is not available.

Display "Email From" as

This parameter specifies the text to be used as the "MAIL FROM" parameter which forms part of the protocol when connecting to the email server. Most SMTP servers will accept an empty string whereas others require that this parameter is present. It may be necessary to consult with the SMTP server administrator (or ISP) to determine whether or not this parameter is required.

Attachment size limit n Kbyte, Mbyte

Some email service providers place a limit on the size of an email attachment that they will accept, this parameter can be used to ensure that the limit is not exceeded. The inbuilt traffic analyser and event logger can generate substantial files and it may be required that these files are truncated when sent as email attachments. The size is specified in kilobytes, so for example, setting this limit to 250 will truncate the attachment to 250kB before transmission. Setting the size to 0 means that no limits are imposed.

If the email template does not contain one, use "Reply To" address

This address will be inserted into the email header if it is found that no reply address exists in the appropriate email template. If the email template does contain an address in the "reply to:" field, that will override the default reply address.

Route using Routing table, Interface x,y

When selected, the routing code is used to determine the outbound interface and that interface will determine the source IP address.

If the "Route using routing table" option is not selected, the settings in the interface and interface instance text boxes are used to determine the outbound interface and source IP address. These are selected from the drop-down selection box and are None, PPP and Ethernet.

Resend the email after s seconds if the first attempt fails

This checkbox and associated text entry box enable the retry mechanism. If the first attempt to deliver the email fails, the router will wait the specified number of seconds (which must be non-zero) before making another attempt.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
smtp	n	server	Valid hostname or IP address	Hostname or IP address mailserver.isp.com 122.134.156.178
smtp	n	port	Valid port number, e.g. 25	Port n
smtp	n	username	Free text field containing a valid account username e.g. my_account	Username
smtp	n	password	Free text field containing account password, e.g. my_password	Password
smtp	n	mail_from	Free text field	Display "Email From" as
smtp	n	att_lim	0 – 65535	Attachment size limit This CLI value is entered in Kilobytes only.
smtp	n	reply_to	Free text field	If the email template does not contain one, use "Reply To" address
smtp	n	userouting	0,1	Route using routing table
smtp	n	ll_ent	Blank,PPP,ETH	Route using Interface x,y x = Interface type
smtp	n	ll_add	0 - 255	Route using Interface x,y y = interface number
smtp	n	retry_dly	0 - 255	Resend the email after s seconds if the first attempt fails

Configuration – System > Device Identity

This configuration section describes how to configure the identity of the router.

Description
This free-form text input field is for entering a description of the router that can be used to uniquely identify it. This is useful where there are a large number of routers on a site and a descriptive name would be easier to use when referring to the router, rather than having to use the serial number or other unique parameter. This parameter is used by the SNMP function within the router.

Contact
This is another SNMP parameter which is used to enter a contact name.

Location
This SNMP parameter sets a location string for the router, which again may be helpful when referring to a particular router within a site or for identifying a particular site.

Device ID
This field is taken from the iDigi configuration and should not normally need to be changed. When using iDigi to manage the router, the configuration procedure assigns a device ID to the router. The device ID is a 64-byte value, with each 8-byte section separated with a "-" character. Valid digits are upper case hexadecimal. The first 16 digits (reading from left to right) are normally set to "0" and the second 16 comprise the MAC address of the primary Ethernet interface and the digits "FF" in order make up the full 8-digit. The following device ID illustrates the format:

00000000-00000000-001122FF-FF334455

This example uses the MAC address 00:11:22:33:44:55.

Router Identity
This is a string of up to 20 characters that can be used to identify the router in email alert messages generated by the event logger. This is also the prompt string that appears when logging on to the router remotely. The factory configuration uses the character sequence "%s" which gets replaced by the serial number of the router when the unit identity is displayed. This character sequence may be used when creating a custom identity for the router. For example, if the serial number of the router is **012345**, entering the string "**My_Router_%s>**" would show the prompt "**My_Router_012345**>" during a remote login.

Hostname
This parameter assigns a hostname to the local IP address of the router.

Secondary Hostname
This parameter allows a second hostname to be assigned to a router. This is associated with the secondary IP address.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
snmp	n	Name	Free text field	Description
snmp	n	Contact	Free text field	Contact
snmp	n	Location	Free text field	Location
cmd	n	Unitid	Free text field	Router Identity
cmd	n	Hostname	Free text field	Hostname
cmd	n	sec_hostname	Free text field	Secondary Hostname

Configuration – System > Date and Time

The router keeps track of calendar time using an internal real time clock (RTC) device. The clock is used to time/date stamp logfiles. The date and time configuration pages allow the system time to be set and maintained. Since maintaining an accurate system clock can be important for routers on the Internet, NTP and SNTP services are supported and the router may be configured to use one of these protocols for maintaining the internal system time. The router uses the 24-hour clock.

Current system time

The current system time appears at the top of this web page.

Manually set the time h hours, m minutes s seconds, M month D day Y year

These parameters are set using the associated drop-down selection menus.

Hours

Select from the drop-down list to set the hours.

Minutes
Select from the drop-down list to set the minutes.

Seconds
Select from the drop-down list to set the seconds.
(This may have limited use due to human reaction times).

Month
Select from the drop-down list to set the month.

Day
Select from the drop-down list to set the day.

Year
Select from the drop-down list to set the year.

Set
Click this button to cause the above settings to take effect.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
n/a	n/a	time	hh [mm [ss [DD [MM [YYYY]]]]]	Manually set the time

Configuration – System > Date and Time > Autoset Date and Time

Do not auto-set the system time
This is the system default and this radio button will appear filled in when the unit is new unless a different default configuration has been supplied. Click this radio button to close the SNTP or NTP configuration pages.

Auto-set the system time
Selecting this radio button expands the page to include the SNTP settings. These are described below.

SNTP server
The hostname or IP address of the desired SNTP server is entered here.

Check on Power-up
This checkbox, when checked, will cause the router to attempt to connect to the SNTP server every time it boots.

Update every h hours
Enter the interval, in hours that the router should wait between updating the system clock.

Randomly between s1 and s2 seconds
It is possible to use a random update interval rather than a fixed interval. There are two text-entry boxes for this purpose, enter the minimum interval into the left-hand box and the maximum desired interval into the right-hand box. Selecting the random update will clear the fixed interval.

Offset from GMT
This parameter should be set to + or - the number of hours the unit's time should be ahead or behind Greenwich Mean Time.

Update for Daylight Saving Time.
When checked, this checkbox causes the following parameters to appear, the router will then use those settings to automatically adjust the system time to ensure that local daylight saving is used.

Start

Month
Use this drop-down selection box to select the month in which to switch to daylight saving time.

Day
Use this drop-down selection box to select the day on which to switch to daylight saving time.

Hour
Use this drop-down selection box to select the hour at which to switch to daylight saving time.

End

Month
Use this drop-down selection box to select the desired month in which to switch back to GMT (UTC).

Day
Use this drop-down selection box to select the desired day on which to switch back to GMT.

Hour
Use this drop-down selection box to select the desired hour at which to switch back to GMT.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
sntp	n	server	Valid hostname or IP address sntp.timeserve.org	SNTP Server
sntp	n	pwrchk	0,1	Check on Power-up 0 = Off 1 = On
sntp	n	interval	0 – 255	Update every h hours Default = 24
sntp	n	randintsecs	0 - 86400	randomly between s1 and s2 seconds Use format [s1,s2] eg min 50, max 500 would be: [50,500]
sntp	n	offset	-12 - +13	Offset from GMT
sntp	n	dstonmon	0 – 12	Start: Month Update for Daylight Saving Time 0 disables daylight saving
sntp	n	dstonday	0 - 31	Start: Day
sntp	n	dstonhr	0 - 23	Start: Hour
sntp	n	dstoffmon	0 - 12	End: Month
sntp	n	dstoffday	0 - 31	End: Day
sntp	n	dstoffhr	0 - 23	End: Hour
sntp	n	ntp	0,1	0 = SNTP 1 = NTP Default = OFF

Use NTP for greater accuracy
Selecting this checkbox expands the page to show the NTP settings. These are described below.

NTP is much more accurate than SNTP, with NTP an accuracy of 200 microseconds (1/5000 second) can be achieved. The NTP functionality is in accordance with RFC1305.

Up to 4 remote peers can be configured, all the peers are polled at intervals and the "best" peer is selected for using as the time source.

SNTP should be configured prior to using NTP. The router will calculate the accuracy of the NTP time servers over a period of time (up to 2 hours), once the drift compensation is calculated the NTP client will be used.

The drift compensation value will be stored in NVRAM and written to the config.da0 file, if the router looses power or is rebooted it will not need to re-calculate the accuracy of the NTP servers again. The compensation value is constantly monitored to ensure it remains correct.

Note:
If SNTP is used the accuracy of around 1 second is achieved.
If NTP is used 200 microsecond accuracy can be achieved.
Not all models support NTP – this option will only appear for models that do.

Initial Drift Compensation n ppm
NTP incorporates compensation for clock drift. If this parameter is known, it can be entered here. Otherwise, the router will calculate this value over a period of time. Once calculated, the value will be displayed in the text box.

Clock Precision Limit

Select the clock precision limit from the drop-down selection box.

Disable NTP when interface x,y is out of service

If the specified interface is out of service, the NTP is disabled until the interface is available again.

NTP Servers 1 - 4

The router has the capability of configuring up to four NTP server connections. The more servers that are used, the more accurate the time setting will be. The following section describes the configuration of the connections.

NTP Server 1/2/3/4 Hostname
This field sets the NTP server hostname or IP address.

Broadcast Mode
When enabled, the NTP client will operate in a different manner. Rather than sending out an NTP client message and expecting a reply, the NTP module will send out a broadcast mode packet to the IP address configured in 'NTP host' field. The broadcast interval will be determined by the value of 'Minimum poll interval'.

Poll Interval s1 to s2 seconds
These two parameters define the minimum and maximum intervals between poll broadcasts. The values are time in seconds represented as a power of 2. This means that a value of 4 means that the minimum poll interval is 2^4 = 16 seconds.

Startup burst Interval s seconds
When connecting to an NTP time server in polled mode, it may be necessary to send polls at intervals shorter than the minimum poll interval in order to speed up the synchronization process. This parameter controls the interval between polls during the startup process. This feature is useful in situations where the router only has an intermittent Internet connection.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ntp	n	driftppm	-10000 - +10000	Initial Drift Compensation
ntp	n	precision	-10 - 0	Clock Precision Limit
ntp	n	inhibit_int	Blank,PPP,Ethernet	Disable NTP when interface x,y is out of service x = Interface type
ntp	n	inhibit_add	0 - 255	Disable NTP when interface x,y is out of service y = interface number
ntp	n	server	Valid IP address or hostname, e.g. ntp1@timeserver.org	NTP Server
ntp	n	bcast	0,1	Broadcast Mode 0 = disabled 1 = enabled
ntp	n	minpoll	3 - 14	Poll Interval s1, s2 3 = 8 4 = 16 5 = 32 6 = 64 7 = 128 8 = 256 9 = 512 10 = 1024 11 = 2048 12 = 4096 13 = 8192 14 = 16384
ntp	n	maxpoll	3 – 14	Poll Interval s1, s2 See 'minpoll' for values
ntp	n	burstint	0 – 255	Startup burst Interval s seconds
ntp	n	server2	Valid IP address or hostname, e.g. ntp2@timeserver.org	NTP Server
ntp	n	bcast2	0,1	Broadcast Mode 0 = disabled 1 = enabled
ntp	n	minpoll2	3 - 14	Poll Interval s1, s2 See 'minpoll' for values
ntp	n	maxpoll2	3 - 14	Poll Interval s1, s2 See 'minpoll' for values
ntp	n	burstint2	0 – 255	Startup burst Interval s seconds

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ntp	n	server3	Valid IP address or hostname, e.g. ntp3.timeserver.org	NTP Server
ntp	n	bcast3	0,1	Broadcast Mode 0 = disabled 1 = enabled
ntp	n	minpoll	3 - 14	Poll Interval s1, s2 See 'minpoll' for values
ntp	n	maxpoll	3 - 14	Poll Interval s1, s2 See 'minpoll' for values
ntp	n	burstint3	0 – 255	Startup burst Interval s seconds
ntp	n	server4	Valid IP address or hostname, e.g. ntp4.timeserver.org	NTP Server
ntp	n	bcast4	0,1	Broadcast Mode 0 = disabled 1 = enabled
ntp	n	minpoll4	3 - 14	Poll Interval s1, s2 See 'minpoll' for values
ntp	n	maxpoll4	3 - 14	Poll Interval s1, s2 See 'minpoll' for values
ntp	n	burstint4	0 – 255	Startup burst Interval s seconds

To check the status of the NTP client, the following commands can be used:

To view NTP system status information

```
ntpstat sys
```

To view NTP peer information

```
ntpstat peers
```

To reset system information and allow NTP to recalculate the drift compensation

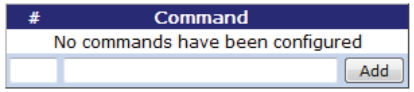
```
ntpstat rst
```

Configuration – System > General

This section describes the configuration of router functionality that applies to the router in general rather than specific features.

Configuration – System > General > Autorun Commands

The router may be configured to run a number of commands once it has booted. These commands are associated with specific asynchronous serial interfaces. Configuration of this facility is via a table on this web page. As an example, it may be required that a Script Basic script, sample.bas needs to be run at boot up. Auto commands are normally associated with an ASY port, but running a script for example is not ASY port specific.



#
This parameter is the command interface to be associated with the command. In the above example, this would be set to the number "0".

<Command>
This parameter is the CLI command to run on start-up. In the above example, this field would be set to the string "bas sample.bas".

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
cmd	n	autocmd	Valid CLI command	Autorun Commands

Configuration – System > General > Web / Command Line Interface

The router may be configured using several different methods. This section describes how to configure the web GUI and CLI (Command Line Interface) options.

Automatically log user out if idle for h hours m minutes s seconds
In order to limit the probability of unauthorised users gaining access to the router, login timeouts are applied. These cause an existing connection to be closed after a predefined period. The default is 20 minutes.

For users connected on the local Async port

Use access level None, Low, Med, High, Super
For security purposes, logging into the unit is controlled by a user access level. This parameter controls the access level that applies when logging in via the local asynchronous serial port.

Automatically log user out Never / If idle for h hrs m mins s secs
These radio buttons control how long the local port allows access before terminating the connection and requiring the user to log in again. Selecting the "Never" buttons allows permanent access to the router via the local asynchronous serial port. If, for security reasons, it is required that the access should be limited, the appropriate time period can be entered into the text entry boxes.

Disable Remote command echo for Telnet sessions
This checkbox enables/disables command echo for remote access. This applies to telnet and TRANSIP sessions.

CLI Pre-Login Banner
The router offers the facility to display a banner before any login information is requested. The parameter specifies the name of a file that is stored in the flash filing system and contains the text to be displayed before the request for the username and password. This can be useful for displaying a standard welcome message or any site-specific user instructions.

CLI Post-Login Banner
Once the user has successfully logged on to the router, a second message may be displayed - this parameter specifies the name of a file containing the text to display. As above, the file may contain site-specific instructions to be carried out once the user has logged in.

Allow CLI access from X.25 address n
This parameter enables/disables logging into the router over an X.25 connection. The paramtern n must be a valid X.25 NUA (Network User Address).

With TRANSIP, use access level None, Low, Med, High, Super
This drop-down selection box controls the security access level when using TRANSIP to access the router.

Relevant CLI Parameters

Entity	Instance	Parameter	Values	Equivalent Web Parameter
cmd	n	tremto	0 – 86400 seconds	Automatically log user out if idle for h hrs m mins s seconds This CLI value is entered in seconds only.
local	n	access	0 – 4	Use access level 0 = Super

Entity	Instance	Parameter	Values	Equivalent Web Parameter
				1 = High 2 = Medium 3 = Low 4 = None 8 = Read only
local	n	tlocto	Free text field	Never, h hrs, m mins, s secs
cmd	n	noremecho	0,1	Enable Remote command echo 0 = Off (default) 1 = On
cmd	n	prebanner	Valid filename e.g. "welcome1.txt"	CLI Pre-Login Banner
cmd	n	postbanner	Valid filename e.g. "welcome2.txt"	CLI Post-Login Banner
cmd	n	cmdnua	0 - 1023	Allow CLI access from X.25 address
local	n	transaccess	0 – 4	With TRANSIP, use access level 0 = Super 1 = High 2 = Medium 3 = Low 4 = None 8 = Read only

Configuration - System > General > Miscellaneous

This section is for those configuration items that do not fit neatly into any other section.

Note:
Depending on the router model, some of these options may not be available.

Use Config n when the router powers up
The router maintains two configuration files, either of which may be invoked on power-up. Select the required one from the drop-down selection box. Use this option with care as selecting the incorrect configuration file can cause confusion.

Allow anonymous FTP login
When checked, this checkbox will enable the router to accept anonymous logins. The default state is Off and the security implications of enabling this option should be considered carefully before applying.

Additional FTP NAT port n
Standard FTP uses two well-known ports, a control port and data port. These are low number ports and may be blocked by firewall rules. As such, it may be that an FTP server may be listening on a non-standard control port. This parameter is used to specify the port that the router should monitor for the FTP "PORT" and "PASV" commands. These commands contain information relating to IP addresses and Ports which should be modified during the NAT process. The NAT modifications may result in different sized packets being generated that then require that the TCP sequence numbers be modified to allow for the changes.

SNMP Enterprise number
This parameter specifies the value of the OID (Object IDentifier) to be used by SNMP management tools when accessing the MIB (Management Information Block). This number must form part of the OID used to access individual items in the MIB as a prefix.
For example: SNMPv2-SMI::enterprises.16378.10001.

SNMP Enterprise Name
This is the name corresponding to the above Enterprise Number.

Only resolve DNS request for domain
Entering a domain name here will restrict DNS requests to the specified domain only.

W-WAN LED to display W-WAN, ISDN/PSTN
On the front panel of the display of models fitted with a W-WAN module, is an LED that may be used to display the status of the W-WAN module or the status of the PSTN/ISDN connection. Use the drop-down selection box to choose which. The ISDN/PSTN settings depend upon which of these two options are available on the router.

Serial LED to display Connection, DTR
On the front panel of the router is an LED dedicated to indicating the status of various signals on the asynchronous serial line. Use the drop-down selection box to choose which signal status to display. On modules fitted with W-WAN, this LED has additional functionality, it can also be used to display the W-WAN signal strength.

CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
config	n	powerup	0,1	Use Config n when the router powers up
cmd	n	anonftp	0,1	Allow anonymous FTP login 0 = Off (default) 1 = On
snmp	n	ftpnatport	0 - 65535	Additional FTP NAT port
snmp	n	ent_nb	0 – 65535	SNMP Enterprise Number Default 16378
cmd	n	ent_name	Free text field	SNMP Enterprise Name
cmd	n	dnsname	Valid Domain name, e.g. mydomain.org	Only resolve DNS request for domain
cmd	n	gprsled_mode	0,1	W-WAN LED to display W-WAN, ISDN/PSTN 0 = W-WAN 1 = ISDN/PSTN
cmd	n	asyled_mode	0,1	Serial LED to display Connection, DTR 0 = Connection 1 = DTR status 2 = W-WAN signal strength

Configuration – Remote Management > iDigi > Connection Settings

iDigi is a hosted remote configuration and management system that has been designed to facilitate the management of large numbers of routers. Before this service can be used, an iDigi account must be set up. Applying for an account is a straightforward procedure; the local sales representative will have details. The iDigi homepage is to be found at ***www.idigi.com***.

The service is hosted on the iDigi servers and these provide a web-based interface that shows the configuration of selected routers, allows the configuration to be changed and also facilitates remote firmware upgrade. The iDigi servers also provide a data storage facility.

Enable Remote Management using a client-initiated connection
Select this checkbox to display the basic configuration parameters and enable the unit to make the connection to the remote iDigi server.

Server Address
This text entry box is used to enter the IP address or (more usually) the domain name of the iDigi host, for example idigi.com. (This information will be supplied when your iDigi account is activated).

Automatically reconnect to the server after being disconnected
The protocol used to communicate with the server allows the router to detect that it is no longer connected to the server. Ticking this checkbox will cause the router to attempt a reconnection when it discovers that the connection has been lost.

Reconnect after h hours m minutes s seconds
If the reconnect checkbox is enabled, these parameters specify the interval to wait before attempting to reconnect to the server.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
idigi	n	clientconn	0,1	Enable Remote Management and Configuration using a client-initiated connection 0 = Off 1 = On
idigi	n	server	Valid IP address e.g. 1.2.3.4 or domain name e.g. idigi.com	Server Address
idigi	n	reconnect	0,1	Automatically reconnect the server after being disconnected 0 = Off 1 = On
idigi	n	reconnectsecs	0 – 86400	Reconnect after h, m, s This CLI value is entered in seconds only.

Configuration – Remote Management > iDigi > Advanced

The settings in the previous section, along with the system defaults are sufficient to establish a connection to the iDigi server. The settings in the advanced section allow the connection to be fine-tuned. The parameters described here are concerned with detecting loss of connection. When the router first connects to the iDigi server, the link parameters are sent to it. The WAN settings and Ethernet settings described below are identical, but it should be noted in the command line descriptions that the default keepalive intervals are different. This is due to the different characteristics of PPP and Ethernet links.

Configuration – Remote Management > iDigi > Advanced > Connection Settings

Disconnect when the iDigi server is idle
Once the router has connected to the iDigi server, and the server has established that all the settings it holds for the router are current, and no new changes are being requested, the traffic between the router and iDigi server reduces to the sending of keep-alive packets. In this situation, it may be advantageous to terminate the connection in order to reduce bandwidth or to keep data costs down. Ticking this checkbox will cause the router to negotiate termination of the connection.

Idle Timeout h hours, m minutes, s seconds
The timeout entered here defines how long the router should wait after detecting the idle condition before negotiating termination of the link. Default is 10 seconds.

Configuration – Remote Management > iDigi > Advanced > WAN Settings

Receive Interval s seconds
This is the time between keep-alive packets that the router should wait before considering that the connection may be lost.

Transmit Interval s seconds
This is the interval between transmission of keep-alive packets.

Assume connection is lost after n timeouts

Occasional packet loss is to be expected, this parameter will allow for a specified number of lost keep-alive packets before the connection is deemed to have failed.

Configuration – Remote Management > iDigi > Advanced > Ethernet Settings

Receive Interval s seconds
This is the time between keep-alive packets that the router should wait before considering that the connection may be lost.

Transmit Interval s seconds
This is the interval between transmission of keep-alive packets.

Assume connection is lost after n timeouts
Occasional packet loss is to be expected, this parameter will allow for a specified number of lost keep-alive packets before the connection is deemed to have failed.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
idigi	n	idledisconn	0,1	Disconnect when iDigi server is idle 0 = Do not disconnect 1 = disconnect
idigi	n	disconnsecs	0 - 28800	Idle Timeout h,m,s This CLI value is entered in seconds only.
idigi	n	ppprxkeepalive	0 - 28800	WAN - Receive Interval seconds
idigi	n	ppptrxkeepalive	0 - 28800	WAN - Transmit Interval seconds
idigi	n	pppwaitfor	1 - 255	WAN - Assume connection is lost after n timeouts
idigi	n	ethrxkeepalive	0 - 28800	Ethernet - Receive Interval seconds
idigi	n	ethtxkeepalive	0 - 28800	Ethernet - Transmit Interval seconds
idigi	n	ethwaitfor	1 - 255	Ethernet - Assume connection is lost after n timeouts

There is an additional iDigi CLI command "**idigistat**". Using this command with no extra syntax returns the status of the socket connections, i.e. whether there is a live connection to the iDigi server or not.

Configuration – Remote Management > SNMP

The Simple Network Management Protocol (SNMP) is a well established way of managing clusters of remote routers – the TransPort routers support versions 1, 2c and 3 of this protocol. The standard Management Information Bases (MIBs) that are supported by the router are detailed below. Alongside these, there are two other MIBs that are supplied as standard. This is a MIB that is generated after the firmware has been installed. This is accomplished using the "mibprint" CLI command and the "MIBEXE" DOS tool which is available from the Technical Support Team. This MIB changes with every firmware release since the firmware revision is embedded in the Object Identifiers (OIDs). This MIB provides access to most of the configuration and statistics that are associated with the router.

The second MIB is the "Monitor MIB" which is a standard MIB that gives access to various Digi TransPort proprietary objects. The OIDs in this MIB do not change with every release although it is possible for new objects to be added to it. This MIB is available from the Technical Support team.

The standard MIBs supported are:

SNMP MIB (RFC3418)

Interfaces MIB (RFC2233)*

IP MIB (RFC2011)

IP Forwarding Table MIB (RFC2096)

TCP MIB (RFC2012)

UDP MIB (RFC2013)

VRRP MIB (RFC2787)

SNMP MPD MIB (RFC3412)

SNMP USM MIB (RFC3414)**

* The following groups/tables in RFC2233 are not supported: ifXTable, ifStackTable, ifRcvAddressTable.

** The following groups/tables in RFC3414 are not supported: usmUserTable.

Other MIBs may be available on request.

Enable SNMPv1
Ticking this checkbox enables support for version 1 of the protocol.

Enable SNMPv2c
Ticking this checkbox enables support for version 2c of the protocol.

Enable SNMPv3
Ticking this checkbox enables support for version 3 of the protocol.

Use UDP Port n
This is the UDP port number to use. The default is UDP port 161.

SNMPv3 Engine ID
This is required as part of the SNMP v3 protocol. This is a 24 hexadecimal character string; any trailing zeroes in this string making the value up to 24 characters can be omitted. A remote engine ID is required when a SNMP v3 Inform is configured. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
snmp	n	v1enable	0,1	Enable SNMPv1 0 = Off 1 = On
snmp	n	v2cenable	0,1	Enable SNMPv2c 0 = Off 1 = On
snmp	n	v3enable	0,1	Enable SNMPv3 0 = Off 1 = On
snmp	n	port	0 - 65535	Use UDP Port Default = 161
snmp	n	engineid	String	SNMPv3 Engine ID

Configuration – Remote Management > SNMP User > SNMP User n

This page controls the configuration of the SNMP users.

SNMPv1 / SNMPv2c

Community
The text in this text entry box specifies the community string for Version 1 and Version 2c SNMP packets.

Confirm Community

The community string is echoed as dots in the text entry box and so having a second confirmation field where the string is retyped, allows a simple check to be performed for correct entry.

SNMPv3

Username
This field is the name of the SNMP user.

Authentication None, MD5, SHA1
These three radio buttons select what authentication algorithm is to be applied to the SNMP transactions.

Authentication Password
This is the authentication password for the user.

Confirm Authentication Password
The authentication password is not shown as clear text. The confirmation box allows a simple check that the password has been entered correctly.

Encryption None, DES, AES
These three radio buttons select which encryption (privacy) algorithm should be applied to the SNMP data.

Encryption Password
The user's password that is used to control the privacy of the SNMP transactions is entered into this text entry box.

Confirm Encryption Password
The encryption password is not shown as clear text. The confirmation box allows a simple check that the password has been entered correctly.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
snmpuser	n	community	public / private	Community
snmpuser	n	name	user_dave	Username
snmpuser	n	auth	Off,MD5,SHA1	Authentication, None, MD5, SHA1
snmpuser	n	authPassword	my_password	Authentication Password
snmpuser	n	priv	Off,DES,AES	Encryption, None, DES, AES
snmpuser	n	privPassword	my_password	Encryption Password

Configuration – Remote Management > SNMP Filters

SNMP filters allow the system administrator to control access to the router MIBs via SNMP. This functionality is controlled by a table on the web configuration page. This table has three columns, two main headed columns as described below and a control column containing button widgets. The table has a capacity of ten entries, snmp filter instances range from 0 to 9.

Username
The username (as configured in the ***Configuration – Security > Users section***) of the user to whom the access restriction is applied.

OID Prefix
The Object ID prefix for the range of objects in the MIB that the user is not allowed to view. e.g. 1.3.6.1.2.1.4

Add
This button adds the username and OID prefix into the table.

Delete
This button causes the associated entry in the table to be deleted.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
snmpfilter	n	user	username	Username
snmpfilter	n	oid	Valid SNMP OID	OID Prefix

Configuration – Remote Management > SNMP Traps

SNMP traps are events that are generated when the specified condition is met. The web page and CLI configuration parameters are described here. The TansPort routers support two trap servers.

Generate Enterprise traps

When this check box is ticked, the router will generate product-specific traps.

Generate Generic traps
SNMP specifies several generic traps (Cold Start, Warm Start, Link Down, Link Up etc). When this checkbox is ticked, generic traps are generated.

Generate Authentication Failure traps
This checkbox enables the generation of authentication failure traps.

Generate VRRP traps
Checking this checkbox enables the generation of VRRP traps. See the VRRP section in this manual for the configuration of VRRP.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
snmp	n	enterprisetraps	0,1	Generate Enterprise traps 0 = Off 1 = On
snmp	n	generictraps	0,1	Generate Generic traps 0 = Off 1 = On
snmp	n	authtraps	0,1	Generate Authentication traps 0 = Off 1 = On
snmp	n	vrrptraps	0,1	Generate VRRP traps 0 = Off 1 = On

Configuration – Remote Management > SNMP Traps > SNMP Trap Server n

Digi TransPort routers support two SNMP trap servers. The following options and description explain how to configure a trap server.

Trap Server IP Address a.b.c.d
This is the IP address of the server running the SNMP software and determines the destination for the trap notifications.

Port n
This is the UDP port number that the SNMP server is listening on, the default is 162 which is the standard port number for this service.

Use SNMP Version
Select the required SNMP version number from this drop-down selection box.

Send "Inform Request" message
If SNMP version 2c or 3 is selected, the router can send a SNMP Inform Request message instead of a Trap message. Inform Request messages are acknowledged by the SNMP Trap server whereas Trap messages are not.

If no response, retransmit the Inform Request message after n seconds
The period after which the Inform Request message is retransmitted if no response has been received.

Retransmit a maximum n times
The maximum number of times an Inform Request message will be retransmitted. If no acknowledgement is received after the maximum number of retransmissions, an event is logged.

Community
Enter the desired community string into this text entry box.

Confirm Community
Entering the community string again here enables verification of the string since the string is not displayed.

Trap Server Engine ID
This item will be configured within the application and is the SNMP server software engine ID which is used for authentication and encryption.

SNMP User
This is the username that should be associated with the trap server. This should match a user from one of the previously configured SNMP users (***Configuration – Remote Management > SNMP > Users***).

User Security Level
Select the desired security level from this drop-down selection box. The choices are these:
No Authentication, No Privacy
Authentication, No Privacy
Authentication, Privacy

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
snmptrap	n	IPaddr	Valid IP address e.g. 1.2.3.4	Trap Server IP Address a.b.c.d
snmptrap	n	port	0 - 65535	Port Default = 162
snmptrap	n	version	v1, v2c, v3	Use SNMP Version
snmptrap	n	sendInforms	on | off	Send "Inform Request" messages
snmptrap	n	informto	Integer	If no response, retransmit the Inform Request message after n seconds
snmptrap	n	informretries	Integer	Retransmit a maximum n times
snmptrap	n	community	String	Community
snmptrap	n	engineid	String	Trap Server Engine ID
snmptrap	n	securityname	String	SNMP User
snmptrap	n	securitylevel	noauthnopriv authnopriv authpriv	User Security Level noauthnopriv = No Authentication, No Privicy authnopriv = Auth, No Priv authpriv = Auth & Priv

Configuration – Security > Users > User n

These pages allow you to configure a number of authorised users. The number of users available depends on the firmware build the router is running. Each user has a password and access level that determines what facilities the user has access to.

Username
The name of the user. Up to 14 characters are allowed.
There are some special usernames that can also be used, these are:
%s This uses the serial number of the router as the username.
%i This uses the IMEI of the cellular module as the username.
%c This uses the ICCID of the SIM as the username.

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

Password / Confirm Password
The password for the user. Up to 14 characters are allowed.

Access Level
Selects the access level for the User. There are the following options

Super	Allows full access to all facilities.
High	Allows user to reconfigure the general configuration of the router and to change some settings such as the time and date. Not allowed to change user settings.
Medium	Allows user to access medium level configuration commands which allow some configuration of the router.
Low	Allows user to access low level commands which tend to be status and statistics commands.
Read Only	Read only access of the configuration.
None	User is not allowed to login via Web, FTP, SSH and Telnet.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
user	0	name	String (up to 14 chars)	Username
user	0	password	String (up to 14 chars)	Password
user	0	access	0 = Super 1 = High 2 = Medium 3 = Low 4 = None 8 = Read Only	Access Level

Configuration – Security > Users > User n > Advanced

Allow this user to log in over a PPP network
Enabling this will allow the user to log in to the router using PPP. Disabling this will disable PPP login for the user no matter what the user's access level is.

Use this number x when PPP dial-back is required for this user
The telephone number for the user in the event that "dial-back" is required. If the username that the remote router uses during the PPP authentication matches the username of the user where a dial-back number is configured, the user's dial-back number will override any dial-back number configured in the answering PPP interface.

Alternate IKE Key / Confirm Alternate IKE Key
When IKE is the initiator, the responder supplied HASH is checked using the normal password (above) and if that fails, the Alternate Key (here). The initiator will remember which password was successful, and use that password to create the HASH if it becomes the responder of some new negotiation. If the IKE becomes a responder and IKE negotiations fail after supplying the HASH, the other password will be used during the next negotiation. Using this Alternate Key, it should be possible to configure new passwords into both ends of a tunnel, and not have too many failed negotiations. The process would be to add the Alternate Key into the remote router, then update the local router with the Alternate Key. Once that has been done, the administrator would then be able to move the Alternate Key to the usual location (Password) and remove the Alternate Key (newpwd) from the configuration. Should a negotiation take place during the period where the Alternate Key has been entered into the remote router, but not the local router, there should be no more than one failed negotiation, and only if the remote router is the initiator.

Remote Peer IP address
In certain circumstances, it may be desirable for a user connecting in over a PPP connection to be allocated a specific IP address, rather than be allocated an address from a pool configured on a PPP interface. When this parameter is configured, the IP address negotiated on the PPP link will be this one, not an address from the regular IP address pool.

Remote Peer IP subnet
In the event that multiple PPP interfaces are enabled for answering and that multiple remote routers can dial into the local router, static routes cannot always be used to ensure that packets which should be routed to the remote network are sent through the correct PPP interface. This parameter can be used in conjunction with the 'Remote Peer IP subnet mask' parameter to associate a network subnet with a user.
When a remote unit "connects in" and authenticates with the unit, the unit will then create a dynamic route (that will override any static routes) for the duration of the PPP session. The interface for the dynamic route will be the PPP interface that answered the call. The network address for the dynamic route will be taken from the entry in the user table that matches the username that the remote unit used during the PPP authentication.

Remote Peer IP subnet mask
The remote subnet mask parameter is used in conjunction with the 'Remote Peer IP subnet' parameter above to fully qualify the network address for the user.

Public Key file
The name of the file containing the public key for that user. If the public key matches the client supplied public key, the user is allowed access.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
user	0	dun_en	on, off	Allow this user to log in over a PPP network
user	0	phonenum	Number	Use this number x when PPP dial-back is required for this user
user	0	newpwd	String (up to 14 chars)	Alternate IKE Key
user	0	fieldip	IP Address	Remote Peer IP address
user	0	ipaddr	IP Address	Remote Peer IP subnet
user	0	mask	IP Mask	Remote Peer IP subnet mask
user	0	keyfile	Filename	Public Key file

Configuration – Security > Firewall

All Digi TransPort routers incorporate a comprehensive firewall facility. A firewall is a security system that is used to restrict the type of traffic that the router will transmit or receive based on a combination of IP address, service type, protocol type, port number and IP flags. Firewalls are used to minimise the risk of unauthorised access to the local network resources by external users or to restrict the range of external resources to which local users have access. A more detailed description of how firewalls operate on Digi routers is given in the "Firewall Scripts" section. Refer to this section before attempting to implement a firewall.

The rules governing the operation of the firewall are contained in a pseudo-file called "fw.txt". This file can be created either by using the controls in the web page described below or by using a text editor on a PC and then loading the resulting file onto the router using FTP or XMODEM. Digi Routers are shipped with a default fw.txt file that can be used as the starting point for a custom firewall configuration.

Configuration of the firewall is carried out by using the table described below. There are three other buttons that appear just below the table. Their use will also be described.

Since a default file is supplied, when this page loads it will show the rules in the default "fw.txt" file. If "fw.txt" does not exist, a blank table will be shown.

Hits
The numbers that appear in this column of the table are the number of hits for the rule that appears to the right.

#
This is non-editable and is simply the rule number.

Delete
Clicking this button deletes the rule that appears to its left.

Insert
These buttons are used to insert new lines. The insert buttons that appear alongside existing rules insert new blank lines above the line on which they appear. The button at the bottom creates a new blank line at the end of the table. (An empty table will only have the one button at the bottom). To create a new rule, click the button at the point the new rule should appear and a new text box should appear. Type the rule into the text box and once complete, click the "ok" button. To abandon any changes click the "cancel" button. Once the "ok" button has been clicked the firewall task will validate the rule and if valid, will add it the table. If errors are detected, a warning message will be displayed, at which point the rule may be edited or deleted.

Edit
These buttons that appear to the right of the rule open up the rule in an edit text box which allows the text to be edited. Click on the "ok" button to commit the changes or "cancel" to abandon the edit.

Reset Hit Counters
Clicking this button resets (to zero) all the rule hit counts that appear in the left-hand column of the table.

Save
Clicking this button saves changes to the table to the "fw.txt" file. If the changes are not saved using this button, they will be lost if the router is rebooted or loses power.

Restore
If, after reviewing changes to the table it is decided that the edit should be abandoned, clicking this button will restore the original "fw.txt" to the table, provided that they have not been saved.

Below the firewall editor table is another table that controls which interfaces the firewall rules apply to.

Interface
This column is simply a list of the available interfaces to which the firewall rules may be applied.

Enabled
Check the checkbox next to the interface(s) that the firewall should operate on in order to enable the firewall for that interface.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
fw	n/a	logclr	-	Reset Hit Counters
fw	n/a	save	-	Save
fw	n/a	-	-	Restore

The firewall rule hits may be viewed from the command line console by using the command:

```
type fwstat.hit
```

Configuration – Security > Firewall > Stateful Inspection Settings

The page described below contains timer timeout values and other options that are used by the firewall stateful inspection module. This module establishes firewall rules that last for the duration of a single connection only. Typically, the first packet of a TCP connection (SYN packet) is used to create a stateful inspection rule that only allows subsequent packets for that TCP connection through the firewall. The timers described below are used to set limits on how long such rules persist.

Timers

TCP Opening s seconds
The value in this text box specifies the length of time following receipt of a TCP packet that causes a stateful inspection rule to be created before a TCP connection must be established. If a TCP connection is not established within this period, the associated stateful rule will be removed.

TCP Open s seconds
The value in this text box specifies the length of time that an established TCP connection may remain idle before the stateful inspection rule created for it is removed. The timer is restarted each time a packet is processed by the associated stateful inspection rule.

TCP Closing s seconds
The value in this text box specifies the length of time that is allowed for a TCP socket to close once the first FIN packet has been received. If the timer expires before the socket has completed closing, the stateful inspection rule is removed.

TCP Closed s seconds
The value in this text box specifies the length of time that a stateful inspection rule will remain in place after a TCP connection has closed.

UDP s seconds
The value in this text box specifies the length of time that a stateful inspection rule will remain in place following the receipt of UDP packet. The timer is restarted each time packets matching the rule pass in each direction. As a consequence, rules based on UDP should only be used if it anticipated that packets will travel in both directions.

ICMP s seconds
Some ICMP packets – for instance the ECHO request – generate response packets. The value in this text box specifies the length of time that a stateful inspection rule created for an ICMP packet will remain in place if the response is not received. The rule is removed immediately following receipt of the response.

Other protocols s seconds
If a stateful inspection rule is created from a packet type other than TCP, UDP or ICMP, a rule timeout should be created for it. The parameter in this text box specifies the length of time such a rule persists. The timer is restarted each time a packet is processed by the rule.

Other Options

Expire entry after n consecutive packets in one direction
The value in this text box specifies the maximum number of consecutive packets that should pass in one direction before the corresponding rule entry is expired.

Count missed UDP echo packets as dropped
When checked, this checkbox will cause the firewall to increment the dropped packet count for each failed echo request in the situation where UDP echo is active on an interface that becomes disconnected.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
fwall	0	opening	0 - 4294967296	TCP Opening s seconds
fwall	0	open	0 – 4294967296	TCP Open s seconds
fwall	0	closing	0 - 4294967296	TCP Closing s seconds
fwall	0	closed	0 – 4294967296	TCP Closed s seconds
fwall	0	udp	0 – 4294967296	UDP s seconds
fwall	0	icmp	0 – 4294967296	ICMP s seconds
fwall	0	other	0 – 4294967296	Other protocols s seconds
fwall	0	maxuni	0 - 2147483647	Expire entry after n consecutive packets in one direction
fwall	0	cntmissedecho	OFF,ON Default OFF	Count missed UDP echo packets as dropped