Console Commands Guide

Part Number: 90-001813-00

Revision D, March 1998

NOTICE

The information in this document is subject to change without notice. Olicom assumes no responsibility for any damages arising from the use or inability to use this document, including, but not limited to, lost revenue, lost data, claims by third parties or other damages. For complete warranty information, refer to the product warranty card that covers this document and its product.

Copyright Notice

Software Copyright Notice

Trademark Notice

3Com is a trademark of 3Com Corporation.

DEC and DECnet are trademarks of Digital Equipment Corporation.

Ethernet and XNS are trademarks of Xerox Corporation.

IBM and, OS/2 are registered trademarks of International Business Machines Corporation.

ClearSight is a trademark of Olicom.

ILAN is a trademark of I-LAN, Inc.

Internetwork Packet Exchange (IPX) is a trademark of Novell, Inc.

NetWare and Novell are registered trademarks of Novell, Inc.

Stratacom is a registered trademark of Stratacom, Inc.

Ungerman-Bass is a registered trademark of Ungerman-Bass, Inc.

VINES is a registered trademark of Banyan Systems, Inc.

Contents

Introduction

What's in this manual

The Olicom Console Commands Guide documents the available console commands for both the XL products and Olicom family of switches. Some of the commands contained in this guide may not be applicable to your XL product because they are feature dependent.

Intended audience

This manual is for technical personnel with training or experience with network devices.

When to use console commands

ClearSight should be used to manage an integrated network of Olicom devices. If ClearSight becomes unavailable or you need out–of–band management capabilities, however, console commands can be used to configure and manage your devices. Remember, however, that using these commands during normal operation can seriously impact the performance of your device.

How to use console commands

Olicom devices offer several ways to issue console commands:

- **local console**
  A console terminal attached to the console port of your device. Refer to the installation manual you received with your device for information on how to connect the console.
- **remote console**
  A console terminal using a modem connected to the modem port of your device.
- ClearSight In-Band Console
  An ClearSight window in which you can enter console commands. From the ClearSight device panel for the device you want to control, select **system menu | Tools | In-Band Console** to open the window.

What commands apply to your device

The set of available console commands is dependent on the type of device you have, the device configuration, and the installed features. To determine the commands which are applicable to your device:

- At the console, enter **HELP** to list the commands available for your device.
- Check the *Configuration Sheet* shipped with your device for information about your configuration and the installed features.

Console Commands

1. General Console Commands

ATTACH

This command establishes a logical connection between the router module you are physically connected to and another module. If you want to reconnect to another router module, you must first Detach. Applies to XL routers only.

Syntax: **ATTACH n**

Parameter	Description
n	This is the slot number where the console interface (to which you want to attach) is installed. The command will return a prompt indicating the slot to which you are connected in parentheses.

DETACH

This command is used to remove a logical connection. After this command is invoked, you will be connected to the router module with the physical console connection. The command will return a prompt indicating the slot to which you are connected in parentheses. Applies to XL routers only.

Syntax: **DETACH**

HELP

This command displays the highest level of the console commands online help.

Syntax: **HELP**

It displays various the categories of help you can view by adding parameters to the HELP command.

PASSWORD

This command allows you to enter the password required to access a router or one of its features. A password is required if the router or one of the features is write or read/write protected. When using this command, you are prompted to enter the current password. If you enter the incorrect password, the screen does not display an error, but access is denied.

Syntax: **PASSWORD**

SET PASSWORD

This command allows you to change the password. When using this command, you are prompted to enter the new password requirement (N, W, R). Enter **n** for none, **w** for write, and **r** for read/write. After you enter the password, you are prompted to enter the new password again.

Syntax: **SET PASSWORD**

SHOW INTERFACE

This command displays the status and statistics for a specified interface or all interfaces if the optional argument is omitted.

Syntax: **SHOW INTERFACE [n]**

Parameter	Description
n	The interface number for which you want to display statistics.

SHOW PORT

This command is used to display port parameters, Spanning Tree information and port statistics for a specified port or all ports if the optional argument is omitted.

Syntax: SHOW PORT [n]

Parameter	Description
n	The port number in the range from 0 to 7 for which you want to display parameters and statistics.

Example:

```
ILAN/XL(1)>show port 1
Port Information        Tuesday June 11, 1996 10:23:25 AM
Port: Port LA0-1 (1)     State: Active
Spanning Tree Information
                        Operator state: Operational on
                        Actual state: Forwarding,   Info age: 1,   Root cost: 10
                        DP: FALSE, DB prio: 1, DB addr: 00-00-98-00-35-b9,
                        PORT Cost: 10
Routing Parameters
                        Lan segment #002, SRB forwarding is ENABLED
                        Hop count limit 13
                        Connected to other PIR

Bridge ID Parameters             pdb_idm = f
                        Turned on
                        RIF type: Follow bridge mode
Port Statistics
                        Received Packets:   Total: 4031345,      Multicast: 863971
                                            Normally filtered:   3152179, Forwarded: 0
                                            Filtered by Kept:    Off 0,  On 0
                        Transmit Pkts:      Total: 8240,    Dropped/Congestion: 0
Act as backup: NOT ALLOWED
```

SHOW BRIDGE

This command is used to display router parameters and statistics, including Spanning Tree parameters, DSPF parameters and Broadcast Resolution statistics.

Syntax: **SHOW BRIDGE**

Example:

```
ILAN/XL(1)>show bridge

Bridge Parameters @ 85194 seconds
                    Name:
                    Ethernet Address: 00-00-98-13-74-40
                    Token Ring Address: 00-00-19-c8-2e-02
                    Bridge Id Message Interval: 60 Priority: 2,
                    Bridge Id length type: Short
                    Password valid: FALSE
                    Mode: Source Route Transparent, Bridge #1,
                    SRB mode = AUTOMATIC
                    IP Address 98.19.116.64
                    IP Default Gateway 0.0.0.0
                    IP Subnet Mask 255.0.0.0
Spanning Tree Database
                    Bridge Prio: 128, Hello Time: 2, State Delay:  11
                    Root Sister: FALSE, Bridge Root Cost: 10
                    Root Priority: 1,  Root Address: 00-00-98-00-35-b9
                    Aging Timer: 120 seconds
Bridge-Wide Statistics
              Number of addresses learned:  334
              Number of transplants:  0
Bridge Wide Priority Values
              Number priorities supported:  6
              BridgeId Priority:  2
              IPX Priority:   Normal [2]
              System Default Priority: 2
Other
              Master Reset: FALSE
              DSPF state: STOPPED
```

SHOW CONFIG

This command is used to display the configuration of a specified interface (or all interfaces).

Syntax: **SHOW CONFIG [n]**

Parameter	Description
n	The interface number for which you want to display parameters. If you do not specify an interface number n, all interface configurations will be displayed.

SHOW TXGROUP

In an XL, Transmission groups allow multiple WAN lines connected point-to-point to the same two routers to form a single transmission pipe. This command is used to display the status of WAN lines configured as a transmission group. (XL only)

Syntax: **SHOW TXGROUP**

SHOW ADDRESS

This command is used to display, one screen at a time, the table of addresses known by your router. Repeat the command to show the next screen.

Syntax: **SHOW ADDRESS [n]**

Parameter	Description
n	Number of the entry in the table you wish to display. The optional argument allows you to specify where (entry number *n*) in the table you want to begin listing the addresses.

SHOW CAM

(ILAN only.) This command is used to display the CAM Mirror Address Table. The optional argument allows you to specify a particular entry in the table.

Syntax: **SHOW CAM [n]**

Parameter	Description
n	Number of the entry in the table you wish to display.

SET CAM

(ILAN only.) This command can be used only with the New TRECH feature. It adds an address to the CAM Mirror Address Table and, optionally, sets bits SACopy, DACopy, and SANoCopy.

Syntax: **SET CAM n address SAB[IT] DAB[IT] SAN[OCOPY]**

Parameter	Description
n	The interface number.
address	The physical (MAC) address.
SAB[IT]	Sets the SACopy bit.
DAB[IT]	Sets the DACopy bit.
SAN[OCOPY]	Sets the SANoCopy bit.

CLEAR CAM

(ILAN only.) This command can be used only with the New TRECH feature. It deletes an address from the CAM Mirror Address Table.

Syntax: **CLEAR CAM n address**

Parameter	Description
n	Number of the table entry to delete.
address	The physical (MAC) address.

SHOW TRADDR

(ILAN only.) This command is used to display the Token Ring Open Adapter address used by LM or LNM.

Syntax: **SHOW TRADDR [n]**

Parameter	Description
n	The interface number.

SET TRADDR

(ILAN only) This command is used to set the Token Ring Open Adapter address used by LM or LNM.

Syntax: **SET TRADDR [n] address**

Parameter	Description
n	The interface number.
address	The physical (MAC) address.

NETBIOS

This command is used to display the table of NetBIOS Names with their corresponding MAC addresses. The optional argument allows you to specify the starting entry number of the display or a specific NetBIOS Name.

Syntax: **NETBIOS [X] {[n] | [N netbios_name]}**

Parameter	Description
X	NetBIOS name in hexadecimal form.
n	The entry number in the table from which you want the display to begin.
netbios_name	NetBIOS name.

SHOW STTYPE

This command is used to display the Spanning Tree type that is currently set. It will display one of the following: CrossComm ST, IEEE 802.1d ST, or IBM MAC Bridge ST.

Syntax: **SHOW STTYPE**

SHOW BOOT

This command is used to display the current boot parameters for the router.

Syntax: **SHOW BOOT**

SHOW DIR

This command is used to display the storage device directory for the flash device. (XL only)

Syntax: **SHOW DIR**

SHOW MESSAGES

This command is used to display the threshold for printing messages for a specified facility or for all facilities.

Syntax: **SHOW MESSAGES {facility | ALL}**

You can select a facility for which you want to display the threshold for printed messages. The following facilities can be displayed (depending on your router type).

Facility	Description
ALL	When ALL is selected, the threshold for printed messages is displayed for all facilities. Otherwise, you can select one of the facilities listed below.
ATR	AppleTalk Router
DEBUG	Debugger
FF	Forwarding Engine
FR	Frame Relay
HB	Heterogeneous Bridging
IMS	ClearSight (former IMS) messages
IP	Internet Protocol
IPBRES	IP Resolution messages
IPR	IP Router
IPX	IPX router messages
IPXTRACE	IPX router packet trace messages
KERNEL	Kernel
LLC	Link–Level Communication
LNM	LAN Manager
NETBRES	NetBIOS Resolution messages

NM	Network Management
NT	Parallel lines (network)
PIR	Protocol Independent Routing
SLCS	SNA Link Conversion Services
SNA	Systems Network Architecture
SNM	SNMP
ST	Spanning Tree messages
SWUPGR	Software Upgrades messages
TABLE	Table maintenance messages
TR	Token Ring
WD	Ethernet
WN	WAN interface
X25	X.25 interface
ZE	Zenith–type interface

SHOW EVLOG

This command is used to display the volatile or non–volatile Event Log. (XL only)

Syntax: **SHOW EVLOG {N | V} [lognumber | FROM timestamp]**

Parameter	Description
N	This parameter is used to display a non–volatile copy of the Event Log.
V	This parameter is used to display a volatile copy of the Event Log.
lognumber	You may optionally display the log number from which you want to start the display.
timestamp	You may optionally display the time from which you want to start displaying log entries in the form: ***dd*/*mm*/*yy*** **[*hh*:*mm*:*ss* [A | P]]**

SHOW PROTECT

This command is used to display flash memory write protection. (XL only)

Syntax: **SHOW PROTECT**

SHOW NUMBERS

This command is used to display the internal and SNMP numbers for Port, Interface and Adapter. The internal numbers are used in console commands and the SNMP numbers are used in ClearSight screens. (XL only)

Syntax: **SHOW NUMBERS**

GMU ENABLE | DISABLE ALL

This command enables or disables protection and detection mechanisms for all features using a predefined schedule (code, data, internal ram). To view the effects of this command, use GMU and GMU CGF commands (they are only available for the NWS and the programmers.)

Note: This command does not force the default settings. It enables memory protection if any GMU register is free. In other case, the command's settings are written into battram.

Syntax: **GMU {ENABLE | DISABLE} ALL**

CYCLE

This command stops and starts the specified interface.

Syntax: **CYCLE n**

Parameter	Description
n	The number of the interface you want to cycle.

STOP

This command stops the specified interface.

Syntax: **STOP n**

Parameter	Description
n	The number of the interface you want to stop.

START

This command starts the specified interface.

Syntax: **START n**

Parameter	Description
n	The number of the interface you want to start.

STOP BUS

This command stops the bus. (XL only)

Syntax: **STOP BUS**

START BUS

This command starts the bus. (XL only)

Syntax: **START BUS**

HELP SET BRIDGE

This command is used to display the list of all Set Bridge commands.

Syntax: **HELP SET BRIDGE**

SET BRIDGE MODE

This command is used to set general bridging modes for the router.

Syntax: **SET BRIDGE MODE {TRN | SRT | SR}**

Parameter	Description
TRN	Sets the bridging mode to Transparent.
SRT	Sets the bridging mode to Source Routing Transparent.
SR	Sets the bridging mode to Source Routing.

SET BRIDGE SRB

This command is used to set the Single Route Broadcast routing mode.

Syntax: **SET BRIDGE SRB {AUTOMATIC | MANUAL | MANUALTXO}**

Parameter	Description
AUTOMATIC	Sets the SRB routing mode to Automatic.
MANUAL	Sets the SRB routing mode to Manual. If the port is set to blocking, SRBs will not be received on the port or transmitted from this port.
MANUALTXO	Sets the SRB routing mode to Manual Transmit Only. If the port is set to blocking, SRBs will not be transmitted from this port but will be received on this port.

SET BRIDGE NAME

This command is used to set the name of the bridge.

Syntax: **SET BRIDGE NAME name**

Parameter	Description
name	The name you want to set for the bridge (up to 32 characters).

SET BRIDGE NUMBER

This command is used to set the bridge number.

Syntax: **SET BRIDGE NUMBER n**

Parameter	Description
n	The number you want to identify the bridge on the Source Routing network. The valid numbers are from 1 to F (hex).

SET ADV INTERFACE MODEM

Use this command to select the modem type number.

Syntax: **SET ADV INTERFACE n MODEM=i**

Parameter	Description
n	The interface number
i	The modem number from the list of supported modems. You can display the list by using the command SHOW MODEM [i] on page 25 (omit [i] parameter).

SET ADV INTERFACE UARTSPEED

Use this command to set UART (Universal Asynchronous Receiver/Transmitter) speed. It is the speed between the modem and the router.

The Asynchronous Driver cannot read speed between modems in reliable way. The cost of an port is calculated based on DTE DCE speed (UART speed). Sometimes this cost is too small, especially when transmitted data are difficult to compress. In such case the cost on port must be modified manually.

Syntax: **SET ADV INTERFACE n UARTSPEED=i**

Parameter	Description
n	The interface number
i	The speed value (bytes per second). Possible values: 300, 1200, 2400, 4800, 9600, 14400, 19200, 38400, 57600, 115200, 124800

SET ADV INTERFACE PARITY

Use this command to set parity bit type.

Syntax: **SET ADV INTERFACE n PARITY=<EVEN | ODD | NONE>**

Parameter	Description
n	The interface number

SET ADV INTERFACE STOP

Use this command to stop bits per character.

Syntax: **SET ADV INTERFACE n STOP=<1 | 2 | 1.5>**

Parameter	Description
n	The interface number

SET ADV INTERFACE CALLRETRY

Use this command to set the number of call retries.

Syntax: **SET ADV INTERFACE n CALLRETRY=i**

Parameter	Description
n	The interface number
i	The number of retries

SET ADV INTERFACE RETRYINTV

Use this command to set call retry interval.

Syntax: **SET ADV INTERFACE n RETRYINTV=i**

Parameter	Description
n	The interface number
i	The call retry interval in seconds

SET ADV INTERFACE LOOPRETRY

Use this command to set number of retries of whole phone book.

Syntax: **SET ADV INTERFACE n LOOPRETRY=i**

Parameter	Description
n	The interface number
i	The number of retries

SET ADV INTERFACE TIMEOUT

Use this command to set waiting time for establishing call.

Syntax: **SET ADV INTERFACE n TIMEOUT=i**

Parameter	Description
n	The interface number
i	The waiting time in seconds

SET ADV INTERFACE {SLAVE | MASTER | AUTO}

Use this command to set calling mode.

Syntax: **SET ADV INTERFACE n mode**

Parameter	Description
n	The interface number
mode	SLAVE - only accepts calls MASTER - only establishes calls AUTO - accepts and establishes calls

SET ADV INTERFACE {TONE | PULSE}

Use this command to set dial mode to tone or pulse.

Syntax: **SET ADV INTERFACE n {TONE | PULSE}**

Parameter	Description
n	The interface parameter
TONE	Sets dial mode to tone
PULSE	Sets dial mode to pulse

SET ADV INTERFACE {RECON | NORECON}

Use this command to enable or disable autoreconnection. When asynchronous interface is used for Dial Backup, Dial on Demand or Bandwidth on Demand, the autoreconnect option must be disabled.

Syntax: **SET ADV INTERFACE n {RECON | NORECON}**

Parameter	Description
n	The interface number
RECON	Enables autoreconnection
NORECON	Disables autoreconnection

SET ADV INTERFACE SETPHN

Use this command to set phone number at i-th position in the Phone Book.

Syntax: **SET ADV INTERFACE n SETPHN i phn**

Parameter	Description
n	The interface number
i	The position number
phn	The phone number

SET ADV INTERFACE INSPHN

Use this command to insert phone number at i-th position in the Phone Book.

Syntax: **SET ADV INTERFACE n INSPHN i phn**

Parameter	Description
n	The interface number
i	The position number
phn	The phone number

SET ADV INTERFACE DELPHN

Use this command to remove i-th phone number in the Phone Book.

Syntax: **SET ADV INTERFACE n DELPHN i**

Parameter	Description
n	The interface number
i	The position number

SET ADV INTERFACE CLRALL

Use this command to clear entire Phone Book.

Syntax: **SET ADV INTERFACE n CLRALL**

Parameter	Description
n	The interface number

SET ADV INTERFACE {UP | DOWN}

Use this command to shifts i-th phone number up or down.

Syntax: **SET ADV INTERFACE n {UP | DOWN} i**

Parameter	Description
n	The interface number
i	The phone number position in the Phone Book
UP	Shifts the i-th number up
DOWN	Shifts the i-th number down

SET ADV INTERFACE INIT

Use this command to set initialize mode string.

Syntax: **SET ADV INTERFACE n INIT str**

Parameter	Description
n	The interface number
str	The string number. To choose this number refer to the module manual. Terminate it with ^M.

SET ADV INTERFACE {TONEPREF | PULSEPREF}

Use this command to set dial mode (tone or pulse) dial prefix string.

Syntax: **SET ADV INTERFACE n {TONEPREF | PULSEPREF} str**

Parameter	Description
n	The interface number
str	The string number. To choose this number refer to the module manual.
TONEPREF	Sets dial mode to tone
PULSEPREF	Sets dial mode to pulse

SET ADV INTERFACE SUFFIX

Use this command to set suffix string.

Syntax: **SET ADV INTERFACE n SUFFIX str**

Parameter	Description
n	The interface number
str	The string number. To choose this number refer to the module manual. Terminate it with ^M.

SET ADV INTERFACE HANGUP

Use this command to set hang up command string.

Syntax: **SET ADV INTERFACE n HANGUP str**

Parameter	Description
n	The interface number
str	The string number. To choose this number refer to the module manual. Terminate it with ^M.

SET ADV INTERFACE {ANSON | ANSOFF}

Use this command to set answer enable or answer disable string.

Syntax: **SET ADV INTERFACE n {ANSON | ANSOFF} str**

Parameter	Description
n	The interface number
str	The string number. To choose this number refer to the module manual. Terminate it with ^M.

SHOW ADV [ALL] or SHAC

Use this command to display all asynchronous parameters for an interface.

Syntax: **SHOW ADV n [ALL]**

or

Syntax: **SHAC n [ALL]**

Parameter	Description
n	The interface number
ALL	ALL is redundant here. Whether or not you specify this option, all parameters will be displayed.

SHOW MODEM or SHM

Use this command to display the list of supported modems or single modem configuration

Syntax: **SHOW MODEM [i]**

or

Syntax: **SHM [i]**

Parameter	Description
i	The modem number. If you specify this parameter, modem configuration will be displayed. If you omit this parameter, the list of supported modems will be displayed.

SHOW HIST or SHH

Use this command to display history of messages between DTE and DCE. The Asynchronous Driver keeps history of the last 16 messages sent to or received from modem.

Syntax: **AS SHC n HIST**

Parameter	Description
n	The interface number

SET PORT NUMBER

This command is used to set the LAN segment corresponding to a specified port.

Syntax: **SET PORT n NUMBER x**

Parameter	Description
n	The number of the port in the range from 0 to 7.
x	A segment number in the range from 0 to FFF (hex).

SET PORT LEARN ON and SET PORT LEARN OFF

Every WAN port has a new parameter indicating whether automatic learning from KA frames is enabled on this port or not. This parameter is stored in Battram, so it is not lost after power cycle. By default all ports have learning disabled. The SHP (show port) console command shows the state of learning for a port.

These commands turn on and off learning from KA frames on a given port

Syntax: **SET PORT *n* LEARN {ON | OFF}**

Parameter	Description
n	The number of the port.
ON	Enables automatic port learning.
OFF	Disables automatic port learning.

Note: This command is relevant only for ports on which automatic learning is available, for example on CrossComm Point-to-Point WAN ports and ISDN ports. For all other ports this command has no effect and the SHP command does not display the state of the automatic learning parameter.

When the WAN interface becomes active, the router with learning enabled will set the same LAN segment number on its WAN port as the remote router has on the appropriate port.

SET PORT n BRIDGE IP {ON | OFF}

This command enables and disables IP traffic bridging on a port.

Note: When an ordinary port is disabled, it becomes internally connected to a Virtual Port (VP), and it will take part in bridge flooding procedures.

Syntax: **SET PORT n BRIDGE IP {ON | OFF}**

Parameter	Description
n	The port number

SET PORT n BRIDGE IPX {ON | OFF}

This command enables and disables IPX traffic bridging on a port.

Note: When an ordinary port is disabled, it becomes internally connected to a Virtual Port (VP), and it will take part in bridge flooding procedures.

Syntax: **SET PORT n BRIDGE IPX {ON | OFF}**

Parameter	Description
n	The port number

SET PORT BRIDGE {ON | OFF}

This command enables and disables bridging on a port.

Syntax: **SET PORT p BRIDGE {ON | OFF}**

Parameter	Description
ON	Enables bridge on port p
OFF	Disables bridging on port p
p	The port number

SET PORT OPSTATE

This command is used for setting port operating state.

Syntax: **SET PORT p OPSTATE option**

Parameter	Description
p	port number
option	operating state: **B -** no bridging **O** - Operational **S** - Standby **N** - No Spanning Tree.

RSITE

In certain situations we may not be able to use learning from KA frames (for example when we have router with WAN186 adapter or when the code on one of the routers does not support automatic learning).

The following command with no parameters displays the table of remote sites and with the three mentioned parameters it adds (or modifies) an entry in the table. Each entry consists of a router's MAC address, LAN segment number and the port number

Syntax: RSITE

or

Syntax: RSITE <*mac_address*> <*lan_segment_number*> <*port_number*>

Parameter	Description
mac_address	The MAC address which should be given in the form xx-xx-xx-xx-xx-xx. The last digit of the MAC address is irrelevant in this case, so it is always displayed in a form xx-xx-xx-xx-xx-x0.
lan_segment_number	The LAN Segment Number which should be a hexadecimal number in the range 1 to FFF.
port_number	The port_number which should be a decimal number in the range 0 to 255 (port numbering is as for most of console commands - for example SET PORT).

RSITE DELETE and RSITE DELETE ALL

This command deletes all entries or one entry from the table of remote sites.

Syntax: **RSITE DELETE [*entry_number* | ALL]**

Parameter	Description
entry_number	This is the entry_number which is a decimal number in the range 1 to 5, as displayed by the command RSITE on page 28.

The table can store up to 5 entries. The table of remote sites is stored in BattRAM so it is not lost after the power cycle.

When a WAN port becomes active and the router on the other side of the WAN line is present in the table (by its MAC address and the port number), the appropriate segment number from the table will be set on this port. If a known router connects to you over a WAN line but on a different port than set in the table, the segment number learning will be aborted.

SET MESSAGES MACMAINT

This command allows you to see the details of the learning process.

Syntax: **SET MESSAGES MACMAINT**

SET PORT HOP

This command is used to set the Hop Count Limit corresponding to a specified port. The Hop Count Limit is the maximum number of bridges a Source Routing broadcast may travel through including the current bridge.

Syntax: **SET PORT n HOP x**

Parameter	Description
n	The number of the port in the range from 0 to 7.
x	The maximum number of bridges a broadcast can pass through in the range from 1 to 7.

SET PORT SRB

This command is used to enable and disable SRB traffic on a port for SRB Manual and SRB MANUALTXO modes. In MANUALTXO mode, this command will enable and disable only transmitted SRBs through the specified port.

Syntax: **SET PORT n SRB {ON | OFF}**

Parameter	Description
n	The number of the port in the range from 0 to 7.

SET PORT NAME

This command is used to set the name of a specified port.

Syntax: **SET PORT n NAME name**

Parameter	Description
n	The number of the port in the range from 0 to 7.
name	The name you want to set for the port.

SET PORT PRIO

This command is used to set a priority on a specified port.

Syntax: **SET PORT n PRIO x**

Parameter	Description
n	The number of the port in the range from 0 to 7.
x	The priority for the specified port in the range from 0 to 0xFF (hex). This priority is used in Spanning Tree mode IEEE 802.1d St.

SET PRI BRIDGEID

This command is used to set a priority for Bridge ID messages.

Syntax: **SET PRI BRIDGEID prio**

Parameter	Description
prio	A value in the range from 1 to 3, 1 being the highest priority.

SET BRIDGE PRIO

This command is used to set the Spanning Tree priority for the bridge.

Syntax: **SET BRIDGE PRIO n**

Parameter	Description
n	A value used to define the Spanning Tree priority for the bridge.

SET PRI NORMAL

This command is used to set the router default priority. If a packet is not assigned a priority using one of the transmit prioritization features (SNA, MAC Address, SmartFilters, etc.), the router default priority will be assigned. (XL only)

Syntax: **SET PRI NORMAL prio**

Parameter	Description
prio	A value in the range from 1 to 3, 1 being the highest priority.

SET STTYPE

This command is used to set a Spanning Tree mode.

Syntax: **SET STTYPE {CCC | 802 | IBM}**

Parameter	Description
CCC	Sets the Spanning Tree mode to CrossComm ST. This is the default.
802	Sets the Spanning Tree mode to IEEE 802.1d ST.
IBM	Sets the Spanning Tree mode to IBM MAC Bridge ST.

SET TFTP TIMEOUT

This command is used to set the time–out value for TFTP.

Syntax: **SET TFTP TIMEOUT n**

Parameter	Description
n	A value used to set the time–out value for TFTP.

SET INTERFACE ASYNC

Use this command to set asynchronous mode on the interface.

Syntax: **SET INTERFACE ASYNC**

SET INTERFACE NOASYNC

Use this command to set synchronous mode on the interface.

Syntax: **SET INTERFACE NOASYNC**

SET INTERFACE SPEED

This command is used to set the speed on an interface. Make sure the interface is stopped before you use this command. When you start the interface, the parameter change will take effect.

Syntax: **SET INTERFACE n SPEED = {4 | 16}**

Parameter	Description
n	The interface number for which you want to set the interface speed.
4	Sets the interface speed to 4 Mbps.
16	Sets the interface speed to 16 Mbps.

SET INTERFACE UTP and SET INTERFACE STP

This command is used to set the media type on a Token Ring interface. Make sure the interface is stopped before you use this command. When you start the interface, the parameter change will take effect.

Syntax: **SET INTERFACE n {UTP | STP}**

Parameter	Description
n	The interface number for which you want to set the media type.
UTP	Sets the interface to Unshielded Twisted Pair (UTP).
STP	Sets the interface to Shielded Twisted Pair (STP).

SET INTERFACE {WAN parameters}

This command sets configuration parameters for a WAN interface. Make sure the interface is stopped before you use this command. When you start the interface, the parameter change will take effect.

Syntax: **SET INTERFACE n option1 & [option 2 & option 3 ...]**

option1, ***option2***, ***option3*** ... can be any one of the options listed below.

Option Description

SET INTERFACE n RS232
or
SET INTERFACE n V35
or
SET INTERFACE n RS422
or
SET INTERFACE n X21
or
SET INTERFACE n FR

Sets the serial interface type.

SET INTERFACE n GENERATE
or
SET INTERFACE n RECOVER

Sets the clock source to Generate or Recover.

SET INTERFACE n INVERT
or
SET INTERFACE n NOINVERT

Sets the data inversion. No invert should only be used for T1 interfaces.

SET INTERFACE n ESF
or
SET INTERFACE n D4

Sets the T1 frame type.

SET INTERFACE n FRAC *f*

Sets fractional T1 on the DS1 connection.
Range: 1..24

SET INTERFACE n SPEED = x

When clock source is in generate mode, this option sets the clock speed. The parameter *x* can be 2400, 4800, 9600, 19200, 38400, 56000, 64000, 128000, 256000, 512000, 1024000, 1544000, or 2048000 (bps).

SET INTERFACE n COMPRESS {ON | OFF}

Sets data compression on or off.

SET INTERFACE n MAXTIME *t*

Sets the maximum time a packet can be placed in the WAN queue. ***t*** is a time in tics (1 tic = 50 msecs) in the range from 0 to 255. A time of 0 tics means that there is not time limit for queued packets.

SET INTERFACE n PASSTHRU *m*
or
SET INTERFACE n SDLC *m*
or
SET INTERFACE n NOPASS

PASSTHRU enables General Pass Through mode for circuit *m*.
SDLC enables SDLC Specific Pass Through mode for circuit *m*
and NOPASS disables Pass Through mode and disables Backup Mode.

SET INTERFACE n STATION *s*

Used with Pass Through, this option sets the station number to *s* (a hex value). In General Pass Through mode, *s* can only be 1 or 2.

SET INTERFACE n NRZ
or
SET INTERFACE n NRZI

Sets the interface encoding to NRZ or NRZI. NRZ is the default.

SET INTERFACE n RESYNC ON
SET INTERFACE n RESYNC OFF

Sets sync–resync DCE ability on the WAN interface.

SET INTERFACE n RTS ON
SET INTERFACE n RTS OFF

Drops or raises the RTS line.

SET INTERFACE n DTR ON
SET INTERFACE n DTR OFF

Drops or raises the DTR line.

SET INTERFACE n BACKUP

Sets the interface Backup Mode and designates this interface as a backup line for Dial Backup service. (NOPASS disables Backup Mode.)

SET INTERFACE n FLAG
or
SET INTERFACE n MARK
or
SET INTERFACE n MIXED

Idle the interface with FLAG, MARK, or MIXED (both FLAGs and MARKs are permitted). FLAGs is the default. Use MIXED when the remote SDLC device is an AS/ 400

SET INTERFACE n IDLE *s*

Sets IDLE mode seconds on a WAN interface for Dial on Demand. ***s*** is a decimal value of IDLE time in the range from 0 to 999 seconds. If ***s*** = 0 the IDLE mode is disabled. If s is greater than 0, the IDLE mode is enabled.

SET INTERFACE n MULTIDROP {ON | OFF}

Enables or disables SDLC PassThrough Multidrop Mode. In Multidrop Mode, the router transmits FLAGS after frames with the P/F bit OFF and transmits MARKS after frames with the P/F bit ON.

SET INTERFACE n TDR
or
SET INTERFACE n NOTDR

Enables or disables the Transition Detection mechanism used to detect broken lines for CrossComm Point-to-Point, SMDS and FR. When there is no transition on data lines the interface enters the remote disconnect state. Transition detection is disabled for all PassThrough modes when the line is set in MARK or MIXED mode. It should be disabled for slow lines (slower than 56kbps).

SET INTERFACE n KATIMER=*s*

Determines the interval (s) between sending keep-alive frames. The range for XLP and WAN186 is from 1 second to 7 seconds. The range for QWMA is from 0 to 7 seconds. The default value is 7 seconds. Zero seconds for QWMA means: sending KA is disabled. When this period is shorter, an interface should start faster.

Note: The next three parameters (below) are available only for dialling, synchronous interfaces.

SET INTERFACE n CALLRETRY=*x*

Sets the number of retries (x) to establish a connection.

SET INTERFACE n RETRYINTV=*s*

Determines the interval (s) between respective retries of establishing a connection on the interface.

SET INTERFACE n AUTORECON {ENABLE | DISABLE}

Enables or disables call Autoreconnection feature. When the feature is enabled, interface tries to reestablish a connection. It rises DTR signal and forces a modem to call.

Note: The last four parameters (below) are available only for interfaces with DDS SIM installed. They add test capabilities to DDS SIM and allow the user to check connectivity on the physical layer between two routers.

SET INTERFACE n NETLOOP

Sets local network loopback on DDS SIM.

SET INTERFACE n LOCLOOP

Sets local unit loopback on DDS SIM.

SET INTERFACE n REMLOOP

Sets remote unit loopback on DDS SIM.

SET INTERFACE n NOLOOP

Resets any of Loopback modes

SET INTERFACE TXGROUP and SET INTERFACE NOTXGROUP

In an XL router, transmission groups allow multiple WAN lines connected point-to-point to the same two routers to form a single transmission pipe. This command is used to enable or disable Transmission Groups on the specified WAN interface. (XL only)

Syntax: **SET INTERFACE n {TXGROUP | NOTXGROUP}**

Parameter	Description
n	The interface number for which you want to enable or disable Transmission Groups.
TXGROUP	Enables Transmission Groups for the WAN interface. This means that this interface will automatically participate in a Transmission Group, if it, and one or more other WAN interfaces are configured in parallel (point-to-point between the same two routers). This is the default for all WAN interfaces.
NOTXGROUP	Disables Transmission Groups for the WAN interface. This means that this interface will not participate in a Transmission Group, even if it and one or more other WAN interfaces are configured in parallel.

CLEV

This command is used to clear the volatile and/or non–volatile copies of the Event Log. (XL only)

Syntax: **CLEV {N | V | B}**

Parameter	Description
N	Clears the non–volatile copy of the Event Log.
V	Clears the volatile copy of the Event Log.
B	Clears both the volatile and non–volatile copies of the Event Log.

SET MESSAGES

This command is used to set the threshold for printing messages for a specified facility or for all facilities.

Syntax: **SET MESSAGES {facility | ALL} n**

n	Description
0..3	The default value of 0 means that only critical error information will be displayed. The higher the value of n, the more debugging information will be displayed for the facility.

You can select a facility for which you want to set the threshold for printed messages. The following facilities can be set:

Facility	Description
ALL	When all is selected, the threshold for printed messages is set for all facilities.
IMS	ClearSight (former IMS) messages
IPBRES	IP Resolution messages
IPX	IPX router messages
IPXTRACE	IPX router packet messages
NETBRES	NetBIOS Resolution messages
ST	Spanning Tree messages
SWUPGR	Software Upgrades messages
TABLE	Table maintenance messages
WNMISC	WAN various messages
CCPP	CrossComm Point-to-Point messages
ZM	Zmodem messages
MC	Modem Control messages
WNHDC	WAN Hardware depend Code Messages
DOD	Dial on Demand messages

PAGE

This command is used to enable and disable paging. (XL only)

Syntax: **PAGE**

SET AGETIMER

This command is used to set the Learned Information Age Out Timer.

Syntax: **SET AGETIMER n**

Parameter	Description
n	Period of time in which if a MAC address is not seen as a source address, it is marked as inactive in the router's address table.

SET BRIDGE SNMP

This command is used to enable and disable SNMP on your router.

Syntax: **SET BRIDGE SNMP {ENABLE | DISABLE}**

SET IP ADDRESS

This command is used for setting an IP address for SNMP.

Syntax: **SET IP ADDRESS address**

Parameter	Description
address	The IP address specified in dotted decimal notation.

SET IP MASK

This command is used for setting an IP mask. This mask identifies all network bits (bits set to 1) and host bits (bits set to 0) in the associated IP address.

Syntax: **SET IP MASK address**

Parameter	Description
address	The IP address specified in dotted decimal notation.

SET IP GATEWAY

This command is used for setting a default gateway for SNMP.

Syntax: **SET IP GATEWAY address**

Parameter	Description
address	The IP address specified in dotted decimal notation.

SET BOOT DEFAULT

This command is used to set the default procedure for booting your XL.

Syntax: **SET BOOT {DEFAULT | FLSH | NETWORK | EPROM}**

Parameter	Description
DEFAULT	Causes the router to boot by the default procedure.
FLSH	Causes the router to boot from EPROM or the ACARD. This is valid only for XL.
NETWORK	Causes the router to boot from the network by the BOOTP protocol.
EPROM	Causes the router to boot from EPROM. It is valid only for ILAN.

SET BOOTDEV

This command is used to specify the order in which locations are to be searched when looking for software to boot the ILAN XL.

Syntax: **SET BOOTDEV n1 [& n2 & n3 ...]**

Parameter	Description
n1, n2, n3 ...	These are options selected from the table below which correspond to locations to search for software on power–up. If more than one option is selected, the order they appear in the command is the order they will be searched: 0 = Feature Pack 1 = Integrated Flash Memory 2 = Neighboring XL Modules 3 = Network 4 = Query All locations 5 = ROM based monitor

SET FP PROTECT

This command is used to enable and disable Feature Pack write protection. It is important for downloading using the network and a serial line. (Applies to ILAN software version 5.05 and higher.)

Syntax: SET FP PROTECT {ON | OFF}

PROTECT

This command toggles on and off the write protection settings for four general areas (see table below). All of these images are loaded by TFTP transfer, and the first unprotected and existing storage is updated by TFTP transfer.

(Use SHOW PROTECT on page 14 to check the current value of this setting.)

Syntax: PROTECT {FPACK | INTFLASH | CFGMEM | ISDNSIMS}

parameter	effect
FPACK	Toggles on or off write protection for the Feature Pack.
INTFLASH	Toggles on or off write protection for integrated flash memory.
CFGMEM	Toggles on or off write protection for non-volatile configuration memory (battRAM).
ISDNSIMS	Toggles on or off write protection for the ISDN SIMs firmware image.

SET BOOTP TIMEOUT

This command is used to set the time–out for BOOTP responses. (Applies to ILAN software version 5.50 and higher.)

Syntax: SET BOOTP TIMEOUT n

Parameter	Description
n	The time is seconds the router will wait for a BOOTP response.

HBOOT

This command causes a hardware reset to be performed and a reboot of the router. With this command, all controllers receive a hardware reset.

Syntax: HBOOT

SBOOT

This command causes a software reset to be performed and a reboot of the router. Adapters do not receive a hardware reset.

Syntax: SBOOT

EBOOT

(ILAN only.) This command causes a software reset to be performed and a reboot of the router by down loading the software from an EPROM on the A–CARD (Base Version) instead of from the Feature Pack. This command only works properly when the 5.04 Boot Prom is installed on the motherboard.

Syntax: EBOOT

NBOOT

(ILAN only.) This command causes a reboot of the router with a download using a BOOTP request. Adapters do not receive a hardware reset and the Feature Pack is not blasted. (Applies to ILAN software version 5.05 and higher with at least 4MB RAM.)

Syntax: NBOOT

MBOOT

(ILAN only.) This command is used to perform a Master Reset or a Selective Master Reset on the router. All adapters receive a hardware reset and the database is set with default values.

Syntax: **MBOOT n**

n	Description
0 or {blank}	If zero or no number *n* is specified, then Global Master Reset; otherwise, see below.
1	Master Reset for Cfg1 variable area
2	Master Reset for Cfg2 variable area
3	Master Reset for Cfg3 variable area
4	Master Reset for Adapter Record area
5	Master Reset for Address Filters area
6	Master Reset for Smart Filters area
7	Master Reset for Port List
8	Master Reset for X.25 parameters
9	Master Reset for HB parameters
11	Master Reset for Frame Relay area
12	Master Reset for AppleTalk Router area
13	Master Reset for IPX area
14	Master Reset for Dial Backup area
15	Master Reset for Port Names area
16	Master Reset for Address Table Maintenance Area
17	Master Reset to Cfg 9 variable area

BOOTLOCK

This command sets a manual lock which prevents the reboot of device from the console or ClearSight.

Syntax: **BOOTLOCK**

BOOTUNLOCK

This command removes a manual lock used to prevent the reboot of device from the console or ClearSight.

Syntax: **BOOTUNLOCK**

TIME

This command is used to set the time. If the optional argument is omitted, the command displays the current time.

Syntax: **TIME [hh:mm:ss]**

Parameter	Description
hh:mm:ss	The time in hours, minutes and seconds.

DATE

This command is used to set the date. If the optional argument is omitted, the command displays the current date.

Syntax: **DATE [mm–dd–yy]**

Parameter	Description
mm–dd–yy	The date in the form of month, day and year.

SET CFG_MEM TIMEOUT

This command is used to set an update of the sections set (CFG_MEM) timeout.

Syntax: **SET CFG_MEM TIMEOUT n**

Parameter	Description
n	Timeout period expressed in seconds.

SHOW CFG_MEM

This command is used to display information about CFG_MEM. This information includes:

- The place to store CFG — on board NVRAM or INTERNAL FLASH
- In the case of storage on the INTERNAL FLASH MODULE, the time–out value.

Syntax: **SHOW CFG_MEM**

SET MESSAGES CFG_MEM

This command is used to enable the CFG_MEM update debug.

Syntax: **SET MESSAGES CFG_MEM**

BattRam Loader

Use the commands below (SET TFTPGET and SET PROTECT) and standard TFTP commands to copy the binary image from nonvolatile RAM to a file or to copy such a file to nonvolatile RAM. You can use these procedures to back up a device's settings (which are stored in nonvolatile memory) and later copy those settings back to the same device or to a different device that you want to configure in the same way.

Remember that parameters downloaded to a device in this manner do not become operational until after you reboot the device.

SET TFTPGET

The device configuration settings can be copied to a file using the standard TFTP Get command in binary transfer mode. To prepare for this, however, you must first set the device's TFTP Get selector to Configuration Memory.

Syntax: **SET TFTPGET {CFGMEM | CAPTMSG}**

Parameter	Description
CFGMEM	Use this parameter to enable TFTP to copy configuration settings from a device to a file.
CAPTMSG	This is the default setting for the device's TFTP Get.

You can check the setting for the device's TFTP Get using the following command:

Syntax: **SHOW TFTPGET**

The response will be either CFGMEM or CAPTMSG. In this case, you want a response of CFGMEM.

Use TFTP Get to Upload to a File

After SET TFTPGET CFGMEM, use the standard TFTP get command *in binary transfer mode* to copy the device configuration settings to a file on the local system. This file can later be used to download settings to the same device or to another device (see below).

Use TFTP Put to Download to a Device

After SET PROTECT CFGMEM, use the standard TFTP put command to copy the device configuration settings from the file to the device. The device settings will be stored in nonvolatile memory. These settings will be used by the device only after you reboot it (software reboot, software reboot with master reset, or device off/on reboot). Remember that you must reboot the device after a download because the download process stops the normal nonvolatile memory update task, and this task will not be restarted until after reboot.

2. ABC Commands

The ATM ABC is a set of Permanent Virtual Circuits (PVCs) as seen by a single XLT module. The ABC internally connects XLT modules installed in either an XL20 or XL80 chassis to the XL20 or XL80 backplane, thereby creating a collapsed backbone network configuration.

HELP ABC

The HELP ABC command displays the available ABC commands related to the ATM backplane connection.

Syntax: **HELP ABC**

ABC SHOW APU

The ABC SHOW APU command displays low level counts maintained by the ATMizer Processor Unit (APU). The APU is a high–performance RISC–based Segmentation and Reassembly (SAR) component designed for processing ATM cells.

Syntax: **ABC SHOW APU**

Example:

```
APU information @ 107437 seconds
APU status =  2 (Active)
Received Cells:       37694
Transmitted Cells:    19536
Source Strip Errors:  49
Hop Count Errors:     0
No Buffer Errors:     0
CRC Errors:           2
Packet Size Errors:   0
No Descriptor Errors: 0
```

Display Field	Description
Receive Cells:	The number of 53–byte cells received by the APU.
Transmitted Cells:	The number of 53–byte cells transmitted by the APU.
Source Strip Errors:	Occasionally, an XLT module may place a cell onto the ABC that cannot be delivered. When this happens, the cell circles the ring, and the originating XLT module removes it and counts the event. Source Strip Errors are normal in small numbers, particularly when the ring is being reconfigured, for example when an XLT module is inserted or removed from the chassis.
Hop Count Errors:	To avoid a cell circling the ring indefinitely, each cell has a Hop Count field. Each XLT module that switches the cell, decrements the Hop Count field. The XLT module discards cells with zero hops left. Hop Count Errors are normal, in small numbers, particularly when the ring is being reconfigured, for example when XLT modules are being inserted or removed from the chassis.

No Buffer Errors:
: The number of cells discarded due to congestion caused by buffer shortages. Buffer Errors can also cause CRC Errors.

CRC Errors:
: The number of reassembled packets discarded due to CRC Errors. A small number of CRC Errors is normal, and can be caused by events such as the removal and insertion of boards, power fluctuations, and normal error rates.

Packet Size Errors:
: The number of packets reassembled by the APU that exceeded the maximum of 18314 bytes of user data.

No Descriptor Errors:
: The number of packets the APU has discarded due to congestion caused by a shortage of internal data structures.

ABC SHOW DEVICE

The ABC SHOW DEVICE command displays the current status of the ABC interface. This command corresponds to the standard SHOW INTERFACE command, but contains information specific to the ABC.

Syntax: **ABC SHOW DEVICE**

Example:

```
Device information @ 110290 seconds
Dev State:  Active,  Ext State:  On,  Cost:  0
Device Statistics:
Pkts Rx:  105418,   Pkts Tx:
Kbytes tx:  4773,   Kbytes rx:  24707
rx congestion:  0,  CRC errors:  0, length errors:  0
rx VPC errors:  0
tx congestion:  0
Device state changes:  0
Driver Counters
Cells received       610368
MegaCells received   0
Cells transmitted    110988
```

MegaCells transmitted	Description
Dev State:	The current device state.
Ext State:	The operator external state.
Pkts Rx:	The number of packets received from the ABC.
Pkts Tx:	The number of packets sent to the ABC.
KBytes Rx:	The number of kilobytes received from the ABC.
KBytes Tx:	The number of kilobytes sent to the ABC.
rx congestion:	The number of packets dropped by the ABC due to a lack of buffers.
CRC errors:	The number of packets received on the ABC with AAL5 CRC errors.

length errors: The number of packets received on the ABC with invalid lengths (e.g., not a multiple of 48 for AAL5 conformance).

rx VPC errors: The number of packets received from an invalid ATM address (invalid module installed in the chassis).

tx congestion: The number of dropped packets due to a lack of buffers when being transmitted to the ABC.

Device state changes:
The number of times the ABC changed state from “ACTIVE."

Cells received The number of cells received from the ABC. This counter “rolls over" frequently.

MegaCells received
Number of cells, in millions, received from the ABC.

Cells transmitted
The number of cells sent to the ABC. This counter “rolls over" frequently.

MegaCells transmitted
Number of cells, in millions, sent to the ABC.

ABC SHOW PORT

The ABC SHOW PORT command displays the network parameters, Spanning Tree information, and port statistics for the ABC interface. The format and content of the output is identical to the standard SHOW PORT command.

Syntax: **ABC SHOW PORT**

Example:

```
Network information @ 110699 seconds
Port: Port IR2-0 (17) State: Operational on
Spanning Tree Information
   State:  Forwarding, Info age:  0,  Root cost:  Unreachable
   DP:True, DB prio: 128, DB addr: 00-00-98-13-df-b0,
   PORT cost: 0
Routing Parameters
   Lan segment #012 , SRB forwarding is ENABLED
   Hop count limit
   Connected to other PIR
Bridge ID Parameters      pdb_idm = f
   Turned on
   RIF type: Follow bridge mode
Port Statisticc
    Received Packets:  Total: 96205, Multicast: 83888
            Normally filtered:56,     Forwarded: 12261
            Filtered by Kept:  Off 0, On 0
    Transmit Pkts:     Total: 21618,  Dropped/Congestion:  0
```

Display Field	Description
Network information	The amount of time statistics have been kept for the ABC.
Port:	The port name. (You cannot set the port name.)
State:	The current operational state, either on or off.
State: (Spanning Tree)	The current state of the Spanning Tree, either Forwarding, Blocking, Listening, or Learning.

Info age: (Spanning Tree)
: The age of the Spanning Tree information from the last received packet on the port.

Root cost: (Spanning Tree)
: The Spanning Tree cost to the root, if reachable through the ABC. If not reachable through the ABC, the value is zero.

DP: (Spanning Tree)
: Indicates if the XLT module is the designated bridge on this port, either True or False.

DB prio: (Spanning Tree)
: The Spanning Tree priority of the ABC.

DB addr: (Spanning Tree)
: The address of the designated bridge through the ABC.

PORT cost: (Spanning Tree)
: The Spanning Tree cost of the ABC. The value is always zero.

LAN segment: (Routing)
: The source route segment number of the ABC.

SRB forwarding is: (Routing)
: Indicates if the SRBs are allowed to forward to and from the ABC, either Enabled or Disabled.

Hop count limit: (Routing)
: The maximum Hop Count allowed to and from the ABC.

Connected to other PIR (Routing)
: Indicates if other modules in the chassis are configured with PIR.

Turned on: (Bridging)
: Indicates if Bridge IDs can be sent by this XLT module onto the ABC.

RIF type: (Bridging)
: Indicates the format in which bridge IDs are sent, either Transparent, Source–Routed, Both, or Follow Bridge Mode.

Receive Packets:
: Total: The total number of packets received.

Receive Packets: Multicast:
: The number of multicast/broadcasts received.

Receive Packets: Normally filtered:
: The number of packets dropped due to normal bridging functions.

Receive Packets: Forwarded:
: The number of packets that were forwarded.

Transmit Pkts: The total number of packets that were transmitted.

ABC SHOW PHYSICAL

The ABC SHOW PHYSICAL command displays the ABC physical layer status and statistics. The display provides current Sonet Universal Network Interface (SUNI)–Lite statistics, as well as statistics since:

- Power–on
- SONET error counters for the last hour (in 15 minute intervals)

Syntax: **ABC SHOW PHYSICAL**

Example:

```
Physical information @ 110722 seconds
                           SUNI-Lite Statistics:
RSOP BIP8 errors:          40070
RLOP BIP8 errors:          7859
RPOP BIP8 errors:          6078
RLOP FEBE errors:          9734
RPOP FEBE errors:          6724
RACP HCS errors (fixed):464
RACP HCS errors:           193
RACP Cells received:  610426
RACP Cells transmitted:0
                           Sonet Statistics:
Sonet Medium code is NRZ
Sonet medium type is Other
Sonet line status is No Defect
Sonet path width  is sts3cSTM1
Sonet path status is No Defect
```

	ES	SES	CV	SEFS	US
Current (771 secs)					
Line:	34	0	34	----	0
Path:	33	0	33	----	0
F/E Line:	34	0	34	----	0
F/E Path:	33	0	33	----	0
Section:34	0	34	0	0	
15 minutes ago					
Line:	30	0	31	----	0
Path:	29	0	30	----	0
F/E Line:	30	0	31	----	0
F/E Path:	29	0	30	----	0
Section:	30	0	31	0	0
30 minutes ago					
Line:	38	0	38	----	0
Path:	38	0	38	----	0
F/E Line:	38	0	38	----	0
F/E Path:	38	0	38	----	0
Section:	38	0	38	0	0
45 minutes ago					
Line:	51	0	53	----	0
Path:	51	0	53	----	0
F/E Line:	51	0	53	----	0
F/E Path:	51	0	53	----	0
Section:	51	0	53	0	0
60 minutes ago					
Line:	46	0	50	----	0
Path:	46	0	50	----	0
F/E Line:	46	0	50	----	0
F/E Path:	46	0	50	----	0
Section:	46	0	50	0	0

Display Field	Description
RSOP BIP8 errors:	The number of SONET Section Bit–Interleaved Parity (BIP8) errors since power–on. Typically, a large number of these errors (tens of thousands) occur during insertion and removal of XLT modules from a chassis. The insertion and removal of XLT modules causes ATM reconfiguration. Under normal operation, there will be very few or no errors.
RLOP BIP8 errors:	The number of SONET Line Bit–Interleaved Parity (BIP8) errors since power–on. Typically, a large number of these errors (thousands) occur during insertion and removal of XLT modules from a chassis. The insertion and removal of XLT modules causes ATM reconfiguration. Under normal operation, there will be very few or no errors.
RPOP BIP8 errors:	The number of SONET Path Bit–Interleaved Parity (BIP8) errors since power–on. Typically, a large number of these errors (thousands) occur during insertion and removal of XLT modules from a chassis. The insertion and removal of XLT modules causes ATM reconfiguration. Under normal operation, there will be very few or no errors.
RLOP FEBE errors:	The number of SONET Line Far End Block Errors (FEBE) since power–on. Typically, a large number of these errors (thousands) occur during insertion and removal of XLT modules from a chassis. The insertion and removal of XLT modules causes ATM reconfiguration. Under normal operation, there will be very few or no errors.
RPOP FEBE errors:	The number of SONET Path Far End Block Errors (FEBE) since power–on. Typically, a large number of these errors (thousands) occur during insertion and removal of XLT modules from a chassis. The insertion and removal of XLT modules causes ATM reconfiguration. Under normal operation, there will be very few or no errors.
RACP HCS errors (fixed):	The number of correctable Header Checksum errors that have occurred since power–on. Under normal operation, there will be very few or no errors.
RACP HCS errors:	The number of uncorrectable Header Checksum errors that have occurred since power–on. Under normal operation, there will be very few or no errors.
RACP Cells received:	The number of cells received by the PHY device since power–on.

RACP Cells transmitted:
The number of cells transmitted by the PHY device since power–on. This field should be zero at all times.

Sonet Medium Code:
This field always displays “NRZ”.

Sonet Medium Type:
This field always displays “Other”.

Sonet Line Status:
The current state of the SONET Line. This field usually displays “No Defect,” meaning the SONET Line is currently not erring. If “AIS” (Alarm Indication Signal) is displayed, the local console is detecting a problem in the SONET Line. If “RDI” (Remote Defect Indication) is displayed, the local XLT module is receiving notification that the nearest upstream XLT module has declared Line Loss of Framing, Loss of Signal, or Line AIS.

Sonet Path Width:
This field always displays “sts3CSTM1”.

Sonet Path Status:
The current state of the SONET Path. This field usually displays “No Defect,” meaning the SONET Path is currently not erring. If “AIS” (Alarm Indication Signal) is displayed, the local XLT module is detecting a problem with the SONET Path. If “LOP” (Loss of Pointer) is displayed, the local XLT module has lost synchronization with the data stream. If “RDI” (Remote Defect Indication) is displayed, the local XLT module is receiving notification that the nearest upstream XLT module has declared Path LOP or Path AIS.

CV: The number of Coding Violations (CVs) that have occurred in the current and past 15 minute intervals. CVs are BIP8 errors. During ring reconfiguration, there can be many (hundreds or thousands) CVs. Under normal operation, there will be very few or no CVs.

ES: The number of Erred Seconds (ESs) that have occurred in the current and past 15 minute intervals. An ES represents a second in which one or more CV, SEF, LOS, AIS, or LOP occurs. During ring reconfiguration, there could be some ESs. Under normal operation, there will be very few or no ESs.

SES: The number of Severity Erred Seconds (SESs) that have occurred in the current and past 15 minute intervals. A Line SES represents a second in which more than 32 Line CVs occurred or Line AIS were declared. Path SES represents a second in which more than 16 Path CVs occurred, or Path AIS or Path LOP were declared. A F/E Line SES represents a second in which more than 32 Line FEBEs occurred or a Line RDI was received.

A F/E Path SES represents a second in which more than 16 Path FEBEs occurred or Path RDI was received. A Section SES represents a second in which more than 32 Section CVs occurred, or a second in which the section declared Loss of Frame, Out of Frame, or Loss of Signal. During ring reconfiguration, there could be some SESs. Under normal operation, there will be very few or no SESs.

SEFS: The number of Severity Erred Framing Seconds (SEFSs) that have occurred in the current and past 15 minute intervals. An SEF represents a second in which the Section is Out of Frame. During ring reconfiguration, there could be some SEFSs. Under normal operation, there will be very few or no SEFSs.

US: The number of Unavailable Seconds (US) that have occurred in the current and past 15 minute intervals. Each layer (Path, Line, and Section), will become unavailable at the onset of 10 continuous SESs. Once unavailable, a layer becomes available at the onset of 10 continuous seconds with no SESs. Under normal operation, there will be very few or no USs.

ABC SHOW VC

The XLT creates a Virtual Circuit (VC) to each XLT module installed in the chassis. The ABC SHOW VC command displays statistics kept on a per–Virtual Circuit basis.

Syntax: **ABC SHOW VC**

Example:

```
VC information @ 110744 seconds

Virtual Circuit Statistics

                          Frames   Octets   K octets  Congests

 Circuit 0  Sent          0        0        0         0

      Received  0         0        0        0

 Circuit 1  Sent          33791    714      4773      0

      Received  105418    686      24707    0

 Circuit 2  Sent          0        0        0         0

      Received  0         0        0        0

 Circuit 3  Sent          0        0        0         0

      Received  0         0        0        0

 Circuit 4  Sent          0        0        0         0

      Received  0         0        0        0

 Circuit 5  Sent          0        0        0         0

      Received  0         0        0        0

 Circuit 6  Sent          0        0        0         0

      Received  0         0        0        0

 Circuit 7  Sent          0        0        0         0

      Received  0         0        0        0
```

Display Field	Description
Circuit 0..7	For each circuit, from 0 to 7, counters provide the number of packets and bytes sent to or received from the XLT module in slot 1, 3, 5...15. Each XLT module has a Virtual Circuit to itself. This Virtual Circuit should show no activity.

ABC SHOW SMR

The ABC SHOW SMR command displays the current setting of the ABC Slot Mask Register (SMR).

Syntax: **ABC SHOW SMR**

Display Field	Description
SMR configured to x	Where x is the hexadecimal value in the SMR.

ABC SHOW HARD

The ABC SHOW HARD command displays information about the various ABC hardware registers.

Syntax: **ABC SHOW HARD**

Example:

```
CSR @ 110808 seconds

ATM Ports

Backplane ports

Board Avail Register:     1

Slot Mask Register:       ff

Switch Present Register:  0

Control/Status Register:  a1

... Board is inserted into the ABC

... Board is slot 0

... Receive Frame Error is not asserted

... Back Pressure Enable is asserted

... Frame Error Enable is not asserted

... ABC/ATM Interface selected
```

Display Field	Description
Board Avail Register: **x**	Where **x** is a hexadecimal value of a bitmap representing the XLT modules installed with active ABCs. For example, a Board Avail Register of **22** represents active XLT modules in Slots 3 and 11. The field can be decoded as follows: 01 - Slot 1 10 - Slot 9 02 - Slot 3 20 - Slot 11 04 - Slot 5 40 - Slot 13 08 - Slot 7 80 - Slot 15
Slot Mask Register: **x**	Where **x** represents the current SMR being used. Currently, the SMR must be **ff**.
Switch Present Register: **0**	This is for future use. Zero is always displayed.
Control/Status Register: **x**	Where **x** is the hexadecimal value currently in the Control Status Register (CSR). The meaning of the CSR, and the displayed value, is expanded in the output below the field.
...Board is/is not inserted into the ABC	Indicates whether or not the XLT module is active on the ABC.
...Board is in slot x	Indicates which slot the XLT module is in.
...Receive Frame Error is/is not asserted	Indicates whether the XLT module is currently receiving the frame error signal from its downstream neighbor.
...Back Pressure Enable is/is not asserted	Indicates whether the back pressure flow control mechanism is enabled.
...Frame Error Enable is/is not asserted	Indicates whether the Frame Error Signal can be generated by this XLT module.
...ABC/ATM Interface selected	Indicates which physical device the XLT module is using.

ABC SET SMR

The ABC SET SMR command is used to specify which XLT modules form a virtual workgroup on the ABC. A virtual workgroup allows all XLT modules that are part of that workgroup to create ATM connections with each other. This is a hardware function. It is impossible for an XLT module from one virtual workgroup to create an ATM Virtual Circuit with an XLT module from a different workgroup.

In essence, the SMR can be used to create multiple ABCs. Since the ClearSight management software does not presently support multiple ABCs, the Slot Mask Register should be left at the power–up setting of **ff**. In the future, the SMR will allow you to configure multiple, independent router groups. Currently, the SMR must be the same for each installed XLT module.

Syntax: **ABC SET SMR**

Display Field	Description
SMR configured to **x**	Where **x** is the hexadecimal value in the SMR. The value for the SMR must be **ff**.

ABC SET CSR

The ABC SET CSR command is used to specify control information regarding the ABC. This command is primarily used by software developers and should not be changed.

Syntax: **ABC SET CSR**

The ATM SET PORT CSR command requires a new port value

Display Field	Description
CSR configured to **x**	Where **x** is the hexadecimal value in the CSR. The value for the CSR should be left at the software default value.

Configuring ABC Port Parameters

To determine the port number associated with the ABC, you can use the ABC WHATPORT command. Note that the ABC port number is typically 17.

Syntax: ABC WHATPORT

Display Field	Description
<decimal number>	The port number of the ABC, in decimal notation, in the range of 17 to 255.

All ABC port parameters are accessed in the same manner as ports related to “physical interfaces,” such as Ethernet and Token Ring, including:

- Source Route configuration
- Spanning Tree configuration
- IP
- IPX
- PIR
- OSPF router configuration

ABC SET DMABURST

Enables and disables DMA burst mode access between ICP and APU units. By default, DMA burst mode is disabled on an XLT and enabled on an XLT-F.

Syntax: ABC SET DMABURST {ENABLE | DISABLE}

Parameter/Option	Description
Enable	Enables DMA burst mode.
Disable	Disables DMA burst mode.

3. ATM Backbone and Backplane Connections Commands

Console commands for viewing and managing ATM Backbone or Backplane Connections configuration for XL versions 5.1, 5.2 and 5.6.

General Information

The two groups of commands listed below are completely compatible, and the only difference is in the operational mode of the XLT module. Only one of the listed groups is available at a time

- An XLT module with an interface in *ABC over XLX* mode supports:

- **ATM** SET RING <...>
- **ATM** SET NORING <...>
- **ATM** SET BACKBONE <...>

- **ATM** SHOW RING
- **ATM** SHOW BACKBONE
- **ATM** SHOW CPDIAG
- **ATM** SHOW CPAUTODIAG

- An XLT module with an interface in *ABC* mode supports:

- **ABC** SET RING <...>
- **ABC** SET NORING <...>(New in release 5.2)
- **ABC** SET BACKBONE <...> (New in release 5.2)

- **ABC** SHOW RING

Note on reserved VPI/VCI ranges

In *ABC over XLX* mode, XLT modules reserve a group of PVCs for ATM PVC Backbone or Backplane Connections resources that therefore cannot be configured by the user. The table below describes the reserved VPI/VCI ranges, which are dependent on the number of chassis involved in the configuration (it is assumed that each chassis is populated with seven XLT modules and one ATM Switch XLX 08/08).

Chassis count	VPI/VCI ranges reserved by modules (not user-assignable)		
1	15/219	-	15/255
2	15/119	-	15/255
3	14/210	-	15/255
4	13/237	-	15/255
5	12/200	-	15/255
6	11/99	-	15/255
7	9/189	-	15/255
8	7/215	-	15/255

ATM SET RING or ABC SET RING

Sets general parameters for Backplane Connections.

Syntax: **ATM SET RING <ring> <mode> <modules_mask> <LAN_segment> <traffic_profile>**

or

Syntax: **ABC SET RING <ring> <mode> <modules_mask> <LAN_segment> <traffic_profile>**

Note: The traffic_profile parameter is supported in 5.1 and 5.6 releases only.

Parameter	Description
ring	This is the number of ring in which appropriate XLT modules participate. Range: 0..3
mode	This is the type of the logical ring. The keyword ‘ABC’ or ‘XLX’ can be used.
modules_mask	This is the 8 bits mask in hexadecimal notation, where each bit corresponds to an XLT module in the particular ring.
LAN_segment	This is the LAN segment number for ports associated with a particular ring.
traffic_profile	This is the ATM traffic profile for CCPath Point-to-Point PVCs connecting modules in a particular ring.

Note: If the ‘ABC’ mode is issued, this parameter should not be specified.

Note: The traffic_profile parameter is supported in 5.1 and 5.6 releases only.

ATM SET NORING or ABC SET NORING

Removes particular XLT modules from a ring in Backplane Connections configuration.

Syntax: ATM SET NORING <modules_mask>

Syntax: orABC SET NORING <modules_mask>

Parameter	Description
modules_mask	This is an 8-bit mask in hexadecimal notation, where each bit corresponds to an XLT module excluded from a ring.

ATM SET BACKBONE or ABC SET BACKBONE

Sets general parameters for ATM Backbone.

Syntax: ATM SET BACKBONE <numb_of_chass> <chassis_id> <modules_mask> <LAN_segment>

or

Syntax: ABC SET BACKBONE <numb_of_chass> <chassis_id> <modules_mask> <LAN_segment>

Parameter	Description
numb_of_chass	This is the number of chassis in ATM Backbone configuration. Range: 1..8
chassis_id	This is the unique identification number for chassis. Range: 1 .. (numb_of_chass)
modules_mask	This is an 8-bit mask in hexadecimal notation, where each bit corresponds to an XLT module.
LAN_segment	This is the LAN segment number for ports associated with ATM Backbone.

ATM SHOW RING

Displays the current settings of Backplane Connections.

Syntax: **ATM SHOW RING**

or

Syntax: **ABC SHOW RING**

ATM SHOW BACKBONE

Displays the current settings of ATM Backbone configuration. Additionally, for LAN Emulation Backbone, the configuration of the Redundant XLX feature is displayed.

Syntax: **ATM SHOW BACKBONE**

ATM SHOW CPDIAG

Displays the ATM Backbone connections diagnostics.

Syntax: **ATM SHOW CPDIAG <chassis_id> <module_slot>**

Parameter	Description
chassis_id	The chassis identification number on which diagnostics are performed.
module_slot	The slot number of the XLT module on which diagnostics are performed.

Note: If you don’t specify any of these two parameters, the default value (current chassis or XLT slot number) will be used.

This command's output means:

[XLX]	- an XLX module works properly;
[XLT(n)]	- an XLT module in slot (n) works properly;
[empty]	- slot is empty;
[!!!]	- bad configuration;
[???]	- there is no configuration information available.

ATM SHOW CPAUTODIAG

Displays the ATM Backbone connections automatic diagnostics.

Syntax: **ATM SHOW CPAUTODIAG <chassis_id> <module_slot>**

Parameter	Description
chassis_id	The chassis identification number on which the diagnostics are initially performed.
module_slot	The slot number of an XLT module on which the diagnostics are initially performed.

Note: If you don’t specify any of these two parameters, the default value (the lowest chassis ID or the lowest XLT slot number) will be used.

Note: For a detailed description of the symbols displayed by this command, see the ATM SHOW CPDIAG command.

ATM SET PVCKA

Sets global threshold delays for PVC operational status (for any RFC1483 PVCs on which the ‘Keep-Alive’ option is enabled).

Syntax: **ATM SET PVCKA <up_tics> <down_tics>**

Parameter	Description
up_tics	If there are incoming traffic on this PVC for this many tics (2-second units), the PVC changes its operational state to ACTIVE. Default: 2
down_tics	If there are no incoming traffic on this PVC for this many tics (2-second units), the PVC changes its operational state to INACTIVE. Default: 5

ATM ATM SET BACKBONE TOPOLOGY {ENABLE | DISABLE}

This command enables and disables LinkUp topology reconfiguration and it is effective only in multichassis configuration. You need XLX 3.0 to change results of this command.

Syntax: **ATM ATM SET BACKBONE TOPOLOGY {ENABLE | DISABLE}**

Option	Description
ENABLE	This is the default value. Every link state change starts the topology reconfiguration process.
DISABLE	When the link between two chassis goes up, the topology reconfiguration process is not started and this link stays unused, until some other link goes down or until manual intervention by console command ATM SET BACKBONE TOPOLOGY CHANGE. An exception to the above rule occurs when the link was not connected to current configuration with any other link.

ATM SET BACKBONE TOPOLOGY CHANGE

This command enforces the start of the topology reconfiguration process when some links are not currently used. After this configuration all links working properly will be used. This command is effective only in multichassis configuration. You need XLX 3.0 to change results of this command.

Syntax: **ATM SET BACKBONE TOPOLOGY CHANGE**

ATM SET BACKBONE LANE {ETH | TR | USER}

This command switches from any other ClearPath configuration (single chassis backplane rings or many chassis) to LAN Emulation Backbone. It therefore creates a default ELAN.

Syntax: **ATM SET BACKBONE LANE {ETH | TR | USER}**

Option	Description
ETH	Deletes all existing ELANs and creates one default Ethernet ELAN
TR	Deletes all existing ELANs and creates one default Token Ring ELAN
USER	Does not change any existing LANE configurations

ATM SET BACKBONE LANE XLT

The Redundant XLX feature provides this command to choose the XLX module to which the XLT modules will connect rear facing ATM interfaces. This command is available for XLT modules in LANE Backbone configuration and for XLT modules running LANE Server software.

Syntax: **ATM SET BACKBONE LANE XLT [<xlt_slot> [, <xlt_slot>, ...]] | [ALL] [XLX <xlx_slot>]**

Option	Description
<xlt_slot>	Decimal value representing the slot number of the XLT (or a keyword “ALL”); selected XLT modules will be connected to this XLX module, which slot number is given after “XLX” keyword.
<xlx_slot>	Decimal value representing the slot of the XLT module. If this parameter is not specified, the “Automatic XLX Selection” mode is chosen for XLT modules listed in <xlt_slot> parameter.

ATM SHOW SRDIAG

This command displays the CCPath PVCs to Route Descriptors mapping for Source Route Transparent bridges in the ATM PVC Backbone configuration.

Syntax: **ATM SHOW SRDIAG <bridge_number>**

Parameter	Description
<bridge_number>	The bridge number related to the mapping between route descriptors and PVCs.

4. ATM Commands

HELP ATM

You can obtain a list of the ATM edge node interface console commands directly from the device by entering **HELP ATM** at the console.

Syntax: **HELP ATM**

Many of the parameters in the help explanations are followed by an abbreviation. The command line abbreviations include:

Abbreviation	Meaning
<b>	Bandwidth (in decimal notation) or Burst size in cells (2-32)
<c>	Cells per second (0–350000) to pass through a circuit
<d>	Decimal notation
<n>	Port number (1-128)
<p>	Pace Group (1-8): A group defining the number of times per second the ATM edge node looks for cells to transmit.
<r>	User Rate (0-135000): The usable rate in Kb/s of data to be transmitted on a circuit.
<s>	String of characters
<vci>	Virtual Channel Identifier (0-255)
<vpi>	Virtual Path Identifier (1-15)
<x>	Traffic Table Index (1-128)

ATM START and ATM START DEVICE

The ATM START (DEVICE) command starts the ATM interface. The word 'DEVICE' is required on the AES.

Syntax: **ATM START (DEVICE)**

ATM STOP and ATM STOP DEVICE

The ATM STOP (DEVICE) command stops the ATM interface. The word 'DEVICE' is required on the AES.

Syntax: **ATM STOP (DEVICE)**

ATM CYCLE and ATM CYCLE DEVICE

The ATM CYCLE (DEVICE) command causes the ATM interface to be stopped and then restarted. The word 'DEVICE' is required on the AES.

Syntax: **ATM CYCLE (DEVICE)**

ATM SHOW CONFIG TRAFFIC

The ATM SHOW CONFIG TRAFFIC command displays the traffic profile configuration.

Syntax: **ATM SHOW CONFIG TRAFFIC <x>**

Display Field	Description
Profile Index	A row entry in the Traffic Table that describes the control and rate at which traffic is transmitted or expected to be received on this particular Virtual Channel or Virtual Path.
Cells/Sec	Indicates the number of transmitted cells per second.
User–Rate	Indicates the usable data rate in Kb/s. This is the rate of data to be transmitted on this circuit. This rate is based on 48 bytes per cell. While a cell is 53 bytes long, 5 bytes are used for AAL5 encapsulation.
Pace Group	A group defining the number of times per second the ATM edge node looks for cells to send. The interface will send <b> cells at each interval, where <b> is the Burst size in cells (between 2 and 32).
Burst Size	Indicates the Burst size in cells (between 2 and 32).
Type	A traffic descriptor indicating that there is no Cell Loss Priority (CLP) and no Sustained Cell Rate control. This is a description of how the rate of traffic is regulated or controlled. To prioritize traffic during resource congestion, cells are assigned one of the two types of Cell Loss Priority (CLP): CLP=0 and CLP=1. Cells with CLP=0 have a higher priority in regards to cell loss than cells with CLP=1. Therefore, during resource congestions, CLP=1 cells are dropped before any CLP=0 cells are dropped. **Currently, the XLT–F and the AES do not support CLP.**
Class	A Virtual Channel Connection (VCC) or a Virtual Path Connection (VPC) is associated with one of a number of Quality of Service (QoS) classes. The following service classes have been specified: Service Class A-Constant bit rate video and circuit emulation; Service Class B-Variable bit rate video/audio; Service Class C-Connection–oriented data; Service Class D-Connectionless data. Four QoS classes, numbered 1, 2, 3, and 4, have been specified with the aim of supporting service classes A, B, C, and D, respectively. The VCLs (or VPLs) concatenated to form a VCC (or VPC) have the same QoS class as that of the VCC (or VPC). The Cell Loss Ratio (CLR), Cell Delay Variation (CDV), and end–to–end Cell Delay (CD) parameters are defined as part of QoS class definition. In addition, an unspecified QoS class numbered 0 is specified for best effort traffic. **Currently, the XLT–F and the AES only support Class D QoS.**

Status	Indicates the current status. **Active** indicates that the conceptual row is available for use by the VCs or VPs. **NotInSrv** indicates that the conceptual row exists in the agent, but is unavailable for use by the VCs or VPs. (This is the state necessary to change its parameters.) **NotReady** indicates that the conceptual row exists in the agent, but is missing information necessary to be available for use by the VCs and VPs.

ATM SHOW CONFIG INTERFACE

The ATM SHOW CONFIG INTERFACE command displays the ATM interface configuration.

Syntax: **ATM SHOW CONFIG INTERFACE**

Display Field	Description
Interface:	Indicates the ATM interface number.
Type:	Indicates the type of interface, either SONET OC3 or PLCP DS3.
Name:	Indicates the link name.
Port:	Indicates the port number.
Dev–State:	Indicates the internal status of the interface.
Dev–Ext–State:	Indicates the external status of the interface.
Medium Interface:	Indicates the type of ATM interface; either DS3 or OC3.
Neighbor IP address:	Indicates the IP address of the neighbor connected to the other side of this ATM interface. (This parameter is user configurable. However, if ILMI is enabled, it is defined by ILMI and therefore not user configurable.) **Currently, ILMI is not available on the XLT–F or AES.**
Name:	The SNMP name of the neighbor. (This parameter is user configurable. However, if ILMI is enabled, it is defined by ILMI and therefore not user configurable.)
Maximum Cells Xmt:	Indicates the maximum number of transmit cells per second that can be configured on this ATM interface. The actual number of committable cells is 350,000. This parameter allows the ATM interface to be over committed (up to 999,999 cells per second) or under committed.
Maximum Cells Rcv:	Indicates the maximum number of receive cells per second that can be configured on this ATM interface. The actual number of committable cells is 350,000. This parameter allows the ATM interface to be over committed (up to 999,999 cells per second) or under committed.

Available Cells Xmt:

Indicates the number of transmit cells per second available for use. If this number is equal to zero, you cannot create any more VCs or VPs because there is no more bandwidth on the ATM interface. If you want to over commit the ATM interface, you can use the ATM SET TRAFFIC CAPACITY <c> command to change the overall capacity of the ATM interface.

Available Cells Rcv:

Indicates the number of receive cells per second available for use. If this number is equal to zero, you cannot create any more VCs or VPs because there is no more bandwidth on the ATM interface. If you want to over commit the ATM interface, you can use the ATM SET TRAFFIC CAPACITY <c> command to change the overall capacity of the ATM interface.

Circuit Type — Indicates the circuit type. The circuit type can be either DS3 (Coax) or OC3 (Fiber).

Bits — Indicates the maximum range definition (2^4 - 1 = 15).

LoRng — Low Range (LoRng). The bit value must be within 0-15.

HiRng — High Range (HiRng). The bit value must be within 0-15 and equal to or higher to LoRng.

Max — The total number of possible configurable VPs or VCs. This can be configured from 0 to Max Bits using ClearSight.

Cfgd — Configured (Cfgd). The currently configured VPs or VCs.

ATM SHOW CONFIG MEDIUM

The ATM SHOW CONFIG MEDIUM command displays the physical medium configuration.

Syntax: **ATM SHOW CONFIG MEDIUM**

Display Field	Description
C–BIT	C-Bit parity is a count of CP–Bit parity errors occurring in the accumulation interval. For SYNTRAN, it is a count of CRC–9 errors occurring in the accumulation interval.
Clock	The source of Transmit Clock is derived from the recovered receive clock of another DS3 interface.
XOR with 55	Tests the FIFO data path between the ATM Layer, Atomizer, and PHY/TC Layer. Normally this option is disabled.
SCRAMBLING	Scrambles the cell payload using a self–synchronizing scrambler with an XX^43 + 1. It is required by ITU-T in I.432. It is not used on ATMF UNI DS3 interface, but may be required in the future.
PLCP delineation	Provides ATM cell delineation based on the cell HEC byte or by the PLCP direct based mapping of ATM cells into the DS3 payload envelopes. Normally, PLCP delineation is enabled.
HCS passthru	Allows cells with detected HCS (Header Checksum) errors to pass to the receive FIFO. HCS passthru is usually disabled.
8k reference	Selects an internal frame reference clock. When the interface is used to source line timing, this reference clock should be active.
Long Cable	Changes the DS3 Line build–out characteristics. Do not use cables longer than 450 feet. The cable should be good quality RG-59/U, 75 ohm coax. Do not use 50 ohm coax, normally used for Ethernet applications. If the coax cables attached to the DS3 interface are 225 feet or less, select the Short Cable parameter. If the length is greater than 225 feet, do not select the Short Cable parameter.
Count uncorrectable HCS	If this parameter is enabled, the CPPM HCS (Header Checksum Errors) counter counts the number of correctable HCS. If the parameter is disabled, the CPPM HCS counter counts the number of uncorrectable HCS errors.

Loopback — Indicates if the interface is in Loopback Mode. **NoLoop** means the interface is not in Loopback Mode. A device that is not capable of performing a loopback on the interface always returns this value. **PayloadLoop** means the received signal at this interface is looped through the device. Typically, the received signal is looped back for retransmission after it has passed through the device's framing function. **LineLoop** means the received signal at this interface does not go through the device (minimum penetration), but is looped back out.

SONET

Display Field	Description
Sonet Medium code	Indicates the line coding for this interface. The B3ZS and CMI are used for electrical SONET/SDH signals (STS–1 and STS–3). The Non–Return to Zero (NRZ) and the Return to Zero are used for optical SONET/SDH signals.
Sonet Medium type	Indicates the line type for this interface. The line types are Short and Long Range Single–Mode fiber or Multi–Mode fiber interfaces, and coax and UTP for electrical interfaces. The value **sonetOther** should be used when the Line Type is not one of the listed values.
Sonet line status	Indicates the status of the interface. The **sonetLineCurrentStatus** is a bit map represented as a sum. Therefore, it can represent multiple defects simultaneously. The **sonetLineNoDefect** should be set if and only if no other flag is set. The various bit positions are: 1 sonetLineNoDefect 2 sonetLineAIS 4 sonetLineRDI
Line Alarm Indication Signal (L-AIS)	Defined in ANSI T1.105. The following criteria are specific to the L–AIS defect: Line AIS defect is detected as a 111 pattern in bits 6, 7, and 8 of the K2 byte in five consecutive frames.
Line Remote Defect Indication (RDI) (aka Line FERF) signal	The occurrence of a 110 pattern in bit positions 6, 7, and 8 of the K2 byte in STS-1 #1 of the STS-N signal. Line RDI is defined in ANSI T1.105. The following criteria are specific to Line RDI defect: Line RDI defect is a 110 code in bits 6, 7, and 8 of the K2 byte of in STS-1 #1 in five consecutive frames.

Note: Only STS3c-STM1 is supported for the XLT–F and AES.

Sonet path width

Indicates the type of the SONET/SDH Path. For SONET, the assigned types are the STS-Nc SPEs, where N = 1, 3, 12, 24, and 48. STS-1 is equal to 51.84 Mbps. For SDH, the assigned types are the STM-Nc VCs, where N = 1, 4, and 16.

Sonet path status

Indicates the current status of the interface. The **sonetPathCurrentStatus** is a bit map represented as a sum. Therefore, it can represent multiple defects simultaneously. The **sonetPathNoDefect** should be set if no other flag is set. The various bit positions are:

1 sonetPathNoDefect
2 sonetPathSTSLOP
4 sonetPathSTSAIS
8 sonetPathSTSRDI
16 sonetPathUnequipped
32 sonetPathSignalLabelMismatch

STS-Path Loss of Pointer: A Loss of Pointer (LOP) defect is declared when either a valid pointer is not detected in eight consecutive frames, or when eight consecutive frames are detected with the New Data Flag (NDF) set to 1001 without a valid concatenation indicator (see ANSI T1.105).

STS-Path Alarm Indication Signal: The STS-Path Alarm Indication Signal (AIS) is defined in ANSI T1.105 as all ones in bytes H1, H2, and H3 as well as all ones in the entire STS SPE.

STS-Path Remote Defect Indication: STS-Path RDI (aka STS-Path FERF) signal are generated within 100 milliseconds by the STS PTE upon detection of an AIS or LOP defect. Transmission of the STS-Path RDI signal ceases within 100 milliseconds when the STS PTE no longer detects STS-Path AIS or STS-Path LOP defect. The STS-Path RDI accurately reports the presence or absence of STS-Path AIS or STS-Path LOP defects.

Unequipped: If a path connection is not provisioned (idle) the SONET equipment will signal this state by transmitting the Path Signal Label as follows--Byte C2 of the STS Path Overhead equal to 0 for an unequipped path.

Signal Label Mismatch: A path connection is not correctly provisioned if a received Path Signal Label mismatch occurs. A received Signal Label is considered mismatched if it does not equal either the locally provisioned value or the value equipped non-specific (1 hex). Any received non–zero Signal Label is considered a locally provisioned value of equipped non–specific.

Only in–service, provisioned Path Terminating equipment can detect mismatched Signal labels. It is considered provisioned if it has been configured for a mapping, and has been assigned signals to and from which the mapping takes place.

ATM SHOW VC

The ATM SHOW VC command lists all the Virtual Channels and their current states.

Syntax: **ATM SHOW VC <vpi> <vci>**

Display Field	Description
VPI	Indicates the Virtual Path Identifier (VPI) number. The range is from 1 to 15.
VCI	Indicates the Virtual Channel Identifier (VCI) number. The range is from 0 to 255.
STT	Indicates the current state of the channel. A plus (+) means it is enabled. A minus (-) means it is disabled.
Type	Indicates the type of circuit; either a Permanent Virtual Channel (PVC) or a Switched Virtual Channel (SVC).
Port	Indicates the port associated with a Virtual Channel (VC).
Owner	Indicates the application connected to a Virtual Channel (VC).
Xmt	Indicates the Traffic Profile Index and the number of transmitted cells.
Rcv	Indicates the Traffic Profile Index and the number of received cells.
Connection Name	Indicates the user–definable field that describes the two end stations the Virtual Channel (VC) supports.

ATM SHOW VP

The ATM SHOW VP command lists all the Virtual Paths and their current states.

Syntax: **ATM SHOW VP <vpi>**

Example:

ATM - Virtual Path SummarySaturday July 10, 1995 05:22:45 PM

Dev: 4 MAX Xmt:350100 Rcv:350100AVL Xmt:011302Rcv:011302

VPI	Stt	Type	Xmt	Rcv	XmtAvl	RcvAvl	Connection Name
12	+	PVP	1:001208	1:001208	001208	001208	Connection Name
13	+	PVP	1:001208	1:001208	001208	001208	Connection Name
15	+	PVP	1:001208	1:001208	001208	001208	Connection Name

Display Field	Description
VPI	Indicates the Virtual Path Identifier (VPI) number. The range is from 1 to 15.
STT	Indicates the current state of the Virtual Path. A plus (+) means it is enabled. A minus (-) means it is disabled. If disabled, all VCs relating to this VPI are disabled. If enabled, all VCs relating to this VPI can be enabled.
Type	Indicates the type of circuit; either a Permanent Virtual Path (PVP) or a Switched Virtual Path (SVP).
Xmt	Indicates the number of transmitted cells.
Rcv	Indicates the number of received cells.
XmtAvl	Indicates the available transmit cells per second for adding VCs to this VP. In the above example, there are 1208 cells left on VP 12. If you configured VC 12/1 with a rate of 600 cells per second, the VP available **XmtAvl** would drop to 608 cells per second.
RcvAvl	Indicates the available receive cells per second for adding VCs to this VP. In the above example, there are 1208 cells left on VP 12. If you configured VP 12/1 with a rate of 600 cells per second, the VP available **RcvAvl** would drop by 608 cells per second.
Connection Name	Indicates the user–definable field that describes the two end stations the Virtual Path (VP) supports.

ATM SHOW STATS VC

The ATM SHOW STATS VC command displays the Virtual Channel statistics.

Syntax: **ATM SHOW STATS VC <vpi> <vci>**

Display Field	Description
VPI	Indicates the Virtual Path Identifier (VPI) number. The range is from 1 to 15.
VCI	Indicates the Virtual Channel Identifier (VCI) number. The range is from 0 to 255.
STT	Indicates the current state of the channel. A plus (+) means it is enabled. A minus (-) means it is disabled.
Type	Indicates the type of circuit; either a Permanent Virtual Channel (PVC) or a Switched Virtual Channel (SVC).
Port	Indicates the port associated with a Virtual Channel (VC).
Owner	Indicates the application connected to a Virtual Channel (VC).
SarTmo	Indicates the number of partially re–assembled AAL5 CPCS PDUs that were discarded on this AAL5 VCC at the interface associated with an AAL5 entity because they were not fully re–assembled within the required time period. If the re–assembly timer is not supported, then this field contains a zero value.
CrcErr	Indicates the number of AAL5 CPCS PDUs received with CRC–32 errors on the AAL5 VCC at the interface associated with an AAL5 entity.
OvrSzPdus	Indicates the number of AAL5 CPCS PDUs discarded on this AAL5 VCC at the interface associated with an AAL5 entity because the AAL5 SDUs were too large.

ATM SHOW STATS MEDIUM

The ATM SHOW STATS MEDIUM command displays the physical medium statistics.

Syntax: **ATM SHOW STATS MEDIUM**

Display Field	Description
PMON LCVs errors:	Indicates the number of Line Code Violations (LVCs) since last polled.
PMON F & M Bit errors:	Indicates the number of DS3 F and M bit errors since last polled.
PMON Excessive Zeros:	Indicates the number of summed excessive zeros that occurred during the previous accumulation period. One or more excessive zeros occurrence within an 85 bit DS3 information block is counted as one summed excessive zero.
PMON P Bit errors:	Indicates the number of DS3 P–bit errors that have been detected since last polled.
PMON Path Parity errs:	Indicates the number of DS3 path parity errors that have been detected since last polled.
PMON FEBE errors:	Indicates the number of DS3 Far End Block Errors (FEBEs) that have been detected since last polled.
CPPM B1 BIP8 errors:	Indicates the number of B1 Bit–Interleaved Parity (BIP8) errors since last polled.
CPPM Framing errors:	Indicates the number of PLCP frame errors that have occurred since last polled.
CPPM FEBE errors:	Indicates the number of PLCP Far End Block Errors (FEBEs) that have occurred since last polled.
Uncorrectable HCS:	If enabled, this counter indicates the number of correctable Header Checksum (HCS) errors that have occurred since last polled. If disabled, this counter indicates the number of uncorrectable HCS errors that have occurred since last polled.

Cells received: Indicates the number of cells received by the PHY device since power on.

Megacells received:
Indicates the number of Megacells (in millions) received by the PHY device since power on.

Cells transmitted:
Indicates the number of cells transmitted by the PHY device since power on.

Megacells transmitted:
Indicates the number of Megacells (in millions) transmitted by the PHY device since power on.

Idles received: Indicates the number of idle cells received by the PHY device since power on.

Megaidles received:
Indicates the number of Megaidle (millions) cells received by the PHY device since power on.

UAS Indicates the number of Unavailable Seconds (UAS). UAS are calculated by counting the number of seconds that the interface is unavailable.

SEFS Indicates the number of Severely Errored Framing Seconds (SEFS). An SEFS is a second with one or more Out–of–Frame defects or a detected incoming AIS (Alarm Indication Signal).

LCVS Indicates the number of Line Coding Violation (LCV) Error Events. This parameter is a count of both BPVs and EXZs occurring over the accumulation period. An EXZ increments the LCV by one regardless of the length of the zero string.

LES Indicates the number of Line Errored Seconds (LES). An LES is a second in which one or more CVs (Coding Violation) occurred or there were one or more LOS (Loss of Signal) defects.

PCV Indicates the number of P–bit Coding Violation (PCV) Error Events. For all DS3 applications, a coding violation error event is a P–bit.

PES Indicates the number of P–bit Errored Seconds (PES). A PES is added when there is a second with one or more PCVs or when there are one or more Out-of-Frame defects. PES can also occur when there is a detected incoming AIS (Alarm Indication Signal). This gauge is not incremented when UASs are counted.

PSES Indicates the number of P–bit Severely Errored Seconds (PSES). A PSES is a second with 44 or more PCVs, or one or more Out–of–Frame defects. PSES can also occur when there is a detected incoming AIS (Alarm Indication Signal). This gauge is not incremented when UASs are counted.

CCV	Indicates the number of C–bit Coding Violation (CCV) Error Events. For C–bit Parity and SYNTRAN DS3 applications, this is the count of coding violations reported via the C–bits. For C–bit Parity, it is a count of CP–bit parity errors occurring in the accumulation interval. For SYNTRAN, it is a count of CRC–9 errors occurring in the accumulation interval.
CES	Indicates the number of C–bit Errored Seconds (CES). A CES is a second with one or more CCVs (C–bit Coding Violations), or one or more Out–of–Frame defects. CES can also occur when there is a detected incoming AIS (Alarm Indication Signal). This count is only for the SYNTRAN and C–bit Parity DS3 applications. This gauge is not incremented when UASs are counted.
CSES	Indicates the number of C–bit Severely Errored Seconds (CSES). A CSES is a second with 44 or more CCVs or one or more Out–of–Frame defects. CSES can also occur when there is a detected incoming AIS (Alarm Indication Signal). This count is only for the SYNTRAN and C–bit Parity DS3 applications. This gauge is not incremented when UASs are counted.

Display Field	Description
RSOP BIP8 errors:	Indicates the number of SONET Section Bit–Interleaved Parity (BIP8) errors since power–on. Typically, a large number of these errors (tens of thousands) occur during insertion and removal of XLT–F modules from a chassis. The insertion and removal of XLT–F modules causes ATM reconfiguration. Under normal operation, there will be very few or no errors.
RLOP BIP8 errors:	Indicates the number of SONET Line Bit–Interleaved Parity (BIP8) errors since power–on. Typically, a large number of these errors (thousands) occur during insertion and removal of XLT–F modules from a chassis. The insertion and removal of XLT–F modules causes ATM reconfiguration. Under normal operation, there will be very few or no errors.
RPOP BIP8 errors:	Indicates the number of SONET Path Bit–Interleaved Parity (BIP8) errors since power–on. Typically, a large number of these errors (thousands) occur during insertion and removal of XLT–F modules from a chassis. The insertion and removal of XLT–F modules causes ATM reconfiguration. Under normal operation, there will be very few or no errors.
RLOP FEBE errors:	Indicates the number of SONET Line Far End Block Errors (FEBE) since power–on. Typically, a large number of these errors (thousands) occur during insertion and removal of XLT–F modules from a chassis. The insertion and removal of XLT–F modules causes ATM reconfiguration. Under normal operation, there will be very few or no errors.

RPOP FEBE errors:

Indicates the number of SONET Path Far End Block Errors (FEBE) since power–on. Typically, a large number of these errors (thousands) occur during insertion and removal of XLT–F modules from a chassis. The insertion and removal of XLT–F modules causes ATM reconfiguration. Under normal operation, there will be very few or no errors.

RACP HCS errors (fixed):

Indicates the number of correctable Header Checksum errors that have occurred since power–on. Under normal operation, there will be very few or no errors.

RACP HCS errors:

Indicates the number of uncorrectable Header Checksum errors that have occurred since power–on. Under normal operation, there will be very few or no errors.

RACP Cells received:

Indicates the number of cells received by the PHY device since power–on.

RACP Cells transmitted:

Indicates the number of cells transmitted by the PHY device since power–on. This field should be zero at all times.

Sonet Medium Code:

This field always displays “NRZ”.

Sonet Medium Type:

This field always displays “Other”.

Sonet Line Status:

Indicates the current state of the SONET Line. This field usually displays “No Defect,” meaning the SONET Line is currently not erring. If “AIS” (Alarm Indication Signal) is displayed, the local console is detecting a problem in the SONET Line. If “RDI” (Remote Defect Indication) is displayed, the local ATM edge node is receiving notification that the nearest upstream ATM edge node has declared Line Loss of Framing, Loss of Signal, or Line AIS.

Sonet Path Width:

This field always displays “sts3CSTM1”.

Sonet Path Status:

Indicates the current state of the SONET Path. This field usually displays “No Defect,” meaning the SONET Path is currently not erring. If “AIS” (Alarm Indication Signal) is displayed, the local ATM edge node is detecting a problem with the SONET Path. If “LOP” (Loss of Pointer) is displayed, the local ATM edge node has lost synchronization with the data stream. If “RDI” (Remote Defect Indication) is displayed, the local ATM edge node is receiving notification that the nearest upstream ATM edge node has declared Path LOP or Path AIS.

CV: Indicates the number of Coding Violations (CVs) that have occurred in the current and past 15 minute intervals. CVs are BIP8 errors. During ring reconfiguration, there can be many (hundreds or thousands) CVs. Under normal operation, there will be very few or no CVs.

ES: Indicates the number of Errored Seconds (ESs) that have occurred in the current and past 15 minute intervals. An ES represents a second in which one or more CV, SEF, LOS, AIS, or LOP occurs. During ring reconfiguration, there could be some ESs. Under normal operation, there will be very few or no ESs.

SES: Indicates the number of Severity Errored Seconds (SESs) that have occurred in the current and past 15 minute intervals. A Line SES represents a second in which more than 32 Line CVs occurred or Line AIS were declared. Path SES represents a second in which more than 16 Path CVs occurred, or Path AIS or Path LOP were declared. A F/E Line SES represents a second in which more than 32 Line FEBEs occurred or Line RDI was received.

A F/E Path SES represents a second in which more than 16 Path FEBEs occurred or Path RDI was received. A Section SES represents a second in which more than 32 Section CVs occurred, or a second in which the section declared Loss of Frame, Out of Frame, or Loss of Signal. During ring reconfiguration, there could be some SESs. Under normal operation, there will be very few or no SESs.

SEFS: Indicates the number of Severity Errored Framing Seconds (SEFSs) that have occurred in the current and past 15 minute intervals. An SEF represents a second in which the Section is Out Of Frame. During ring reconfiguration, there could be some SEFSs. Under normal operation, there will be very few or no SEFSs.

US: Indicates the number of Unavailable Seconds (US) that have occurred in the current and past 15 minute intervals. Each layer (Path, Line, and Section), will become unavailable at the onset of 10 continuous SESs. Once unavailable, a layer becomes available at the onset of 10 continuous seconds with no SESs. Under normal operation, there will be very few or no USs.

ATM SHOW STATS APU

The ATM SHOW STATS APU command displays the current status of the ATM Processor Unit (APU). The APU is a chip produced by LSI Logic. It accepts data in packet format and breaks it down into ATM cell format.

Syntax: **ATM SHOW STATS APU**

Display Field	Description
Receive Cells:	Indicates the number of 53–byte cells received by the APU. These cells may or may not be forwarded to the ICP.
Transmitted Cells:	Indicates the number of 53–byte cells transmitted by the APU.
No Buffer Errors:	Indicates the number of errors encountered by the APU when a buffer was not available to insert the incoming cells. This condition will show up as a receive congestion in the device statistics.
No Descriptor Errors:	Indicates the number of packets the APU has discarded due to congestion caused by a shortage of internal data structures. The ICP handles the management of receive data descriptors for the APU. When the APU tries to obtain a descriptor, but none are available, this error is logged. This usually means that the ICP is too busy to process the descriptors that it is currently holding for the APU.
Discarded Cells:	In the event that an errored cell arrives at the APU, or a cell stream does not complete transmission, the cells are discarded.
CRC Errors:	Indicates the number of reassembled packets discarded due to CRC Errors. A small number of CRC Errors is normal, and can be caused by events such as the removal and insertion of boards, power fluctuations, and normal error rates.
BOC Errors:	BOC (Beginning of Cell) errors are logged by the APU when it was unable to find the Beginning of Cell marker for a cell. This can result in the previous cell being perceived as too long.
Packet Size Errors:	Packet size errors are logged when the APU receives a frame that is too long. The frame size is set by the **ATM SET VC XMT SIZE** command.

ATM SHOW DEVICE

The ATM SHOW DEVICE command displays the current state and statistics of the ATM device.

Syntax: **ATM SHOW DEVICE**

Display Field	Description
Pkts in:	Indicates the number of received packets.
Pkts out:	Indicates the number of transmitted packets.
tx underruns:	Indicates the number of times a packet was discarded from this line because the transmitting device could not get sufficient memory to store the packet at the receiving frequency.
rx overruns:	Indicates the number of times a packet was discarded from this line because the receiving device could not get sufficient memory to store the packet at the receiving frequency.
carrier lost:	Indicates whether the carrier is up and running. The carrier is generally the external line or medium that connects to other devices. (This field is not applicable for ATM.)
excess collisions:	Indicates the amount of collisions. (This field is not applicable for ATM.)
rx congestion:	Indicates the number of packets dropped from the line due to receiver congestion. This means that a receive buffer could not be allocated for the packet.
tx congestion:	Indicates the number of packets dropped from the line due to transmit congestion. This means that the transmit queue exceeded the maximum queue length. This could indicate that the Virtual Circuit bandwidth is not high enough.
CRC errors:	Indicates the number of AAL5 CPCS PDUs received with CRC–32 errors on the AAL5 VCC at the interface associated with an AAL5 entity.
alignment errors:	Indicates the number of times a frame or token was received with a code violation. A code violation can be a frame check sequence (FCS) error or a Manchester code violation. (This field is not applicable for ATM.)
heartbeat errors:	Indicates the number of times the collision detect hardware failed to detect a heartbeat signal. (This field is not applicable for ATM.)
length errors:	Indicates the number of times a packet was discarded from this line because it was longer than the maximum packet length.

Recovered device hangs:
: Indicates the number of times the line was re–initialized due to the detection of problems on the line.

sequence errors:
: Indicates the number of times the serial line driver received a packet that contained the wrong sequence number.

Device state changes:
: Indicates the number of state changes for this line (i.e., inactive to active.)

Driver Counters:
: Driver counters are determined during ICP transmit and receive processing. These are the number of cells that were passed to the APU, and/or received from the APU. These counters will not necessarily agree with the APU statistics.

Cells received
: Indicates the number of cells received.

Megacells received
: Indicates the number of Megacells (in millions) received.

Cells transmitted
: Indicates the number of cells transmitted.

MegaCells transmitted
: Indicates the number of Megacells (in millions) transmitted.

ATM CREATE VC

The ATM CREATE VC command creates an ATM Virtual Channel with default values. An optional Traffic Profile Index can be included to assign a default index.

Important: There are Reserved VPI/VCI ranges for ATM Backplane/Backbone Connections. See Note on reserved VPI/VCI ranges on page 65

Syntax: **ATM CREATE VC <vpi> <vci> [<x>]**

ATM CREATE VP

The ATM CREATE VP command creates an ATM Virtual Path with default values. An optional Traffic Profile Index can be included to assign a default index.

Syntax: **ATM CREATE VP <vpi> [<x>]**

ATM DELETE VC

The ATM DELETE VC command deletes an ATM Virtual Channel.

Syntax: **ATM DELETE VC <vpi> <vci>**

ATM DELETE VP

The ATM DELETE VP command deletes an ATM virtual path.

Syntax: **ATM DELETE VP <vpi>**

ATM SET VC

The ATM SET VC command sets the Virtual Channel parameters.

Syntax: **ATM SET VP <vpi> <vci> <parameter>**

parameters	description
TRAFFIC <x>	Displays the Virtual Channel Traffic Profile Index
XMT TRAFFIC <x>	Sets the Virtual Channel transmit Traffic Profile Index
RCV TRAFFIC <x>	Sets the Virtual Channel receive Traffic Profile Index
SIZE <d>	Displays the Virtual Channel frame size
XMT SIZE <d>	Sets the Virtual Channel transmit frame size (0-4096)
RCV SIZE <d>	Sets the Virtual Channel receive frame size (0-4096)
NAME <s>	Sets the Virtual Channel connection name (22 characters)
ENABLE	Enables the specified Virtual Channel
DISABLE	Disables the specified Virtual Channel

ATM SET VC TRAFFIC

The ATM SET VC TRAFFIC command displays the Virtual Channel Traffic Profile Index.

Syntax: **ATM SET VC <vpi> <vci> TRAFFIC <x>**

ATM SET VC XMT TRAFFIC and ATM SET VC RCV TRAFFIC

The ATM SET VC {XMT | RCV} TRAFFIC commands set the Virtual Channel transmit or receive Traffic Profile Index.

Syntax: **ATM SET VC <vpi> <vci> XMT TRAFFIC <x>**

Syntax: **ATM SET VC <vpi> <vci> RCV TRAFFIC <x>**

ATM SET VC SIZE

The ATM SET VC SIZE command displays the Virtual Channel traffic frame size.

Syntax: **ATM SET VC <vpi> <vci> SIZE <d>**

ATM SET VC XMT SIZE and ATM SET VC RCV SIZE

The ATM SET VC {XMT | RCV} SIZE commands set the Virtual Channel transmit or receive traffic frame size.

Syntax: **ATM SET VC <vpi> <vci> XMT SIZE <d>**

Syntax: **ATM SET VC <vpi> <vci> RCV SIZE <d>**

ATM SET VC NAME

Sets the Virtual Channel connection name. The maximum number of characters is 22.

Syntax: **ATM SET VC <vpi> <vci> NAME <s>**

ATM SET VC ENABLE and ATM SET VC DISABLE

The ATM SET VC {ENABLE | DISABLE} commands enable and disable a Virtual Channel.

Syntax: **ATM SET VC <vpi> <vci> ENABLE**

Syntax: **ATM SET VC <vpi> <vci> DISABLE**

ATM SET VP

The ATM SET VP command sets the Virtual Path parameters.

Syntax: **ATM SET VP <vpi> <parameter>**

parameters	description
TRAFFIC <x>	Displays the Virtual Path Traffic Profile Index
XMT TRAFFIC <x>	Sets the Virtual Path transmit Traffic Profile Index
RCV TRAFFIC <x>	Sets the Virtual Path receive Traffic Profile Index
NAME <s>	Sets the Virtual Path connection name (22 characters)
ENABLE	Enables the specified Virtual Path
DISABLE	Disables the specified Virtual Path

ATM SET VP TRAFFIC

The ATM SET VP TRAFFIC command displays the Virtual Path transmit Traffic Profile Index.

Syntax: **ATM SET VP <vpi> TRAFFIC <x>**

ATM SET VP XMT TRAFFIC and ATM SET VP RCV TRAFFIC

The ATM SET VP {XMT | RCV} TRAFFIC commands set the Virtual Path transmit and receive Traffic Profile Index.

Syntax: **ATM SET VP <vpi> XMT TRAFFIC <x>**

Syntax: **ATM SET VP <vpi> RCV TRAFFIC <x>**

ATM SET VP NAME

The ATM SET VP NAME command sets the Virtual Path connection name.

Syntax: **ATM SET VP <vpi> NAME <s>**

ATM SET VP ENABLE and ATM SET VP DISABLE

The ATM SET VP {ENABLE | DISABLE} commands enable and disable a Virtual Path.

Syntax: **ATM SET VP <vpi> ENABLE**

Syntax: **ATM SET VP <vpi> DISABLE**

ATM SET TRAFFIC

The ATM SET TRAFFIC command sets the ATM interface traffic parameters.

Syntax: **ATM SET TRAFFIC <parameter>**

parameters	description
PROFILE <x>	Sets the traffic row entry (10 - 128)
RATE <r>	Sets the User Rate (kilo bytes/sec: 0 - 135000)
CELLS <c>	Sets the cells/sec rate (0 - 350000)
PACE <p>	Sets the Pace Group (1 - 8)
BURST <b>	Sets the Burst size in cells (2 - 32)
CAPACITY	Sets the capacity for the ATM interface (usually 350000)
XMT CAPACITY	Sets the limit for cells/sec on the transmit ATM interface
RCV CAPACITY	Sets the limit for cells/sec on the receive ATM interface

ATM SET TRAFFIC PROFILE

The ATM SET TRAFFIC PROFILE command sets the traffic row entry (10 - 128).

Syntax: **ATM SET TRAFFIC PROFILE <x>**

ATM SET TRAFFIC PROFILE RATE

The ATM SET TRAFFIC PROFILE RATE command sets the User Rate (kilo bytes/sec: 0 - 135000). The User Rate is the rate of the data to be transmitted on a given circuit. This rate is based on 48 bytes per cell. Although a cell is 53 bytes long, 5 bytes are used for AAL5 encapsulation.

Syntax: **ATM SET TRAFFIC PROFILE <x> RATE <r>**

ATM SET TRAFFIC PROFILE CELLS

The ATM SET TRAFFIC PROFILE CELLS command sets the cells/sec rate (0 - 350000).

Syntax: **ATM SET TRAFFIC PROFILE <x> CELLS <c>**

ATM SET TRAFFIC PROFILE PACE

The ATM SET TRAFFIC PROFILE PACE command sets the Pace Group (1 - 8). The Pace Group defines the number of times per second the ATM edge node looks for cells to transmit. You can assign the Burst size after the Pace Group.

Syntax: **ATM SET TRAFFIC PROFILE <x> PACE <p>**

ATM SET TRAFFIC PROFILE BURST

The ATM SET TRAFFIC PROFILE BURST command sets the Burst size in cells (2 - 32).

Syntax: **ATM SET TRAFFIC PROFILE <x> BURST <b>**

ATM SET TRAFFIC CAPACITY

The ATM SET TRAFFIC CAPACITY command sets the limit for the total capacity (maximum bandwidth) for the ATM Interface. The range is from 0 to 999,999. The default value is 350,000.

Syntax: **ATM SET TRAFFIC CAPACITY <c>**

ATM SET TRAFFIC XMT CAPACITY and ATM SET TRAFFIC RCV CAPACITY

The ATM SET TRAFFIC {XMT | RCV} CAPACITY commands set the limit for the total capacity (maximum bandwidth) for the transmit and receive ATM Interface.

Syntax: **ATM SET TRAFFIC XMT CAPACITY <c>**

Syntax: **ATM SET TRAFFIC RCV CAPACITY <c>**

ATM SET DS3

The ATM SET DS3 command sets the DS3 interface parameters.

Syntax: **ATM SET DS3 <parameter>**

Parameters	Description
M13	Enables M13 encoding
C-BIT	Enables C-Bit parity encoding
XOR-55	Enables XOR-55
NOXOR-55	Disables XOR-55
SCRAMBLING	Enables scrambling
NOSCRAMBLING	Disables scrambling
TCLOCK	Sets transmit clock generation
LOOP-TIME	Sets transmit clock recovery
PLCP	Enables PLCP delineation
HEC	Enables HEC delineation
HCS-PASS	Enables HCS errors past SUNI
HCS-STOP	Blocks HCS errors past SUNI
8K-REF	Enables 8K reference signal
NO8K-REF	Disables 8K reference signal
PAY-LOOP	Enables payload loopback
DIAG-LOOP	Enables diagnostic loopback
CELL-LOOP	Enables cell loopback
NO-LOOP	Disables loopback
SHORT-CABLE	Enables short cable
LONG-CABLE	Enables long cable
CNT-FIXED	Counts fixed HCS errors
CNT-ERRORED	Counts uncorrectable HCS errors

ATM SET DS3 M13

The ATM SET DS3 M13 command enables M13 encoding. M13 coding is different from C–Bit parity encoding.

Syntax: **ATM SET DS3 M13**

ATM SET DS3 C–BIT

The ATM SET DS3 C-BIT command enables C–Bit parity encoding. When C–Bit parity encoding is enabled, the ATM edge node device accumulates C–Bit parity events. In the even that there is a C–Bit error, the statistics will be updated accordingly. This also enables the ATM edge node device to correctly update the C–Bits in the transmitted frames.

Syntax: **ATM SET DS3 C–BIT**

ATM SET DS3 XOR–55 and ATM SET DS3 NOXOR–55

The ATM SET DS3 {XOR–55 | NOXOR–55} commands enable and disable XOR–55. XOR–55 is a method of applying the polynomial x^6 + x^4 + x^2 + 1 to the header of a cell. It tests the FIFO data path between the ATM Layer, Atomizer, and the PHY.TC Layer. Normally, XOR–55 is disabled.

Syntax: **ATM SET DS3 XOR–55**

Syntax: **ATM SET DS3 NOXOR–55.**

ATM SET DS3 SCRAMBLING and ATM SET DS3 NOSCRAMBLING

The ATM SET DS3 {SCRAMBLING | NOSCRAMBLING} commands enable and disable scrambling. The payload is scrambled with the self–synchronizing Polynomial x^43 + 1. If scrambling is not enabled, the payload is not scrambled.

Syntax: **ATM SET DS3 SCRAMBLING**

Syntax: **ATM SET DS3 NOSCRAMBLING**

ATM SET DS3 TCLOCK

The ATM SET DS3 TCLOCK command sets transmit clock generation. This allows the transmitter to generate clock. In a point–to–point connection, one side should be TCLOCK and the other side should be LOOP–TIME.

Syntax: **ATM SET DS3 TCLOCK**

ATM SET DS3

The ATM SET DS3 LOOP-TIME command sets transmit clock recovery. The receiver will loop the received clock to use as its transmit clock.

Syntax: **ATM SET DS3 LOOP–TIME**

ATM SET DS3 PLCP

The ATM SET DS3 PLCP command enables the Physical Layer Convergence Protocol (PLCP) delineation.

Syntax: **ATM SET DS3 PLCP**

ATM SET DS3 HEC

The ATM SET DS3 HEC command enables Header Check Sum (HEC) delineation. HEC delineation is the methodology of handling PLCP versus HCS–based delineation of the cell header.

Syntax: **ATM SET DS3 HEC**

ATM SET DS3 HCS–PASS and ATM SET DS3 HCS–STOP

These commands enable and block HCS errors past SUNI. HCS–PASS allows cells with detected HCS errors to pass to the receive FIFO. HCS–PASS is usually disabled.

Syntax: **ATM SET DS3 HCS–PASS**

Syntax: **ATM SET DS3 HCS–STOP**

ATM SET DS3 8K–REF and ATM SET DS3 NO8K–REF

The ATM SET DS3 {8K-REF | NO8K-REF} commands enable and disable the 8K reference signal. The PLCP frame rate can be locked to an external 8 kHz reference signal. Setting this allows the XLT-F module to synchronize to this reference signal.

Syntax: **ATM SET DS3 8K–REF**

Syntax: **ATM SET DS3 NO8K–REF**

ATM SET DS3 PAY–LOOP

The ATM SET DS3 PAY-LOOP command enables payload loopback.

Syntax: **ATM SET DS3 PAY–LOOP**

ATM SET DS3 DIAG–LOOP

The ATM SET DS3 DIAG-LOOP command enables diagnostic loopback.

Syntax: **ATM SET DS3 DIAG–LOOP**

ATM SET DS3 CELL–LOOP and ATM SET DS3 NO–LOOP

The ATM SET DS3 {CELL-LOOP | NO-LOOP} commands enable and disable cell loopback.

Syntax: **ATM SET DS3 CELL–LOOP**

Syntax: **ATM SET DS3 NO–LOOP**

ATM SET DS3 SHORT–CABLE

The ATM SET DS3 SHORT-CABLE command enables a short cable. If the coax cables attached to the DS3 interface are 225 feet or less, select the Short–Cable parameter. If the length is greater than 225 feet, select the Long–Cable parameter.

Syntax: **ATM SET DS3 SHORT–CABLE**

ATM SET DS3 LONG–CABLE

The ATM SET DS3 LONG-CABLE command enables a long cable. Do not use cables longer than 450 feet. The cable should be good quality RG-59/U, 75 ohm coax. Do not use 50 ohm coax, normally used for Ethernet applications. If the coax cables attached to the DS3 interface are 225 feet or less, select the Short–Cable parameter.

Syntax: **ATM SET DS3 LONG–CABLE**

ATM SET DS3 CNT–FIXED and ATM SET DS3 CNT–ERRORED

The ATM SET DS3 {CNT-FIXED | CNT-ERRORED} commands count the fixed and the uncorrectional HCS errors. The CPPM HCS counter counts the number of correctable HCS errors. If the CNT–FIXED parameter is disabled, the CPPM HCS counter counts the number of uncorrectable HCS errors.

Syntax: **ATM SET DS3 CNT–FIXED**

Syntax: **ATM SET DS3 CNT–ERRORED**

ATM SET DMABURST

Enables and disables DMA burst mode access between ICP and APU units. By default, DMA burst mode is disabled on an XLT and enabled on an XLT-F.

Syntax: **ATM SET DMABURST {ENABLE | DISABLE}**

Option	Description
Enable	Enables DMA burst mode.
Disable	Disables DMA burst mode.

ATM SET APUDECAP

Enables and disables RFC 1483 decapsulation on APU.

Syntax: **ATM SET APUDECAP {ENABLE | DISABLE}**

Option	Description
Enable	Enables RFC1483 decapsulation on APU.
Disable	Disables RFC1483 decapsulation on APU. This option is the default.

ATM SHOW HARD

Displays the current settings of hardware related ATM interface parameters, including DMABURST.

Syntax: **ATM SHOW HARD**

ATM SET PRIOQ {OLD | NEW}

This command toggles the queue management between the old and the new style.

Syntax: **ATM SET PRIOQ {OLD | NEW}**

Option	Description
OLD	Old queue management style: the queue is 64 items long and there is a single pool available for all traffic profiles
NEW	New queue management style: the queue is 256/128 items long and it is divided into 4 pools, each for two neighboring traffics profiles

ATM SET PRIOQ {HQ | NQ}

This command is used to manually set queue parameters.

Syntax: **ATM SET PRIOQ {HQ | NQ} <total pool> <tr n pool>**

Option	Description
HQ	Special traffic queue for ILMI / UNI / PVC keep alives
NQ	Normal traffic queue
<total pool>	The total queue length (maximum value: 256)
<tr n pool>	The pool size for relevant traffic profiles. Possible sizes: <tr9/8 pool> <tr7/6 pool> <tr4/3 pool> <tr2/1 pool>

ATM SET PRIOQ FLOW {ENABLE | DISABLE}

Enables and disables usage of Tx descriptors by neighboring pace groups.

Syntax: **ATM SET PRIOQ FLOW {ENABLE | DISABLE}**

Option	Description
ENABLE	If one pace group is unassigned (there are no VCs having relevant traffic profile), its descriptors will be split between assigned pace groups. This option is a default.
DISABLE	Tx descriptors cannot be used by neighboring pace groups.

ATM SET PRIOQ RX {HQ | NQ}

Specifies the length of the rx ATM queue.

Syntax: **ATM SET PRIOQ RX {HQ | NQ} n**

Option	Description
HQ	Special traffic queue for ILMI / UNI / PVC keep alives
NQ	Normal traffic queue
n	The length of the rx ATM queue. Range for XLT: HQ 4…32, NQ 4…64 Range for XLV: HQ 4…32, NQ 4…128 Default length: HQ 32, NQ 64

5. BGP Commands

BGP AS

Creates a new instance of the BGP.

Syntax: **BGP AS as_number**

Parameter	Description
as_number	The autonomous system number. Range: 0..65535

- The newly created instance remains inactive until you explicitly enable it with BGP ENABLE on page 106.
  To reverse this command (delete an instance), use BGP DEL on page 107.
- When creating a new BGP instance, the BGP Router ID is set to 10.0.0.1 by default. You may have to configure Router ID, which uniquely identifies this BGP router in the routing domain.
- Only one BGP instance per router is accepted. To create a new BGP instance, the existing one must be deleted first.

Example:

The command

BGP AS 101

creates a new BGP instance and assigns it to AS 101.

BGP ENABLE

Enables a created BGP instance.

Syntax: **BGP ENABLE**

To reverse this command (disable an instance), use BGP DISABLE.

Example:

The command BGP ENABLE enables the current BGP instance.

BGP DISABLE

Disables the current BGP instance.

Syntax: **BGP DISABLE**

The created instance remains inactive unless you explicitly enable it.

To reverse this command (enable an instance), use BGP ENABLE on page 106.

BGP DEL

Deletes the BGP instance.

Syntax: **BGP DEL**

Comments

BGP instance has to be explicitly disabled prior to delete execution.

BGP RTRID

Specifies the router ID number by which each BGP router is uniquely identified.

Syntax: **BGP RTRID router_id**

Parameter	Description
router_id	The router ID number. While the router ID is not the IP address, it is in a similar format and you can use one of the router's IP addresses as the ID. Default: 10.0.0.1

BGP PREF

Sets the default preference for BGP routes imported into the routing table.

Syntax: **BGP PREF pref**

Parameter	Description
pref	A routing table value used to compare routes to the same destination but that are known from different protocols (for example, RIP and OSPF routes to the same net). The lower the preference the better the route. Preference set by this command is used when no preference was specified by the command IPR IMPORT policy-id1 [BEFORE policy-id2] FROM scope on page 264. Range: 1 to 253 Default: 20

BGP METRIC

Sets the default metric for routes installed in the routing table which are to be exported by BGP.

Syntax: **BGP METRIC metric**

Parameter	Description
metric	The metric is a routing table value used to compare routes to a destination that belongs to the same protocol (for example, two RIP routes with the same preference to the same destination). The lower the **metric** value, the better the route. Range: 0..65535 Default: 0

The metric, explicitly configured with export policy or by default, is only used when BGP routers are configured to work with Multi-Exit-Discriminator BGP path attribute, which may be used to discriminate among multiple exit or entry points to the same neighboring AS.

BGP ASWEIGHT

Sets the weight of the specified autonomous system.

Syntax: **BGP ASWEIGHT as_number {weight | INFINITY | DEFAULT}**

Parameter	Description
as_number	The number of the specified autonomous system.
weight	The number assigned to the specified autonomous system by the user. The weight of a BGP route is the sum of weights of the autonomous systems the given route traverses. Range: 1..255 Default: 128
INFINITY	If a BGP route traverses an autonomous system with weight INFINITY, the route is not used for forwarding packets. It is the same as a weight of 255.
DEFAULT	The default AS weight, when not configured explicitly. It is the same as a weight of 128.

If you prefer routes passing through some specific autonomous systems rather than through others, you can enforce your preferences with this command. From all BGP routes with the same preference and metric, the one with the lowest total weight is used. (Total weight is the sum of the weights of ASs the route passes through). Assigning a lower weight to an AS therefore makes it more likely to be used than an AS with a higher weight. If you want to avoid an AS altogether, use INFINITY.

For the changes to become effective and consistent, the possible active and affected BGP sessions are to be explicitly restarted.

Example:

The command BGP ASWEIGHT 110 INFINITY determines that all routes that traverse autonomous system 110 will be ignored.

BGP AGGREGATE

Combines (aggregates) several routes that belong to the same net range.

Note: To export aggregate routes to BGP peers, the export policy has to specify explicitly that aggregate routes will be exported.

Syntax: **BGP AGGREGATE net mask [OSPF_TAG tag] [BGP_AS as_number]**

Parameter	Description
net, mask	Expressed as IP addresses, they determine to what range the route should belong to be aggregated.
tag	The TAG field of the OSPF advertisement that indicates the route to be aggregated. This parameter applies only to external OSPF routes.
as_number	The number of the autonomous system that contains the route to be aggregated. This parameter applies only to external BGP routes.

Aggregation saves memory and processing time: for example 30 routes usually require 30 entries in a routing table and each must be advertised separately. If you aggregate these routes, they require just one entry instead and can be advertised as a single entity. Also, an aggregate route is advertised only if there are active routes that fall within the specified address range. An aggregate route automatically becomes active with routes to be aggregated becoming active, and becomes inactive when all routes to be aggregated have become inactive.

To reverse this command, use BGP AGGRDEL index on page 110.

BGP AGGRDEL

Deletes the specified aggregation.

Syntax: **BGP AGGRDEL index**

Parameter	Description
index	A variable that uniquely identifies the net range of aggregated routes.

BGP IMPORT ROUTES

Selects BGP routes to be imported to or blocked from the routing table.

Syntax: **BGP [DONT] IMPORT ROUTES [option]**

Option	Description
FROM RANGE	Import routes that belong to a net range, specified by its IP address (addr) and IP mask (mask).
FROM AS	Import routes from the specified Autonomous System (as_number).
FROM PEER	Import routes from the peer specified by its IP address (peer_addr).
FROM HOME_AS	Import routes that originate from the specified Autonomous System (as_number).
USING PREF	Import routes with the specified preference (pref). If the preference is not specified the routes will be imported with 1. LOCAL_PREF attribute if LOCAL_PREF is enabled, or 2. Default preference
WITH ORIGIN	Import routes with the specified origin (EGP, IGP or OTHER).

An import policy can be positive or negative. If you use the word **DONT** in the command, the described routes will not be imported. Combining positive and negative policies, you can define overlapping policies, with a more specific negative policy within a less specific positive policy. To import routes it is necessary to explicitly specify the policy; the default is "import nothing".

For the policy to become effective, any changes to policy require the possible active, and affected BGP sessions to be explicitly restarted.

If a route matches more than one import policy definition, the policy with the highest precedence is chosen. A given policy has higher precedence than another if the sum of priorities of its keys is greater.

The priorities of import policy keys are:

FROM PEER16
FROM RANGE8
FROM AS4
FROM HOME_AS2
WITH ORIGIN1

To reverse this command (to delete an import policy), use BGP IMPDEL index on page 112.

BGP IMPDEL

Deletes a specified import policy.

Syntax: BGP IMPDEL index

Parameter	Description
index	A variable that uniquely identifies the import policy entry.

Comments

To reverse this command (to add an import policy), use BGP [DONT] IMPORT ROUTES [option] on page 111 (omit the [DONT] option).

BGP EXPORT ROUTES

Selects routes to be exported from the routing table.

Syntax: BGP [DONT] EXPORT protocol ROUTES [option]

Option	Description
protocol	The specific protocol name of routes to be exported or blocked: LOCAL, REMOTE, OSPF, OSPFEXT, RIP, BGPEXT, BGPINT, BGPAGGR, EGP, or ALL
TO AS	Export routes to the specified Autonomous System (as_number).
TO PEER	Export routes to the peer specified by IP address (peer_addr).
USING METRIC	Export routes with a specified metric. The metric is advertised to peers only if the router is configured to use (i.e. send) MED attribute. Three options exist for this parameter: Specified - a value supplied by the user (metric). This value is used regardless of the metric value in the routing table or the default value. Not specified - the default metric is used, with default value set to 0. The default metric value can be changed with the BGP METRIC command. PROTO - the metric value that exists in the routing table.
FROM RANGE	Export routes that belong to a net range specified by its IP address (addr) and IP mask (mask).
WITH OSPF_TAG	Export routes with the specified TAG field of the OSPF advertisement (tag).
WITH RIP_PORT	Export RIP routes learned on the port specified by IP address (port_addr).

WITH RIP_NH	Export RIP routes learned from the gateway (another RIP router) specified by IP address (nh_addr). An export policy can be positive or negative. If you use the word DONT in the command, the described routes will not be exported. You can define overlapping policies, with a more specific negative policy within a less specific positive policy by combining positive and negative policies. To import routes it is necessary to specify the policy explicitly; the default is "export nothing". For the policy to become effective, you must restart any involved BGP sessions. The priorities of export policy keys are: TO PEER32 TO AS16 protocol ROUTES8 (in case of ALL ROUTES this key is ignored) WITH OSPF_TAG2 (only if OSPF ROUTES) WITH RIP_PORT4 (only if RIP ROUTES) WITH RIP_NH2 (only if RIP ROUTES) FROM RANGE1

To reverse this command (delete an export policy), use BGP EXPDEL index on page 114.

BGP EXPDEL

Deletes a specified Export Policy.

Syntax: **BGP EXPDEL index**

Parameter	Description
index	The variable that uniquely identifies the export policy entry.

Comments

To reverse this command (to add an export policy), use BGP [DONT] EXPORT protocol ROUTES [option] on page 113 (omit the [DONT] option).

BGP PEER NEW

Specifies the BGP peer.

Syntax: **BGP PEER NEW peer_addr as_number**

Parameter	Description
peer_addr	The IP address of the specified peer router.
as_number	The Autonomous System to which the peer router belongs.

BGP does not discover neighbor routers (peers) that run BGP on its own. To establish connections, you must first specify these peer routers with this command.

A newly created peer remains inactive until it is explicitly enabled.

To reverse this command (delete a BGP peer), use BGP PEER DEL peer_addr on page 115.

BGP PEER DEL

Deletes the specified peer router.

Syntax: **BGP PEER DEL peer_addr**

Parameter	Description
peer_addr	The address of the specified peer router.

To reverse this command (to add a BGP peer), use BGP PEER NEW peer_addr as_number on page 115.

BGP PEER ENABLE

Enables the specified peer router.

Syntax: **BGP PEER ENABLE peer_addr**

Parameter	Description
peer_addr	The address of the peer router to be enabled.

A peer remains inactive unless it is explicitly enabled.

It is best to specify routing policies (import, export, aggregate routes, AS weights) prior to enabling BGP peer. This allows you to avoid unnecessary protocol traffic.

To reverse this command (to disable a BGP peer), use BGP PEER DISABLE peer_addr on page 116.

BGP PEER DISABLE

Disables a specified peer.

Syntax: BGP PEER DISABLE peer_addr

Parameter	Description
peer_addr	The address of the specified peer router.

A peer remains inactive unless it is explicitly enabled.

To reverse this command (to enable a BGP peer), use BGP PEER ENABLE peer_addr on page 115.

BGP PEER ACTIVE and BGP PEER PASSIVE

Sets the connection type (ACTIVE or PASSIVE).

Syntax: BGP PEER {ACTIVE | PASSIVE} peer_addr

Parameter	Description
ACTIVE	The connection state if the specified router is to initiate the TCP connection with a peer. The ACTIVE state is the default.
PASSIVE	The connection state if the router is not to initiate the TCP connection. In the PASSIVE state the router only accepts the incoming requests from a peer.
peer_addr	The address of the specified peer router.

BGP uses Transmission Control Protocol (TCP) as its transport layer protocol. A BGP router can initiate a TCP connection with a peer (ACTIVE) or wait and accept only the incoming requests for the connection (PASSIVE).

BGP PEER TIMERS

Sets the timers of a peer to specified values.

Syntax: **BGP PEER TIMERS peer_addr <keepalive> <holdtime> [<connretry> <minorig> <minadver>]**

Parameter	Description
peer_addr	The address of the specified peer router.
keepalive	The router sends keepalive messages to its peer every keepalive seconds. Suggested value is 1/3 of the holdtime. Default: 30 seconds Range: 0..21845
holdtime	If no keepalive message is received during holdtime, the router assumes that the peer is dead. Suggested value is 3 times the keepalive time. If you use 0, no keepalive messages are exchanged. Default: 90 seconds Range: 0, 3..65535
connretry	BGP uses TCP as its transport protocol. When trying to establish a TCP connection, it waits connretry seconds between successive attempts. Default: 120 seconds Range: 1..65535
minorig	BGP waits at least minorig seconds between successive advertisements of UPDATE messages, which report changes within the autonomous systems of the advertising BGP speaker. Default: 15 seconds Range: 1..65535
minadver	BGP waits at least minadver seconds between route advertisements Default: 30 seconds Range: 1..65535.

BGP PEER LADDR

Forces the router to use a specified address (one of its port addresses) for the connection with a peer.

- This command is rarely needed.
- Timer settings must be consistent on all co-operating BGP peers.

Syntax: **BGP PEER LADDR peer_addr local_addr**

Parameter	Description
peer_addr	The address of the specified peer router.
local_addr	The IP address of the router that is communicating with the peer router. The address should be one of the router's port addresses.

When trying to establish session with its BGP neighbor with no local address configured, BGP router determines dynamically the local port (and its address) to be used during the session.

When peers are not directly connected, i.e. they have no shared network, we recommend that peer local address is configured.

BGP SHOW IMPORT

Shows the BGP import policy.

Syntax: **BGP SHOW IMPORT**

BGP SHOW EXPORT

Displays the BGP export policy.

Syntax: **BGP SHOW EXPORT**

BGP SHOW PEER

Displays information about a specified peer. Without parameters, it lists all peers in the BGP instance.

Syntax: **BGP SHOW PEER [DETAILED] [TIMERS] [peer_addr]**

Parameter	Description
peer_addr	The address of the specified peer router. If you don’t specify the address, all peers in the BGP instance will be listed.

BGP SHOW GEN

Shows the general parameters of the BGP instance.

Syntax: **BGP SHOW GEN**

BGP SHOW GROUPS

Lists all peers within their groupings.

Syntax: **BGP SHOW GROUPS**

The peer groups are:

- External — contains all the peers from a given autonomous system.
- Internal Direct — a single grouping that contains all internal direct peers. Note that there can be only one such grouping.
- Internal IGP — a single grouping that contains all internal IGP, i.e. not directly connected, peers. There can be only one such grouping.

BGP SHOW PATHS

Displays all BGP paths.

Syntax: **BGP SHOW PATHS**

BGP SHOW ASWEIGHT

Shows the weights of the Autonomous System.

Syntax: **BGP SHOW ASWEIGHT**

BGP SHOW AGGR

Displays the BGP aggregation policy.

Syntax: **BGP SHOW AGGR**

BGP PEER MED

If a router can access another AS via more than one peer belonging to that AS, this command forces the system to use Multi-Exit-Discriminator attribute in BGP updates, and to choose the route suggested by the remote AS administration.

Syntax: **BGP PEER MED {ENABLE | DISABLE} peer_addr**

Parameter	Description
peer_addr	The address of the specified peer router.

After using this command, BGP will add metric (MED attribute) information to each update it sends to the specified peer according to locally configured export policy. A router which receives such information from peers, and is configured to accept MED, will choose the route with the lower MED (when preferences are equal). Usually this is used when you want to use one of these connections as the primary one and the other as a backup.

BGP PEER USEPREF

Determines what preference to use when importing a route from a peer. Possible preferences:

- the locally configured import preference specified by the command IPR IMPORT policy-id1 [BEFORE policy-id2] FROM scope on page 264
- the command BGP [DONT] IMPORT ROUTES [option] on page 111 9omit the [DONT] option)
- the default preference value specified by the command BGP PREF pref on page 107
- the preference value imported from the peer's routing table with BGP updates

Syntax: **BGP PEER USEPREF {ENABLE | DISABLE} peer_addr**

Parameter	Description
peer_addr	The address of the specified peer router.

This command applies only to the peers within the same AS. In the routing table, BGP associates with each route a preference value that is used to determine which route to use when two or more go to the same destination: the route with the lowest preference value is chosen. With the command BGP PREF pref on page 107, you set the default preference value. Now you determine whether, when importing a route from a peer, to use the locally configured import preference value, or default preference value or to use the preference value imported in BGP updates as LOCAL_PREF attribute from that peer's routing table (BGP PEER USEPREF ENABLE). Preference set by this command is used when no preference was specified by the command IPR IMPORT policy-id1 [BEFORE policy-id2] FROM scope on page 264. When no preference was specified by the import policy and you didn't set the local preference option, the default preference is used.

6. BonD Console Commands

These commands let you configure, enable, disable and set the parameters of the Bandwidth on Demand feature.

When you are using the asynchronous interface, disable the autoreconnect option. Use the command SET ADV INTERFACE n {RECON | NORECON} on page 21
You can use ? after every command to display help.

PP BOND ENABLE

Enables BonD on a parallel port. After issuing this command BonD service defined on the parallel port starts to work.

Syntax: **PP n BOND ENABLE**

Parameter	Description
n	The parallel port number

PP BOND DISABLE

Disables BonD on a parallel port number. After issuing this command BonD service defined on the parallel port stops to work and all of the auxiliary ports are stopped.

Syntax: **PP n BOND DISABLE**

Parameter	Description
n	The parallel port number

PP BOND VALID

Validates the invalid auxiliary ports in BonD service defined on the parallel port.

Syntax: **PP n BOND VALID a1 a2 a3 …**

Parameter	Description
n	The parallel port number
a1 a2 a3 …	The numbers of ports to activate (the port for which an Invalid Time is down counted).

PP BOND BASIC

Defines parallel port members as basic ports in BonD service for the parallel port.

Syntax: **PP n BOND BASIC b1 b2 b3 …**

Parameter	Description
n	The parallel port number
b1 b2 b3 …	One or more of the parallel port members to be defined as basic ports

PP BOND AUX

Defines parallel port members as auxiliary ports in BonD service for the parallel port. After defining, BonD does not start to work; to start BonD service it is necessary to enable BonD on basic port b. See: PP n BOND BASIC b1 b2 b3 … on page 123.

Syntax: **PP n BOND AUX a1 a2 a3 …**

Parameter	Description
n	The parallel port number
a1 a2 a3 …	One or more of the parallel port members to be defined as auxiliary ports

PP BOND SHC

Displays BonD configuration on the parallel port.

Syntax: **PP n BOND SHC**

Parameter	Description
n	The parallel port number where BonD service is defined.

PP BOND TIMER

Sets the time interval between sending calls to the main BonD procedure.

Syntax: **PP n BOND TIMER t**

Parameter	Description
n	The parallel port number
t	The time interval in seconds. Default value: 1 Parameter range: 1..30 s Higher values are useful for slow ports.

PP BOND TCTR

Sets traffic thresholds for starting successive auxiliary ports.

Syntax: **PP n TCTR BOND t1 t2 t3 …**

Parameter	Description
n	The parallel port number
t1 t2 t3 …	The successive percentage traffic thresholds Parameters range: 0..100%

PP BOND TDTR

Sets traffic thresholds for stopping successive auxiliary ports.

Syntax: **PP n BOND TDTR t1 t2 t3**

Parameter	Description
n	The parallel port number
t1 t2 t3	The successive percentage traffic thresholds Parameters range: 0..100%

PP BOND BSPEED

Sets the speed of the basic ports, which is used to calculate load on BonD ports.

Syntax: **PP n BOND BSPEED s1 s2 s3 …**

Parameter	Description
n	The parallel port number
s1s2 s3 …	The speeds of successive basic ports

PP BOND ASPEED

Sets the speed of auxiliary ports, which used to calculate load on BonD ports.

Syntax: **PP n BOND ASPEED s1s2s3**

Parameter	Description
n	The parallel port number
s1s2 s3 …	The speeds of successive auxiliary ports

PP BOND TRTM

Sets the trigger time parameter (the time period during which the traffic must be true before starting an auxiliary port).

Syntax: **PP n BOND TRTM t**

Parameter	Description
n	The parallel port number
t	The trigger time (in seconds) Default value: 15 s Parameter range: 1..999 s

PP BOND DRTM

Sets the drop time parameter (the time period during which the drop condition must be true before stopping an auxiliary port).

Syntax: **PP n BOND DRTM t**

Parameter	Description
n	The parallel port number
t	The drop time (in seconds) Default value: 15 s Parameter range: 1..999 s

PP BOND INVT

Sets the Invalid Time.

Syntax: **PP n BOND INVT t**

Parameter	Description
n	The parallel port number
t	The invalid time (in seconds) Default value: 60 s Parameter range: 1..86400 s

PP BOND DEBUG

Sets the class and level of detail for BonD debugging messages.

Syntax: **PP n BOND c l**

Parameter	Description
n	The parallel port number
c	The class of debugging messages. There are four available classes: FSM - behavior of BonD Finite State Machine ERRORS - errors, e.g. NULL pointers VAR - values of some variables CTRL - information about flow control in BonD application
l	The detail level for the messages Default value: 0 Parameter range: 0..4 (0 means - no messages)

PP BOND SOFTDROP

Sets the mode for stopping auxiliary ports. When soft drop is on, auxiliary ports are flushed before the port is stopped.

Syntax: PP n BOND SOFTDROP [ON | OFF]

Parameter	Description
n	The parallel port number
ON/OFF	ON is the default value (auxiliary ports are flushed)

PP BOND HISTSIZE

Sets the maximum size of BonD Event History.

Syntax: PP n BOND HISTSIZE s

Parameter	Description
n	The parallel port number
s	Event History size Default value: 100 Parameters range: 50..500

PP BOND REGEV

Sets the registering events mode in BonD Event History. When ALL is set all events are logged; When CHNG is set only events that change BonD FSM state are logged.

Syntax: PP BOND n REGEV [ALL | CHNG]

Parameter	Description
n	The parallel port number
ALL	All events are logged
CHING	Only the events that change BonD FSM state are logged. CHING is the default value.

PP BOND EVSHC

Displays the contents of BonD Event History.

Syntax: **PP BOND n EVSHC [ALL | FROM timestamp]**

Parameter	Description
n	The parallel port number
ALL	Prints all the log contents
FROM timestamp	Prints the log contents from a specified moment of time

PP BOND DIAG

Displays BonD diagnostic information.

Syntax: **PP n BOND DIAG**

Parameter	Description
n	The parallel port number

PP BOND ?

Displays the list of all BonD commands.

Syntax: **PP n BOND ?**

Parameter	Description
n	The parallel port number

HELP PP BOND

Displays information about BonD commands.

Syntax: **HELP PP BOND**

7. Broadcast Resolution Commands

SET BRES TCPIP

This command is used to enable and disable TCP/IP Broadcast Resolution.

Syntax: **SET BRES TCPIP {ON | OFF}**

SET BRES TCPRES

This command is used to enable and disable TCP/IP Broadcast Resolution on a port by port basis.

Syntax: **SET BRES TCPRES {ON | OFF} n**

Parameter	Description
n	A port number in the range from 0 to 7 on which you want to enable or disable TCP/IP Broadcast Resolution.

SET BRES TCPLRN

This command is used to enable and disable the learning of IP addresses on a specified port.

Syntax: **SET BRES TCPLRN {ON | OFF} n**

Parameter	Description
n	A port number in the range from 0 to 7 on which you want to enable or disable IP Address Learning.

SET BRES NETBIOS

This command is used to enable and disable NetBIOS Broadcast Resolution.

Syntax: **SET BRES NETBIOS {ON | OFF}**

SET BRES NETBRES

This command is used to enable and disable NetBIOS Broadcast Resolution on a port by port basis.

Syntax: **SET BRES NETBRES {ON | OFF} n**

Parameter	Description
n	A port number in the range from 0 to 7 on which you want to enable or disable NetBIOS Broadcast Resolution.

SET BRES NETBLRN

This command is used to enable and disable the learning of NetBIOS names on a specified port.

Syntax: **SET BRES NETBLRN {ON | OFF} n**

Parameter	Description
n	A port number in the range from 0 to 7 on which you want to enable or disable NetBIOS Name Learning.

SET BRES ADDNAME

This command is used to enable and disable the learning of a NetBIOS names from ADD_NAME_QUERY frames. Normally, the NetBIOS Broadcast Resolution engine learns NetBIOS names from DATAGRAM, NAME QUERY and STATUS QUERY frames and resolves DATAGRAM, NAME QUERY, STATUS QUERY and ADD NAME QUERY frames.

Note: Only use this command in a stable internetwork that has unique NetBIOS names. This command does not detect duplicate names. This can result in loss of connectivity for the user with duplicate names.

Syntax: **SET BRES ADDNAME {ON | OFF}**

SET BRES UNLEARN

This command is used to enable and disable Unlearn Name Packets generating. Unlearn Name Packets generating is used to correct NetBIOS names in the table when there are multiple paths to the destination.

Syntax: **SET BRES UNLEARN {ON | OFF}**

SET BRES FULLNAME

This command is used to enable and disable 16 bytes/15 bytes NetBIOS Name comparing. (ILAN XL only)

Syntax: **SET BRES FULLNAME {ON | OFF}**

Setting MAC Address Learning on a Port

This command is used to enable and disable the learning of MAC addresses from Source Route frames on a specified port.

Syntax: **SET ADDRLRN {ON | OFF} n**

Parameter	Description
n	A port number in the range from 0 to 7 on which you want to enable or disable MAC Address Learning.

SET BRES CHAR

This command is used to set the number of characters (the length) of the NetBIOS name distinguished during the learning process.

Syntax: **SET BRES CHAR n**

Parameter	Description
n	A number in the range from 0 to 16 which will determine the number of characters distinguished during learning.

SET BRES MAXNAMES

This command is used to set the maximum number of NetBIOS names that can be learned.

Syntax: **SET BRES MAXNAMES n**

Parameter	Description
n	The maximum number of NetBIOS names that can be learned.

SHOW BRES CHAR

This command is used to display the number of characters of the NetBIOS name distinguished during the learning process.

Syntax: **SHOW BRES CHAR**

SHOW BRES MAXNAMES

This command is used to display the maximum number of NetBIOS names that can be learned.

Syntax: **SHOW BRES MAXNAMES**

8. CNNI Configuration Commands

CNNI SET METHOD

Sets the routing method used by CNNI.

Syntax: **CNNI SET METHOD {First | Best}**

Parameter	Description
First	The first received copy of SETUP message is used and all consecutive copies are discarded. This is a simpler method but it does not necessarily let us choose the optimal path since real messages use a different channel than a SETUP message.
Best	Before notifying the destination station we wait for some time in order to collect all copies of SETUP and choose the best one.

CNNI SET PORT {ENABLE | DISABLE}

Enables or disables the CNNI algorithm on the specified port.

Syntax: **CNNI SET PORT <port> {Enable | Disable}**

Parameter	Description
port	The port to which this command applies.

CNNI SET PORT BORDER

Determines whether this port is an end port for CNNI routing. By default all UNI ports are border ports and all NNI ports are not.

Syntax: **CNNI SET PORT <port> BORDER {ON | OFF}**

Parameter	Description
port	The port to which this command applies.

CNNI SET PORT AUTOREROUTE

On a UNI port, if autorerouting is turned ON, when the link goes down, CNNI tries to automatically reroute all calls from this port to a different path.

Syntax: **CNNI SET PORT <port> AUTOREROUTE {ON | OFF}**

Parameter	Description
port	The port to which this command applies.

CNNI SET PORT REROUTE

For an NNI port, if rerouting is turned ON, this port can be used for automatic rerouting when another link goes down.

Syntax: **CNNI SET PORT <port> REROUTE {ON | OFF}**

Parameter	Description
port	The port to which this command applies.

CNNI SET PORT ASSIGN

If set to ON, VPCI/VCI identifiers are assigned to calls going through this port. Only one end of a link should have this parameter enabled.

Syntax: **CNNI SET PORT <port> ASSIGN {ON | OFF}**

Parameter	Description
port	The port to which this command applies.

CNNI SET PORT SEND_CP

Determines whether CALL PROCEEDING frames will be sent to a specified port during connection establishment.

Syntax: **CNNI SET PORT <port> SEND_CP {ON | OFF}**

Parameter	Description
port	The port to which this command applies.

CNNI DIAG ALIAS ADD

Adds an alias to the ATM address. An alias can be used for other console commands.

Syntax: **CNNI DIAG ALIAS ADD <ATMAddr> <alias>**

Parameter	Description
ATMAddr	The ATM address to which the alias is added.
alias	The alias added to the ATM address. Maximum length: 14 characters.

CNNI DIAG CAPTURE ADD

Enables message tracing for frames between two ATM addresses.

Syntax: **CNNI DIAG CAPTURE ADD <CdATMAddr> <CgATMAddr>**

Parameter	Description
CdATMAddr, CgATMAddr	The ATM addresses between which you want to trace messages.

CNNI DIAG CAPTURE TRACE

Sets or clears the trace flag for a particular session.

Syntax: **CNNI DIAG CAPTURE TRACE <SessNo> {ON | OFF}**

Parameter	Description
SessNo	Session identifier, which is the decimal number displayed in the left column of the CNNI DIAG CAPTURE SHOW output.

CNNI SHOW CONFIG

Displays CNNI global parameters: routing method and routing algorithm.

Syntax: **CNNI SHOW CONFIG**

CNNI SHOW PORT

Displays CNNI port parameters: routing algorithm, type of the port (border, internal), and its settings: stations automatically rerouted, rerouting settings, VPCI/VCI identifiers assigned.

Syntax: **CNNI SHOW PORT <port>**

Parameter	Description
port	The port to which this command applies.

CNNI DIAG ADDR

Displays all addresses (all active parties) known by CNNI.

Syntax: **CNNI DIAG ADDR**

CNNI DIAG ALIAS SHOW

Displays the alias table.

Syntax: **CNNI DIAG ALIAS SHOW**

CNNI DIAG CAPTURE SHOW

Displays the contents of the capture table (all sessions for which traces are displayed). The session number displayed by this command is required for the CNNI DIAG CAPTURE TRACE command.

Syntax: **CNNI DIAG CAPTURE SHOW**

CNNI DIAG STATS GLOBAL

Displays global CNNI statistics: current number of sessions in various states (CREATED, ONE WAY, CONNECTED, BROKEN LEAF, BROKEN ROOT, REROUTE WAITING).

Syntax: **CNNI DIAG STATS GLOBAL**

CNNI DIAG STATS ADDR

Displays CNNI statistics for the given address, first as a calling party, then as a called party.

Syntax: **CNNI DIAG STATS ADDR <alias>**

Parameter	Description
alias	The address alias for which you want to display the statistics.

CNNI DIAG CONN

Displays information about connections to and from a given address.

Syntax: **CNNI DIAG CONN <alias>**

Parameter	Description
alias	The address alias for which you want to display information.

9. ClearSession Protocol (CSP) Commands

The following groups of commands are available:

CSP General Commands for IP Routing

Configuration of ClearSession Protocol for IP Routing consists in specification which devices within a single LAN segment should compete for becoming virtual router. Set of such devices forms a group, identified by a decimal number called *group_id*. Each device in a group has to be manually configured.

CSP IP ENABLE

This command globally enables CSP feature for IP Routing.

Syntax: **CSP IP ENABLE**

This command enables CSP group on IP port.

Syntax: **CSP IP port group_id ENABLE**

Parameter	Description
port	The number of IP port on which you want to disable CSP group. Range: 0...128
group_id	The number of the group which you want to disable on IP port. Range: 0...255

CSP IP DISABLE

This command disables CSP feature for IP Routing.

Syntax: **CSP IP DISABLE**

This command disables CSP group on IP port.

Syntax: **CSP IP port group_id DISABLE**

Parameter	Description
port	The number of IP port on which you want to disable CSP group. Range: 0...128
group_id	The number of the group which you want to disable on IP port. Range: 0...255

CSP IP STATE

This command shows current CSP state. The following states are defined: DISABLE or ENABLE and STARTED or STOPPED.

Syntax: **CSP IP STATE**

CSP IP GAP

This command sets the interval in seconds between single frames in one hello message (one hello message may consist with several frames). message.

Syntax: **CSP IP GAP *gap_t***

Parameter	Description
gap_t	The interval in seconds between single frames in one hello message Range: 0.01… 0.2 Default: 0.1

CSP IP CREATE

This command creates CSP group *group_id* on port *port* and establishes *ip_addr* as the IP address of the virtual router. The configuration for at least one of the routers in the CSP group must specify the IP address of the virtual router; specifying the addresses of the virtual router is optional for other routers in the same CSP group.

Virtual MAC Address is automatically assigned to the group. It is of the following form:

46-00-98-00-00-*group_id* (for Token Ring networks this value is bit-reversed).

Syntax: **CSP IP *port group_id* CREATE [IP *ip_addr*]**

Parameter	Description
port	The number of port on which you want to create CSP group. Range: 0…128
group_id	The number of the group which you want to create. This number must be an unique. Range: 0...255
ip_addr	IP address of the virtual router. Format: x.x.x.x, Range of x: 0…255

CSP IP PRIO

This command sets the priority of the router.

Syntax: **CSP IP port group_id PRIO prio**

Parameter	Description
port	The number of IP port Range: 0...128
group_id	The number of the CSP group Range: 0...255
prio	The priority of the router in group *group_id* on port *port*. Range: 0...255 Default: 100

CSP IP TIMERS

This command sets the interval between *hello messages* and sets the duration that a router waits before it declares the neighbor to be down. If these timers are modified, a user must configure each device within a group to use the same *hello time* and *hold time*.

Syntax: **CSP IP *port group_id* TIMERS *hello_t hold_t***

Parameter	Description
port	The number of the port on which you want to set timers Range: 0...128
group_id	The number of the CSP group Range: 0...255
hello_t	The interval in seconds between hello messages. It must be lover than hold time *hold_t.* Range: 0.1...600.0 Default: 1
hold_t	The duration in seconds that a router waits before it declares the neighbor to be down. It must be greater than hello time *hello_t.* Range: 0.1...600.0 Default: 3.5

CSP IP TRACE

This command enables port tracing. If the traced port becomes unavailable, router's priority will be decreased. Traced port number (*tr_port*) must be different than port number (*port*). It is impossible to set the two pairs: <port, tr_port> and <tr_port, port> at the same time.

Syntax: **CSP IP *port group_id* TRACE *tr_port [d_prio]***

Parameter	Description
port	The number of the port on which you want to enable tracing. Port number (*port*) must be different than traced port number (*tr_port).* Range: 0...128
group_id	The number of the CSP group Range: 0...255
tr_port	The number of port that will be tracing. Traced port number (*tr_port*) must be different than port number (*port*). Range: 0...128
d_prio	The value by which router's priority will be decreased. Range: 0...255 Default: 10

CSP IP TRACE DISABLE

This command disables port tracing that was enabled by above command

Syntax: **CSP IP *port group_id* DISABLE**

Parameter	Description
port	The number of the port on which you want to disable tracing. Range: 0 to 128
group_id	The number of the CSP group Range: 0 to 255

CSP IP DELETE

This command deletes CSP definition.

Syntax: **CSP IP *port group_id* DELETE**

Parameter	Description
port	The number of the port on which you want to delete CSP Range: 0...128
group_id	The number of the CSP group Range: 0...255

CSP IP UDPPORT

This command specifies what UDP port is assigned to CSP IP frames.

Syntax: **CSP IP UDPPORT *udp_port***

Parameter	Description
udp_port	The value specifies what UDP port is assigned to CSP IP frames. Range: 1024...65535 Default: 20000

CSP Diagnostic Commands for IP Routing

CSP IP CONFIG

This command displays configuration of group *group_id* configured on port *port*.

Syntax: CSP IP *port group_id* CONFIG

To display configuration of all groups configured on port *port*, omit the *group_id* parameter:

Syntax: CSP IP *port* CONFIG

To display configuration of all groups configured on all ports, omit the *port* and *group_id* parameters:

Syntax: CSP IP CONFIG

Parameter	Description
port	The number of port which configuration you want to see. Range: 0...128
group_id	The number of the group which configuration you want to see. Range: 0...255

CSP IP NGBRS

This command displays known neighbors from group *group_id*, discovered on port *port*, along with their parameters.

Syntax: CSP IP *port group_id* NGBRS

To display known neighbors from all groups on a specified port *port*, omit the *group_id* parameter:

Syntax: CSP IP *port* NGBRS

To display known neighbors from all groups on all ports, omit the *port* and *group_id* parameters:

Syntax: CSP IP NGBRS

Parameter	Description
port	The number of IP port on which you want to enable CSP group Range: 0...128
group_id	The number of the group which you want to enable on IP port. Range: 0...255

CSP IP SHOW MSG

This command is used to display CSP messages associated with specified group on specified port. *In* specifies that only incoming messages should be displayed, *out* - only outgoing. Omitting the last word causes that both, incoming and outgoing, messages are displayed.

Syntax: CSP IP *port group_id* SHOW MSG [in | out]

To display CSP messages associated with all groups configured on specified port, omit the *group_id* parameter:

Syntax: CSP IP *port* SHOW MSG [in | out]

To display CSP messages associated with all groups configured on all ports, omit the *port* and *group_id* parameters.

Syntax: CSP IP SHOW MSG [in | out]

Parameter	Description
port	The number of IP port with which are associated messages that you want to see Range: 0...128
group_id	The number of the group with which are associated messages that you want to see. Range: 0...255

CSP IP SHOW MSG STOP

This command is used to stop CSP messages associated with specified group on specified port. *In* specifies that only incoming messages should be stopped, *out* - only outgoing. Omitting the last word causes that both, incoming and outgoing, messages are stopped.

Syntax: **CSP IP *port group_id* SHOW MSG STOP [in | out]**

To stop CSP messages associated with all groups configured on specified port, omit the *group_id* parameter:

Syntax: **CSP IP *port* SHOW MSG STOP [in | out]**

To stop CSP messages associated with all groups configured on all ports, omit the *port* and *group_id* parameters:

Syntax: **CSP IP SHOW MSG STOP [in | out]**

Parameter	Description
port	The number of IP port with which are associated messages that you want to stop Range: 0...128
group_id	The number of the group with which are associated messages that you want to stop. Range: 0...255

CSP IP SHOW EVENTS

This command is designed to display the events related to CSP protocol.

Syntax: **CSP IP *port group_id* SHOW EVENTS *category level***

To display the events related to all CSP groups defined on port *port*, omit the *group_id* parameter:

Syntax: **CSP IP *port* SHOW EVENTS *category level***

To display the events related to all CSP groups defined on all ports, omit the *port* and *group_id* parameters:

Syntax: **CSP IP SHOW EVENTS *category level***

Parameter	Description
port	The number of IP port with which are associated events that you want to see Range: 0...128
group_id	The number of the group with which are associated events that you want to see. Range: 0...255
category	The category of events which a user wants to display The following categories are defined: `HELLO` - events related to hello message exchange `STATE` - events related to CSP protocol state machine `TIME` - events caused by timer's expiration `NGBR` - events related to neighborhood discovery part of CSP protocol `BACKUP` - events related to backup actions performed by CSP protocol `ALL` - covers all types of events
level	The level specifies how important events should appear on a console screen. There are three levels of event importance specified as *level*: `LL` - covers all types of events 1 - crucial 2 - important 3 - normal Level of 3 causes that events assigned to levels 1 and 2 are also displayed.
STOP	Terminating events display.

CSP IP SHOW EVENTS STOP

This command is designed to stop displaying events related to CSP protocol.

Syntax: **CSP IP *port group_id* SHOW EVENTS STOP *category***

To stop displaying events related to all CSP groups defined on port *port*,, omit the *group_id* parameter:

Syntax: **CSP IP *port* SHOW EVENTS STOP *category***

To stop displaying events related to all CSP groups defined on all ports, omit the *port* and *group_id* parameters:

Syntax: **CSP IP SHOW EVENTS STOP *category***

Parameter	Description
port	The number of IP port with which are associated events that you want to stop Range: 0...128
group_id	The number of the group with which are associated events that you want to stop. Range: 0...255
category	The category of events which displaying a user wants to stop The following categories are defined: `HELLO` - events related to hello message exchange `STATE` - events related to CSP protocol state machine `TIME` - events caused by timer's expiration `NGBR` - events related to neighborhood discovery part of CSP protocol `BACKUP` - events related to backup actions performed by CSP protocol `ALL` - covers all types of events

CSP IP SHOW STATE

This command displays the current state of CSP protocol agent in terms of CSP protocol definition. It displays the name of the current state, how long this state has been lasting, what was the previous state, what caused the transition.

Syntax: **CSP IP *port group_id* SHOW STATE *n***

Parameter	Description
port	The number of IP port which CSP protocol state you want to see Range: 0...128
group_id	The number of the group which CSP protocol state you want to see Range: 0...255
n	The number of states of CSP protocol agent that will be logged. Range: 1…60 Default: 20

CSP IP SHOW STATE HISTORY

This command displays all logged states of CSP protocol agent that are in the buffer.

Syntax: **CSP IP *port group_id* SHOW STATE HISTORY *n***

Parameter	Description
port	The number of IP port Range: 0...128
group_id	The number of the group Range: 0...255
n	The number of states of CSP protocol agent that will be logged Default: 5

CSP General Commands for Source Route Bridging

Configuration of ClearSession Protocol for SR Bridging consists in a specification which devices within a single LAN segment should provide redundancy backup for themselves. Set of such devices forms a group, identified by a decimal number called *group_id*. Each device in a group has to be manually configured.

Note: These commands are not allowed on XLP/XLA devices

CSP SR ENABLE

This command enables CSP feature for SR Bridging.

Syntax: **CSP SR ENABLE**

This command enables CSP group on port.

Syntax: **CSP SR *port group_id* ENABLE**

Parameter	Description
port	The number of port on which you want to enable CSP group Range: 0...128
group_id	The number of the group which you want to enable on port. Range: 0...255

CSP SR DISABLE

This command disables CSP feature for SR Bridging.

Syntax: **CSP SR DISABLE**

This command disables CSP group on port.

Syntax: **CSP SR *port group_id* DISABLE**

Parameter	Description
port	The number of port on which you want to disable CSP group Range: 0...128
group_id	The number of the group which you want to disable on port. Range: 0...255

CSP SR STATE

This command shows current CSP state for SR Bridging. The following states are defined: DISABLE or ENABLE and STARTED or STOPPED.

Syntax: **CSP SR STATE**

CSP SR GAP

This command sets interval in seconds between single frames in one hello message (one hello message may consist with several frames). message.

Syntax: **CSP SR GAP *gap_t***

Parameter	Description
gap_t	The interval in seconds between single frames in one hello message Range: 0.01…0.2 Default: 0.1

CSP SR CREATE

This command creates CSP group *group_id* on port *port*. Port *tr_port* (traced port) is the one which must be active to send hellos over port *port*. *Tr_port* also specifies the link through which LE_NARP_REQUESTS about LAN segment of port *port* are sent.

Syntax: **CSP SR *port group_id tr_port* CREATE**

Parameter	Description
port	The number of port on which you want to create CSP group. The value port must be different than the traced port number Range: 0...128
group_id	The number of the group which you want to create. This number must be an unique. Range: 0...255
tr_port	The port which must be active to send hellos over port. The value of traced port must be different than port number. Range: 0...128

CSP SR PRIO

This command sets the priority of the router.

Syntax: **CSP SR *port group_id* PRIO *prio***

Parameter	Description
port	The number of port. Range: 0...128
group_id	The number of the CSP group Range: 0...255
prio	The priority of the router in group *group_id* on port. Range: 0...255 Default: 100

CSP SR TIMERS

This command sets the interval between hello messages and sets the duration that a router waits before it declares the bridge to be down. If these timers are modified, a user must configure each bridge within a group to use the same hello time and hold time. Hello time must be less than hold time.

Syntax: **CSP SR *port group_id* TIMERS *hello_t hold_t***

Parameter	Description
port	The number of the port on which you want to set timers Range: 0...128
group_id	The number of the CSP group Range: 0...255
hello_t	The interval in seconds between hello messages. It must be less than hold time *hold_t.* Range: 0.1…600.0 Default: 0.4
hold_t	The duration in seconds that a router waits before it declares the neighbor to be down. It must be greater than hello time *hello_t* Range: 0.1… 600.0 Default: 3.5

CSP SR DELETE

This command deletes CSP definition.

Syntax: **CSP SR *port group_id* DELETE**

Parameter	Description
port	The number of the port on which you want to delete CSP Range: 0...128
group_id	The number of the CSP group Range: 0...255

CSP Diagnostic Commands for Source Route Bridging

CSP SR CONFIG

This command displays configuration of group *group_id* configured on port *port*.

Syntax: CSP SR *port group_id* CONFIG

To display configuration of all groups configured on port *port*, omit the *group_id* parameter:

Syntax: CSP SR *port* CONFIG

To display configuration of all groups configured on all ports, omit the *port* and *group_id* parameters:

Syntax: CSP SR CONFIG

Parameter	Description
port	The number of port which configuration you want to see. Range: 0...128
group_id	The number of the group which configuration you want to see. Range: 0...255

CSP SR NGBRS

This command displays known neighbours from group *group_id*, discovered on port *port*, along with their parameters.

Syntax: **CSP SR *port group_id* NGBRS**

To display known neighbours from all groups on a specified port *port*, omit the *group_id* parameter:

Syntax: **CSP SR *port* NGBRS**

To display known neighbors from all groups on all ports, omit the *port* and *group_id* parameters:

Syntax: **CSP SR NGBRS**

Parameter	Description
port	The number of port on which you want to enable CSP group Range: 0...128
group_id	The number of the group which you want to enable on port. Range: 0...255

CSP SR SHOW MSG

This command is used to display CSP messages associated with specified group on specified port. *In* specifies that only incoming messages should be displayed, *out* - only outgoing. Omitting the last word causes that both, incoming and outgoing, messages are displayed.

Syntax: **CSP SR *port group_id* SHOW MSG [in | out]**

To display CSP messages associated with all groups configured on specified port, omit the *group_id* parameter:

Syntax: **CSP SR *port* SHOW MSG [in | out]**

Parameter	Description
port	The number of port with which are associated messages that you want to see Range: 0...128
group_id	The number of the group with which are associated messages that you want to see. Range: 0...255

CSP SR SHOW MSG STOP

This command is used to stop CSP messages associated with specified group on specified port. *In* specifies that only incoming messages should be stopped, *out* - only outgoing. Omitting the last word causes that both, incoming and outgoing, messages are stopped.

Syntax: CSP SR *port group_id* SHOW MSG STOP [in | out]

To stop CSP messages associated with all groups configured on specified port, omit the *port* and parameter:

Syntax: CSP SR *port* SHOW MSG STOP [in | out]

To stop CSP messages associated with all groups configured on all ports, omit the *port* and *group_id* parameters:

Syntax: CSP SR SHOW MSG STOP [in | out]

Parameter	Description
port	The number of port with which are associated messages that you want to stop Range: 0...128
group_id	The number of the group with which are associated messages that you want to stop. Range: 0...255

CSP SR SHOW EVENTS

This command is designed to display events related to CSP protocol.

Syntax: **CSP SR *port group_id* SHOW EVENTS *category level***

To display events related to all CSP groups defined on port *port*, omit the *port* and parameter:

Syntax: **CSP SR *port* SHOW EVENTS *category level***

To display events related to all CSP groups defined on all ports, omit the *port* and *group_id* parameters:

Syntax: **CSP SR SHOW EVENTS *category level***

Parameter	Description
port	The number of port with which are associated events that you want to see. Range: 0...128
group_id	The number of the group with which are associated events that you want to see. Range: 0...255
category	The category of events which a user wants to display The following categories are defined: `HELLO` - events related to hello message exchange `STATE` - events related to CSP protocol state machine `TIME` - events caused by timer's expiration `NGBR` - events related to neighborhood discovery part of CSP protocol `BACKUP` - events related to backup actions performed by CSP protocol `ALL` - covers all types of events
level	The level specifies how important events should appear on a console screen. There are three levels of event importance specified as *level*: `LL` - covers all types of events 1 - crucial 2 - important 3 - normal Level of 3 causes that events assigned to levels 1 and 2 are also displayed.

CSP SR SHOW EVENTS STOP

This command is designed to stop displaying events related to CSP protocol.

Syntax: **CSP SR *port group_id* SHOW EVENTS STOP *category***

To stop displaying events related to all CSP groups defined on port *port*, omit the *port* parameter:

Syntax: **CSP SR *port* SHOW EVENTS STOP *category***

To stop displaying events related to all CSP groups defined on all ports, omit the *port* and *group_id* parameters:

Syntax: **CSP SR SHOW EVENTS STOP *category***

Parameter	Description
port	The number of port with which are associated events that you want to stop. Range: 0...128
group_id	The number of the group with which are associated events that you want to stop. Range: 0...255
category	The category of events which displaying a user wants to stop The following categories are defined: `HELLO` - events related to hello message exchange `STATE` - events related to CSP protocol state machine `TIME` - events caused by timer's expiration `NGBR` - events related to neighborhood discovery part of CSP protocol `BACKUP` - events related to backup actions performed by CSP protocol `ALL` - covers all types of events

CSP SR SHOW STATE

This command displays current state of CSP protocol agent in terms of CSP protocol definition. It displays name of current state, how long this state lasts, what was previous state, what caused the transition. This command displays history of 5 most recent state transitions.

Syntax: **CSP SR *port group_id* SHOW STATE**

Parameter	Description
port	The number of port which CSP protocol state you want to see Range: 0...128
group_id	The number of the group which CSP protocol state you want to see Range: 0...255

CSP SR SHOW STATE HISTORY

This command sets number of states of CSP protocol agent that will be logged (see above).

Syntax: **CSP SR *port group_id* SHOW STATE HISTORY *n***

Parameter	Description
port	The number of port Range: 0...128
group_id	The number of the group Range: 0...255
n	The number of states of CSP protocol agent that will be logged Default: 5

10. DLSw Commands

DLSW SET

This command sets the general parameters of the DLSw router.

Syntax: **DLSW SET parameter value**

Parameter	Description
NETNAME	The IP address for your DLSw. It should be the address of the port taking part in TCP/IP connections. If there are several such ports, use the internal network address for the best fault tolerance.
VRN	The virtual ring number (taking into account the current segment configuration) used for a Token Ring configuration. Range: 0x1..0xFFF Default: 0x1
BRIDGE	The DLSw bridge number according to the current bridge configuration (used for a Token Ring configuration). Range: 0x0..0xF Default: 0 If you choose 0, the virtual hop will be disabled and the virtual ring number and the bridge number won't be put into the RIF of the Token Ring frames sent through the DLSw.
MAX_BTU	The maximum size of the BTU. In current version this setting also decides about frame size used on LLC. Range: 274..4472 Default: 4468. Values from allowed range are mapped to one of four values: range btu_sizeframe_size 274 - 1465 512 546 1466 - 2047 1500 1534 2048 - 4395 2048 2082 4395 - 4472 4468 4502
HEAP	The heap memory limit. Range: 256kB. For system free memory: 512kB Default: 1024 kB
SSP_RETRY	SSP connection retry time. Range: 1..100 Default: 10
SNA_SINGLE_T	SNA remote link establishment timeouts (single DLSw). Range: 1..120 Default: 10

SNA_MULTI_TSNA remote link establishment timeouts (multiple DLSw).
Range: 1..120
Default: 15

SNA_ACK_T SNA remote link establishment timeouts (awaiting RECH_ACK).
Range: 1..120
Default: 20

IDLE_T Idle circuit timeout.
Range: 1..120
Default: 20

NB_RETRY The number of NetBIOS retries.
Range: 1..100
Default: 4

NB_T NetBIOS link establishment timeout.
Range: 1..120 s
Default: 25

MAC_LIMIT MAC address table entry limit.
Range: 1..2000
Default: 100

NAME_LIMIT NetBIOS name address table limit.
Range: 1..2000
Default: 50

NEG_MAC_LOC_FLT
Allowing filtered local MAC addresses.
Range: ON/OFF
Default: OFF

NEG_MAG_REM_FLT
Allowing filtered remote MAC addresses.
Range: ON/OFF
Default: OFF

NEG_NB_LOC_FLT
Allowing filtered local NetBIOS names.
Range: ON/OFF
Default: OFF

NEG_NB_REM_FLT
Allowing filtered remote NetBIOS names.
Range: ON/OFF
Default: OFF

LOCAL_ONLYLocally initiated SST links only.
Range: ON/OFF
Default: OFF

NAMES_15 NetBIOS names significant to 15 bytes.
Range: ON/OFF
Default: OFF

DLSW SET LLC

This command sets the LLC parameters for the DLSw router.

Syntax: **DLSW SET LLC parameter value**

Parameter	Description
MAC_TYPE	The type of media. If the router uses for LLC both Token Ring and Ethernet medium it is recommended to set media type to Token Ring. Range: TR, ETH Default: TR
FRAME_SIZE	The maximum buffer size for the LLC frames. In current software version the value entered is ignored and has no effect. DLSw calculates optimal value from DLSW SET MAX_BTU command. Range: 512..4502 Default: 4502
SEND_WINDOW	Default send window size. Range: 1..128 Default: 1
RCV_WINDOW	Default receive window size. Range: 1..128 Default: 1
T1_T	Acknowledgment timeout. Range: 1..60000 ms Default: 1000 ms
P_BIT_T	POLL response timeout. Range: 1..60000 ms Default: 2000 ms
T2_T	Acknowledgment delay. Range: 1..60000 ms Default: 100 ms
REJ_T	REJ response timeout. Range: 1..120 s Default: 2 s
BUSY_T	Remote busy timeout. Range: 1..120 s Default: 5 s
Ti_T	Idle RR interval. Range: 1..60 s Default: 30 s

MAX_RETRY	Maximum number of retries for any response. Range: 1..100 Default: 10
Q_THRESH	Frames queued for station awaiting credit. Range: 0..32 Default: 10
INC_THRESH	The number of positively acknowledged I-frames after which the dynamic window will be incremented by 1 during the recovery after an error. Range: 1..10 Default: 4
XID_TIMER	XID retry interval. Range: 1.120 s Default: 2 s
XID_RETRY	XID retry limit. Range: 1..100 Default: 4
TEST_TIMER	TEST retry interval. Range: 1..120 s Default: 2 s
TEST_RETRY	TEST retry limit. Range: 1..100 Default: 4

DLSW SET LLC SAP

Use this command if you want to use (ON) some SAP numbers and not to use (OFF) the others.

Syntax: **DLSW SET LLC SAP sap_number {ON|OFF}**

This command enables (ON) or disables (OFF) all SAPs.

Syntax: **DLSW SET LLC SAP ALL {ON|OFF}**

Example

In the following example SAP 04 has been disabled and then enabled again. After using the command the SAP list is displayed.

```
ILAN/XL(1)>dlsw set llc sap 04 off

ILAN/XL(1)>dlsw set llc sap 04 on
```

The following table shows how the SAP numbers are coded.

Offset	SAPs	Binary	Hex
0	0, 4, 8, C	1010 1010	0xAA
1	10, 14, 18, 1C	1010 1010	0xAA
2	20, 24, 28, 2C	1010 1010	0xAA
3	30, 34, 38, 3C	1010 1010	0xAA
4	40, 44, 48, 4C	1010 1010	0xAA
5	50, 54, 58, 5C	1010 1010	0xAA
6	60, 64, 68, 6C	1010 1010	0xAA
7	70, 74, 78, 7C	1010 1010	0xAA
8	80, 84, 88, 8C	1010 1010	0xAA
9	90, 94, 98, 9C	1010 1010	0xAA
A	A0, A4, A8, AC	1010 1010	0xAA
B	B0, B4, B8, BC	1010 1010	0xAA
C	C0, C4, C8, CC	1010 1010	0xAA
D	D0, D4, D8, DC	1010 1010	0xAA
E	E0, E4, E8, EC	1010 1010	0xAA
F	F0	1000 0000	0x80

DLSW SET PARTNER

This command defines a DLSw partner your DLSw will establish a transport connection with. You can specify the partners either before or after starting DLSw.

Syntax: **DLSW SET PARTNER address**

Parameter	Description
address	The IP address of the remote DLSw router.

DLSW DEL PARTNER

This command deletes a DLSw partner.

Syntax: **DLSW DEL PARTNER address**

Parameter	Description
address	The IP address of the remote DLSw router.

DLSW UP

This command starts the DLSw functions in the router.

Syntax: **DLSW UP**

DLSW DOWN

This command stops the DLSw functions in the router.

Syntax: **DLSW DOWN**

DLSW SHOW

This command displays all global parameters or one specified.

Syntax: **DLSW SHOW parameter**

Parameter	Description
CONF	General parameters.
MAC	MAC address cache.
NAME	NetBIOS name cache.
MEM	Memory usage.
HEAP	DLSw memory heap limit.

Example 1

```
ILAN/XL(1)>dlsw show conf
ILAN/XL(1)>
 DLSw State: UP              up_time:     308 [s]
 vendor_id: 0x000019
 sap_list: AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA 80
 version: 1.0
 version_str: CCC DLSW V. 1.10
 vrn:       0x92B            mac_cache_limit:   100
 bridge_num: 0x0             name_cache_limit:   50
 max_btu_size:     4472 [B] mac_local_filter:     FALSE
 sst_connect_retry:  10 [s] mac_remote_filter:    FALSE
 single_circ_tmout:  10 [s] nb_local_filter:      FALSE
 multi_circ_tmout:   15 [s] nb_remote_filter:     FALSE
 ack_tmout:          20 [s] backlvl_flow_control: TRUE
 idle_tmout:         20 [s] local_connect_only:   FALSE
 nb_retries:          4     fifteen_byte_names:   FALSE
 nb_tmout:            2 [s] netname: 20.20.20.2
 Heap memory limit:  1024 kB
 local_def_TC_number:    1
 loc_mac_flt_number:     0      rem_mac_flt_number:     0
 loc_name_flt_number:    0      rem_name_flt_number:    0
```

Which displays:

- DLSw state (UP or DOWN) and how long it has remained in this state.
- Vendor identifier (0x000019 indicates "Olicom").
- The SAP list. For the description of coding the SAP numbers refer to the command DLSW SET LLC SAP on page 166.
- Version number and name.
- Parameters set by the command DLSW SET on page 162.
- The number of transport connections defined on this DLSw.
- The number of MAC address filters (defined locally or remotely).
- The number of NetBIOS name filters (defined locally or remotely).

Example 2

ILAN/XL(1)>dlsw show mac

```
ILAN/XL(1)>

MAC Cache Statistics:
 mac_cache_entries:       1
 mac_cache_hits:          8
 mac_cache_misses:        0

      MAC ADDRESS            REMOTE DLSw
   1) 40-00-00-00-01-01      20.20.20.1
```

----- End of MAC Address Cache -----

Which displays:

- The number of entries in the cache.
- How many times the router hit or missed while searching for an address in the cache.
- A list of MAC addresses and the proper IP addresses of remote DLSw routers.

Example 3

```
ILAN/XL(1)>dlsw show name
ILAN/XL(1)>

NetBIOS Name Cache Statistics:
 name_cache_entries:      2
 name_cache_hits:         1
 name_cache_misses:       0

     NETBIOS NAME              REMOTE DLSw
   1) ”TKOWALSK      <00>”      20.20.20.1
   2) ”ANOWAK          ”        20.20.20.1

-----  End of NetBIOS Name Cache  -----
```

Which displays:

- The number of entries in the cache.
- How many times the router hit or missed while searching for a name in the cache.
- A list of NetBIOS names and the proper IP addresses of remote DLSw routers. Unprintable characters in NetBIOS names are displayed within <> brackets in hex.

Example 4

```
ILAN/XL(1)>dlsw show heap
DLSw heap memory limit = 512 kB.
```

Example 5

```
ILAN/XL(1)>dlsw show mem
  396 kB XL Heap memory allocated
  247 kB of memory type 1 used (Buffers)
  23 kB of memory type 2 used (Control Blocks)
```

DLSW SHOW LLC

This command displays all LLC parameters.

Syntax: DLSW SHOW LLC

Example

```
ILAN/XL(1)>dlsw show llc
ILAN/XL(1)>

  LLC CONFIGURATION

      mac_type:         TR       frame_size:     4502
      xid_timer:         2       send_window:    1
      test_timer:        2       rcv_window:     1
      xid_timer_retry:   4       upward_cred_q_threshold:    10
      test_timer_retry:  4       window_inc_threshold:       4
      max_retry:        10

  LLC TIMEOUTS
      T1 timeout:       1000 [ms]
      Poll bit timeout: 2000 [ms]
      T2 timeout:        100 [ms]
      REJ timeout:         2 [s]
      Busy timeout:        5 [s]
      Ti timeout:         30 [s]
```

Which displays the values of the parameters set by the DLSW SET LLC command.

DLSW SHOW LLC SAP

This command displays a list of enabled SAP numbers.

Syntax: DLSW SHOW LLC SAP

Example

ILAN/XL(1)>dlsw show llc sap
Enabled SAP list:
0x00 0x04 0x08 0x0C 0x10 0x14 0x18 0x1C
0x20 0x24 0x28 0x2C 0x30 0x34 0x38 0x3C
0x40 0x44 0x48 0x4C 0x50 0x54 0x58 0x5C
0x60 0x64 0x68 0x6C 0x70 0x74 0x78 0x7C
0x80 0x84 0x88 0x8C 0x90 0x94 0x98 0x9C
0xA0 0xA4 0xA8 0xAC 0xB0 0xB4 0xB8 0xBC
0xC0 0xC4 0xC8 0xCC 0xD0 0xD4 0xD8 0xDC
0xE0 0xE4 0xE8 0xEC 0xF0

DLSW SHOW PARTNER

These commands display all DLSw partners or details about a particular one.

Syntax: DLSW SHOW PARTNER

or details about a particular one.

Syntax: DLSW SHOW PARTNER {ip_address | index}

Parameter	Description
ip_address	The IP address of the partner DLSw.
index	The number of the partner DLSw. If you display all partners using the DLSW SHOW PARTNER command every entry starts with this number.

Example 1

```
ILAN/XL(1)>dlsw show partner
ILAN/XL(1)>

Transport Connections Statistics:
 active_tc:          1
 close_idle_tc:      0
 close_busy_tc:      0
             IP ADDRESS   STATE
    1)        20.20.20.1   Connected
Total number of Transport Connections = 1
```

Which displays:

- The number of active transport connections.
- The number of transport connections closed when they were inactive.
- The number of transport connections closed when they were active.
- A list of active transport connections (IP address of the partner DLSw, the state of the connection).

Example 2

```
ILAN/XL(1)>dlsw show partner 1
ILAN/XL(1)>
    LOCAL ADDR       PARTNER ADDR    DEFINED     STATE
    20.20.20.2        20.20.20.1     Locally     Connected

 tc_type:            ACTIVE_PERSISTENT   connected_count:      1
 disconnected_reason: NEVER_DISCONNECTED  created_time:        2 [s]
 created_circuits:            7        modified_time:       0 [s]
 connected_circuits:          4         connected_time:     504 [s]
 disconnected_circuits:       0         disconnected_time:    0 [s]

PARTNER'S INFORMATION:
 initial_pacing:     1     vendor_id: 0x000019
 sap_list: AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA 80
 version: 1.0   version_str: CCC DLSW V. 1.10

STATISTICS:
             received    sent                received      sent
 CANUREACH_ex:       5       3    NETBIOS_NQ_ex:       0         0
 ICANREACH_ex:       3       5    NETBIOS_NR_ex:       0         0
 data_packets:       0     7972    data_bytes:          0     782926
 cntl_packets:   13097       55
```

Which displays:

- The addresses of both the local and the remote DLSw.
- Where the connection was defined (locally or on the partner DLSw).
- The state of the connection (CONNECTING, INITCAPEXCHANGE, CONNECTED, DISCONNECTING or DISCONNECTED).
- Connection type: PERSISTENT if the local DLSw tries to connect to the partner or PASSIVE if the partner tries to connect to the local DLSw.
- The reason for disconnection. It may be one of the following: NEVER_DISCONNECTED, CAP_EXCH_FAIL, SST_FAIL, OP_CMD, PROTOCOL_ERROR, OTHER_REASON.
- The number of circuits ever created, connected or disconnected.
- Time since last creation, connection or disconnection of a circuit.
- Partner's information: initial pacing (the number of frames the receiver can get), vendor identifier, SAP list, version number and name.
- The number of different messages sent or received.

DLSW SHOW CIRC

These commands display all active DLSw circuits or details about a particular one.

Syntax: **DLSW SHOW CIRC**

or details about a particular one.

Syntax: **DLSW SHOW CIRC n [R]**

Syntax: **DLSW SHOW CIRC <src_mac> <src_sap> <dst_mac> <dst_sap> [R]**

Parameter	Description
n	The number of the circuit. If you display all circuits using the DLSW SHOW CIRC command every entry starts with this number.
R	Use this option if you want to reset statistic counters after reading.
src_mac	Source MAC address.
src_sap	Source SAP.
dst_mac	Destination MAC address.
dst_sap	Destination SAP.

Example 1

```
ILAN/XL(1)>dlsw show circ
ILAN/XL(1)>
Circuits Statistics:
 active_circuits:      4
 created_circuits:      9
     LOCAL MAC/SAP       REMOTE MAC/SAP       STATE
   1) 40-00-00-00-01-00 04  40-00-00-00-01-01 04   Connected
   2) 40-00-00-00-01-00 08  40-00-00-00-01-01 08   Connected
   3) 40-00-00-00-01-00 0C  40-00-00-00-01-01 0C   Connected
   4) 40-00-00-00-01-00 10  40-00-00-00-01-01 10   ConnectPending
Total number of Circuits = 4
```

Which displays:

- The number of active circuits.
- The number of created circuits.
- A list of active circuits.

Example 2

```
ILAN/XL(1)>dlsw show circ 1
ILAN/XL(1)>
 LOCAL MAC/SAP        REMOTE MAC/SAP        INITIATED  STATE
 40-00-00-00-01-00 04  40-00-00-00-01-01 04   Locally    Connected
 Remote DLSw: 20.20.20.1
   circuit_priority: LOW
   local_circuit_id:  0x16ED009C170E00BD circuit_create_time:  88 [s]
   remote_circuit_id: 0x16F300A216F800A7 circuit_state_time:  105 [s]
PACING_STATISTICS:
   send_granted_units:       0       total_halve_windows_sent:      0
   receive_granted_units:    0       total_halve_windows_received:  0
   send_current_window:      2       total_reset_windows_sent:      0
   receive_current_window:   3       total_reset_windows_received:  0
   max_send_window_size:     2
   max_receive_window_size:  3
DLC STATISTICS:
 RIF: backward 01A 1 022 1 010 0
   max_btu_size:       3808        remote_busy:               0
   send_window:          1         t1_expiry_count:           9
   receive_window:       1         t2_expiry_count:           0
   i_frames_rcvd:      256         i_frames_sent:          4317
   i_bytes_rcvd:     60868         i_bytes_sent:        1007816
   i_frames_rjctd:      50         i_frames_rexmit:           5
   i_bytes_rjctd:    13452         i_bytes_rexmit:          756
   rej_frames_rcvd:      0         xid_frames_rcvd:           0
   rej_frames_sent:      9         xid_frames_sent:           0
```

Which displays:

- MAC address and SAP number of the local and remote end station.
- Where the circuit was created (locally or remote).
- The state of the circuit (DISCONNECTED, CIRCUITSTART, RESOLVEPENDING, CIRCUITESTABLISHED, CONNECTPENDING, CONTACTPENDING, CONNECTED, DISCONNECTPENDING, HALT-PENDING, HALTPENDINGNOACK, CIRCUITPENDING or RESTART-PENDING).
- The priority of the circuit (LOW, MEDIUM, HIGH, HIGHEST, UNSUPP).
- Local and remote circuit identifiers put into SSP frames to identify circuits.
- When the circuit was created, how long it remains in the current state.
- The number of flow control messages (e.g., granting permission, setting the size of the window, reducing the size of the window) sent or received.
- The number of different kind of frames (e.g., information, xid, reject) sent or received.

SET MESSAGES DLSW

This command enables displaying different kind of messages sent from your DLSw.

Syntax: SET MESSAGES DLSW n

This command turns off the display of extended diagnostics.

Syntax: SET MESSAGES DLSW

n	Message type
1	Problem messages.
2	Exception and problem messages.
3	Audit, exception and problem messages.

DLSW DEL CIRC

This command disconnects an active DLSw circuit.

Syntax: DLSW DEL CIRC n

Syntax: DLSW DEL CIRC <src_mac> <src_sap> <dst_mac> <dst_sap>

Parameter	Description
n	The number of the circuit obtained from the DLSW SHOW CIRC command.
src_mac	Source MAC address.
src_sap	Source SAP.
dst_mac	Destination MAC address.
dst_sap	Destination SAP.

Example 1

```
ILAN/XL(1)>dlsw del circ 1
ILAN/XL(1)>
```

Example 2

```
ILAN/XL(1)>dlsw del circ 400000000100 04  400000000101 04
ILAN/XL(1)>
```

11. Dial Backup Commands

When you are using the asynchronous interface, disable the autoreconnect option. Use the command SET ADV INTERFACE {RECON | NORECON} on page 21

BKP SHC

This command displays Dial Backup parameters for a specified port.

Syntax: **BKP SHC p**

Parameter	Description
p	The number of the port for which you want to display parameters.

BKP SEC

This command adds port s to the pool of ports that can be assigned as secondary ports to primary ports. It does not make port s the secondary port for any specific primary port; to do that, use the command BKP PRI SEC on page 178.

Syntax: **BKP SEC s**

Parameter	Description
s	The number of the port that you want to designate as a potential secondary (backup) port.

BKP PRI SEC

This command designates potential secondary port s as the assigned secondary port for specific primary port p. All Dial Backup parameters will be set to their default values. To use this command, you must first use the command BKP SEC on page 178 for secondary port s.

Syntax: **BKP PRI p SEC s**

Parameter	Description
p	The number of the primary port
s	The number of the secondary port

BKP DEL

This command cancels the backup service for a specified primary port. This command breaks the association created by the command BKP PRI SEC on page 178 between a primary port and secondary port.

Syntax: **BKP DEL p**

Parameter	Description
p	The number of the primary port whose backup service you want to cancel.

BKP SET

This command sets the backup parameters for a specified primary port p. It is available for ports on which Dial Backup was previously set.

Syntax: **BKP SET p option value**

Parameter	Description
p	The number of the port on which you want to set parameters.
option	The parameter that you want to set for the specified port.
value	A parameter associated with the selected option. Not all options have associated values. Refer to the Option and Value listing that follows.

Variation	Description
BKP SET p TRTM s	Sets the trigger timer minimum: minimum seconds (s) that the activating event must remain in effect before the backup process starts. Range: 0 to 999 seconds Default: 15
BKP SET p DTRM s	Sets the drop timer minimum: minimum seconds (s) that the dropping event must remain in effect before the backup process terminates. Range: 0 to 999 seconds Default: 10
BKP SET p MINT m	Sets the Minimum Time: minimum minutes (m) that the backup process remains active. The timer starts at the first attempt to establish a connection over the secondary port. Range: 1 to 999 minutes Default: 1

BKP SET p ACT

This command allows you to set a period of time on a daily basis in which the dial backup service needs to be active on a port. The period begins with b and ends with e.

Syntax: **BKP SET p ACT d FROM b TO e**

Parameter	Description
p	The number of the port
d	The day of the week, indicated as follows: SU Sunday MO Monday TU Tuesday WE Wednesday TH Thursday FR Friday SA Saturday
b	The time the activity period begins. This time is expressed in hh:mm format.
e	The time the activity period ends. This time is expressed in hh:mm format.

BKP RMV

This command removes a dial backup activity period on a specified port. After removing the designated activity period, dial backup will be active all day on the port.

Syntax: **BKP p RMV d**

Parameter	Description
p	The number of the port
d	The day of the week, indicated as follows: SU Sunday MO Monday TU Tuesday WE Wednesday TH Thursday FR Friday SA Saturday

BKP DROP

This command establishes how a secondary port assigned to a primary port is to be dropped. The choices are either automatically or manually.

Syntax: BKP p DROP {AUT | MAN}

Parameter	Description
p	the number of the primary port for which the dial backup service is defined.
AUT	secondary port is to be dropped automatically
MAN	secondary port is to be dropped manually.

BKP DROPSEC

This command drops a secondary port assigned to a primary port.

Syntax: BKP p DROPSEC

Parameter	Description
p	The primary port number.

BKP DEBUG

This command sets a level of Dial Backup diagnostic messages.

Syntax: BKP DEBUG level

Parameter	Description
level	The debug info messages level (0-no debug information, 4-highest detail level). Range: 0 to 4 Default: 0

12. Dial on Demand Console Commands

When you are using the asynchronous interface, disable the autoreconnect option. Use the command SET ADV INTERFACE {RECON | NORECON} on page 21

DOD ENABLE

This command enables Dial on Demand on a specific port.

Syntax: **DOD p ENABLE**

Parameter	Description
p	The number of the port on which you want to enable Dial on Demand service. Default: Disabled

DOD DISABLE

This command disables Dial on Demand on a specific port.

Syntax: **DOD p DISABLE**

Parameter	Description
p	The number of the port on which you want to disable Dial on Demand service. Default: Disabled

DOD IDLETIME

This command defines the minimum number of seconds that a Dial on Demand link must remain idle before it is put into the Idle state.

Syntax: **DOD p IDLETIME value**

Parameter	Description
p	The number of the port on which you want to set this parameter.
value	The minimum time period for which there must be no traffic on a Dial on Demand link before it is put into the Idle state. Range: 1 to 3600 seconds Default: 60 seconds

DOD HOLDUPDATETIME

This command sets the maximum time for which the network topology updates can be held up by the router in anticipation of some other data transfer to be sent within this data connection time.

Syntax: **DOD p HOLDUPDATETIME value**

Parameter	Description
p	The number of the port on which you want to set this parameter.
value	The maximum time for which network topology updates can be held up by the router in anticipation of another data transfer to be sent within this data connection time. If there is no other traffic over the link for the hold update time, the updates are transmitted after this time elapses. If you reduce the value of this parameter, it is recommended you disable and enable the Piggyback option. Range: 1 to 1440 minutes Default: 30 minutes

DOD PIGGYBACKON

Enables the piggyback option on a specific port.

Syntax: **DOD p PIGGYBACKON**

Parameter	Description
p	The number of the port of a Dial on Demand link.

DOD PIGGYBACKOFF

Disables the piggyback option on a specific port.

Syntax: **DOD p PIGGYBACKOFF**

Parameter	Description
p	The number of the port of a Dial on Demand link.

DOD CONFIG

This command shows the Dial on Demand configuration parameters for a specific port.

Syntax: **DOD p CONFIG**

Parameter	Description
p	The number of the port of a Dial on Demand link.

DOD ACT FROM TO

Sets daily activity period for Dial on Demand service. By default the activity is set to ALLDAY (see next command).

Syntax: **DOD <p> ACT <d> FROM <s> TO <e>**

Parameter	Description
p	The port number
d	The day of the week: {MO|TU|WE|TH|FR|SA|SU}
s	The start time in hh:mm format, where: hh:mm ranges from 00:00 to 23:59 in 24 hour mode or from 00:00 am to 12:59 pm in 12 hour mode.
e	The end time in hh:mm format, where: hh:mm ranges from 00:00 to 23:59 in 24 hour mode or from 00:00 am to 12:59 pm in 12 hour mode.

DOD ACT ALLDAY

Clears the daily activity period selection for Dial on Demand service (sets the activity to ‘all day’).

Syntax: **DOD <p> ACT <d> ALLDAY**

Parameter	Description
p	The port number
d	The day of the week: {MO|TU|WE|TH|FR|SA|SU}

DOD MAXCALLNR

Sets the maximum number of connections per day.

Syntax: **DOD <p> MAXCALLNR {value | NOLIMIT}**

Parameter	Description
p	The port number
value	The maximum number of connections. Range: 1…200.
NOLIMIT	The unlimited number of connections. This is the default value.

DOD MAXCONTIME

Sets maximum time of all connections per day.

Syntax: **DOD <p> MAXCONTIME {value | NOLIMIT}**

Parameter	Description
p	The port number
value	The maximum time of all connections (cumulative) Range: 1…1440.
NOLIMIT	The unlimited time of all connections. This is the default value.

DOD BLOCKPORT {ENABLE | DISABLE}

Sets Dial on Demand port block when MAXCALLNR and MAXCALLTIME parameters are expired. The port block is disabled by default.

Syntax: **DOD <p> BLOCKPORT {ENABLE | DISABLE}**

or

Syntax: **DOD <p> BLOCKPORT {ON | OFF}**

Parameter	Description
p	port number.

DOD AUTOREC {TIME | DISABLE}

Sets the interval between the attempts to autoreconnect after the Call Failure.

Syntax: **DOD p AUTOREC {TIME n | DISABLE}**

Parameter	Description
p	The port number
TIME n	The attempt to autoreconnect will take place n seconds after the Call Failure. Port will enter *Inactive* state after the Call Failure
DISABLE	The port will enter *Idle* state after the Call Failure and there will be no attempts to reestablish the connection. This is the default option.

DOD STRS or DOD STATS RESET

Resets all statistics.

Syntax: **DOD <p> STRS**

or

Syntax: **DOD <p> STATS RESET**

Parameter	Description
p	The port number

DOD EVLOG {ENABLE | DISABLE} or DOD EVLOG {ON | OFF}

Enables or disables recording events into eventlog. Recording is disabled by default.

Syntax: **DOD <p> EVLOG {ENABLE | DISABLE}**

or

Syntax: **DOD <p> EVLOG {ON | OFF}**

Parameter	Description
p	The port number

DOD EVLOG MAXENT

Sets the maximum number of eventlog entries.

Syntax: **DOD <p> EVLOG MAXENT <n>**

Parameter	Description
p	The port number
n	The maximum number of eventlog entries. Range: 1…1000 Default: 100

DOD EVLOG FRLEN

Sets the maximum length of recorded frame. If the frame length exceeds the set value, only nbytes will be saved.

Syntax: **DOD <p> EVLOG FRLEN <n>**

Parameter	Description
p	The port number
n	The maximum length of recorder frame (in bytes). Range: 1…1024 Default: 64

DOD SHEV or DOD SHOW EVLOG

Displays the contents of the eventlog.

Syntax: **DOD <p> SHEV**

or

Syntax: **DOD <p> SHOW EVLOG**

Parameter	Description
p	The port number

DOD SHCFG or DOD SHOW CONFIG

Shows Dial on Demand configuration on a port.

Syntax: **DOD <p> SHCFG**

or

Syntax: **DOD <p> SHOW CONFIG**

Parameter	Description
p	The port number

DOD SHSTAT or DOD SHOW STATS

Shows Dial on Demand statistics (without eventlog) on a port.

Syntax: **DOD <p> SHSTAT**

or

Syntax: **DOD <p> SHOW STATS**

Parameter	Description
p	The port number

13. Frame Relay Commands

FR SET SYS MAXBUFR

This is a system wide parameter, which defines the maximum frame length that may be set on interfaces which are subsequently configured for Frame Relay operational-mode.

Syntax: **FR SET SYS MAXBUFR value**

Parameter	Description
value	The maximum buffer size in bytes. The default is 8182.

FR SET SYS PVCTRAP

This command is used to enable or disable system-wide generation of a trap each time a VC changes state.

Syntax: **FR SET SYS PVCTRAP {ENABLE | DISABLE}**

FR SET INTERFACE LMI

This command is used to select the appropriate LMI (Local Management Interface) Protocol for a given interface in the operation–mode Frame Relay. Selecting the correct LMI is crucial to proper operation with most switches.

Syntax: **FR SET INTERFACE n LMI {NONE | LMI | STRATACOM | ANNEXD}**

Parameter	Description
n	The interface (which must have been previously set into Frame Relay operational-mode) that you want to dedicate to using the Frame Relay Protocol.
NONE	means that no LMI protocol will be used. This is especially useful when running two routers back–to–back without a Frame Relay DCE switch. This mode of operation can be used for testing purposes.
LMI	Use it to select the LMI Rev. 1 protocol. This is an early protocol no longer in common use today.
STRATACOM	The original LMI protocol.
ANNEXD	Use it to select the ANSI T1.617 Annex–D LMI protocol. This is the default.

FR SET INTERFACE LMIVC

This parameter sets the VC for LMI communication.

Syntax: **FR SET INTERFACE n LMIVC {0 | 1023}**

Parameter	Description
n	The interface (which must have been previously set into Frame Relay operational–mode) for which you want to set an LMI Virtual Circuit number.
0	The value normally used when No LMI, Annex–D or Stratacom is selected.
1023	The value normally used when LMI Rev 1 is selected.

FR SET INTERFACE N1

This command sets the value of DTE full status poll frequency. For every N1 status requests sent, one full status request will be sent to the FR switch.

Syntax: FR SET INTERFACE n N1 value

Parameter	Description
n	The interface (which must have been previously set into Frame Relay operational–mode) for which you want to change the N391 value.
value	An integer in the range 1 to 255. When an interface is set to operational–mode Frame Relay, N391 is set to the default value of 6.

FR SET INTERFACE N2

This command sets the value of DTE Error threshold - this is the number of errors which must occur within the last N3 events before an error condition is recognized.

Syntax: FR SET INTERFACE n N2 value

Parameter	Description
n	The interface (which must have been previously set into Frame Relay operational–mode) for which you want to change the N392 value.
value	An integer in the range 1 to 10. When an interface is set to operational–mode Frame Relay, N392 is set to the default value of 3.

FR SET INTERFACE N3

This command sets the value of DTE monitored events count - this is the number of events which are monitored, of which N2 must be in error, for an error condition to be recognized.

Syntax: FR SET INTERFACE n N3 value

Parameter	Description
n	The interface (which must have been previously set into Frame Relay operational–mode) for which you want to change the N393 value.
value	An integer in the range 1 to 10. The N393 value should be greater than the N392 value. When an interface is set to operational–mode Frame Relay, N393 is set to the default value of 4.

FR SET INTERFACE T1

This command sets the value of DTE poll timer. This is the delay in seconds between successive status message requests.

Syntax: **FR SET INTERFACE n T1 value**

Parameter	Description
n	The interface (which must have been previously set into Frame Relay operational–mode) for which you want to change the T391 value.
value	An integer in the range 5 to 30 representing seconds. When an interface is set to operational–mode Frame Relay, T391 is set to the default value of 10.

FR SET INTERFACE LMI_BAND

This command is applicable only to interfaces configured with the Stratacom protocol.

Syntax: **FR SET INTERFACE n LMI_BAND {ON | OFF}**

Parameter	Description
n	The interface (which must have been previously set into Frame Relay operational–mode) for which you want to change the bandwidth control response in Stratacom LMI mode.
ON	Allows LMI to dynamically control the current CIR.
OFF	Disables LMI bandwidth control. This is the default.

FR SET INTERFACE LEARNING

This command enables and disables the ability of the router to learn new PVCs advertised by a switch. This ability is only applicable when using one of the LMI protocols. If no LMI is configured, learning is not possible.

Syntax: **FR SET INTERFACE n LEARNING {ON | OFF}**

Parameter	Description
n	The interface (which must have been previously set into Frame Relay operational–mode) for which you want to enable/disable learning.
ON	Enables automatic learning. This is the default setting.
OFF	Disables automatic learning.

FR SET INTERFACE LMIXONXOFF

This command is applicable only to interfaces configured with the Stratacom protocol.

Syntax: **FR SET INTERFACE n LMIXONXOFF {ON | OFF}**

Parameter	Description
n	The interface (which must have been previously set into Frame Relay operational–mode) for which you want to enable/disable flow control.
ON	Enables flow control.
OFF	Disables flow control. This is the default.

FR SET INTERFACE STATS

This commands enables and disables collecting statistics.

Syntax: **FR SET INTERFACE n STATS {ON | OFF}**

Parameter	Description
n	The interface (which must have been previously set into Frame Relay operational–mode) for which you want to change statistics collection.
ON	Allows statistics to be collected for display by either console commands or through SNMP (ClearSight). This is the default.
OFF	Disables the collection of statistics. Statistics are unavailable for both the console and SNMP.

FR SET INTERFACE LINKNAME

This command sets the linkname.

Syntax: **FR SET INTERFACE n LINKNAME name**

Parameter	Description
n	The interface (which must have been previously set into Frame Relay operational–mode) for which you want to change the name.
name	An alphanumeric field of up to 17 characters. The name field defaults to *UNNAMED LINK*.

FR SET INTERFACE MAX_FRAME

The maximum frame size is the largest number of bytes Frame Relay will attempt to transmit on this interface in a single frame.

Syntax: **FR SET INTERFACE n MAX_FRAME value**

Parameter	Description
n	The interface (which must have been previously set into Frame Relay operational–mode) for which you want to change the maximum frame size.
value	An integer in the range from 150 to 8182. The default value is 1974.

FR SET INTERFACE NEWVCS

This command defines the state that new Virtual Circuits will default to when they are created.

Syntax: **FR SET INTERFACE n NEWVCS {ON | OFF}**

Parameter	Description
n	The interface (which must have been previously set into Frame Relay operational–mode) for which you want to enable/disable new Virtual Circuits that are created.
ON	This means that new Virtual Circuits will automatically be enabled when they are created. This is the default.
OFF	This means that new Virtual Circuits will automatically be disabled when they are created.

FR CREATE VC

This command allows you to manually add a Virtual Circuit to a particular interface. It is usually not necessary unless you are not using LMI or have Automatic Learning disabled.

Syntax: **FR CREATE VC n c**

Parameter	Description
n	The interface (which must have been previously set into Frame Relay operational–mode) for which you want to create a Virtual Circuit.
c	The DLCI number in the range from 16 to 991.

FR CREATE PORT

This command allows you to manually add a Frame Relay Port to a particular interface. Even if VCs are learned automatically from a Frame Relay switch, ports must be created manually.

Syntax: **FR CREATE PORT n portname**

Parameter	Description
n	The interface (which must have been previously set into Frame Relay operational–mode) for which you want to create a Port.
portname	An alphanumeric field of up to 32 characters.

FR MAP VC

This command allows you to map a VC to a Frame Relay Port. VCs must be mapped to a port before they become operational. Many VCs may be mapped to the same port (provided the VCs and port exist on the same interface).

Syntax: **FR MAP VC n c p**

Parameter	Description
n	The interface (which must have been previously set into Frame Relay operational–mode) for which you want to create a Virtual Circuit.
c	The DLCI number of the VC.
p	The Port number.

FR UNMAP VC

This command allows you to unmap a VC from a Frame Relay Port. VCs may be unmapped from a port and remapped to the same or a different port

Syntax: **FR UNMAP VC n c**

Parameter	Description
n	The interface (which must have been previously set into Frame Relay operational–mode) from which you want to unmap a Virtual Circuit.
c	The DLCI number of the VC.

FR DELETE PORT

This command allows you to manually remove a Frame Relay Port from a particular interface. Frame Relay ports may only be deleted if there are no VCs mapped to them.

Syntax: **FR DELETE PORT n portname**

Parameter	Description
n	The interface (which must have been previously set into Frame Relay operational–mode) on which the Port exists.
portname	The alphanumeric name of the port.

FR DELETE VC

This command allows you to manually delete a Virtual Circuit on a particular interface. If you have an LMI configured and are using Automatic Learning, the DLCI may be relearned automatically if it is still being advertised by the switch (Frame Relay DCE).

Syntax: **FR DELETE VC n c**

Parameter	Description
n	The interface (which must have been previously set into Frame Relay operational–mode) for which you want to delete a Virtual Circuit.
c	The DLCI number in the range from 16 to 991.

FR SET INTERFACE BECN

Syntax: **FR SET INTERFACE n BECN {ON | OFF}**

Parameter	Description
n	The interface (which must have been previously set into Frame Relay operational–mode) for which you want to change the response to BECNs received on the Frame Relay interface.
ON	When BECNs are received, congestion management is invoked resulting in a dynamic reduction in Bc. This is the default setting.
OFF	BECNs are ignored, except for counting statistics.

FR SET INTERFACE INJECT

This command allows you to vary how packets are treated by Frame Relay when using congestion avoidance mechanisms.

Syntax: **FR SET INTERFACE n INJECT {STANDARD | FORCED}**

Parameter	Description
n	The interface (which must have been previously set into Frame Relay operational–mode) for which you want to change the injection mode.
STANDARD	Enforces CIR and drops all packets in excess of Bc + Be in a time interval of Tc. This is the default setting.
FORCED	Also known as Zero CIR. CIR is not enforced in Forced Injection Mode. This is the most desirable mode of operation if the Frame Relay Service Provider provides a Zero CIR service.

FR SHOW LASTLMI

This command allows you to print the last Full Status Message received by the router on an interface. This is primarily designed as a diagnostic tool.

Syntax: **FR SHOW LASTLMI n**

Parameter	Description
n	The interface which must have been previously set into Frame Relay operational–mode, for which you want to print the last Full Status Message received.

FR SET VC CIR

This command allows you to set the Committed Information Rate for a Virtual Circuit.

Syntax: **FR SET VC n c CIR value**

Parameter	Description
n	The interface for which the Virtual Circuit is defined.
c	The Virtual Circuit number.
value	A value representing the number of bits per second. The default value is 256000 bps.

FR SET VC BCMAX

This command allows you to set the Committed Burst Size for a Virtual Circuit. If you are using congestion avoidance techniques (the default), this is considered the maximum Burst size achievable, but the operational burst size may drop to the value BC MIN.

Syntax: **FR SET VC n c BCMAX value**

Parameter	Description
n	The interface for which the Virtual Circuit is defined.
c	The virtual circuit number.
value	A value representing the number of bits in a burst period. The default is 256000 bits.

FR SET VC BCMIN

This command allows you to set the lowest value that Bc will be adjusted to under the conditions of congestion. When BECNs are received from the Frame Relay network, indicating congestion, and if BECN response is enabled, the Committed Burst Size for a Virtual Circuit will be lowered in stages until it reaches BC MIN. When congestion is alleviated, the actual Burst Size Bc will be returned, in stages, to the original BC MAX value.

Syntax: **FR SET VC n c BCMIN value**

Parameter	Description
n	The interface for which the Virtual Circuit is defined.
c	The Virtual Circuit number.
value	A value representing the number of bits in a burst period. The default is 128000 bits.

FR SET VC BE

This command allows you to set the Excess Burst Size (Be) for a Virtual Circuit. The excess Burst Size is the number of bytes, in addition to Bc (Bc MAX), that are allowed to be transmitted in an interval Tc.

Syntax: **FR SET VC n c BE value**

Parameter	Description
n	The interface for which the Virtual Circuit is defined.
c	The Virtual Circuit number.
value	A value representing the number of bits in a burst period. The default is 0.

FR SET VC CMP

This command allows you to set the Congestion Monitoring Period. This is the interval during which received BECNs are counted and congestion avoidance procedures are taken.

Syntax: **FR SET VC n c CMP value**

Parameter	Description
n	The interface for which the Virtual Circuit is defined.
c	The Virtual Circuit number.
value	A value representing seconds. The default value is 10.

FR SET VC VC_NAME

This command allows you to set a name for the Virtual Circuit.

Syntax: **FR SET VC n c VC_NAME string**

Parameter	Description
n	The interface for which the Virtual Circuit is defined.
c	The Virtual Circuit number.
string	An alphanumeric string of up to 10 characters.

FR SET VC ENABLE

This command allows you to activate a Virtual Circuit.

Syntax: **FR SET VC n c ENABLE**

Parameter	Description
n	The interface for which the Virtual Circuit is defined.
c	The Virtual Circuit number.

FR SET VC DISABLE

This command allows you to deactivate a Virtual Circuit.

Syntax: **FR SET VC n c DISABLE**

Parameter	Description
n	The interface for which the Virtual Circuit is defined.
c	The Virtual Circuit number.

FR SET VC RFC1490

This command allows you to set encapsulation to RFC1490 standard or CrossComm proprietary on a Virtual Circuit.

Syntax: **FR SET VC n c RFC1490 {CCC|STANDARD}**

Parameter	Description
n	The interface for which the Virtual Circuit is defined.
c	The Virtual Circuit number.
CCC	sets CrossComm proprietary encapsulation.
STANDARD	sets RFC1490 compliant encapsulation.

FR SET VC {MULTICAST | UNICAST}

This command allows you to set the PVC type to multicast or unicast.

Syntax: **FR SET VC n dlci {MULTICAST | UNICAST}**

Parameter	Description
n	interface number
dlci	Frame Relay Data Link Connection Identifier

FR SHOW CONFIG

This command allows you to display all the Frame Relay parameters associated with a physical interface or a specific Virtual Circuit. If no parameters are provided, the configuration parameters for all Frame Relay interfaces are displayed.

Syntax: **FR SHOW CONFIG n [c]**

Parameter	Description
n	The interface for which you want to display the configuration information.
c	The DLCI number (Data Link Connection Identifier) in the range from 16 to 991 for which you want to display configuration information.

FR SHOW INTERFACE

This command allows you to display all the Frame Relay statistics associated with a physical interface. These statistics include LMI statistics (if LMI is operational) and the total number of octets/Packet received and transmitted. If an optional DLCI number is specified, only the statistics for that Virtual Circuit will be displayed. If no parameters are provided, the statistics for all Frame Relay interfaces are displayed.

Syntax: **FR SHOW INTERFACE n [c]**

Parameter	Description
n	The interface that you want to display statistics.
c	The DLCI number in the range from 16 to 991 for which you want to display statistics.

FR SHOW STATS

This command allows you to display the total number of octets/packets transmitted and received on a specific Virtual Circuit. It also displays congestion management statistics (packets transmitted below Bc, below Bc+Be, and packets dropped due to CIR exceeded).

Syntax: **FR SHOW STATS n c**

Parameter	Description
n	The interface for which you want to display statistics.
c	The DLCI number in the range from 16 to 991 for which you want to display statistics.

FR SHOW SYSTEM

This command allows you to display Frame Relay System wide information.

Syntax: **FR SHOW SYSTEM**

FR SHOW RFC1490

This command allows you to display all the Frame Relay Encapsulation statistics, for a particular protocol, associated with a virtual circuit.

Syntax: **FR SHOW RFC1490 n c type**

Parameter	Description
n	The interface for which you want to display statistics.
c	The Virtual Circuit number.
type	You can select the specific protocol you want to display statistics for. Statistics for the following protocols are available: **ETHERNET_FCS** or **ETH_FCS** **ETHERNET** or **ETH** **TOKEN_RING_FCS** or **TR_FCS** **TOKEN RING** or **TR** **BPDU** or **SPANTREE** or **ST** **IPX** **IP** **CCC** **ARP** ALL

FR SHOW VIRTUAL_CIRCUIT

This command allows you to display the state and type (multicast or unicast) of a Virtual Circuit. If only the interface is specified, all the Virtual Circuits for that interface will be displayed. If no parameters are provided, all Virtual Circuits on all Interfaces will be displayed.

Syntax: **FR SHOW VIRTUAL_CIRCUIT [n [c]] or**

Syntax: **FR SHVC [n [c]]**

Parameter	Description
n	The interface for which the Virtual Circuit is defined.
c	The Virtual Circuit number.

FR SHOW PORT

This command allows you to display information about Frame Relay Ports (providing port number to port name correlation). If an interface is specified, all the Ports for that interface will be displayed. If no parameters are provided, all Frame Relay Ports on all Interfaces will be displayed.

Syntax: **FR SHOW PORT [n]**

Parameter	Description
n	The interface for which the Port is defined.

FR IPX MAP

Syntax: **FR IPX MAP n ipxmac d**

Parameter	Description
n	The port to which the virtual circuit is assigned.
ipxmac	The IPX next hop MAC address.
d	The DLCI of the virtual circuit through which the IPX next hop MAC address is accessible.

FR IPX UNMAP

Syntax: **FR IPX UNMAP n ipxmac**

Parameter	Description
n	The port on which the address mapping has previously been defined.
ipxmac	The IPX next hop MAC address.

FR IPX SHOW

This command displays existing FR-IPX address mapping for a specified port, or for all ports.

Syntax: **FR IPX SHOW {n | ALL}**

Parameter	Description
n	The port to which the virtual circuit is assigned.

FR SHOW SNA1490 FEPLIST

This command displays a list of all configured remote SNA1490 devices.

Syntax: **FR SHOW SNA1490 FEPLIST**

FR SHOW SNA1490 VCLIST

This command displays all virtual circuits for a specified remote device. If the device is not specified, virtual circuits are displayed for all remote devices.

Syntax: **FR SHOW SNA1490 VCLIST n**

Parameter	Description
n	The number of the remote devices in the entry table (0 to 15).

FR SHOW SNA1490 SESSIONLIST

This command displays all sessions on a specified virtual circuit.

Syntax: **FR SHOW SNA1490 SESSIONLIST i dlci**

Parameter	Description
i	Interface number
dlci	The dlci number, specifies the virtual circuit

FR SHOW SNA1490 RSESSIONS

This command displays all configured remote sessions.

Syntax: **FR SHOW SNA1490 RSESSIONS**

FR SET SNA1490 FEPADD

This command adds a remote device.

Syntax: **FR SET SNA1490 FEPADD xx-xx-xx-xx-xx-xx**

Parameter	Description
xx-xx-xx-xx-xx-xx	MAC address of remote device.

FR SET SNA1490 FEPDELETE

This command deletes a remote device.

Syntax: **FR SET SNA1490 FEPDELETE xx-xx-xx-xx-xx-xx**

Parameter	Description
xx-xx-xx-xx-xx-xx	MAC address of remote device.

FR SET SNA1490 RSESSIONADD

This command adds a remote session.

Syntax: FR SET SNA1490 RSESSIONADD i dlci sap xx-xx-xx-xx-xx-xx

Parameter	Description
i	Interface number
dlci	DLCI number, specifies the virtual circuit
sap	SSAP of local station
xx-xx-xx-xx-xx-xx	MAC address of local station

FR SET SNA1490 RSESSIONDEL

This command deletes a remote session.

Syntax: FR SET SNA1490 RSESSIONDEL n

Parameter	Description
n	Number of the remote session (1 - 64)

FR SET SNA1490 SESSIONDELETE

This command deletes an active session.

Syntax: FR SET SNA1490 SESSIONDELETE i dlci n

Parameter	Description
i	Interface number
dlci	DLCI number
n	Session index in sessions list (1 - 61)

FR SET SNA1490 VCAUTOSENSE

This command sets the autosense mode on a specified virtual circuit. When the autosense mode is set to ON, the virtual circuit transmits only SNA frames until it receives a non–SNA frame. When the autosense mode is set to OFF, the virtual circuit transmits frames of any protocol requested.

Syntax: **FR SET SNA1490 VCAUTOSENSE i dlci {ON|OFF}**

Parameter	Description
i	Interface number
dlci	DLCI, specifies the virtual circuit
On **or** OFF	Sets autosense mode

FR SET VC SNA1490FEP

This command attaches a specified virtual circuit to a specified remote device. This command also registers the SNA protocol for use on this virtual circuit.

Syntax: **FR SET VC i dlci SNA1490FEP n**

Parameter	Description
i	Interface number
dlci	DLCI, specifies the virtual circuit
n	Index in the remote devices list

FR SET VC SNA1490DELETE

This command detaches a specified virtual circuit from a remote device. It also unregisters the SNA protocol for use on this virtual circuit.

Syntax: **FR SET VC i dlci SNA1490DELETE**

Parameter	Description
i	Interface number
dlci	DLCI, specifies the virtual circuit

FR SET SNA1490

This command is used to set the session mode for a specified remote device.

Syntax: **FR SET SNA1490 value n**

Parameter	Description
value	**SRSESSIONS** (for Source Route) **TRNSESSIONS** (for transparent) **AUTOSESSIONS** (for automatic)
n	Remote device index. Range: 0..15

FR SHOW VC

This command lists all Frame Relay virtual circuits on one or all interfaces.

Syntax: **FR SHOW VC i**

Parameter	Description
i	The interface number on which you want to display VCs. If no interface is specified, all virtual circuits on all interfaces will be displayed.

FR SHOW PORT

This command shows (for all FR ports on all FR interfaces) the port number, number of assigned VCs, number of active VCs, and port name.

Syntax: **FR SHOW PORT**

You can specify an interface i to display the above information for only that interface:

Syntax: **FR SHOW PORT i**

Parameter	Description
i	The interface number (optional) on which you want to display the port mapping.

FR SET SYS SRBAGE

This is a system wide parameter, which defines the age limit for entries in the Frame Relay Group Mode Source Route Bridging Cache.

Syntax: **FR SET SYS SRBAGE value**

Syntax: **(or FR SET SYS SRBCACHEAGE value**

Syntax: **or FR SET SYS CACHEAGE value)**

Parameter	Description
value	The cache aging time in seconds. Range: 30…255 (an integer value). Default: 120.

FR SRB SHOW

This Command displays the contents of the Frame Relay Group Mode Source Route Bridging Cache.

Syntax: **FR SRB SHOW**

FR SRB DEL

This Command manually deletes an entry from the Frame Relay Group Mode Source Route Bridging Cache.

Syntax: **FR SRB DEL lanId bridgeNum port**

Parameter	Description
lanId	The route descriptor LAN ID portion of the entry to delete.
bridgeNum	The route descriptor Bridge Number portion of the entry to delete.
port	The port number of the entry to delete.

FR SET PORT {FULLMESH | NONFULLMESH}

This Command configures the type of network access provided by a group mode port. This configuration is essential to prevent possible data loops for transparent bridged broadcast frames in a fully-meshed network, in the event of one or more VCs failing.

It also enables extended FR group mode Source Route bridging for non fully-meshed networks, whereby branch sites may intercommunicate via source routing.

Syntax: FR SET PORT p {FULLMESH | NONFULLMESH}

Parameter	Description
p	Index of the port.
FULLMESH	Use this option if the port accesses a fully-meshed FR network.
NONFULLMESH	Use this option if the port is a group mode port in a non fully-meshed (star topology) network.

FR SET AUTOMAP {ENABLE | DISABLE}

This command enables or disables automatic port creation for newly learned PVC. When new PVC is learned from the Frame Relay switch, new port will be created with given PVC mapped to it.

Syntax: FR SET AUTOMAP {ENABLE | DISABLE} ifc

Parameter	Description
ifc	interface number on which this setting will be made

14. GEN Commands

GEN INIT

This command initializes the tool. It must be issued on each XLT module that you want to participate in the test. During initialization the tool searches for either ethernet or token-ring LEC port. After the generator's default parameters are set, the tool is in the *IDLE* state.

Syntax: **GEN INIT**

The following messages can be displayed:

Message	Description
GenTaskInit: LEC port not found	The command fails, because there is no LEC port in the system.

GEN DEL

This command deactivates the generator. It can be issued only in *IDLE* or *INIT_DONE* states. It restores system settings altered by *GEN INIT*. When performed in *INIT_DONE* state, the *GEN CLEAR* command is issued automatically before. *GEN DEL A* additionally sends *test delete* multicast packet to other test modules.

Syntax: **GEN DEL [A]**

Field	Description
A	Message is sent to all the modules

GEN BEGIN

This command starts the advertising process. The XLT module is searching for active LAN interfaces, registers a manual test MAC addresses on each of them, sends *station advertisement* multicast packet and enters the *STARTING* state. After 2 second this state changes into *INIT_DONE*. Other modules in *IDLE* state perform the same functions as *GEN BEGIN* command when they receive the *station advertisement* packet.

From the advertising packets, the test modules in the *STARTING* state being to learn about other modules, remote stations MAC addresses and their source-route path. The MAC addresses are put into forwarding database as automatically learned and **the aging mechanism is turned off** to protect the addresses from being aged out. To discover the source-route path, the *station advertisement* packets are sent as SRBs. It is important to provide proper network conditions that allow to build a source-routing information in SRB packets (SR or SRT bridge mode).

Once the test modules reach the *INIT_DONE* state, you cannot add any new module or activate new LAN interfaces to participate in the test until *GEN CLEAR* or *GEN CLEAR A* command is issued.

Syntax: **GEN BEGIN**

GEN SHOW

This command displays current generator state, parameters and statistics.

Syntax: **GEN SHOW**

Example:

```
ILAN/XL(3)>gen show
LEC port #: 20 Token-Ring  seg# 014
SR mode: SRF
my_state: INIT_DONE
my_address: 00-aa-19-2c-49-02
trace: OFF
active lans: 1
test params: sec=1, tics=9, pkts=10, len=200
     : repeat 20 times, pause=10 sec
alloc failures: 0

Port  LOCAL ADDRreqrespque_err
----------------------------------------------------
  0 00-00-00-2c-49-02230229        1

remote modules : total # of stations: 2

#A  00-aa-19-28-49-02reqresplostque_err
-----------------------------------------------------------
1A1 00-00-00-28-49-0211511500
8C2 00-00-08-28-49-0211411221
```

In the above example the module has token-ring LEC port number 20 with segment number set to 014 hex. The generator works in source-routing mode (SRF) and it is in *INIT_DONE* state. The unicast address registered on **virtual port** is: 00-aa-19-2c-49-02 (token-ring format). Debugging information display is turned off (refer to *GEN TRACE* command). The module had only 1 active LAN interface during advertising process. Next generator's parameters are displayed (refer to GEN PAR and GEN REPEAT commands' description for more details). The *alloc failures* counter shows how many times a memory allocation process failed trying to allocate shared buffer memory for the test packet.

Next there are listed all active LAN ports, local MAC addresses assigned to them and corresponding statistics. The *req* counter informs how many test requests have been received for the address. The *resp* is a number of sent responses. The que_err is a number of responses' queuing errors on the virtual port.

Next the information about known remote stations is displayed. Data from the example screen informs that there is only one module visible for the test with the following unicast address: 00-aa-19-28-49-02, and bridge number equal to A (hex). Under the line there are listed all its local MAC addresses with LAN segment number (hex) on the beginning of the line. Corresponding statistics for the remote stations follow. The *lost* counter is always equal to (*req* - *resp*).

GEN CLEAR

This command removes all the data describing remote stations from the generator database and sets generator to *IDLE* state. *GEN CLEAR A* additionally sends *test reset* multicast packet to other test modules to clear their databases, too.

Syntax: **GEN CLEAR [A]**

Field	Description
A	Message is sent to all the modules

GEN PAR

This command sets generator's parameters and sends *test parameters* packet to all the test modules to synchronize the settings.

Syntax: **GEN PAR seconds [tics [packets [pkt_len]]]**

Parameter	Description
seconds	test duration
tics	timer period (1 tic = 10 ms),
packets	number of packets to transmit by timer routine each time it is invoked
pkt_len	data portion length of test packets. Value: 2 or more.

When the generator is started, it sends packets for a specified number of seconds. During the test a timer routine (*GenTask*) is invoked with a period `tics * 10 ms` and sends <packets> number of test frames.You can calculate the number of packets sent in one second: pps = (*packets* * 100) / *tics*. The generator sends one packet to each remote station in round robin scheme.

The value of *packets* should be kept low (3-9) because of the limited length of the receive queue on virtual port (20 or 64). User should look at que_err counters: any number of congested packets is a sign to decrease the parameter. The more modules participate in the test, the lower the value of *packets* should be (because there are more responses to send).

GEN REPEAT

This command sets a number of test repeats and a duration of pause between the tests (in seconds) and sends *test parameters* packet to all other modules.

Syntax: **GEN REPEAT times [pause]**

Field	Description
times	The number of test repeats
pause	Duration of pause between the tests (in seconds)

GEN START

This command starts a test and sends *test start* packet to all other test modules. It should be noted that the module sending test start command is responsible for issuing the stop command. This module is called *Test Master Module* (TMM). When the generator is running the *GEN SHOW* command, it displays on the TMM how long (in seconds) the test is going to last. Other modules display *INIT_DONE* state at this time. *GEN START L* (local) does not send *test start* packet to other test modules. This means that only the module on which the command was issued sends the *test request* packets.

Syntax: **GEN START [L]**

Field	Description
L	Only the local module will be affected

GEN STOP

This command stops the generator and sends a *test stop* packet to all other test modules. It can be issued on any test module. *GEN STOP L* does not send the *test stop* packet.

Syntax: **GEN STOP [L]**

Field	Description
L	Only the local module will be affected

GEN SRF

This command sets source-routing generator mode. In this mode all sent packets contain source-routing information. Management frames are sent as SRBs. Test packets are specifically routed frames (SRF). *GEN SRF A* sends the *set source-routing mode* command packet to other test modules.

Syntax: **GEN SRF [A]**

Field	Description
A	Message is sent to all the modules

GEN TRANSP

This command sets the transparent generator mode. In this mode all sent packets are transparent (except the *station advertisement* packet). *GEN TRANSP A* sends the *set transparent mode* command packet to other test modules.

Syntax: GEN TRANSP [A]

Field	Description
A	Message is sent to all the modules

GEN STCLR

This command clears all generator statistics. *GEN STCLR A* sends the *clear statistics* command packet to other test modules.

Syntax: GEN STCRL [A}

Field	Description
A	Message is sent to all the modules

15. Heterogeneous Bridging Console Commands

SHOW HB

This command is used to display Heterogeneous Bridging options.

Syntax: **SHOW HB {MCST | DNMC | GENMC | ALL}**

Variations	Description
SHOW HB MCST	Displays the Multicast Conversion Address table for Generic modes.
SHOW HB DNMC	Displays the Multicast Conversion Address table for DECnet modes.
SHOW HB GENMC	Displays the access state for the Multicast Conversion Address table for Generic modes.
SHOW HB ALL	Displays all of the Heterogeneous settings.

SET HB

This command is used to set a Heterogeneous Bridging option.

Syntax: **SET HB option**

- **option** can be any one of the parameters listed below.

Variations	Description
SET HB MCST ethadd tradd index	Sets the Multicast Conversion Address Table for Generic modes. The associated parameters are: Multicast Ethernet address (**ethadd**), Multicast Token Ring address (**tradd**), and the corresponding index in the multicast addresses conversion table for Generic Mode (**index**).
SET HB DNMC tradd index	Sets the Multicast Conversion Address Table for DECnet modes. The associated parameters are: Multicast Token Ring address (**tradd**), and the corresponding index in the multicast addresses conversion table for DECnet Mode (**index**).
SET HB GENMC	Enables Multicast conversions for Generic modes.
SET HB NOVELL [SR]	Enables Novell IPX Normal 802.3 conversion. You can optionally select to enable Source Routing (**SR**).
SET HB NOVELLP [SR]	Enables Novell IPX Portable Ethernet conversion. You can optionally select to enable Source Routing (**SR**).
SET HB NOVELL8022 [SR]	Enables Novell 802.2 frame type on Ethernet. You can optionally select to enable Source Routing (**SR**).
SET HB NOVELLSNAP [SR]	Enables Novell SNAP Ethernet conversion. You can optionally select to enable Source Routing (**SR**).
SET HB NVTRSNAP	Enables Novell IPX SNAP frames on a Token Ring.
SET HB NVTRFUNCT	Enables the use of Functional Addresses on a Token Ring.
SET HB GENIPX	Enables generic IPX conversions.

SET HB IPETH [SR]
Enables TCP/IP Ethernet conversion. You can optionally select to enable Source Routing (**SR**).

SET HB IP802 [SR]
Enables TCP/IP 802.3 conversion. You can optionally select to enable Source Routing (**SR**).

SET HB OS2 [SR]
Enables IBM OS/2 EE conversion. You can optionally select to enable Source Routing (**SR**).

SET HB XNS [SR]
Enables 3Com XNS conversion. You can optionally select to enable Source Routing (**SR**).

SET HB UBXNS [SR]
Enables Ugermann–Bass XNS conversion. You can optionally select to enable Source Routing (**SR**).

SET HB NBP [SR]
Enables 3Com NBP conversion. You can optionally select to enable Source Routing (**SR**).

SET HB VINES [SR]
Enables Banyan VINES IP conversion. You can optionally select to enable Source Routing (**SR**).

SET HB DECNET [SR]
Enables DECnet conversion. You can optionally select to enable Source Routing (**SR**).

SET HB GETH [SR]
Enables Generic Ethernet conversion. You can optionally select to enable Source Routing (**SR**).

SET HB G802 [SR]
Enables Generic Normal 802.3 IPX conversion. You can optionally select to enable Source Routing (**SR**).

SET HB GENETH
Enables the use of Ethernet-style broadcast address (FF-FF-FF-FF-FF-FF) when converting generic broadcast frames from Ethernet/802.3 networks to 802.5 networks.

SET HB TCPETH
Enables the use of Ethernet-style broadcast address (FF-FF-FF-FF-FF-FF) when converting TCP/IP broadcast frames from Ethernet/802.3 networks to 802.5 networks.

CLEAR HB

This command is used to clear a heterogeneous option. If the conversion option is entered without the optional parameter `**SR**', the command disables the conversion. If the command is entered with the optional parameter `**SR**', Source Routing for that conversion is disabled but the conversion remains enabled.

Syntax: CLEAR HB option

Variations	Description
CLEAR HB GENMC	Disables Multicast conversions for Generic modes.
CLEAR HB NOVELL [SR]	Disables Novell IPX Normal 802.3 conversion. You can optionally select to disable Source Routing (**SR**).
CLEAR HB NOVELLP [SR]	Disables Novell IPX Portable Ethernet conversion. You can optionally select to disable Source Routing (**SR**).
CLEAR HB NOVELL8022 [SR]	Resets Novell 802.2 frame type on Ethernet. You can optionally select to enable Source Routing (**SR**).
CLEAR HB NOVELLSNAP [SR]	Resets Novell SNAP Ethernet conversion. You can optionally select to enable Source Routing (**SR**).
CLEAR HB NVTRSNAP	Resets Novell IPX SNAP frames on a Token Ring.
CLEAR HB NVTRFUNCT	Resets the use of Functional Addresses on a Token Ring.
CLEAR HB GENIPX	Resets generic IPX conversions.
CLEAR HB IPETH [SR]	Disables TCP/IP Ethernet conversion. You can optionally select to disable Source Routing (**SR**).
CLEAR HB IP802 [SR]	Disables TCP/IP 802.3 conversion. You can optionally select to disable Source Routing (**SR**).
CLEAR HB OS2 [SR]	Disables IBM OS/2 EE conversion. You can optionally select to disable Source Routing (**SR**).

CLEAR HB XNS [SR]
Disables 3Com XNS conversion. You can optionally select to disable Source Routing (**SR**).

CLEAR HB UBXNS [SR]
Disables Ungermann–Bass XNS conversion. You can optionally select to disable Source Routing (**SR**).

CLEAR HB NBP [SR]
Disables 3Com NBP conversion. You can optionally select to disable Source Routing (**SR**).

CLEAR HB VINES [SR]
Disables Banyan VINES IP conversion. You can optionally select to disable Source Routing (**SR**).

CLEAR HB DECNET [SR]
Disables DECnet conversion. You can optionally select to disable Source Routing (**SR**).

CLEAR HB GETH [SR]
Disables Generic Ethernet conversion. You can optionally select to disable Source Routing (**SR**).

CLEAR HB G802 [SR]
Disables Generic 802.3 conversion. You can optionally select to disable Source Routing (**SR**).

CLEAR HB GENETH
Disables the use of Token Ring - style broadcast address (C0-00-FF-FF-FF-FF) when converting generic broadcast frames from Ethernet/802.3 networks to 802.5 networks.

CLEAR HB TCPETH
Disables the use of Token Ring - style broadcast address (C0-00-FF-FF-FF-FF) when converting TCP/IP broadcast frames from Ethernet/802.3 networks to 802.5 networks.

SET BRIDGE HBR

This command is used to globally enable/disable Heterogeneous Bridging. Globally disabling or enabling Heterogeneous Bridging affects only WAN and ABC interfaces.

Syntax: **SET BRIDGE HBR {ENABLE | DISABLE}**

16. IP RIP Commands

IPRIP ENABLE and IPRIP DISABLE

This command is used to enable and disable IP RIP router.

Syntax: **IPRIP {ENABLE | DISABLE}**

IPRIP RESET

This command is used to Reset the IP RIP Router.

Syntax: **IPRIP RESET**

IPRIP DOWN

This command is used to disable the IP RIP Router after all routes known by it are advertised as dead.

Syntax: **IPRIP DOWN**

IPRIP CONFIG

This command is used to display the IP RIP configuration.

Syntax: **IPRIP CONFIG**

Example:

```
                     GLOBAL IP RIP CONFIGURATION
IP RIP is ENABLED
IP RIP flush timer   = 120
IP RIP update timer  = 30
IP RIP invalid timer = 42
IP RIP default time to live= 32
                     IP RIP CONFIGURATION ON PORT 3
IP RIP on port 3 is DISABLED
IP RIP metric offset in  = 0
IP RIP metric offset out = 1
IP RIP rcv updates are ENABLED
IP RIP snd updates are ENABLED
IP RIP reduced advertising is DISABLED
IP RIP old reduced advertising is DISABLED
IP RIP direct broadcast is DISABLED
IP RIP split horizon is ENABLED
IP RIP poison reverse is DISABLED
                     IP RIP CONFIGURATION ON PORT 17
IP RIP on port 17 is DISABLED
IP RIP metric offset in  = 0
IP RIP metric offset out = 1
IP RIP rcv updates are ENABLED
IP RIP snd updates are ENABLED
IP RIP reduced advertising is DISABLED
IP RIP old reduced advertising is DISABLED
IP RIP direct broadcast is DISABLED
```

```
IP RIP split horizon is ENABLED
IP RIP poison reverse is DISABLED
                      IP RIP CONFIGURATION ON PORT 1
IP RIP on port 1 is ENABLED
IP RIP metric offset in  = 0
IP RIP metric offset out = 1
IP RIP rcv updates are ENABLED
IP RIP snd updates are ENABLED
IP RIP reduced advertising is DISABLED
IP RIP old reduced advertising is DISABLED
IP RIP direct broadcast is DISABLED
IP RIP split horizon is ENABLED
IP RIP poison reverse is DISABLED
```

IPRIP HELP

This command is used to display the available RIP commands.

Syntax: **IPRIP HELP**

IPRIP UPDATET

This command is used to set and display the Update Timer. The Update Timer is the rate at which RIP updates are sent.

Syntax: **IPRIP UPDATET n**

Parameter	Description
n	The Update Timer value in seconds. If you do not enter a value, the command response will display the current Update Timer value. The default is 30 seconds.

Note: The Update Timer value should be greater than Invalid, and Flush timers, or else inconsistencies in routing domain occur.

IPRIP FLUSHT

This command is used to set and display the Flush Timer. When the Invalid Timer expires, the route is removed from the routing tables after the Flush Timer has expired. This built in delay allows the neighbor routers to be notified that the route has been dropped.

Syntax: **IPRIP FLUSHT n**

Parameter	Description
n	The Flush Timer value in seconds. The Flush Timer should be set to three times the value of the Update Timer. If you do not enter a value, the command response will display the current Flush Timer value. The default is 90 seconds. Flush timer value lower than Update timer value is not accepted.

Note: All Flush Timers in the internet should be set to the same value.

IPRIP INVALIDT

This command is used to set and display the Invalid Timer. When an IP router adds a new route to its routing table, it starts the Invalid Timer for that route. The Invalid Timer is restarted each time the router receives a RIP message that advertises the route. If the route has not been advertised before the Invalid Timer expires, the route becomes invalid.

Syntax: **IPRIP INVALIDT n**

Parameter	Description
n	The Invalid Timer value in seconds. The Invalid Timer should be set to three times the value of the Update Timer. If you do not enter a value, the command response will display the current Invalid Timer value. The default is 90 seconds. The Invalid Timer value lower than Update Timer value is not accepted.

Note: All Invalid Timers in the internet should be set to the same value.

IPRIP DEFAULTTTL

This command is used to set and display the Default Time to Live (TTL) counter. The initial TTL counter is assigned to a DATAGRAM originating from the specific router. Any IP router along the DATAGRAM's path decrements the TTL counter when it processes the DATAGRAM. The DATAGRAM is discarded when the TTL counter reaches zero.

Syntax: **IPRIP DEFAULTTTL n**

Parameter	Description
n	is the TTL value in seconds. If you do not enter a value, the command response will display the current TTL value. The default is 32 seconds. Range: 0..255

IPRIP PORTENBL and IPRIP PORTDISBL

This command is used to enable and disable IP RIP on a port.

Syntax: **IPRIP {PORTENBL | PORTDISBL} n**

Parameter	Description
n	is the port on which you want to enable or disable RIP.

IPRIP TRACE

This command toggles between displaying input and output RIP Advertising Packets and not displaying RIP Advertising Packets.

Syntax: **IPRIP TRACE {ON | OFF}**

Example 1:

```
OUT [4:FFFFFFFFFFFF]    [002.000.000.000 02]
[004.000.000.000 02]
[005.000.000.000 02]    [011.000.000.000 01]
[014.000.000.000 01]
IN [4:360098504D9C]     [002.000.000.000 02]
[004.000.000.000 02]
[005.000.000.000 02]    [009.000.000.000 01]
[013.000.000.000 01]
```

Display Field	Description
IN/OUT	Indicates whether the packet is incoming or outgoing.
n:	The port number through which the packet is incoming or outgoing.
360098504D9C	The source MAC address for incoming packets or destination MAC address for outgoing packets.
[a.b.c.d n]	The IP network number, and the hops/delay of the advertised route.

Example 2:

RIP request:

```
OUT [0:6C00190002B3]   RIP 1 Request
IN [4:360098504D9C]   RIP 1 Request
```

Display Field	Description
IN/OUT	Indicates whether the packet is incoming or outgoing.
n:	The port number through which the packet is incoming or outgoing.
6C00190002B3	The source MAC address of the remote router for incoming packets and the MAC address of the interface through which the packet is outgoing.
[a.b.c.d n]	The IP network number, and the hops/delay of the advertised route.

IPRIP FORMAT

This command is used to switch between hexadecimal and decimal network formats. The format change is for display only.

Syntax: **IPRIP FORMAT**

IPRIP METRIC

This command is used to set and display the RIP metric.

Syntax: **IPRIP METRIC {IN | OUT} n offset**

Parameter	Description
IN	When the **IN** option is selected the command applies to incoming metrics.
OUT	When the **OUT** option is selected the command applies to outgoing metrics.
n	The port number (in the range from 0 to 128).
offset	The offset in the range from 1 to 16.

IPRIP UPDATE

This command is used for enabling or disabling the sending of updates on a specified port.

Syntax: **IPRIP UPDATE {ENABLE | DISABLE} n**

Parameter	Description
n	The port (in the range from 0 to 128) for which you want to enable or disable the sending of updates.

IPRIP LISTUPD

This command is used for enabling and disabling the listening to routing updates on a specified port.

Syntax: **IPRIP LISTUPD {ENABLE | DISABLE} n**

Parameter	Description
n	The port (in the range from 0 to 128) for which you want to enable or disable the listening of routing updates.

IPRIP SPECADVOLD

This command is used to enable and disable Smart Advertising in IP RIP in all XL versions, starting with 1.0. Smart advertising commands are to help support on-demand circuits (i.e., X.25 and ISDN) where periodic advertisements, when there have been no changes in the routing domain, should be suppressed. This implementation of smart advertising in RIP advertises the routing information across on-demand circuits several times, then stops without waiting for an acknowledgment from the other side of the link.

Syntax: **IPRIP SPECADVOLD {ENABLE | DISABLE} n**

Parameter	Description
n	The port (in the range from 0 to 128) for which you want to set the Smart Advertising algorithm.

IPRIP SPECADVER

This command is used to enable and disable Smart Advertising for XL version 3.0 and later. With this implementation, advertising across an on-demand circuit is stopped only if an acknowledgment is received from the other side of the link.

Syntax: **IPRIP SPECADVER {ENABLE | DISABLE} n**

Parameter	Description
n	The port (in the range from 0 to 128) for which you want to enable or disable the sending of updates.

IPRIP POISONREV

This command is used for enabling and disabling poison reverse on a port.

Syntax: **IPRIP POISONREV {ENABLE | DISABLE} n**

Parameter	Description
n	The port (in the range from 0 to 128) for which you want to enable or disable poison reverse.

IPRIP SHORIZON

This command is used for enabling and disabling split horizon on a port.

Syntax: **IPRIP SHORIZON {ENABLE | DISABLE} n**

Parameter	Description
n	The port (in the range from 0 to 128) for which you want to enable or disable split horizon.

IPRIP DIRECTBC

This command is used for

setting the type of IP broadcast address used as IP destination address in IP RIP broadcast advertisements.

Syntax: **IPRIP DIRECTBC {ENABLE | DISABLE} n**

Parameter	Description
ENABLE	The direct broadcast address on the network port <n> is connected to is used
DISABLE	The limited broadcast address is used
n	The port (in the range from 0 to 128) for which you want to enable or disable direct broadcasts.

IPRIP FILTERS ADD

This command is used to define a new RIP filter. Use RIP filters to control how the router advertises routing table to, and learns routing tables from, other RIP routers.

Syntax: **IPRIP FILTERS ADD <IP address> <IP mask> {ACCEPT|REJECT}**

Parameter	Description
IP address	The IP address used with the IP MASK to specify the IP address(es) the filter will be applied to. Only one filter can be defined for each IP address.
IP mask	Specifies the portion of the IP address of incoming and outgoing packets that the router should use to determine whether to apply a filter. (See the Olicom Reference Guide.)
ACCEPT	Specifies that advertising and learning on addresses designated by the IP ADDRESS and the IP MASK is enabled. When a filter set to ACCEPT is applied to a particular port, the filter is automatically applied to all other ports in REJECT mode.
REJECT	Specifies that advertising and learning on addresses designated by the IP ADDRESS and the IP MASK is disabled. When a filter set to REJECT is applied to a particular port, the filter is automatically applied to all other ports in ACCEPT mode.

IPRIP FILTERS DEL

This command is used to delete a RIP filter. Use RIP filters to control how the router advertises routing table to, and learns routing tables from, other RIP routers.

Syntax: **IPRIP FILTERS DEL <IP address>**

Parameter	Description
IP address	The IP address used to designate the RIP filter. Only one RIP filter can be defined for each IP address, so naming the address names the associated filter.

IPRIP FILTERS APPLY and IPRIP FILTERS REMOVE

This command is used to apply or remove a RIP filter that has already been defined to a particular port in a particular mode (In or Out). Use RIP filters to control how the router advertises routing table to, and learns routing tables from, other RIP routers.

Syntax: **IPRIP FILTERS {APPLY|REMOVE} {IN|OUT} <IP address> <port>**

Parameter	Description
APPLY	Applies a specified filter to a specified port in either IN or OUT mode.
REMOVE	Ends the application of a specified filter to a specified port.
IN	Indicates that the specified filter will only apply to incoming RIP advertisements.
OUT	Indicates that the specified filter will only apply to outgoing RIP advertisements.
IP ADDRESS	Specifies the filter to be applied or removed. You can only define one filter for each IP address.
Port	An integer that specifies the router port number the filter will be applied to or removed from.

IPRIP FILTERS SHOW

This command is used to display all defined RIP filters. Use RIP filters to control how the router advertises routing table to, and learns routing tables from, other RIP routers.

Syntax: **IPRIP FILTERS SHOW**

17. IP Router Commands

IPR LOCALCFG

This command is used to display the port configuration status.

Syntax: **IPR LOCALCFG n**

Parameter	Description
n	Port (range: 0..7) for which you want to display the status.

This command displays the following:

```
ipr localcfg
Port 0,  State: ENABLED, Configuration status: OK
Port 1,  State: ENABLED, Configuration status: OK
```

IPR ADDRESS

This command is used for setting an IP address for a specified port.

Syntax: **IPR ADDRESS n ipaddress**

Parameter	Description
n	Port for which you want to set an IP address.
ipaddress	IP address in dotted decimal notation.

IPR MASK

This command is used for setting an IP routing mask for a specified port.

Syntax: **IPR MASK n ipmask**

Parameter	Description
n	Port for which you want to set an IP mask.
ipmask	IP mask in dotted decimal notation.

IPR NBRIP

This command is used to set the Point to Point neighbor address, which is used to authenticate protocol data exchange over numbered point-to-point links.

Syntax: **IPR NBRIP n address**

Parameter	Description
n	Port (range: 0..7) for which you want to set the address.
address	The IP address of the neighbor.

IPR TYPE

This command is used to change the port type.

Syntax: **IPR TYPE {BC | PTOP} n**

Parameter	Description
BC	Sets the port type to broadcast. This setting is accepted on any kind of interface.
PTOP	Sets the port type to Point to Point.This setting is not accepted on LAN interfaces.
n	Port (range: 0..7) for which you want to change the type.

IPR SRB

This command is used to enable and disable Source Routing mode on a specified port.

Syntax: **IPR SRB {ENABLE | DISABLE} n**

Parameter	Description
n	Port (range: 0..7) for which you want to enable or disable Source Routing.

IPR PROXYARP

This command is used for enabling and disabling proxy ARP on a specified port. Proxy ARP is useful when the router receives an ARP Request from one network that is destined to a host on another network. If the router port has Proxy ARP enabled, and it knows the route to the destination host, it sends an ARP Reply to the sender with its own physical address. The sender then sends all packets destined for that host to this router port's physical address. By default, this feature is enabled.

Syntax: **IPR PROXYARP {ENABLE | DISABLE} n**

Parameter	Description
n	Port (range: 0..7) for which you want to enable or disable proxy ARP.

IPR ICMPREDIR

This command is used for enabling and disabling the issuing of ICMP redirect messages.

Syntax: **IPR ICMPREDIR {ENABLE | DISABLE} n**

Parameter	Description
n	Port (range: 0..7) for which you want to enable or disable the issuing of ICMP redirect messages.

IPR ICMPMESS

This command is used for enabling and disabling the generating of ICMP unreachable messages on a specified port. Unreachable messages include: destination unreachable, fragmentation needed and DF set, and source route failed.

Syntax: **IPR ICMPMESS {ENABLE | DISABLE} n**

Parameter	Description
n	Port (range: 0..7) for which you want to enable or disable the generating of ICMP unreachable messages.

IPR ICMPMASK

This command is used for enabling and disabling the sending of ICMP reply messages over the specified port.

Syntax: **IPR ICMPMASK {ENABLE | DISABLE} n**

Parameter	Description
n	Port (range: 0..7) for which you want to enable or disable the sending of ICMP reply messages.

IPR SNAP

This command is used to enable and disable 802.3 or Ethernet format on the specified port.

Syntax: **IPR SNAP {ENABLE | DISABLE} n**

Parameter	Description
n	Port (range: 0..7) for which you want to enable or disable Ethernet format.

IPR MTU

This commands sets the MTU on a specified port.

Syntax: **IPR MTU n mtu**

Parameter	Description
n	This is the port (in the range from 0 to 7) for which you want to set the MTU
mtu	The MTU size

IPR PORT

This command is used for enabling and disabling of IP routing on a specified port.This command only sets the administrative status of the port; to make IP active on a port the interface has to be active as well.

Syntax: **IPR PORT {ENABLE | DISABLE} n**

Parameter	Description
n	Port (range: 0..7) for which you want to enable or disable IP routing.

IPR CONFIG

This command is used to display the IP router configuration.

Syntax: **IPR CONFIG**

This command displays the following:

Example:

```
ILAN / XL (1)>IPR CONFIG
IP Router is disabled
Address filters for IP router : ENABLED
Smart filters fo IP router : ENABLED
```

Example:

```
ILAN / XL (1)>IPR CONFIG
IP Router is enabled
Address filters for IP router : ENABLED
Smart filters fo IP router : ENABLED

Port: 0, Addr: 132.177.118.036, Mask 255.255.255.240, ENA-
BLED, ETH,
  MAC: 36-00-98-93-0e-a0- , Format:  ETHER II,  Mode:TRANS-
PARENT,
  Dir. Broad: ON,   Proxy ARP: ON, Old Format BC: OFF,
  ICMP Redirect: ON,  ICMP Unreachable: OFF, ICMP Mask Reply:
OFF
..MTU: 1514,   (14 bytes reserved for MAC/LLC header)
  Port State: UP
Port: 2, Addr: 132.177.118.100, Mask 255.255.255.240, ENA-
BLED, WAN,
  MAC: 36-00-98-93-0e-a1- , Format:  ETHER II
  Dir. Broad: ON,   Proxy ARP: ON, Old Format BC: OFF,
  ICMP Redirect: ON,  ICMP Unreachable: OFF, ICMP Mask Reply:
OFF
..MTU: 8190,   (14 bytes reserved for MAC/LLC header)
  Port State: DOWN
```

Display Field	Description
IP Router	The state of the router (either enabled or disabled)
Address filters...	Indicates whether the address and smart filters are enabled
Smart filters...	
Port:	Port number.
Addr:	IP address assigned to this port.
Mask	IP mask for this port.
ENABLED/DISABLED	Whether IP routing is administratively enabled or disabled on this port.
type	Port type.
MAC	Physical address of the port.
Format:	Whether the format is Ethernet II, 802.3, 802.5, IP_STD_MODE
Mode	Bridging mode enabled.
Dir. Broad	Whether directed broadcasting is enabled on this port.
Proxy ARP	If this is enabled, router is acting as Proxy ARP server on this port
Old Format BC	If this is enabled, the convention that uses 0s to indicate broadcast is used. Otherwise, the convention that uses 1s is used.
ICMP Redirect	If this is enabled, the IP router will generate ICMP redirect messages over this port.
ICMP Unreachable	If this is enabled, the IP router will generate the ICMP unreachable messages for this port.
ICMP Mask Reply	If this is enabled, the IP router will send the ICMP Mask Reply messages over this port.
MTU	The MTU size.
Port State	The operational state of this port

Note: For WAN interfaces, the Point–to–Point Neighbour (PTOP NBr) address can also be displayed.

IPR SRHEADER

This command is used to accept or reject IP DATAGRAMS with the Source Routing Header option.

Syntax: **IPR SRHEADER {ENABLE | DISABLE}**

IPR DFLTGTW

This command is used to enable and disable the default gateway. When it is enabled, the router advertises itself (in routing protocol advertisements) as a default gateway. Other routers (when there is not enough information to forward data to a particular IP destination) forward packets to the router acting as a default gateway; if there is no router acting as default gateway the data packet will be rejected.

Syntax: **IPR DFLTGTW {ENABLE | DISABLE}**

IPR SPLIT

This command is used to enable or disable splitting of traffic when there are several (up to 3) equally good routes to a particular IP destination. Splitting is done per packet in a round-robin fashion

Syntax: **IPR SPLIT {ENABLE | DISABLE}**

Parameter	Description
ENABLE	All routes will be used while forwarding IP datagrams, in a "round-robin" fashion; splitting is done per IP datagram (not per session).
DISABLE	The first route on the list will be used to forward.

IPR ADDNATURAL

This command is used to enable or disable the automatic addition of a natural network entry to the routing table when inserting another (sub)network entry. This is to support RIP protocol over unnumbered point-to-point links, when interoperating with OSPF's routing domain, especially configured classless.

Syntax: **IPR ADDNATURAL {ENABLE | DISABLE}**

IPR ARPTIMEOUT

This command is used to set and display the ARP timeout for an IP router.
If, before the timeout period expires, no ARP request have been received for the specified IP address, the entry is removed from the ARP table.

Syntax: **IPR ARPTIMEOUT [hh[:mm[:ss]]]**

Parameter	Description
hh:mm:ss	You can enter a value for the ARP timeout in hours, or hours and minutes, or hours, minutes, and seconds. If you do not enter a value, the command response will display the current timeout value. The default is 2 hours.

IPR SET GADDRESS

This command is used to set the global IP address. This is to address the device as an IP host. In addition, with routing enabled, and IP global address configured, routing protocols will advertise the global address as a host route, if configured to do so.

Syntax: **IPR SET GADDRESS address**

Parameter	Description
address	The global IP address.

IPR SET GMASK

This command is used to set the global IP mask.

Syntax: **IPR SET GMASK mask**

Parameter	Description
mask	The global IP mask.

IPR SET GATEWAY

This command is used to set the default gateway IP address. When IP routing disabled, the device acting as an IP host will use configured default gateway to answer IP traffic addressed to it.

Syntax: **IPR SET GATEWAY address**

Parameter	Description
address	The default gateway IP address.

IPR CHKSUM

This command lets you enable/disable computing the IP header checksum for incoming packets.

Syntax: **IPR CHKSUM {ENABLE|DISABLE}**

IPR ROUTER

This command is used to enable and disable IP routing. You must also enable IP over specific ports for the device to function as an IP router. The interfaces also have to be active for IP to be active on ports; IP commands only tell you the administrative status of IP router software.

Syntax: **IPR ROUTER {ENABLE | DISABLE}**

IPR SHOW IPTREE

This command displays the routing table in a B–Tree and shows the pointers to the more general route.

Syntax: **IPR SHOW IPTREE**

Display Field	Description
a.b.c.d e.f.g.h	IP address (a.b.c.d) and mask (e.f.g.h) for the route.
Up	Following the address and mask, a pointer (Up) to the more general route, which is another node in the tree.
(x)	Last in the row is an indication of the node balance: (=) the node is balanced (R) the right subtree is higher (L) the left subtree is higher

Example:

```
132.177.118.32 255.255.255.255 Up: 132.177.118.32
255.255.255.240 (=)

132.177.118.32 255.255.255.240 Up: 132.177.0.0 255.255.0.0
(L)

132.177.118.16 255.255.255.240 Up: 132.177.0.0 255.255.0.0
(=)

132.177.118.15 255.255.255.255 Up: 132.177.118.0
255.255.255.240 (=)

132.177.118.4 255.255.255.255 Up: 132.177.118.0
255.255.255.240 (=)
```

IPR INITRTAB

This command initializes the routing table. This means that the routing table is emptied after this operation is performed.

Syntax: **IPR INITRTAB**

IPR MEMORY RTAB

This command sets the routing table size (in number of entries). The setting becomes active after router restart (SBOOT).

Syntax: **IPR MEMORY RTAB size**

Parameter	Description
size	Routing Table size, in number of entries

IPR MEMORY NH

This command sets the next hop table size, in number of entries. It becomes active after the router restart (SBOOT).

Syntax: **IPR MEMORY NH size**

Parameter	Description
size	Next Hop table size, in number of entries

IPR SHOW STATIC

This command shows the static routes as defined in the static routes table. The defined static routes do not automatically become active (i.e., put into the routing table), but only when defined next hops are active (if the router is able to forward IP traffic using the static route's definition).

Syntax: **IPR SHOW STATIC**

IPR STATIC NEW

This command adds a new static route to the routing table. It will be inserted into the routing table when the router knows how to forward packets using the defined next hops (i.e., next hops become active). The number of static route definitions is limited to 100. Static route definition will be accepted only when the IP router is enabled.

Syntax: **IPR STATIC NEW net mask pref metric nh1 [nh2] [nh3]**

Parameter	Description
net	The target network IP address.
mask	The target network IP mask.
pref	Preference for this route. The lower the preference value, the better the route. Predefined preferences: OSPF internal1 RIP 66 OSPF Ext 1 80 OSPF Ext 2 144 SNMP Static Routes 253 Discard router 254 Unpref 255 metricThe metric for this route.
nh1, nh2, nh3	Next hops for this route.The next hop values depend on the type of the IP port the next hop is bound to: • Broadcast port the next hop value should be the address of the IP network the port belongs to • Point-to-point numbered port the next hop value should be the configured point-to-point neighbor IP address • Point-to-point unnumbered port the next hop value should be the IP port index (i.e. for port 3, starting from 0, the next hop would be 0.0.0.3)

When the route is put into the routing table, the next hops will be put there in the same order as in this definition.

IPR STATIC DEL

This command removes static routes from the routing table; if they are in the routing table they will be removed only as the next hops become inactive (port goes down).

Syntax: **IPR STATIC DEL address mask pref**

Parameter	Description
address	The IP address of the target network.
mask	The mask for the target network.
pref	The preference for this route.

IPR SHOW NH

This command shows the next hops.

Syntax: **IPR SHOW NH**

This command displays the following:

NH address: 132.177.0.0 NH type: 1 ndx: 3 refcnt:1

```
NH address: 132.177.0.0 NH type: 1 ndx: 8 refcnt: 1
```

Display Field	Description
NH address	IP address of the next hop.
NH type	How the next hop was learned: 1 (01h) numbered PTOP – IP address is not 0.0.0.0 2 (02h) static remote route 4 (04h) unnumbered PTOP – IP address is 0.0.0.0 8 (08h) PTOP static configured neighbor 16 (10h) OSPF neighbor, MC or PTOP numbered 32 (20h) OSPF neighbor, PTOP unnumbered 64 (40h) ISPF virtual neighbor 128 (80h) EGP neighbor 256 (100h) RIP neighbor 512 (200h) RIP unnumbered 1024 (400h) BGP neighbor ndx The index number of the port through which the next hop is reached.
refcnt	The number of routes that reference the next hop in the routing table. When this value reaches 0, the next hop is removed.

IPR OLDFORMAT

This command is used for enabling and disabling the use of the old format for broadcasts on a specified port. When this option is enabled, zeros are used to indicate broadcast and when it is disabled, ones are used to indicate broadcasts.

Syntax: **IPR OLDFORMAT {ENABLE | DISABLE} n**

Parameter	Description
n	Port (range: 0..7) for which you want to enable or disable the use of the old format for broadcasts.

IPR BC LIMITED

To determine how to treat limited broadcasts

Syntax: **IPR BC LIMITED {ALL | BOOTP | NONE}**

Option	Description
ALL	Forward all limited broadcasts.
BOOTP	Forward only BOOTP limited broadcasts.
NONE	Do not forward limited broadcasts:

Also, to determine how limited broadcasts will be forwarded:

Syntax: **IPR BC LIMITED how**

how	Description
HELPER	Use helper addresses to forward limited broadcasts. To configure helper addresses on the port receiving limited broadcast packets.
ST	Use spanning tree to forward limited broadcasts.

IPR PORT HELPER

To define the helper address on the specified port, use:

Syntax: IPR PORT HELPER port address

The helper address may be any valid IP address, including a directed broadcast address. It is possible to have several helper addresses on a given port. In such a case a copy of a broadcast is sent to each of these helper address. If using helper addresses is enabled but there are no helper addresses defined on a port then the port is excluded from forwarding broadcasts.

To delete the helper address on a specified port, use:

Syntax: IPR PORT HELPER port address DEL

IPR BC DIRECTED

This command determines how directed broadcasts will be treated.

Syntax: IPR BC DIRECTED {RPF | ST | NONE}

Option	Description
RPF	Uses reverse path forwarding to forward directed broadcasts.
ST	Uses spanning tree to forward directed broadcasts.
NONE	Globally disables the forwarding of directed broadcasts.

IPR BROADCAST

To enable/disable forwarding directed broadcasts via a specified port, use:

Syntax: IPR BROADCAST {ENABLE | DISABLE} n

Parameter	Description
n	Port (range: 0..7) for which you want to enable or disable directed broadcasts.

IPR PORT BCSRV

To enable/disable the broadcast server feature on the Frame Relay Group Mode port, use:

Syntax: IPR PORT BCSRV port {ENABLE | DISABLE}

This command applies to both kinds of broadcasts (limited and directed). It also doesn't depend on the method used to forward broadcasts. However it is intend for star topologies only - using it in fully-meshed or having additional PVCs (relative to the star topology) configurations will lead to broadcast loops.

IPR BC SHOW

This command displays all IP broadcasts settings.

Syntax: IPR BC SHOW

IPR FILT

To enable or disable both Address Filters and Smart Filters on an IP router:

Syntax: IPR FILT {SMON | SMOFF | ADDRON | ADDROFF}

Parameter/Option	Description
SMON	Enables smart filters.
SMOFF	Disables smart filters.
ADDRON	Enables address filters.
ADDROFF	Disables address filters.

All filters are enabled by default. If they are not used, they should be disabled not to affect the IP performance.

IPR SHOW ATTAB

To display the ARP cache, use:

Syntax: **IPR SHOW ATTAB**

IPR SHOW ARPSTAT

This command displays the ARP statistics.

Syntax: **IPR SHOW ARPSTAT**

IPR CLARP

To clear the ARP cache, use:

Syntax: **IPR CLARP**

IPR PING

To send an IP ping, use:

Syntax: **IPR PING [addr [cnt [size]]]**

To stop pinging, use this command without any parameters.

Parameter	Description
addr	Destination address.
cnt	Number of packets to send.
size	Packet size.

TELNET ENABLE and TELNET DISABLE

To enable/disable the TELNET subsystem use the command below. By default, after a master reset, Telnet is disabled and all requests to establish a Telnet session are refused.

Syntax: **TELNET {ENABLE | DISABLE}**

TELNET PASSWORD

This command changes the Telnet password - the user is prompted for a new password. By default, after a master reset, there is no password. The maximum password length is 12 characters, none of which may be whitespace (blanks or tabs); the password is not case sensitive. Do not confuse the Telnet password with any other XL passwords.

Syntax: TELNET PASSWORD

The following command deletes the password previously set by the TELNET PASSWORD command. It sets the password length to 0.

Syntax: TELNET PASSWORD DELETE

TELNET IDLE

This command toggles the inactivity timer for the Telnet session from which the command is called. By default, unused sessions are automatically closed after 5 minutes.

Syntax: TELNET IDLE

TELNET EOL

This command toggles between the CR, LF and CR, NUL conversion for the Telnet session which the command is called from. By default CR, LF is generated as a new line sequence.

Syntax: TELNET EOL

TELNET WHO

To view all active Telnet connections, use:

Syntax: TELNET WHO

For each session the following information is displayed:

- local IP address, local socket number, local Telnet options;
- remote IP address, remote socket number, remote Telnet options;
- whether the idle timer is enabled, whether the EOL is enabled.

IPR SHOW RTAB

This command displays the router's routing table. It displays 10 entries per command. If the optional parameters are provided, the command displays only the routing information for the specified node.

Syntax: IPR SHOW RTAB [address mask | STOP]

This command displays the following information:

```
Net:132.177.118.0 Mask:255.255.255.240
  Proto:LOCAL  Fwd Flags: 0x2 Pref:0 Metric:0
  NH: 132.177.118.0
  Proto:OSPF  Fwd Flags: 0x2 Pref:1 Metric:1
  NH: 132.177.118.0
```

Display Field	Description
Net	IP address
Mask	IP mask
Proto	Protocol (owner: LOCAL, REMOTE, OSPF, RIP, etc.)
STOP	Use this option to start displaying from the beginning of the table
Fwd Flags	When a route is being looked–up in the routing table, the flag is used to quickly determine the type of route. This flag can indicate how the route is connected or the type of broadcast address. The flag also indicates routes flag as discard. Packets sent to routes flagged as discard will not be forwarded. A route will be flagged as discard if it is no longer active. Discard can also apply to a route that does not exist in the routing domain but is stored in the routing table because it defines a net–range. The flags are as follows: 0x0001 remote route that is not directly reachable 0x0002 directly connected network 0x0004 address of port on this router 0x0020 static discard 0x0040 OSPF discard 0x0080 RIP discard 0x0100 Ones net broadcast 0x0200 Ones subnet broadcast 0x0400 Zeros net broadcast 0x0800 Zeros subnet broadcast 0x1000 RIP export 0x2000 Remote net broadcast

Pref	Preference for this route. The lower the preference value, the better the route. Default preferences: OSPF internal 1 RIP 66 OSPF Ext 1 80 OSPF Ext 2 144 SNMP Static Routes 253 Discard router 254 Unpref 255
Metric	Metric value for the route.
NH	List of next hops.

IPR BESTMATCH

This command finds the best match route for the specified address. The information displayed is the same as for the IPR SHOW RTAB command.

Syntax: **IPR BESTMATCH address**

Parameter	Description
address	is the IP address for which you want to find the best match route.

Example:

```
ipr bestmatch 132.177.118.69

Searching for 132.177.118.69 - found:

Net:132.177.118.64 Mask:255.255.255.224

  Proto:OSPF Fwd Flags:0x1 Pref:1 Metric:2

  NH: 132.177.118.101
```

IPR SHOW IPNODE

This command displays information about the specified node:

Syntax: **IPR SHOW IPNODE address mask**

Parameter	Description
address	IP address of the node.
mask	IP mask for the node.

Example:

```
the node: 132.177.125.0 255.255.255.0 (=) Up Ptr: 132.177.0.0
255.255.0.0
parent  : 132.177.124.0 255.255.255.0 (=) Up Ptr: 132.177.0.0
255.255.0.0
```

Display Field	Description
the node	IP address and mask of this node.
parent	IP address and mask of the parent of this node.
Up Ptr	A pointer to the more general route which is another node in the tree.
(x)	Information about whether the node is balanced. One of the following will be displayed:
=	The node is balanced
R	The right subtree is higher
L	The left subtree is higher

IPR SHOW LOCAL

This command shows the local protocol thread.

Syntax: **IPR SHOW LOCAL**

IPR SHOW REMOTE

This command shows the remote protocol thread, i.e., static routes that have been defined and are active (present in the routing table).

Syntax: **IPR SHOW REMOTE**

IPR SHOW IPSTAT

To display IP statistics, use:

Syntax: **IPR SHOW IPSTAT**

IPR SHOW ICMPSTAT

This commands displays ICMP statistics.

Syntax: **IPR SHOW ICMPSTAT**

IPR SHOW MEM

This command shows memory information.

Syntax: **IPR SHOW MEM**

This command displays the following:

```
Next Hops’ partition
  Total: 200 Used 31 Peak: 31
  Statistics: allocated 36 times, freed 5 times
Routing Table’s partition
  Total: 500Used: 34 Peak: 34
  Statistics: allocated 34 times, freed 0 times
Free Dynamic Memory: more than 3235 kB
```

The following fields apply to the Next Hops Table and the Routing Table.

Display Field	Description
Total	Number of table entries allocated.
Used	Number of table entries allocated (currently used).
Peak	Maximum number of table entries used at one time.
Statistics	Number of table entries that have been used and the number that have been freed (no longer being used).
Free Dynamic Memory	KB of memory that is not currently allocated.

IPR UNIQMAC

This command enables or disables unique MAC address on an IP port.

Syntax: **IPR UNIQMAC {ENABLE | DISABLE}** ***p***

Parameter	Description
p	The IP port

IPR SPANTREE

Enables and disables spanning tree to forwarding IP Broadcasts.

Syntax: **IPR SPANTREE {ENABLE | DISABLE}**

IPR ABC RING

Enables and disables 802.5 encapsulation on ABC port.

Syntax: **IPR ABC RING {ENABLE | DISABLE} p**

Parameter	Description
p	The port number

IPR ENCAP {ETH | TR}

This command sets encapsulation type (Ethernet or Token Ring) for IP router port. This means that IP router transmits/receives frames with the specified format. You can use this command on IRL and virtual port.

Syntax: **IPR ENCAP {ETH | TR} p**

Parameter	Description
ETH	Ethernet encapsulation type
TR	Token Ring encapsulation type
P	The port number

IPR ADDARP

Adds entry to ARP cache.

Syntax: **IPR ADDARP addr p <ATM | ETH | 802 | FR> <mac level addr> [S]**

Parameter	Description
addr	IP address
p	The port number associated with ARP entry
S	Static entry
mac level addr	for ETH/802 types it is a MAC address, for FR type it is a DCLI address, and for ATM type it is an ATM address

IPR ADDARP ATM

Creates a static ATM ARP.

Syntax: **IPR ADDARP addr p ATM [CIRCUIT vpi vci]**

Parameter	Description
addr	IP address
p	port number associated with ARP entry
S	Static entry
mac level addr	for ETH/802 types it is a MAC address, for FR type it is a DCLI address, and for ATM type it is an ATM address

IPR SECADD

Creates a new secondary address.

Syntax: **IPR SECADD n addr mask**

Parameter	Description
n	The port on which the secondary port is to be defined
addr	The secondary IP address
mask	The secondary IP mask

IPR SECDEL

Deletes a given secondary address.

Syntax: **IPR SECDEL n addr mask**

Parameter	Description
n	The port on which the secondary port is to be defined
addr	The secondary IP address
mask	The secondary IP mask

IPR SECPRI

Changes a given secondary address into a primary one.

Syntax: **IPR SECPRI n addr mask**

Parameter	Description
n	The port on which the secondary port is to be defined
addr	The secondary IP address
mask	The secondary IP mask

IPR BHOPS

Sets the maximum number of hops for bootp requests.

Syntax: **IPR BHOPS n**

Parameter	Description
n	The maximum number of hops

IPR SHOW POLICY

This command displays policies.

Syntax: **IPR SHOW POLICY policy-id**

Parameter	Description
policy-id	The policy identifier. If you use this parameter, only the specified policies will be displayed. If you omit this parameter, all currently defined policies will be displayed.

IPR POLICY NEW {ACCEPT | REJECT}

This command creates a new basic policy. Each basic policy may contain three things:

- information whether a specified route is accepted or not;
- the specification of the route(s);
- and optionally some features which the route should receive when accepted (for example the preference for the route installed in the routing table)

A policy is identified either by its name or a numeric identifier assigned during creation. The **IPR POLICY NEW** command displays the name and this number on a console after successful operation.

Syntax: **IPR POLICY NEW [name] {ACCEPT | REJECT} route-specification [n]**

Parameter	Description
name	The policy name
ACCEPT	Specifies the route as accepted
REJECT	Specifies the route as rejected
route-specification	describes features the route should have to match the policy. See the table below.

n	optional route parameters:
	
	`USING METRIC {metric | PROTO}`
	This parameter specifies a metric value a route is installed with in the routing table or advertised with by another protocol. PROTO is the original metric value. If it is not specified, the default value for a given protocol is used.
	`USING PROTOSPEC1 value`
	`USING PROTOSPEC2 value`
	Some routing protocols may include additional information in their messages. The PROTOSPEC1 is used to specify an OSPF tag the route is advertised with (8-digit hex. number). The PROTOSPEC2 allows you to determine the route's metric type (1 or 2 to select metric type-1 or type-2).
	
	`USING PREFERENCE preference`
	If you want to use a policy to import a route you can specify a preference which the route receives during its insertion into the routing table:

Route specification requires at least one of the following phrases:

Route Specification	Description
protocol1 [protocol2 ...] ROUTES	specifies the protocol(s) a route should be derived from to match the policy. The protocol may be: LOCAL, REMOTE, SPECIAL, OSPF, OSPFEXT, RIP, BGPINT, BGPEXT, BGPAGGR or ALL (it means that any protocol can be used).
FROM RANGE net mask	specifies the net range a route should belong to match the policy. For mask 255.255.255.255 the route's network should be exactly the same as the net to satisfy the policy.
WITH NH ip-address	specifies the next-hop a route should have to match the policy. Notice that for RIP protocol, such next-hop is identical to the address of the router where this route has been learned from.

For RIP routes the following options may be used:

FROM PORT port-number
: specifies port the RIP route should be learned from to match the policy. This option is mainly used to define an export policy and allows protocol instance to advertise considered RIP route (already present in the routing table) only if it has been learned through the specified port.

For BGPINT or/and BGPEXT routes the following options are available:

FROM AS as-number
: specifies the neighboring autonomous system number a route should be received from to match the policy

FROM HOME_AS as-number
: specifies the number of an AS which a route must be originated from to match the policy

WITH ORIGIN {EGP | IGP | OTHER}
: specifies the origin a route should have to match the policy

For OSPF routes (OSPF or/and OSPFEXT) the following options may be used:

FROM OSPF_INSTANCE instance-id
: specifies the OSPF instance identifier where a route should be derived from to match the policy.

For OSPFEXT routes, the following option is available.

WITH OSPF_TAG tag
: specifies the tag value present in OSPF external advertisements which a route should have to satisfy the policy. The tag should be given as a hexadecimal number.

IPR POLICY BUILD FROM

This command creates a new complex policy. Complex policy is several basic policies grouped together for a convenient use.

Syntax: **IPR POLICY BUILD [name] FROM policy-id1 policy-id2 ...**

Field	Description
name	The policy name
policy-id1, policy-id2…	The identifier(s) of previously defined basic policies.

IPR POLICY DELETE

This command deletes a specified policy.

Syntax: **IPR POLICY DELETE policy-id**

Field	Description
policy-id	The identifier of a previously defined basic or complex policy.

IPR POLICY NAME

This command changes the name of the specified policy.

Syntax: **IPR POLICY NAME policy-id new-name**

Field	Description
policy-id	The identifier of a previously defined basic or complex policy
new-name	The new policy name

IPR IMPORT [BEFORE] FROM

This command creates an Import Policy for the given scope.

Syntax: IPR IMPORT policy-id1 [BEFORE policy-id2] FROM scope

Parameter	Description
policy-id1	The identifier of a previously defined policy
BEFORE	Allows you to insert a given policy just before the one specified by the policy-id2.

scope	The policy range. Options:
	
	`OSPF [INSTANCE ospf-instance-id]`
	specifies an OSPF instance where a route are to be imported from. If you omit `ospf-instance-id` then the policy applies to all existing OSPF instances.
	
	`RIP [PORTS port1 port2...]`
	specifies the RIP instance as the one where the routes are to be imported from or exported to. When you specify ports, the policy will apply only to the routes received or sent via these RIP ports. If no ports are specified, the policy applies to all interfaces. Using a group of ports as an entity allows you to use Import/Export policy instead of IP RIP filters and as a consequence to have one mechanism common to all protocols to filter any routing information.
	
	`BGP [PEER peer-address]`
	specifies a BGP peer where the routes are to be imported from or exported to. If the `peer-address` is not given then the policy applies to all existing peers.

IPR EXPORT [BEFORE] TO

This command creates Export Policy for a given scope.

Syntax: **IPR EXPORT policy-id1 [BEFORE policy-id2] TO scope**

Parameter	Description
policy-id1	The identifier of a previously defined policy
BEFORE	Allows you to insert a given policy just before the one specified by the policy-id2.

scope	The policy range. Options:
	
	`OSPF [INSTANCE ospf-instance-id]`
	specifies an OSPF instance where a route is to be exported to. If you omit `ospf-instance-id` then the policy applies to all existing OSPF instances.
	
	`RIP [PORTS port1 port2...]`
	specifies the RIP instance as the one where the routes are to be exported to. When you specify ports, the policy will apply only to the routes received or sent via these RIP ports. If no ports are specified, the policy applies to all interfaces. Using a group of ports as an entity allows you to use Import/Export policy instead of IP RIP filters and as a consequence to have one mechanism common to all protocols to filter any routing information.
	
	`BGP [PEER peer-address]`
	specifies a BGP peer where the routes are to be exported to. If the `peer-address` is not specified, the policy applies to all existing peers.

IPR IMPORT DELETE FROM

This command deletes a specified Import Policy component.

Syntax: **IPR IMPORT DELETE policy-id FROM scope**

Parameter	Description
policy-id	The identifier of a previously defined policy

scope	The policy range from where the policy is to be deleted. Options:
	`OSPF [INSTANCE ospf-instance-id]`
	`RIP [PORTS port1 port2...]`
	BGP [**PEER** peer-address]

IPR EXPORT DELETE FROM

This command deletes a specified Export Policy component

Syntax: **IPR EXPORT DELETE policy-id FROM scope**

Parameter	Description
policy-id	The identifier of a previously defined policy

scope	The policy range from where the policy is to be deleted. Options:
	`OSPF [INSTANCE ospf-instance-id]`
	`RIP [PORTS port1 port2...]`
	BGP [**PEER** peer-address]

IPR SHOW IMPORT [FROM]

Displays Import Policies from a given scope.

Syntax: **IPR SHOW IMPORT [FROM scope]**

Parameter	Description
FROM scope	Displays policies from the given scope. Scope is a policy range. Options: OSPF [INSTANCE ospf-instance-id] RIP [PORTS port1 port2...] BGP [PEER peer-address]

IPR SHOW EXPORT [TO]

Displays Export Policies.

Syntax: **IPR SHOW EXPORT [TO scope]**

Parameter	Description
TO scope	Displays policies to the given scope. Scope is a policy range. Options: OSPF [INSTANCE ospf-instance-id] RIP [PORTS port1 port2...] BGP [PEER peer-address]

IPR DEFAULT ADD [BEFORE]

Defines the Default Policy.

Syntax: **IPR DEFAULT ADD policy-id [BEFORE policy-id2]**

Parameter	Description
policy-id1	The identifier of a previously defined policy
BEFORE	Allows you to add the policy just before the one specified by the policy-id2.

IPR DEFAULT DELETE

Deletes the specified component of Default Policy.

Syntax: **IPR DEFAULT DELETE policy-id**

Parameter	Description
policy-id	The identifier of a previously defined policy

IPR SHOW DEFAULT

Displays the current setting of Default Policy.

Syntax: **IPR SHOW DEFAULT**

IPR SHOW PFLAGS

Displays which applied policies have been changed since protocols were enabled.

Syntax: **IPR SHOW PFLAGS**

18. IP/ATM Commands

Overview

The following abbreviations are used throughout:

IP	Internet Protocol
ARP	Address Resolution Protocol
LIS	Logical IP Subnetwork
MTU	Maximum Transfer Unit
LLC	Logical Link Control

The RFC 1577 commands are governed by the following

(Object) (Verb) (Locator) {Parameter} {Value}

Locators can include one or two words, separated by spaces.

1 The first word, or token, in a command line is the command object. The command object is a category of related commands. All RFC 1577 commands start with **IPR**, followed by **ATM**. The allowable objects after typing **IPR ATM** are: **PORT**, **PVC**, **ARPCLIENT**, and **ARPSERVER**.

2 The next token in the command line is a verb. It defines the action to be performed by the command. The allowable verbs are **CREATE**, **DELETE**, **SHOW**, **ENABLE**, **DISABLE**, **MAP**, and **UNMAP**.

3 The next token in the command line is a locator. A locator further defines the object, specifying which interface, device, or other entity is to be acted upon. The allowable locators are **port numbers**, **Virtual Path/Virtual Channel Identifiers**, and **IP addresses**.

4 The final tokens in the command line are parameters and values. Typing the parameter followed by a question mark (?) provides context sensitive help showing what value is expected.

The following example creates a new RFC 1577 port.

XL> **IPR ATM PORT CREATE**

The RFC console commands are shown in uppercase to improve readability, but you can enter any command in either uppercase or lowercase. The XL console accepts both as input.

The maximum length of an XL console command is 512 bytes. However, you cannot enter that many characters on a single line. If you need to enter a long command, you can enter it on several lines by typing a backslash (\) at the end of each line that is followed by another line. Keep in mind that each of these lines cannot be longer than allowed length for the XL console.

Example:

```
IPR ATM ARPCLIENT SADDR 18 \
47112233445566778899112233445566778899 00
```

The above two lines are concatenated into one XL console command. Notice that there is a space between the 18 and the backslash (\). If you omit the space, you will get 1847112233..... instead of 18 47112233....

For an attached XL console, the command line length is smaller than when directly connected.

The RFC 1577 feature is part of the IP router. However, it is possible to use it when the IP router is disabled. This allows you to use applications such as SNMP, TFTP, and PING (over ATM), when XLT–F does not have the IP router feature. For this purpose, an additional port is automatically created. Some IP router console commands operate on a port number. To specify this option, you must use **RD** (Router Disabled) instead of its port number. This port is not a bridge port; no data is forwarded via the port. For all other RFC 1577 ports, any configuration action can be taken only if you have previously assigned an IP address to that port. From the point of view of IP router, these ports are like any other ports.

See the IP commands section for more information on port configuration.

HELP IPR ATM

RFC 1577 console commands are a part of IP router commands. See the IP commands section for more information on accessing IP help.

Typing **HELP IPR ATM** displays an overview of console commands for IP/ATM.

RFC 1577 Commands Roadmap

IPR ATM PUREPVC {ENABLE|DISABLE}

IPR ATM IDLETIMER time_out

IPR ATM PCR [rate]

IPR ATM ARPFMT [arp_fmt]

IPR ATM PORT CREATE

IPR ATM PORT DELETE port_num

IPR ATM PORT ADDR port_num {atm_addr | AUTO}

IPR ATM PORT DFLTMTU port_num mtu_size

IPR ATM PVC MAP port_num vpi vci

IPR ATM PVC UNMAP vpi vci

IPR ATM PVC AGEARP {ENABLE|DISABLE}

IPR ATM CLRSVC

IPR ATM CLRARP {ALL|INVALID|ip_addr}

IPR ATM ARPSTATIC port_num ip_addr atm_addr

IPR ATM ARPSTATIC port_num ip_addr CIRCUIT vpi vci

IPR ATM ARPSERVER {ENABLE | Disable} port_num

IPR ATM ARPSERVER TO time_out

IPR ATM ARPCLIENT SADDR port_num atm_addr

IPR ATM ARPCLIENT TO time_out

IPR ATM ARPCLIENT SPVC port_num vpi vci

IPR ATM ARPCLIENT KEEPSSVC {ENABLE|DISABLE} port_num

IPR ATM SHOW ARP

IPR ATM SHOW MAP

IPR ATM SHOW CFG

IPR ATM PUREPVC

The IPR ATM PUREPVC command enables or disables a pure PVC environment. If it is enabled, no SVCs are allowed. In addition, there is no address registration with an ATM switch (static ATM addresses are used). This command takes effect after the next reboot.

Syntax: **IPR ATM PUREPVC {ENABLE|DISABLE}**

Example:

```
XL(1)>IPR ATM PURPVC ENABLE
XL(1)>
```

IPR ATM IDLETIMER

The IPR ATM IDLETIMER command specifies an idle timeout. An SVC on which nothing is being received is closed in time_out minutes. The allowable values are from 2 to 600 minutes. The default value is 20 minutes. A value of zero disables the timer.

Syntax: **IPR ATM IDLETIMER <time_out>**

Parameter	Description
<time_out>	The idle timeout in minutes.

Example:

```
XL(1)>IPR ATM IDLETIMER 20
XL(1)>
```

IPR ATM PCR

The IPR ATM PCR command sets the default PCR for SVCs created by the RFC 1577 feature. The default PCR is 370370. If you do not specify the value for the rate parameter, the command displays the current value.

Syntax: **IPR ATM PCR <rate>**

Parameter	Description
<rate>	The PCR value.

Example:

```
XL(1)>IPR ATM PCR 30000
XL(1)>
```

Changing the ATM ARP Packet Format

The IPR ATM ARPFMT command allows you to change the ATM ARP packet format. The default value is 0x04. If you do not specify a value for the arp_format parameter, the current value is displayed. The meaning of the bits is as follows:

Bits	Description
0x02 (ATMARPFORM_NULLISNOSTR)	The null ATM addresses are represented by strings of 0 length.
0x04 (ATMARPFORM_NULLISZEROSTR)	The null ATM addresses are represented by 20 bytes of 0s.

If you specify more than 1 bit, the ARP request/response generates more than 1 packet. Keep in mind that improper changes to the ATM ARP format can make it impossible to communicate with other hosts/routers.

Syntax: **IPR ATM ARPFMT <arp_format>**

Parameter	Description
<arp_format>	The bit mask determining the ATM ARP format (hex. number).

Example:

```
XL(1)>IPR ATM ARPFMT 4
XL(1)>
```

IPR ATM PORT CREATE

The IPR ATM PORT CREATE command creates a new RFC 1577 port for use by IP routers. After successful creation, a new port number is displayed. You can use this port number in all subsequent port console commands to locate this port.

Syntax: **IPR ATM PORT CREATE**

Example:

```
XL(1)>IPR ATM PORT CREATE
    port 19 created successfully
XL(1)>
```

IPR ATM PORT DELETE

The IPR ATM PORT DELETE command deletes an RFC 1577 port.

Syntax: **IPR ATM PORT DELETE <port_num>**

Parameter	Description
<port_num>	The the port number you want to delete.

Example:

```
XL(1)>IPR ATM PORT DELETE 19
XL(1)>
```

IPR ATM PORT ADDR

The IPR ATM PORT ADDR command assigns a unique ATM address to a port. Keep in mind that each RFC 1577 port must have a unique ATM address. This ATM address can be automatically set by the IP router. However, if the ATM address is set by the IP router, there is no guarantee that after cycling the port or after a reboot, the port has the same ATM address.

If the ARP Server feature is enabled on the port, it is recommended to you set the ATM address.

Syntax: IPR ATM PORT ADDR <port_num> <atm_addr> {AUTO}

Parameter	Description
<port_num>	The port number.
<atm_addr>	The full ATM address (20 bytes - 40 hex digits)

Example:

```
XL(1)>IPR ATM PORT ADDR 18 \
    ? 39102000000000000000000000009811223355
XL(1)>
```

IPR ATM PORT DFLTMTU

The IPR ATM PORT DFLTMTU command sets the default MTU size on a given port. The MTU size is used on all PVCs assigned to the port. On SVCs, the actual MTU can be smaller according to the MTU negotiation. The default is 9188 bytes. If you do not specify a value for the mtu_size parameter, the current value is displayed.

Syntax: IPR ATM PORT DFLTMTU <port_num> <mtu_size>

Parameter	Description
<port_num>	The port number.
<mtu_size>	The MTU size (in bytes, including the LLC header).

Example:

```
XL(1)>IPR ATM PORT DFLTMTU 18 5000
XL(1)>
```

ATM CREATE VC RFC1577

The ATM CREATE VC RFC1577 command creates a PVC for RFC 1577.

Syntax: **ATM CREATE VC RFC1577 <vpi> <vci>**

Parameter	Description
<vpi>	The Virtual Path Identifier and **<vci>** is the Virtual Channel Identifier.

Example:

```
XL(1)>atm create vc rfc1577 1 1
XL(1)>
```

ATM DELETE VC

The ATM DELETE VC command deletes a PVC for RFC 1577.

Syntax: **ATM DELETE VC <vpi> <vci>**

Parameter	Description
<vpi>	The Virtual Path Identifier and **<vci>** is the Virtual Channel Identifier of a PVC.

Example:

```
XL(1)>atm delete vc 1 1
XL(1)>
```

IPR ATM PVC MAP

The IPR ATM PVC MAP command maps, or assigns, a given PVC to a specified port. Only unmapped PVCs can be mapped to a port. Unmapped PVCs are not used to receive and send data.

Syntax: **IPR ATM PVC MAP <port_num> <vpi> <vci>**

Parameter	Description
<port_num>	The port that you are mapping a PVC to.
<vpi>	The Virtual Path Identifier and **<vci>** is the Virtual Channel Identifier of a PVC.

Example:

```
XL(1)>IPR ATM PVC MAP 18 0 32
XL(1)>
```

IPR ATM PVC UNMAP

The IPR ATM PVC UNMAP command unmaps a given PVC from a port (if mapped).

Syntax: **IPR ATM PVC UNMAP <vpi> <vci>**

Parameter	Description
<vpi>	The Virtual Path Identifier and **<vci>** is the Virtual Channel Identifier of a PVC.

Example:

```
XL(1)>IPR ATM PVC UNMAP 0 32
XL(1)>
```

IPR ATM PVC AGEARP

The IPR ATM PVC AGEARP command enables/disables aging of ATM ARP entries (ARP cache) associated with PVCs. The default is ENABLE.

Syntax: IPR ATM PVC AGEARP {ENABLE | DISABLE}

Example:

```
XL(1)>IPR ATM PVC AGEARP ENABLE
XL(1)>
```

IPR ATM CLRSVC

The IPR ATM CLRSVC command shuts down all open RFC 1577 SVCs. The associated ATM ARP entries in the ARP cache are not removed.

Syntax: IPR ATM CLRSVC

Example:

```
XL(1)>IPR ATM CLRSVC
XL(1)>
```

IPR ATM CLRARP

The IPR ATM CLRARP command deletes the specified ATM ARP entries from the ARP cache.

Syntax: IPR ATM CLRARP {ALL | INVALID} <ip_addr>

Parameter	Description
<ip_addr>	The IP address that identifies the ATM ARP entry to be deleted.

If you specify...	Then...
ALL	All ATM ARP entries are deleted from the ARP cache.
INVALID	All invalid ATM ARP entries are deleted from the ARP cache.

Example:

```
XL(1)>IPR ATM CLRARP 128.100.118.1
XL(1)>
```

IPR ATM ARPSTATIC

The IPR ATM ARPSTATIC command defines the static ATM ARP entry in ARP cache.

Syntax: **IPR ATM ARPSTATIC <port_num> <ip_addr> <atm_addr>**

Parameter	Description
<port_num>	The port number another station is accessible through.
<ip_num>	The IP address of another station.
<atm_addr>	The ATM address of another station.

All static ARP entries are lost after a reboot or cycling of the IP routing.

The optional form of the command, shown below, can be used to setup a communication via an open VC.

Syntax: **IPR ATM ARPSTATIC <port_num> <ip_addr> CIRCUIT <vpi> <vci>**

Parameter	Description
<vpi>	The Virtual Path Identifier of a VC another station is accessible through.
<vci>	The Virtual Channel Identifier of a VC another station is accessible through.

Example:

```
XL(1)>IPR ATM ARPSTATIC 18 128.100.118.4 CIRCUIT 0 33
XL(1)>IPR ATM ARPSTATIC 18 128.100.118.4 \
    ? 3933330000000000000000000000000101010100
XL(1)>
```

IPR ATM ARPSERVER

The IPR ATM ARPSERVER command enables or disables the ARP server on a specified port. The default is DISABLED.

Syntax: **IPR ATM ARPSERVER {ENABLE|DISABLE} <port_num>**

Parameter	Description
<port_num>	The port number on which the ARP Server is being enabled or disabled.

Example:

```
XL(1)>IPR ATM ARPSERVER ENABLE 18
XL(1)>
```

IPR ATM ARPSERVER TO

The IPR ATM ARPSERVER TO command sets the ATM ARP Server time–out. The allowable values are 20 to 600 minutes. The default is 20 minutes.

Syntax: **IPR ATM ARPSERVER TO <time_out>**

Parameter	Description
<time–out>	The ARP time–out, in minutes, for the ATM ARP Server.

Example:

```
XL(1)>IPR ATM ARPSERVER TO 30
XL(1)>
```

IPR ATM ARPCLIENT SADDR

The IPR ATM ARPCLIENT SADDR command sets the ATM address of an ATM ARP Server.

Syntax: **IPR ATM ARPCLIENT SADDR <port_num> <atm_addr>**

Parameter	Description
<port_num>	The port number.
<atm_addr>	The full ATM address of the ATM ARP Server.

Example:

```
XL(1)>IPR ATM ARPCLIENT SADDR 18 \
    ? 3944330000000000000000000000000101010100
XL(1)>
```

IPR ATM ARPCLIENT TO

The IPR ATM ARPCLIENT TO command sets the ATM ARP Client time–out. The allowable values are 1 to 15 minutes. The default value is 15 minutes.

Syntax: **IPR ATM ARPCLIENT TO <time_out>**

Parameter	Description
<time–out>	The ARP time–out, in minutes, for the ATM ARP Client.

Example:

```
XL(1)>IPR ATM ARPCLIENT TO 10
XL(1)>
```

IPR ATM ARPCLIENT SPVC

The IPR ATM ARPCLIENT SPVC command enables you to set an ATM ARP Server via a specified PVC. The PVC should be mapped to a port number.

Syntax: **IPR ATM ARPCLIENT SPVC <port_num> <vpi> <vci>**

Parameter	Description
<port_num>	The port number.
<vpi>	The Virtual Path Identifier of a PVC to an ARP Server.
<vci>	The Virtual Channel Identifier of a PVC to an ARP Server.

Example:

```
XL(1)>IPR ATM ARPCLIENT SPVC 18 0 34
XL(1)>
```

IPR ATM ARPCLIENT KEEPSSVC

The IPR ATM ARPCLIENT KEEPSSVC command enables you to force the Idle Timer not to close SVCs to an ARP Server on a given port. All SVCs, including those to ARP Server, can be closed by the Idle Timer.

Syntax: **IPR ATM ARPCLIENT KEEPSSVC {ENABLE | DISABLE} <port_num>**

Parameter	Description
<port_num>	The port number.

Example:

```
XL(1)>IPR ATM ARPCLIENT KEEPSSVC ENABLE 18
XL(1)>
```

IPR ATM SHOW ARP

Displays the ATM ARP cache.

Syntax: **IPR ATM SHOW ARP**

For each entry, the following information is displayed:

- Flags: S (Server's entry), I (Invalid entry), P (SVC during establishing)
- IP address of another station
- Port number this station is accessible through
- Full ATM address of this station
- VPI/VCI identifiers of a VC the station is accessible through
- Age of this entry (hh:mm)

Example:

```
XL(1)>IPR ATM SHOW ARP
S-- 128.100.119.005 19 47000580FFE1000000F21514F10000D100053D02 0/217 00:05
-I- 128.100.118.002 18 47000580FFE1000000F21514F100008064760200 0/242 00:15
XL(1)>
```

IPR ATM SHOW MAP

Lists all RFC 1577 VCs (PVC and SVC) and their port associations.

Syntax: **IPR ATM SHOW MAP**

For each VC, the following information is displayed:

- The path and channel identifiers.
- The MTU size, including the LLC header used on the VC.
- The age for the Idle Timer (time elapsed since the last frame has been received over this VC).
- A flag indicating whether the VC is permanent (P), a SVC initiated by the XLT–F (I), or a SVC accepted, i.e., initiated by the other side (A).
- The handle number (debugging information for programmers).

Example:

```
XL(13)>IPR ATM SHOW MAP
VCs for disabled router:
Port 18:
    VPI=0, VCI=242, MTU=9188 00:24 A (3)
Port 19:
    VPI=0, VCI=243, MTU=9188 03:36 I (2)
    VPI=0, VCI=244, MTU=9188 03:08 I (4)
Unassigned VCs:
XL(1)>
```

IPR ATM SHOW CFG

Displays the RFC 1577 configuration, including global and port parameters.

Syntax: IPR ATM SHOW CFG

For each port, the following information is displayed:

- The port number.
- Whether the ARP Server is enabled or not (client) on this port.
- Whether the port's ATM address is configured statically (S), or automatically set by the XLT–F (A).
- The port's ATM address.
- Whether the ATM address is registered with an ATM switch.

For the ARP Client ports, the following information is displayed:

- The ARP Server's ATM address.
- The time (mm:ss) elapsed since the last In ARP request has been received from the ARP Server.
- Whether to keep SVCs to the ARP Server permanently open. This information is displayed only if this feature is enabled on the port.
- The path and channel identifiers of a PVC to the ARP Server. This information is displayed only if the PVC to an ARP Server is defined on this port.

Example:

```
XL(13)>IPR ATM SHOW CFG
Aging ATMARP entries associated with PVCs: ENABLED
ATMARP time-outs: server 20 min., client 15 min.
Idle timer for SVCs: 20 min.
Pure PVC environment is DISABLED now
Pure PVC environment will be DISABLED after reboot
Port RD CLIENT A <no ATM address assigned or registered>
    SERVER ADDR <no ATMARP server address configured> >20:00
Port 18 SERVER S 47000580FFE1000000F21514F1000098D3456801 registered
Port 19 SERVER S 47000580FFE1000000F21514F1000098D3456802 registered
Port 20 CLIENT A 4700000005500000000000000000000098d3456800 registered
    SERVER ADDR 47000580FFE1000000F21514F100000101010100 06:00
                XL(13)>
```

19. IPX Commands

IPXLOCALNET

This command is used to change the IPX network number on a specified IPX circuit. If a unique IPX network number is entered, this network number must be the same as on other IPX routers connected to this network segment. This command can also be used to set Unnumbered RIP.

Syntax: **IPXLOCALNET p[.c] {net_adr | 0}**

Parameter	Description
p[.c]	Specifies the IPX circuit that you want to change the IPX network number.
p	The port number on which the IPX circuit exists. Valid values are from 0 to 255 (0 to 128 for XL 5.1 or later).
c	The IPX circuit on port p that you want to change the IPX network number. If you omit this parameter, the command defaults to the first circuit on that port. Valid values are from 1 to 4.
net_adr	The new IPX network number you want to change to. Enter a maximum of 8 hex digits not equal to 0.
0	This sets Unnumbered RIP on the specified IPX circuit connected to point-to-point line. **Note:** You must set this option for both sides of the point-to-point line.

IPXINTNET

This command is used to set the IPX network number as part of the internal IPX address.

Syntax: **IPXINTNET net_num**

Parameter	Description
net_num	This is a unique IPX network number not equal to 0 or FFFFFFFF that is to be used as part of the internal IPX address (maximum 8 hexadecimal digits). This internal IPX network number must be set when the Unnumbered RIP option is set on any IPX circuit, or if you are using a two XLM boards and IPX Type 20 packets (NetBios over IPX packets) are processed or IPX Ping test is started on the IPX router.

IPXINTNODE

This command is used to set the node part of the internal IPX address.

Syntax: IPXINTNODE mac_add

Parameter	Description
mac_add	This is a maximum of 12 hexadecimal digits that is to be used as the node part of the internal IPX address. The node number does not have to be unique.

IPXRESET

This command is used to reset the IPX Router. This command will re-learn all server tables and update the routing network table. It also adds static paths to IPX networks and servers to the routing and server table.

Syntax: IPXRESET

IPXCLEAR

This command is used to clear the network and server tables and reinitializes the IPX router. The structures describing all registered SPX sessions (if SPX Spoofing is on) will also be removed. After this command is invoked, the router will relearn network and server table information.

Syntax: IPXCLEAR

Use IPXCLEAR carefully: when the IPX router is cleared, all existing connections can be broken.

IPXDOWN

This command is used to bring down the IPX Router before disabling the IPX or before rebooting the device. You can reinitialize a down IPX Router with IPXCLEAR.

Syntax: IPXDOWN

IPXROUTER {ENABLE | DISABLE}

Syntax: **IPXROUTER {ENABLE | DISABLE}**

This command toggles IPX router on and off globally.

IPXPORT {ENABLE | DISABLE}

Syntax: **IPXPORT {ENABLE | DISABLE} p [.c]**

This command enables or disables IPX routing on a selected IPX circuit.

Parameter	Description
p[.c]	Specifies the IPX circuit that you want to change the IPX network number.
p	The port number on which the IPX circuit exists. Valid values are from 0 to 255 (0 to 128 for XL 5.1 or later).
c	The IPX circuit on port p that you want to enable/disable IPX routing. If you omit this parameter, the command defaults to the first circuit on that port. Valid values are from 1 to 4.

IPXMAXSPLIT

This command is used to enable and disable splitting of IPX routed packets (using multiple equivalent routes to balance traffic), and, if enabled, to determine the number of these equivalent routes that may be used.

Syntax: **IPXMAXSPLIT n**

Parameter	Description
n	The maximum number of paths allowed for split paths. A value of 1 disables path splitting. Range: 1..32

IPXSR {ENABLE | DISABLE}

This command is used to enable and disable IPX Source Routing mode on a specific IPX circuit.

Syntax: IPXSR {ENABLE | DISABLE} p[.c]

Parameter	Description
p[.c]	Specifies the IPX circuit that you want to enable/disable IPX Source Routing mode.
p	The port number on which the IPX circuit exists. Valid values are from 0 to 255 (0 to 128 for XL 5.1 or later).
c	The IPX circuit on port p. If you omit this parameter, the command defaults to the first circuit on that port. Valid values are from 1 to 4.

IPXRIP {ENABLE | DISABLE}

Enables and disables IPX RIP packet processing globally.

Syntax: IPXRIP {ENABLE | DISABLE}

IPXSAP {ENABLE | DISABLE}

Enables and disables IPX SAP packet processing globally.

Syntax: IPXSAP {ENABLE | DISABLE}

IPXPORTRIP {ENABLE | DISABLE}

Enables and disables RIP packet processing on a specified IPX circuit.

Syntax: **IPXPORTRIP {ENABLE | DISABLE } p[.c]**

Parameter	Description
ENABLE	Enables RIP packet processing on an IPX circuit.
DISABLE	Disables RIP packet processing on an IPX circuit.
p[.c]	Specifies the IPX circuit on which you want to enable/disable RIP packet processing.
p	Port number on which the IPX circuit resides. Range: 0..255 (0 to 128 for XL 5.1 or later).
c	IPX circuit on port p. If you omit this parameter, the command defaults to the first circuit on that port. Range: 1..4

IPXPORTSAP{ENABLE | DISABLE}

Enables and disables SAP packet processing on a specified IPX circuit.

Syntax: **IPXPORTSAP {ENABLE | DISABLE} p[.c]**

Parameter	Description
ENABLE	Enables SAP packet processing on an IPX circuit c.
DISABLE	Disables SAP packet processing on an IPX circuit c.
p[.c]	Specifies the IPX circuit on which you want to enable/disable SAP pocket processing.
p	Port number on which the IPX circuit resides. Range: 0..255 (0 to 128 for XL 5.1 or later)
c	IPX circuit on port p. If you omit this parameter, the command defaults to the first circuit on that port. Range: 1..4

IPXPORTRIPSM

Select the type of Reduced (Smart) Advertising for RIP packets on point-to-point lines. You must use the same type of the Smart Advertising on each end of a point-to-point line.

Syntax: **IPXPORTRIPSM {OFF | OLD | NEW} p[.c]**

Parameter	Description
OFF	No Reduced Advertising on the specified IPX circuit (regular, periodic advertising is performed).
OLD	Old version of Reduced Advertising (unacknowledged, compatible with all ILAN versions and XL versions prior to Release 4.1)
NEW	New version of Reduced Advertising (acknowledged, recommended for all types of point-to-point lines)
p[.c]	The IPX circuit for which you want to choose the type of RIP Reduced Advertising.
p	Port number on which the IPX circuit resides. Range: 0..255 (0 to 128 for XL 5.1 or later).
c	IPX circuit on port p. If you omit this parameter, the command defaults to the first circuit on port p. Range: 1..4

IPXPORTSAPSM

Select the type of Reduced (Smart) Advertising for SAP packets on point-to-point lines. You must use the same type of the Smart Advertising on each end of a point-to-point line.

Syntax: **IPXPORTSAPSM {OFF | OLD | NEW} p[.c]**

Parameter	Description
OFF	No Reduced Advertising on the specified IPX circuit (regular, periodic advertising is performed).
OLD	Old version of Reduced Advertising (unacknowledged, compatible with all ILAN versions and XL versions prior to Release 4.1)
NEW	Advertising is reduced on port p, circuit c, according to the later (acknowledged) algorithm, which is recommended for all types of point-to-point lines.
p[.c]	The IPX circuit for which you want to choose the type of SAP Reduced Advertising.
p	Port number on which the IPX circuit resides. Range: 0..255 (0 to 128 for XL 5.1 or later).
c	IPX circuit on port p. If you omit this parameter, the command defaults to the first circuit on port p. Range: 1..4

IPXPORTSAP4 {ENABLE | DISABLE}

Enables and disables the sending of Get Nearest Server Reply packets (SAP packet type 4) on the specified IPX circuit.

Syntax: **IPXPORTSAP4 {ENABLE | DISABLE} p[.c]**

IPXNETBIOS {ENABLE | DISABLE}

Enables and disables IPX Type 20 packets (NetBIOS over IPX broadcast packets) on a specified IPX circuit. Type 20 packets are those that refer to any IPX propagated packets, also known as Novell IPX WAN Broadcast packets

Syntax: **IPXNETBIOS {ENABLE | DISABLE} p[.c]**

Parameter	Description
p[.c]	Specifies the IPX circuit on which you want to enable/disable IPX Type 20 packet processing.
p	Port number on which the IPX circuit resides. Range: 0..255 (0 to 128 for XL 5.1 or later).
c	IPX circuit on port p. If you omit this parameter, the command defaults to the first circuit on that port. Range: 1..4

IPXNETBREDUCED {ENABLE | DISABLE}

Globally enables and disables the reduced propagation of IPX Type 20 packets: if enabled, the IPX router will not propagate type 20 packets originating from the same source and received through different IPX circuits. This means that each IPX type 20 packet is propagated through the relevant IPX router only once. If this option is disabled, the IPX router repropagates IPX Type 20 packets through the IPX circuits that these packets have not yet traversed. The split horizon algorithm (under which IPX router does not propagate packets through the IPX circuits on which they are received) is always applied to Type 20 packets, regardless of this option.

Syntax: **IPXNETBREDUCED {ENABLE | DISABLE}**

IPXBACKWARD {ENABLE | DISABLE}

Enables and disables backward routing on the specified IPX circuit (backward routing sends an IPX packet back through the IPX circuit on which it arrived). In some configurations, enabling or disabling this option speeds up the process of switching IPX traffic when the primary path is broken.

Note: Disabling this option can break some connections and prevent you from establishing some sessions.

Syntax: **IPXBACKWARD {ENABLE | DISABLE} p[.c]**

Parameter	Description
p[.c]	The IPX circuit for which you want to enable or disable backward routing.
p	Port number on which the IPX circuit resides. Range: 0..255 (0 to 128 for XL 5.1 or later).
c	IPX circuit on port p. If you omit this parameter, the command defaults to the first circuit on that port. Range: 1..4

IPXNETALOGIC {ENABLE | DISABLE}

Enables and disables the storage of IPX networks in the Address Table.

Syntax: **IPXNETALOGIC {ENABLE | DISABLE}**

Option	Description
DISABLE	Saves space in the Address Table (because IPX network numbers are stored only in the IPX Network Table) but performance of the IPX router is significantly degraded.
ENABLE	Performance of the IPX router is improved (the stored networks are used for fast searching). Recommended for Dial on Demand lines.

IPXSRVALOGIC {ENABLE | DISABLE}

Enables and disables the storage of IPX servers in the Address Table.

Syntax: **IPXSRVALOGIC {ENABLE | DISABLE}**

Option	Description
DISABLE	Saves space in the Address Table (because IPX server names are stored only in the IPX Network Table).
ENABLE	Performance of the IPX router is improved (the stored server names are used for fast searching). Recommended for Dial on Demand lines.

IPXSPOOF {ENABLE | DISABLE}

Enables and disables Watchdog Spoofing for IPX on the specified IPX circuit.

Syntax: **IPXSPOOF {ENABLE | DISABLE} p[.c]**

Parameter	Description
ENABLE	Enables Watchdog Spoofing on the specified IPX circuit. Spoofing reduces the IPX control traffic on the circuit. Each IPX server periodically sends a Watchdog request frame to all IPX workstations logged in and the workstations send a Watchdog response back to the server. IPX router sends watchdog responses to the server instead of workstations, and Watchdog requests are not forwarded via this circuit. It is recommended that you enable spoofing for Dial on Demand lines.
DISABLE	This disables Watchdog Spoofing on the specified IPX circuit, so that IPX Watchdog requests are forwarded through this IPX circuit.
p[.c]	Specifies the IPX circuit on which you want to enable/disable IPX Watchdog Spoofing.
p	Port number on which the IPX circuit resides. Range: 0..255 (0 to 128 for 5.1 or later).
c	IPX circuit on port p. If you omit this parameter, the command defaults to the first circuit on that port. Range: 1..4

IPXMAXHOPS

This command is used to set the maximum number intermediate IPX routers an IPX packet may traverse.

Syntax: **IPXMAXHOPS n**

Parameter	Description
n	The maximum number of hops an IPX packet may take. Range: 1..16

IPXMAXPATHS

This command is used to set the maximum number of registered paths (routes) for each network and server structure.

Syntax: **IPXMAXPATHS n**

Parameter	Description
n	The maximum number of registered paths. Range: 1..128

IPXPORT CREATE

Creates an IPX circuit.

Syntax: **IPXPORT CREATE p[.c] {type}**

Parameter	Description
p	Specifies the IPX port you want to create. Range: 0..255 (0 to 128 for 5.1 or later).
c	The IPX circuit on port p. If you omit this parameter, the command defaults to the first circuit on that port. Range: 1..4
type	Type of frame for circuit c. It must be unique among all IPX circuits residing on the same port. Available types are limited according to the circuit type: An Ethernet port can have up to 4 circuits: ESNAP, E8022, E8023, and PORTABLE. A Token Ring port can have up to 2 circuits: TSNAP and T8022. A point-to-point line, LEC port, SMDS port, and ABC port can have up to six circuits: TSNAP, ESNAP, E8022, T8022, E8023, and PORTABLE. Remember that you cannot use a circuit type more than once on the same port. For example, a Token Ring port can have one circuit (either TSNAP or T8022) or two circuits (TSNAP on one circuit and T8022 on the other), but you cannot assign both possible circuits on a Token Ring port to the same circuit type.

IPXPORT DELETE

Deletes IPX port p, circuit c.

Syntax: **IPXPORT DELETE p[.c]**

Parameter	Description
p[.c]	Specifies the IPX circuit you want to delete
p	Port number on which the IPX circuit resides. Range: 0..255 (0 to 128 for 5.1 or later).
c	IPX circuit on port p. If you omit this parameter, the command defaults to the first circuit on that port. Range: 1..4

IPXFT

Sets the IPX frame type to be processed on the specified IPX circuit.

Syntax: **IPXFT {TSNAP | ESNAP | T8022| E8022 | E8023 | PORTABLE} p[.c] [protocol_type]**

Parameter	Description
E8023	Ethernet 802.3, the older Novell format for Ethernet (Ethernet Raw 802.3). Note that there is no decimal point in the parameter.
E8022	Ethernet 802.2, the newer Novell 4.0 encapsulation (with DSAP and SSAP). Note that there is no decimal point in the parameter.
ESNAP	Encapsulation with SNAP header.
PORTABLE	Ethernet II (Portable Netware)
T8022	Token Ring 802.2, the older Novell format on Token Ring (with DSAP and SSAP). Note that there is no decimal point in the parameter.
TSNAP	Encapsulation with SNAP header. For point-to-point lines, on the LEC port, on the SMDS port, and on the ABC port, any Ethernet and Token Ring frame type can be set, but the same frame type must be set on both sides of this line.
p[.c]	Specifies the IPX port you want to affect. If you omit the circuit number, the command defaults to the first circuit on that port. port range: port 0..255 (0 to 128 for 5.1 or later). Circuit range: 1..4
protocol_type	This optional field determines the protocol type field to use in SNAP or PORTABLE frame encapsulations. Enter it in hexadecimal format. Default = hex 8137.

IPXPKTSIZE

This command sets the maximum size of non-RIP or SAP IPX packets to be processed on the specified IPX circuit.

Syntax: **IPXPKTSIZE p [.c] n**

Parameter	Description
p[.c]	The circuit number to affect.
p	Port number on which the IPX circuit resides. Range: 0..255 (0 to 128 for 5.1 or later).
c	IPX circuit on port p. If you omit this parameter, the command defaults to the first circuit on that port. Range: 1..4
n	The maximum size (in octets) of IPX packet to allow on that circuit. Defaults: 1500 for Ethernet circuits and 4464 for other types. Range: from 30 to 4469 (maximum value depends on interface type and IPX frame type.)

IPXMAXRIP and IPXMAXSAP

Set the maximum number of entries in RIP and SAP packets to be processed on IPX port p, circuit c. A single entry for RIP means a single network number's parameters; a single entry for SAP means a single server's parameters.

Syntax: **IPXMAXRIP p [.c] n**

Syntax: **IPXMAXSAP p [.c] n**

Parameter	Description
p[.c]	The circuit number to affect.
p	Port number on which the IPX circuit resides. Range: 0..255 (0 to 128 for 5.1 or later).
c	IPX circuit on port p. If you omit this parameter, the command defaults to the first circuit on that port. Range: 1..4
n	Maximum number of entries on port p, circuit c. Default: 50(RIP) and 7(SAP) Minimum: 4 Maximum: depends on interface type and the IPX frame type.(182, 183, or 245 for RIP, 22 or 30 for SAP)

IPXRIPTIME and IPXSAPTIME

Set the update time for RIP and SAP packets to be processed on IPX port p, circuit c.

Syntax: **IPXRIPTIME p [.c] n**

Syntax: **IPXSAPTIME p [.c] n**

Parameter	Description
p[.c]	The circuit number to affect.
p	Port number on which the IPX circuit resides. Range: 0..255 (0 to 128 for 5.1 or later).
c	IPX circuit on port p. If you omit this parameter, the command defaults to the first circuit on that port. Range: 1..4
n	Update time (in seconds) for RIP or SAP packets on port p, circuit c. Minimum: 30 Maximum: 65535

IPXRIPAGE and IPXSAPAGE

These commands set the age multiplier for RIP and SAP packets to be processed on the specified IPX circuit.

Syntax: **IPXRIPAGE p [.c] n**

Syntax: **IPXSAPAGE p [.c] n**

Parameter	Description
p[.c]	The circuit number to affect.
p	Port number on which the IPX circuit resides. Range: 0..255 (0 to 128 for 5.1 or later).
c	IPX circuit on port p. If you omit this parameter, the command defaults to the first circuit on that port. Range: 1..4
n	The age multiplier for RIP or SAP packets on port p, circuit c. Range: 2..255

IPXDELAYIN and IPXDELAYOUT

Set the delay offset for RIP and SAP packets to be processed on the specified IPX circuit.

Syntax: **IPXDELAYIN p [.c] n**

Syntax: **IPXDELAYOUT p [.c] n**

Parameter	Description
p[.c]	The circuit number to affect.
p	Port number on which the IPX circuit resides. Range: 0..255 (0 to 128 for 5.1 or later).
c	IPX circuit on port p. If you omit this parameter, the command defaults to the first circuit on that port. Range: 1..4
n	Delay offset (in 50 ms tics) added for each network and server registered (IN) or advertised (OUT) through the specified circuit. Range: 0..255

IPXHOPSIN and IPXHOPSOUT

These commands set the hops offset for RIP and SAP packets to be processed on the specified IPX circuit.

Syntax: **IPXHOPSIN p[.c] n**

Syntax: **IPXHOPSOUT p[.c] n**

Parameter	Description
p[.c]	The circuit number to affect.
p	Port number on which the IPX circuit resides. Range: 0..255 (0 to 128 for 5.1 or later).
c	IPX circuit on port p. If you omit this parameter, the command defaults to the first circuit on that port. Range: 1..4
n	Hops offset added for each network and server registered (IN) or advertised (OUT) through the specified circuit. Range: 0..14

IPXRIPDELAY and IPXSAPDELAY

These commands set the delay between RIP and SAP packets to be sent on IPX port p, circuit c.

Syntax: **IPXRIPDELAY p [.c] n**

Syntax: **IPXSAPDELAY p [.c] n**

Parameter	Description
p[.c]	The circuit number to affect.
p	Port number on which the IPX circuit resides. Range: 0..255 (0 to 128 for 5.1 or later).
c	IPX circuit on port p. If you omit this parameter, the command defaults to the first circuit on that port. Range: 1..4
n	The time (in 10 ms tics) to wait before sending the next packet. Range: 6..12 for LANs and 6..100 for point-to-point lines.

IPXREFRESHSTATIC

This command enables you to add all defined static paths (defined through all active IPX circuits) to IPX networks and servers, to routing and server tables. Normally, a static path to an IPX network or server is added to the routing/server table only during the path definition or modification or when an IPX circuit (through which this path is defined) is activated.

Syntax: **IPXREFRESHSTATIC**

IPXFLUSHT

This command sets the flush time for IPX networks and servers. Flush time is the number of seconds after which aged networks (servers) will be removed from the routing (server) table (aged network or server means entry with hops = 16). The only exception to the flush time setting occurs when the aged network and servers are longer than the flush time when this state was not acknowledged through the IPX circuit using Reduced Advertising Type NEW.

Syntax: **IPXFLUSHT n**

Parameter	Description
n	The flush time for IPX networks and servers in seconds. The minimum value is 1. Maximum value is 65535 sec.

IPXRMVAGED

This command enables you to remove immediately all aged network and server structures from the routing and server tables. This process is performed unconditionally and independent of flush time.

Syntax: **IPXRMVAGED**

Note: When you use this command, be sure that all aged networks and severs were advertised through all active IPX circuits, otherwise your internetwork can be inconsistent.

IPXSMARTCNT

This command sets the Reduced (Smart) Advertising counter for IPX networks and servers. This counter specifies the number of times learned or updated networks or servers will be advertised through the IPX circuit with Reduced Advertising type OLD (Unacknowledged).

Syntax: **IPXSMARTCNT n**

Parameter	Description
n	The Reduced Advertising counter for IPX networks and servers. It is the range from 1 to 255. The default value is 5.

IPXMAXGLOBPROC

This command sets the maximum number of IPX global processes available in an IPX router. Global processes are used to service all RIP1 All Nets, SAP1 All Servers and SAP1 Specified Server Type requests received on LAN ports. If a large number of devices that send these requests are connected directly to LAN segments, you should increase the number of available IPX processes. When you change this value, you should disable then enable the IPX router or reboot an XL device.

Syntax: **IPXMAXGLOBPROC n**

Parameter	Description
n	The maximum number of IPX global processes. Range: 1..255

IPXLOOPTIME

This command sets the maximum time interval for IPX code to execute.

Syntax: **IPXLOOPTIME n**

Parameter	Description
n	The maximum time interval for the executing of IPX code in 10ms tics.

RIPSPLITHORIZON and SAPSPLITHORIZON

These commands are used to control RIP/SAP split horizon algorithm on a specified IPX circuit. When the split horizon is enabled, IPX router does not advertise networks (servers) to the ports from which it learned them with the best metrics. It is enabled by default.

Syntax: **IPX RIPSPLITHORIZON {ON|OFF} p [.c]**

Syntax: **IPX SAPSPLITHORIZON {ON|OFF} p [.c]**

Parameter	Description
p[.c]	The circuit number to affect.
p	The port number on which the IPX circuit resides. Range: 0..255 (0 to 128 for XL 5.1 or later).
c	The IPX circuit on port p. If you omit this parameter, the command defaults to the first circuit on that port. Range: 0..4
ON/OFF	ON enables split horizon, OFF disables it.

IPXFILT

Enables and disables address filters and Smart Filters on an IPX router.

Syntax: **IPXFILT {SMON | SMOFF | ADDRON | ADDROFF}**

Parameter	Description
SMON	Enables Smart Filters
SMOFF	Disables Smart Filters
ADDRON	Enables address filters
ADDROFF	Disables address filters

IPXSPXSPOOF TERMTIME

When no SPX packets are received for this many seconds, the session is closed (all structures of this session are canceled).

Syntax: **IPXSPXSPOOF TERMTIME timeout**

Parameter	Description
timeout	Number of seconds to wait before timing out the session. Range: 30..600 seconds Default: 30 seconds

IPXSPXSPOOF ENABLE and IPXSPXSPOOF DISABLE

Enables and disables SPX Spoofing on a specified circuit.

Syntax: **IPXSPXSPOOF {ENABLE | DISABLE} circuit**

IPXSPXSESSIONS

Displays **all** registered SPX sessions.

Syntax: IPXSPXSESSIONS [sequence_number]

The sequence_number (optional) lets you select the first SPX session with which to start the listing.

The following information is displayed for each SPX session:

- The number of the session on the list.
- Destination IPX address (net:node:socket) and SPX address (identifier) for each direction
  (F - filter direction, S - send-back direction).
- For each direction: Source Connection ID, Destination Connection ID, Sequence Number, Acknowledge Number, Allocation Number.

To display all parameters and the current state of a **specific** SPX session, use:

Syntax: IPXSPXSESSIONS net:node:socket src_connection_id:dst_connection_id

The following information is displayed for the specified SPX session:

The command displays the following information:

- The number of packets forwarded in both directions.
- The state of the Session Cancellation timer (if it exists).
- The number of End-Of-Connection SPX packets sent due to SPX Session Cancellation.
- IPX addresses for both directions (F - filter direction, S - send-back direction).
- SPX address (identifier) for each direction.
- The number of packets detected on a direction (also packets received but filtered and packets generated due to SPX Spoofing).

Parameter	Description
net	IPX network (max 8 hex digits)
node	IPX node (max 12 hex digits)
socket	IPX socket (max 4 hex digits)
src_connection_id	SPX Source Connection ID (max 4 hex digits)
dst_connection_id	SPX Destination Connection ID (max 4 hex digits)

Note: The parameters can be entered for any direction of registered SPX session (for filter direction or for send-back direction); they identify the complete session (both directions).

Example 1

```
ILAN/XL(0)>ipxspxsessions
00001:
F- 33223322:0000C03E8210:400A 2f14:1c60
S- 30B23228:000000000001:8104 1c60:2f14
F- SrcID: 2f14       DstID: 1c60       SeqNo: 31AckNo: 15AllocNo: 15
S- SrcID: 1c60       DstID: 2f14       SeqNo: 15AckNo: 32AllocNo: 37
00002:
F- 33223322:0000C03E8210:4026 7bc:1660
S- 30B23228:000000000001:8104 1660:7bc
F- SrcID: 7bc        DstID: 1660       SeqNo: 0 AckNo: 0AllocNo: 0
S- SrcID: 1660       DstID: 7bcSeqNo: 9AckNo: 60AllocNo: 66
00003:
F- 33223322:0000C0C320AA:4012 9150:1a60
S- 30B23228:000000000001:8104 1a60:9150
F- SrcID: 9150       DstID: 1a60       SeqNo: 70AckNo: 9AllocNo: 9
S- SrcID: 1a60       DstID: 9150       SeqNo: 9 AckNo: 71AllocNo: 76
All SPX session: 3.
```

Example 2

```
ILAN/XL(0)>ipxspxsession 33223322:0000C0C320AA:4012 9150:1a60
Forwarded packets: 166
Session Cancellation: timer not set
F-FORWARD IPX address ID: 33223322:0000C0C320AA:4012
S-FORWARD IPX address ID: 30B23228:000000000001:8104
SPX address ID:
 F- SrcID: 9150      DstID: 1a60       SeqNo: 7 AckNo: 9AllocNo: 9
 S- SrcID: 1a60      DstID: 9150       SeqNo: 9 AckNo: 71AllocNo: 76
Number of packet detected on a F-direction: 6
Number of packet detected on a S-direction: 5
```

IPXSPXSESCANCEL

To cancel (terminate) a session, use:

Syntax: **IPXSPXSESCANCEL net:node:socket src_connection_id:dst_connection_id**

Parameter	Description
net	IPX network (max 8 hex digits)
node	IPX node (max 12 hex digits)
socket	IPX socket (max 4 hex digits)
src_connection_id	SPX Source Connection ID (max 4 hex digits)
dst_connection_id	SPX Destination Connection ID (max 4 hex digits)

Note: The parameters can be entered for any direction of registered SPX session (for filter direction or for send-back direction); they identify the complete session (both directions).

IPXSPXSESRMV

To remove a session, use:

Syntax: **IPXSPXSESRMV net:node:socket src_connection_id:dst_connection_id**

Parameter	Description
net	IPX network (max 8 hex digits)
node	IPX node (max 12 hex digits)
socket	IPX socket (max 4 hex digits)
src_connection_id	SPX Source Connection ID (max 4 hex digits)
dst_connection_id	SPX Destination Connection ID (max 4 hex digits)

Note: The parameters can be entered for any direction of registered SPX session (for filter direction or for send-back direction); they identify the complete session (both directions).

IPXPING and IPXSTOPPING

These commands are used to start and stop the IPX ping test. This test enables you to verify whether you can reach a specified destination (running IPX Diagnostic protocol or Novell's IPX Ping protocol). Most IPX stations, routers and servers can respond to IPX Diagnostic packets. The IPX Ping protocol is a new protocol introduced by Novell. If using this protocol, make sure that the destination supports it (for example, IPXPING.NLM on a server or IPX on XL 4.1 or later).

Syntax: **IPXPING net:node [D | P | Nnumber | Llength | Ttimeout | Ffill | Q]**

This command is used to start the IPX ping test to a specified destination.

Syntax: **IPXSTOPPING**

This command is used to stop running the IPX ping test. If you do not use this command, the ping test will automatically stop when the requested number of pings are processed.

Parameter	Description
net:node	The IPX address of the destination to examine (IPX network number (max 8 hex digits): node (MAC) address (max 12 hex digits). Range: D or P.
D	Enter this character to designate ping using IPX Diagnostic packets (default).
P	Enter this character to designate ping using Novell's IPX Ping protocol packets.
Nnumber	The number of pings to be sent. Range: 1..65535 Default: 1 packet
Llength	Length of the data field in a ping packet. Range: 1..1450 bytes Default: 64 bytes
Ttimeout	Seconds to wait for a response to a ping packet. Range: 1..600 secs Default: 2 secs.
Ffill	The pattern (one byte in hex form) used to fill first 50 bytes of the data field.
Q	Turns off control messages during IPX ping test (quiet option).

The following messages can display when IPX Ping is running:

```
Ping #1 - Timeout

Ping #2 - OK rcv on 1.2

Ping #3 - OK rcv on 1.3 (CORRUPTED DATA)

IPX Ping finished

Sent:40080  Recieved:10000  Timeouts: 10000  Seq. Errrors:
10000  Corrupted: 10000

Avg Round Trip Delay: 10.5 ms
```

Field	Description
Ping #1	The sequential number of IPX ping packets processed.
OK/TIMEOUT	The status of the relevant ping (not displayed if Q option is used): OK: proper response was received before the timeout was reached (if data field was corrupted then the CORRUPTED DATA message displays). TIMEOUT: time was reached and proper response was not received.
rcv on p.c	Identifier of the IPX circuit that received the proper IPX ping.
P	Denotes port number that the IPX circuit resides.
c	Denotes the IPX circuit on port p.
IPX Ping Finished	IPX Ping test complete.
Sent	Statistics (in packets) of the finished IPX Ping tests.
Avg Round Trip Delay	Average round trip delay (in ms) for IPX ping packets (measured and displayed only when Q option is used). If the effective time of the whole IPX ping test is less than 10 ms, this statistic will not be displayed.

IPXSENDRIP1 and IPXSENDSAP1

These commands enable you to send RIP1 and SAP1 All Nets/Servers and Specified Net/Server type requests on a selected IPX circuit. Sending this packet enables you to verify the existence of the path(s) to selected networks and servers or update this paths parameters(metrics) unconditionally. This process is independent of normal advertising processes. These RIP1/SAP1 packets are designed to broadcast MAC addresses. These commands are recommended for service purposes only.

Syntax: **IPXSENDRIP1 net_number p[.c]**

Syntax: **IPXSENDSAP1 server_type p[.c]**

Parameter	Description
net_number	The IPX network number (max 8 hex digits) of the network for which metrics are requested. (net_number = FFFFFFFF means all known networks.)
server_type	The Type of IPX server (max 4 hex digits) for which parameters are requested. (server_type = FFFF means all known IPX servers of any type.)
p[.c]	Specifies the IPX circuit on which relevant RIP1 and SAP1 request packets are sent.
p	The port number on which the IPX circuit resides. Range: 0..255 (0..128 for XL 5.1 or later)
c	The IPX circuit on port p. If you omit this parameter, the command defaults to the first circuit on that port. Range: 1..4

IPXCFG

This command displays IPX Router global configuration information.

Syntax: **IPXCFG**

The IPXCFG command displays the following information:

Field	Description
IPX ROUTER	The IPX routing global state: enabled or disabled.
SPLIT PACKETS	This indicates whether to split packets on equivalent routes: enabled or disabled.
IPXR PRIORITY	The actual priority of IPX routed traffic: High[1], Normal[2], Low[3], Very Low [4], or None.
MAX REGIST PATHS	The maximum number of registered paths for each registered network and server. Range: 1..128.
MAX SPLIT PATHS	The maximum number of equivalent routes (paths) which IPX Router can split when forwarding traffic. Range: 1..32, with a value of 1 disabling split.
MAX HOPS	The maximum number of hops an IPX packet can take. Range: 1..16.
RIP PACKETS	The state of RIP packets global processing: enabled or disabled.
SAP PACKETS	The state of SAP packets global processing: enabled or disabled.
FLUSH TIME	When this timer expires, all aged networks and servers are removed from the tables.
INTRN NET/NODE	Network number and node number parts of an internal IPX address.
NetBios REDUCED	The state of NetBios Reduced Propagation (option: enabled/disabled).
SMART ADV CNT	The Reduced Advertising counter for IPX networks and servers (available for all circuits with Reduced Advertising Type OLD (Unacknowledged)).
MAX LOOPTIME	The maximum time interval for executing IPX code in 10 ms tics.
MAX GLOB PROC	Maximum number of IPX global processes available in an IPX router.

Alogic for nets The state of “Use Address Table for networks” option: ON or OFF.

Alogic for srvs The state of “Use Address Table for servers” option: ON or OFF.

Net on List OnlyThis flag indicates whether any IPX networks are registered only in the IPX Network Table (meaning it is not registered in the Address Table, the state=TRUE). If all IPX networks are registered in both the IPX Network Table and the Address Table, the state=FALSE displays.

Filters This indicates whether the address and smart filters are enabled or not for IPX router.

SRV on list onlyThis flag indicates whether any IPX servers are registered only in the IPX Server Table
TRUE = not registered in the Address Table
FALSE = all IPX servers are registered in both the IPX Server Table and the Address Table

TRACE This flag indicates that IPXTRACE option is active on any IPX circuit: States: ON or OFF.

PORT n.c The circuit number. n=port number, c=IPX circuit number on port n.

Port Type This field identifies the type of circuit: (Token Ring, Ethernet, WAN, X.25, Frame Relay, FPB, IRL, ISDN, ATM, SMDS etc.)

Net: [12341234]
The IPX network number of the network connected to the specified circuit.

Node: [112233445566]
The node address of the specified circuit.

ENABLE/DISABLE
The IPX routing state of the specified circuit.

ACTIVE/INACTIVE
Interface status depends on the proper physical connection and the physical interface state. If the status is ACTIVE, the specified circuit works properly. If the state is INACTIVE, a hardware problem has occurred, such as a break in the physical connection. If IPX routing is disabled on a circuit, the circuit is permanently INACTIVE.

Encap The type of IPX packet encapsulation on Frame Relay or X.25 circuits; ILAN CMPTBL (with MAC/LLC headers), IPX Q922 (RFC 1490 Frame Relay encapsulation), IPX RFC 1356 (X.25 encapsulation).

Fr.Type The type of IPX frame processed on specified circuit: TR 802.2, TR SNAP 8137, ETH 802.2, ETH 802.3, ETH SNAP 8137, ETH II 8137 (8137–protocol–type field).

IPX SR Mode The state of IPX Source Routing mode on specified circuit ON or OFF. Valid for TR, WAN, X.25, IRL, ISDN, ATM, and Frame Relay circuits.

SMADVRIP The state of RIP Reduced (Smart) Advertising on the specified circuit OLD (Unacknowledged), NEW (Acknowledged), or OFF. This is valid for point-to-point lines.

SMADVSAP The state of SAP Reduced (Smart) Advertising on the specified circuit OLD (Unacknowledged), NEW (Acknowledged), or OFF. This is valid for point-to-point lines.

continue This indicates that this is not a complete list of IPX router circuits. To display remaining circuits, enter the IXPCFG command again.

Example:

```
IPX ROUTER configuration:
      IPX ROUTER: Enable            SPLIT PACKETS: Disable        IPXR PRIOR-
            ITY: Normal[2]
      MAX REGIST PATHS: 3           MAX SPLIT PATHS: 1            MAX HOPS:
            16
      RIP PACKETS: Enable           SAP PACKETS: Enable           FLUSH TIME:
            180 sec
      INTRN NET: FFFF1111           INTRN NODE: 000000000001      NetBIOS
            REDUCED: Enable
      SMART ADV CNT: 005            MAX LOOPTIME: 010 tcs         MAX GLOB
            PROC: 010
      ALOGIC for nets: ON           ALOGIC for srvs: ON           TRACE: ON
      NET on list only:FALSE SRV on list only:FALSE
      Filters addr: ENABLED         Smart: ENABLED
PORT 004.1: Token Ring       Net:[00003281] Node:[680019CCBD00]  ENABLE
            ACTIVE
 Fr.Type: TR 802.2           IPX SR Mode: OFF
PORT 005.1: Token Ring       Net:[FFFFFFFF] Node:[680019CCBD80]  ENABLE
            INACTIVE
 Fr.Type: TR 802.2           IPX SR Mode: OFF
PORT 007.2: WANNet:[ABCD0002] Node:[16009833BD05]  ENABLE  ACTIVE
 Fr.Type: ETH 802.3               IPX SR Mode: OFF  Sm.Adv RIP: NEW  Sm.Adv
            SAP: NEW
PORT 008.1: FPBNet:[00000000] Node:[16009833BD08]  ENABLE  INACTIVE
 Fr.Type: ETH II (8137)
PORT 145.1: Fr.Relay         Net:[FFFFFFFF] Node:[16009833BD04]  ENABLE
            INACTIVE
  Encap:   IPX Q922          Sm.Adv RIP: OFF  Sm.Adv SAP: OFF
```

IPXGLOBCFG

This command displays IPX router configuration information in the format similar to the command IPXCFG on page 311. The difference is that the **IPXGLOBCFG** command displays all IPX router circuits, including those from other XLM boards (valid for XL version 3.x).

Syntax: **IPXGLOBCFG**

Field	Description
IPX ROUTER	The IPX routing global state: enabled or disabled.
SPLIT PACKETS	This indicates whether to split packets on equivalent routes: enabled or disabled.
IPXR PRIORITY	The actual priority of IPX routed traffic: High[1], Normal[2], Low[3], Very Low[4], or None.
MAX REGIST PATHS	The maximum number of registered paths for each registered network and server. Range: 1..28.
MAX SPLIT PATHS	The maximum number of equivalent routes (paths) which IPX Router can split when forwarding traffic. Range: 1..32, with a value of 1 disabling split.
MAX HOPS	The maximum number of hops an IPX packet can take. Range: 1..6.
RIP PACKETS	The state of RIP packets global processing: enabled or disabled.
SAP PACKETS	The state of SAP packets global processing: enabled or disabled.
FLUSH TIME	When this timer expires, all aged networks and servers are removed from the tables.
INTRN NET/NODE	Network number and node number ports of internal IPX address.
NetBios REDUCED	The state of NetBios Reduced Propagation (option: enabled/disabled).
SMART ADV CNT	The Reduced Advertising counter for IPX networks and servers (available for all circuits with Reduced Advertising Type OLD (Unacknowledged)).
MAX LOOPTIME	The maximum time interval for executing IPX code in 10 ms tics.

MAX GLOB PROC
: Maximum number of IPX global processes available in IPX routers

Alogic for nets
: The state of “Use Address Table for networks” option: ON or OFF.

Alogic for srvs
: The state of “Use Address Table for servers” option: ON or OFF.

Net on List Only
: This flag indicates whether any IPX networks are registered only in the IPX Network Table (meaning it is not registered in the Address Table, the state=TRUE). If all IPX networks are registered in both the IPX Network Table and the Address Table, the state=FALSE displays.

Filters
: This indicates whether the address and Smart Filters are enabled or not for IPX router.

SRV on List Only
: This flag indicates whether any IPX servers are registered only in the IPX Server Table (meaning it is not registered in the Address Table, the state=TRUE). If all IPX servers are registered in both the IPX Server Table and the Address Table, the state=FALSE displays.

TRACE
: This flag indicates that IPXTRACE option is active on any IPX circuit: States: ON or OFF.

PORT n.c
: The circuit number. n=port number, c=IPX circuit number on port n.

Port Type
: This field identifies the type of port: (Token Ring, Ethernet, WAN, X.25, Frame Relay, FPB, IRL, ISDN, ATM, SMDS etc.).

B: n
: The board number to which this circuit belongs.

Net: [12341234]
: The IPX network number of the network connected to the specified circuit.

Node: [112233445566]
: The node address of the specified circuit.

ENABLE/DISABLE
: The IPX routing state of the specified circuit.

ACTIVE/INACTIVE
: Interface status depends on the proper physical connection and the physical interface state. If the status is ACTIVE, the specified circuit works properly. If the state is INACTIVE, a hardware problem has occurred, such as a break in the physical connection. If IPX routing is disabled on a circuit, the permanent state inactive is set for the IPX router on this circuit.

Encap
: The type of IPX packet encapsulation on Frame Relay circuits, X.25 circuits etc.; ILAN CMPTBL (with MAC/LLC headers), IPX Q922 (RFC 1490 Frame Relay encapsulation), IPX RFC 1356 (X.25 encapsulation).

Fr.TYPE — The type of IPX frame processed on specified circuit TR 802.2, TR SNAP 8137, ETH 802.2, ETH 802.3, ETH SNAP 8137, ETH II 8137 (8137–protocol–type field).

IPX SR MODE — The state of IPX Source Routing mode on specified circuit ON or OFF. Valid for TR, WAN, X.25, IRL, ISDN, ATM, and Frame Relay circuits.

SMADVRIP — The state of RIP Reduced (Smart) Advertising on the specified circuit OLD (Unacknowledged), NEW (Acknowledged), or OFF. This is valid for point-to-point lines.

SMADVSAP — The state of SAP Smart Advertising on the specified circuit OLD (Unacknowledged), NEW (Acknowledged), or OFF. This is valid for point-to-point lines.

continue — This indicates that this is not a complete list of IPX router circuits. To display remaining circuits, enter the **IXPGLOBCFG** command again.

Example:

```
IPX ROUTER configuration:
  IPX ROUTER: EnableSPLIT PACKETS: Disable IPXR PRIORITY: Normal[2]
      MAX REGIST PATHS: 3      MAX SPLIT PATHS: 1        MAX HOPS: 16
      RIP PACKETS: Enable      SAP PACKETS: Enable       FLUSH TIME: 180 sec
      INTRN NET: FFFF1111      INTRN NODE: 000000000001NetBIOS REDUCED:
                 Enable
      SMART ADV CNT: 005       MAX LOOPTIME: 010 tcs     MAX GLOB PROC: 010
      ALOGIC for nets: ON      ALOGIC for srvs: ON       TRACE: ON
      NET on list only:FALSE   SRV on list only:FALSE
      Filters addr: ENABLED    Smart: ENABLED
PORT 004.1: Token RingB:03 Net:[00003281] Node:[680019CCBD00]  ENABLE
                 ACTIVE
 Fr.Type: TR 802.2     IPX SR Mode: OFF
PORT 005.1: Token Ring B:03 Net:[FFFFFFFF] Node:[680019CCBD80]  ENABLE
                 INACTIVE
 Fr.Type: TR 802.2     IPX SR Mode: OFF
PORT 007.2: WANB:03 Net:[ABCD0002] Node:[16009833BD05]  ENABLE  ACTIVE
 Fr.Type: ETH 802.3             IPX SR Mode: OFF  Sm.Adv RIP: NEW  Sm.Adv SAP:
                 NEW
PORT 008.1: FPBB:03 Net:[00000000] Node:[16009833BD08]  ENABLE  INACTIVE
 Fr.Type: ETH II (8137)
PORT 145.1: Fr.RelayB:03 Net:[FFFFFFFF] Node:[16009833BD04]  ENABLE  INAC-
                 TIVE
  Encap:   IPX Q922   Sm.Adv RIP: OFF  Sm.Adv SAP: OFF
ILAN/XL(3)>
```

IPXPORTCFG

This command displays IPX Router configuration information for a specified IPX circuit.

Syntax: **IPXPORTCFG p[.c]**

Field	Description
IPX Port n.c	The circuit number. n=port number, c=IPX circuit number on port n.
Port Type	This field identifies the type of circuit: (Token Ring, Ethernet, WAN, X.25, Frame Relay, FPB, IRL, ISDN, ATM, SMDS etc.).
Net: [11221122]	The IPX network number of the network connected to the specified circuit.
Node: [112233112233]	The node address of the specified circuit.
ENABLE/DISABLE	The IPX routing state of the specified circuit.
ACTIVE/INACTIVE	Interface status depends on the proper physical connection and the physical interface state. If the status is ACTIVE, the specified circuit works properly. If the state is INACTIVE, a hardware problem has occurred, such as a break in the physical connection.
Fr.Type	The type of IPX frame processed on the specified circuit: TR 802.2, TR SNAP 8137, ETH 802.2, ETH 802.3, ETH SNAP 8137, or ETH II 8137 (8137–protocol type field).
IPX SR Mode	The state of IPX Source Routing mode on specified circuit: enabled or disabled. Valid for Token Ring, WAN, X.25, ISDN, ATM, IRL and Frame Relay circuits.
Sm Adv RIP	The state of RIP Reduced (Smart) Advertising on specified circuit: OLD (Unacknowledged), NEW (Acknowledged), or OFF.
Sm Adv SAP	The state of SAP Reduced (Smart) Advertising on specified circuit: OLD (Unacknowledged), NEW (Acknowledged), or OFF.
RIP/SAP	The state of RIP/SAP packet processing on specified circuit: enabled or disabled.
SAP4 pkts	The state of Get Nearest Server Reply packet sending on specified circuit: enabled or disabled.
IPX NetBIOS	The state of NetBIOS over IPX packets processing on specified circuit: enabled or disabled.
Port Delay	The delay (in tics) corresponding to the network connected to the specified circuit.

Delay In/Out	The delay offset (in tics) added for each network or server registered or advertised through the specified circuit. Range: 0..255
Hops In/Out	The hops offset (in tics) added for each network or server registered or advertised through the specified circuit. Range: 0..14
RIP/SAP updt time	The update time (in seconds) for RIP/SAP advertisements on specified circuit. Range: 30..65535
RIP/SAP age mltp	The age multiplier for RIP/SAP advertisements on specified circuit. Range: 2..255
No RIP/SAP entry	The maximum number of RIP/SAP entries in a RIP/SAP packet on the specified circuit. Minimum: 4
RIP/SAP delay	The delay (in tics) between the following RIP/SAP packets sending on specified circuit.
IPX Backw	The state of IPX Backward Routing on specified circuit: enabled or disabled. (IPX Backward Routing is sending an IPX packet on the same circuit on which it was received.)
IPX max pkt size	The maximum size of IPX packets (not RIP and not SAP) processed on specified circuit.
RIP adv	The state of RIP advertising process: ON or OFF. ON state indicates that the process is currently active.
SAP adv	The state of SAP advertising process: ON or OFF. ON state indicates that the process is currently active.
RIP splith	The state of RIP Split Horizon algorithm on the circuit: ON or OFF.
SAP splith	The state of SAP Split Horizon algorithm on the circuit: ON or OFF.
TRACE state	The state of the tracing process (IPXTRACE) on the circuit: ON or OFF. ON state indicates that SAP and RIP packets received/ transmitted on this circuit are displayed.
Spoofing	The state of the Watchdog Spoofing option on a specified circuit. If this option is ON then for each “watchdog” request. packet (which should be forwarded through this circuit), IPX Router will respond to the sender with “watchdog response” (any watch dog request will not be forwarded through this circuit).
Trace parameters	These are detailed parameters of the IPXTRACE process on the circuit. These parameters display only when the TRACE state is ON (on this circuit). See also the command IPXTRACE on page 333 for a description.

IPXNETS

There are two commands that allow you to display routes from the routing table: IPXNET on page 321(which displays a single specified route) and this command, **IPXNETS**, which displays the requested fragment of the routing table (that will fit onto a 24-line terminal). Use the command IPXNOFNET on page 321 to display the number of different IPX network numbers registered in the routing table.

Syntax: IPXNETS [sequential number]

Networks in the routing table are given sequential numbers starting from 1. The optional parameter, **sequential number**, allows you to select the starting network number to be displayed. If the command is entered without a parameter, the routing table will be displayed beginning with the table entry after the last entry displayed.

For all registered routes for the networks, the command will return a main row for each network and, immediately following each of these rows, a row for each registered path for that network. Reading across the row, the display fields are:

Field	Description
number	The sequence number for the network in this row.
D/S/R/I	The protocol type of the network. D Direct (local) network. A direct network is directly connected to the specified circuit. R Remote Network. A network or path learned from a RIP packet. S Static network. A static network is a permanent router stored in non-volatile memory. I Internal network. A unique internal network number can be associated with each device on which the IPX router is enabled. Internal network numbers are usually registered on a unique virtual circuit.
NetNumber	The IPX network number.
Nof Paths	The number of paths registered for this IPX network. There will be this many rows immediately following this row, each of which will contain the information described below.

For each registered path (route) the following information is displayed (reading across the row):

Field	Description
D/N/S/R/I	The protocol type of IPX network for this registered path.
hh/dddd	The hops (hh) and delay (dddd) registered for this path.
nnn.c	The circuit number through which the path has been registered. If n is 008, the path is registered through IBI. In this case, the real circuit number (described below) is the actual circuit through which this path has been registered.
[mmmmmmmmmmmm]	The node (MAC) address from which the path has been learned (next hop MAC address). For XL 3.x devices, if the port number nnn (see above) is 008, the path is registered through IBI and this value is an internal IBI MAC address of the board that originated the advertisement. In this case, the real node address indicates the address from which the path has been received (actual next hop MAC address).
continue	If "continue" is displayed, there are still more items to display.
All nets:	The number of different IPX network numbers registered in the routing table.

Example

```
00001)  D  NetNumber:  99229922     Nof Paths: 1
   D  00/0002  007.1  [160098337445]
00002)  S  NetNumber:  00000400     Nof Paths: 1
   S  00/0002  008.1  [160098137448]
00003)  B  NetNumber:  00000327     Nof Paths: 1
   N  00/0001  008.1  [160098137448]
00004)  R  NetNumber:  00000004     Nof Paths: 1
   R  01/0002 008.1  [160098137448]
00005)  R  NetNumber: 00000080     Nof Paths: 1
   R  01/0002  008.1 [160098137448]
00006)  R  NetNumber:  DADA0000     Nof Paths: 1
   R  01/0002  008.1 [160098137448]
00007)  R  NetNumber:  00022000     Nof Paths: 2
   R  02/0003  008.1 [160098137448]
   R  02/0003  008.1 [160098137448]
00008)  R  NetNumber:  00000777     Nof Paths: 2
   R  02/0003  008.1 [160098137448]
   R  02/0003  008.1 [160098137448]
 continue
All nets: 47
```

IPXNET

There are two commands that allow you to display routes from the routing table: IPXNETS on page 319 (which displays a requested fragment of the routing table) and this command, **IPXNET**, which displays a single specified route. Use the command IPXNOFNET on page 321 to display the number of different IPX network numbers registered in the routing table.

Syntax: IPXNET network number

Field	Description
NetNumber	The IPX network number.
Nof Paths	The number of paths registered for this IPX network.
D/N/S/R/I	The protocol type of IPX network.
Port: ppp.c(ppp.c)	The circuit number and real circuit number through which the path is registered.
NextHopMAC: mmmmmmmmmmmm	The MAC address and from which the path has been received (next hop MAC address).
Hop	The number of hops registered for this path.
Delay	The delay (in tics) registered for this path.
Age	The time (in seconds) from the last RIP update received from Next Hop MAC. The age is always zero for static, direct (local) and internal networks and for a route registered through a circuit with RIP Reduced (Smart) Advertising enabled.

Example

```
NetNumber: 00000080      Nof Paths: 1
R  Port:008.1(000.1)  NextHopMAC: 160098137448  Hop:01  Delay: 02    Age: 010
```

IPXNOFNET

This command, which requires no parameters, displays the number of IPX network numbers registered in the routing table.

Syntax: IPXNOFNET

IPXSTATICNET

The **IPXSTATICNET** command can display all IPX static networks stored in non–volatile memory. With this command, you can monitor the static networks stored in non–volatile memory.

Syntax: **IPXSTATICNET**

This command displays information about all static networks recorded in non–volatile memory.

Field	Description
S	This indicates that the IPX network is Static.
n.c	(in above example, 000.1 and 001.1) The circuit number on which static route is registered.
[123123123123]	The next hop MAC address for this static route.
22112211	The IPX network number of this static route.
03/006	The hops and delay corresponding to this static route.
All static nets: n	This value (n) is the number of different IPX static network numbers registered in non–volatile memory.

Example

```
S:000.1:[123123123123]  22112211  03/006  S 000.1:[222222333333] 21212121  02/003
                All static nets: 2
```

IPXFLTNET

With IPXFLTNET, you can monitor the IPX network filters stored in non–volatile memory.

Syntax: IPXFLTNET

Syntax: IPXFLTNET net_number

Without the net_number parameter, basic information about all networks is displayed. To get more precise information about a specific network, add the net_number parameter. For each type of filter, the complete list of relevant circuits information will be displayed.

Field	Description
NetNumber	The IPX network number of the filter.
OUTPOS: active	This indicates that an output positive filter is defined for at least one circuit (any RIP advertisement with a network number 00000400 will not be sent through this circuit).
OUTNEG: active	This indicates that an output negative filter is defined for at least one circuit (any RIP advertisement with a network number other than 00000400 will not be sent through this circuit).
INPOS: active	This indicates that an input positive filter is defined for at least one circuit (any RIP advertisement with a network number 00000400 will be filtered if it is received through this circuit).
INNEG: active	This indicates that an input negative filter is defined for at least one circuit (any RIP advertisement with a network number other than 00000400 will be filtered if it is received through this circuit).
All network filters	This value indicates the total number of IPX network filters stored in non–volatile memory.

Example 1 (without net_number parameter)

```
NetNumber: 00000400  OUTPOS: active   OUTNEG: active
                     INPOS: active     INNEG: active
 All network filters: 1
```

Example 2 (with net_number parameter)

NetNumber: 00000400
OUTPUT POSITIVE FILTER ON CIRCUITS:
001.1, 005.1, 006.1, 100.1, 101.1, 102.1, 103.1, 104.1, 105.1, 106.1, 107.1, 108.1, 109.1, 110.1, 111.1,
112.1, 113.1, 115.1, 184.1, 185.1, 188.1, 192.1

OUTPUT NEGATIVE FILTER ON CIRCUITS:
001.1, 002.1
INPUT POSITIVE FILTER ON CIRCUITS:
002.1, 104.1, 105.1, 106.1, 107.1, 108.1, 109.1, 112.1
INPUT NEGATIVE FILTER ON CIRCUITS:
001.1, 002.1

IPXSRVS

There are two commands that allow you to display servers registered in the server table: IPXSRV on page 327 (which displays a single specified server) and this command, **IPXSRVS**, which displays a requested fragment of the server table. Use the command IPXNOFSRV on page 328 to display the number of different servers registered in the server table.

Syntax: **IPXSRVS [sequential number]**

Servers in the server table are given sequential numbers starting from 1. The optional parameter, **sequential number**, allows you to select the starting server number to be displayed. If the command is entered without a parameter, the server table will be displayed beginning with the table entry after the last entry displayed. The command will display all registered servers. Reading across the row, the display fields are:

Field	Description
sssss	The server's sequence number.
R or S	The protocol type of the server:
R	Remote server (learned from SAP packet).
S	Static server.
Name	The registered server name.
Type	The type of server.
NetNumber	The network number where the server exists.
MAC	The server's node number.
Socket	The server's socket number.

For each registered path (route) to the server described above, there is a row underneath that described the path. Read across the row, the display fields are:

Field	Description
hop	The number of hops registered for the path.
ppp.c [mmmmmmmmmmmm]	
The circuit number under which this route is registered and the MAC address from which the path is received. If ppp is 008, the path is registered through IBI. In this case, the real circuit number (described below) is the actual circuit through which this path has been registered.	
ppp.c [mmmmmmmmmmmm]	
The real circuit number and real node address for this path.	
continue	If "continue" is displayed, there are more items to display.
All nets:	The number of different servers registered in the server table.

Example

```
ILAN/XL(3) > IPXSRVS 9
00009)  R  Name:  RASTRO
       Type:   0004  NetNumber: 0000CCFC  MAC  000000000001 Socket 045
         Hop: 03  008.1 [160098137448]
00010)  S  Name:  STATIC
       Type:   0004  NetNumber: 00000400  MAC  000000000001 Socket 045
         Hop: 02  008.1 [160098137448]
00011)  R  Name:  STUDENTCI
       Type:   0004  NetNumber: 0000000B  MAC  000000000001 Socket 045
         Hop: 02  008.1 [160098137448]
00012)  R  Name:  TEST
       Type:   0004  NetNumber: 19041994  MAC  000000000001 Socket 045
         Hop: 02  008.1 [160098137448]
00013)  R  Name:  CC_MAIL_PRINTER
       Type:   0047  NetNumber: 00001324  MAC  000000000001 Socket 045
         Hop: 03  008.1 [160098137448]
       Type:   0047  NetNumber: 19041994  MAC  000000000001 Socket 045
         Hop: 03  008.1 [160098137448]
00015)  R  Name:  EURO_LASER
       Type:   0047  NetNumber: 0000CCE1  MAC  000000000001 Socket 045
         Hop: 03  008.1 [160098137448]
  continue
All servers: 24
```

IPXSRV

There are two commands that allow you to display servers registered in the server table: IPXSRV on page 327 (which displays a requested fragment of the server table) and this command, IPXSRV, which displays a single specified server. Use the command IPXNOFSRV on page 328 to display the number of different servers registered in the server table.

Syntax: IPXSRV {sequential number | server_name server_type}

This command displays the parameters of the specified server and all the paths corresponding to the server. You can indicate a particular server by entering its sequential number or its name and type.

Field	Description
Name	The server name.
Type	The type of server.
Protocol	The protocol type of the server: Remote (learned from SAP packet) or Static.
NetNumber	The IPX network number in which this server exists.
MAC	Node (MAC) address of the server.
Socket	The socket on which the server communicates.
Port	The circuit (real circuit) number through which the path to the server is registered.
NextHopMAC	The node (real node) address from which the path to the server was received (next hop MAC address).
Hop	The number of hops registered for this path to the server.
Age	The time (in seconds) from the last SAP update received from Next Hop MAC. The age is always zero for static servers and for a path registered through a circuit with Reduced (Smart) Advertising enabled.

Example

Name: CC_MAIL Type: 0004
Protocol: Remote NetNumber: 00001324 MAC: 000000000001 Socket: 045
Port:008.1 NextHopMAC: 160098137448 Hop: 02 Age 020

IPXNOFSRV

This command, which requires no parameters, displays the count of servers registered in the server table.

Syntax: **IPXNOFSRV**

IPXSTATICSRV

The **IPXSTATICSRV** command displays all IPX static servers stored in non–volatile memory.

Syntax: **IPXSTATICSRV**

Field	Description
Port	The circuit number through which all paths to this server should be registered.
Name	The name of the static server
Type	The type of static server.
NetNumber	The number of IPX network in which the server resides.
MAC	The node (MAC) address of the static server.
Socket	The socket number on which the static server communicates.

All static servers: n

The number of IPX static servers registered in non–volatile memory.

Example

```
00001)  Port: 000.1   Name:  STATIC
        Type: 0004  NetNubmer: 00000400  MAC 000000000001  Socket: 045

Att static servers: 1
```

IPXFLTSRV

With **IPXFLTSRV**, you can monitor the IPX server filters stored in non–volatile memory. With no server number parameter specified, it displays information about all IPX server filters recorded in non–volatile memory. If you specify a server number, it displays circuit details for that server.

Syntax: IPXFLTSRV

Syntax: IPXFLTSRV server_number

Field	Description
fffff	The server filter number.
Type	The server filter type.
Server	The server filter name.
OUTPOS:	This indicates that an output positive filter is defined for at least one circuit (any SAP advertisement with the specified server will not be sent through this circuit).
OUTNEG:	This indicates that an output negative filter is defined for at least one circuit (any SAP advertisement with a server other than this one, will not be sent through this circuit).
INPOS:	This indicates that an input positive filter is defined for at least one circuit (any SAP advertisement with the specified server will be filtered if it is received through this circuit).
INNEG:	This indicates that an input negative filter is defined for at least one circuit (any SAP advertisement with a server other than this one, will be filtered if it is received through this circuit).
All server filters:	The number of server filters stored in non–volatile memory.

Example 1 (with no server specified)

```
00001)  Type:  0004  Name:  STATIC
        OUTPOS: active    OUTNEG: active
         INPOS: active     INNEG: active
All server filters:   1
```

Example 2 (with a server specified)

00001) Type: 0004 Name: STATIC

OUTPUT POSITIVE FILTER ON PORTS:
000.1,001.1, 003.1, 005.1, 009.1, 168.1

OUTPUT NEGATIVE FILTER ON PORTS:
159.1, 160.1, 162.1, 166.1, 168.1

INPUT POSITIVE FILTER ON PORTS:
104.1, 107.1, 108.1, 111.1, 115.1, 117.1, 146.1, 150.1, 155.1

INPUT NEGATIVE FILTER ON PORTS:
021.1, 022.1, 025.1, 147.1, 152.1, 153.1

IPXGLOBSTATS

This command displays IPX global statistics.

Syntax: **IPXGLOBSTATS**

Field	Description
total rcv	The total number of IPX packets received, including those received in error.
hdr err	The number of IPX packets discarded due to errors in the headers, including any IPX packets with a size less than the minimum of 30 bytes.
unkn skt	The number of IPX packets discarded because the destination socket was not open.
rcv flt	The number of incoming IPX packets discarded due to filtering.
rcv dscrd	The number of IPX packets received but discarded due to reasons other than those accounted for by: hdr err, unkn skt, and rcv dscrd.
rcv loc	The number of IPX packets delivered locally.
too many	The number of IPX packets discarded due to exceeding the maximum hop count.
rip incor	The number of times that an incorrectly formatted RIP packet was received.
sap incor	The number of times that an incorrectly formatted SAP packet was received.
NetBIOS	The number of NetBIOS over IPX packets (IPX Type 20 packets) received.
tot srvc	The number of IPX frames serviced and routed.
tot rout	The number of IPX packets forwarded.
no space	The number of times the IPX router has been unable to obtain memory.
no rbuf	The number of times the IPX packet was not received because of a shortage or receive buffers.
total out	The total number of IPX packets transmitted.
out req	The number of IPX packets that were supplied locally for transmission, not including any packets counted in tot rout.
no rout	The number of times no route to a destination was found.
out filt	The number of outgoing IPX packets discarded due to filtering.
out dscrd	The number of outgoing IPX packets discarded due to a processing problem.
dst cnt	The number of currently reachable destinations known to the IPX router.

srvdst cnt	The number of services known to this IPX router.
max skt	The configured maximum number of IPX sockets that may be opened at one time.

Example

IPX Global Statistics

total rcv 0000000231

hdr err	0000000000	unkn skt	0000000000		
rcv flt	0000000000	rcb dscrd	0000000000		
rcv loc	0000000231	too manu	0000000000		
rip incor	0000000000	sap incor	0000000000		
NetBIOS	0000000000	tot srvc	0000000231		
tot rout	0000000000	no space	0000000000		

total out 0000001015

out req	0000000003	no rout	0000000000		
out filt	0000000000	out dscrd	0000000000		
dst cnt	00048	srvdst cnbt	00024	max skt	006

IPXTRACE

These commands toggle between displaying input and output RIP, SAP and NetBIOS over IPX Packets and not displaying RIP, SAP, and NetBIOS over IPX Packets. There are several servers and NetWare networks registered through an IPX router. Switching to TRACE ON mode causes RIP and SAP frames to display, causing a loss in router performance.

Syntax: **IPXTRACE ON [p[.c]] [RIP1 | RIP2 [net_no] | SAP1 | SAP3 | SAP4 | SAP2[n=srv_name][srv_type]]L=name_len]|TYPE20|SPX]**

This command enables you to display input and output by RIP, SAP, SPX and NetBios over IPX either globally or on a specified IPX circuit. Specified types of RIP | SAP | SPX | NetBIOS packet can be displayed globally or on a selected circuit.

Syntax: **IPXTRACE OFF [p[.c]]**

This command stops the display of any input and output by RIP, SAP, SPX and NetBios over IPX either globally or on a specified IPX circuit.

Parameter	Description
p[.c]	Specifies the circuit to enable/disable the trace. If this parameter is omitted, the command applies to all circuits available in the IPX router.
p	The port number on which the IPX circuit resides. Range: 0..255 (0..128 for XL 5.1 or later).
c	The IPX circuit on port p. If you omit this parameter, the command defaults to the first circuit on that port. Valid values are from 1 to 4.
RIP1	Display all input/output RIP1 request packets only.
RIP2 [net_no]	Display all input/output RIP2 response packets and RIP2 acknowledged packets on point-to-point lines with RIP Reduced Advertising Type NEW(acknowledged). You can also select only those packets that contain specified IPX network numbers only (net_no= max 8 hex digits)
SAP1/SAP3/SAP4	Display all input/output SAP1 requests; or input SAP3 Get Nearest Server Requests; or output from SAP4 Get Nearest Server Replies only.

SAP2 [N=srv_name] [srv_type] [L=name_len]

Display all input/output SAP2 response packets only (on packet–to–packet lines with SAP Reduced Advertising type NEW (acknowledged) SAP2 acknowledge packets are also displayed). You can optionally select only those SAP2 packets which contain IPX servers with specified server type (maximum of 9 hexadecimal digits) and/or with specified server names(s) which matches srv_name pattern (maximum of 47 ASCII characters). You can also specify the length of the displayed server names. Only a single server name can be used at the same time. This means that the last specified srv_name is valid for IPXTRACE on all IPX circuits.

TYPE20 Display all input/output NetBios over IPX (IPX Type 20) packets only.

Example (RIP response)

RIP response:	
IN [007.1:111111222222]	RIP2 Response
22221111 01/002	
Net entries: 1	
IN [007.1:16009839E218]	RIP2 Acknowledgment
22221111 02/003	
Net entries: 1	
OUT [002.1:FFFFFFFFFFFF]	RIP2 Response
22221111 02/003	
11223344 01/002	
Net entries: 2	

Display Field	Description
IN or OUT	Whether the packet is incoming or outgoing.
[ppp.c:mmmmmmmmmmmm]	The circuit number (ppp.c) through which the packet is incoming or outgoing, followed by the source node MAC address (for an incoming packet) or destination node MAC address (for an outgoing packet). An mmmmmmmmmmmm of FFFFFFFFFFFF indicates a broadcast IPX address.
RIP2 Response/Acknowledge	The type of RIP2 packet. A RIP2 Acknowledge packet is the acknowledgment for a RIP2 Response packet sent on point–to–point lines with RIP Reduced Advertising type NEW (Acknowledged).
nnnnnnnn hh/ddd	The IPX network number (nnnnnnnn), hops (hh), and delay (ddd) of the advertised route.
Net entries	The number of advertised IPX networks in this RIP2 packet.

Example (SAP response)

```
IN [007.1:111111222222]                          SAP2 Response

CROSS_COMM_SERVER_1     0004 03

Net entries: 1
IN [007.1:16003839E218]                          SAP2 Acknowledge
CROSS_COMM_SERVER_1     0004 04
Net entries: 1

OUT [002.1:FFFFFFFFFFFF]                         SAP2 Response
CROSS_COMM_SERVER_1     0004 04
Net entires: 1

OUT [002.1:FFFFFFFFFFFF]                         SAP1

CROSS_COMM_SERVER_1
```

Field	Description
IN or OUT	Whether the packet is incoming or outgoing.
[ppp.c:mmmmmmmmmmmm]	The circuit number (ppp.c) through which the packet is incoming or outgoing, followed by the source node MAC address (for incoming packets) or destination node MAC address (for outgoing packets). An mmmmmmmmmmmm of FFFFFFFFFFFF indicates a broadcast IPX address.
SAP2 Response or Acknowledge	The type of SAP2 packet. SAP2 Acknowledge packets are for the acknowledgment to SAP2 Response packets sent on point–to–point lines with SAP Reduced Advertising type NEW (Acknowledged).
server	The server type and registration of the advertised server.
SAP 4 srv_name	The Get Nearest Server Reply, with relevant server name.
Net entries	The number of advertised IPX servers in the SAP2 packet.

Example (RIP request)

```
RIP Request:

                                        RIP 1 Request – All Nets

IN [002.1:111111222222]
IN [002.1:111111222222]                 RIP 1 Request – 00112233
```

Field	Description
IN or OUT	Whether the packet is incoming or outgoing.
[ppp.c:mmmmmmmmmmmm]	The circuit number (ppp.c) through which the packet is incoming or outgoing, followed by the source node MAC address (for incoming packets) or destination node MAC address (for outgoing packets). An mmmmmmmmmmmm of FFFFFFFFFFFF indicates a broadcast IPX address.
RIP 1 Request All Nets	This means to return all known networks.
RIP 1 Request nnnnnnnn	This means to return specified network information on the indicated circuit.

Example (SAP request)

```
SAP Request:
IN [002.1:111111222222]                 SAP 1 Request  –  All Servers
IN [002.1:111111222222]                 SAP 1 Request –  Server Type: 04
IN [002.1:111111222222]                 SAP 3 Request
```

Field	Description
IN or OUT	Whether the packet is incoming or outgoing.
[ppp.c:mmmmmmmmmmmm]	The circuit number (ppp.c) through which the packet is incoming or outgoing, followed by the source node MAC address (for incoming packets) or destination node MAC address (for outgoing packets). An mmmmmmmmmmmm of FFFFFFFFFFFF indicates a broadcast IPX address.
SAP 1 Request – All Servers	This is a General Service Query request on the specified circuit.
SAP 1 Request – Server Type: t	This is a Service Query request for specified type t servers.
SAP 3 Request	The Get Nearest Service Query request on the specified circuit.

Example (SPX session registration)

SPX:> Insert session's descriptor,
SPX:> SRC:AAB00002:000000000001:8104 eb0:910e
SPX:> DST:00003109:0000C09010EE:4022 910e:eb0
Indicates that an SPX session has been registered in the router, with the following display fields:

Field	Description
SRC:AAB00002:000000000001:8104 eb0:910e	The source address of the received frame.
DST:00003109:0000C09010EE:4022 910e:eb0	The destination address of the received frame.

```
SPX:> RECEIVED:  AAB00002:000000000001:8104 db0:900e S:23 A:7
data_t:00 ctrl_t:80 Circ:001.1  FORWARD
SPX:> RECEIVED:  00003109:0000C09010EE:4022 900e:db0 S:7 A:23
data_t:00 ctrl_t:80 Circ:000.1  SPOOF
SPX:> SNDOUTAS: 00003109:0000C09010EE:4022 900e:db0 S:7 A:23
data_t:fe ctrl_t:10 Circ:000.1  SPX_EOC
SPX:> RECEIVED:  AAB00002:000000000001:8104 db0:900e S:23 A:8
data_t:ff ctrl_t:10 Circ:001.1  SPX_EOC_ACK
```

Field	Description
SPX:> RECEIVED:/SNDOUTA:	The SPX trace prefix with the direction signs, RECEIVED - if the frame was received, SNDOUTAS - if the frame was reconstructed in the router and sent out as a frame from a station on a send back direction.
AAB00002:000000000001:8104	The IPX address (NET:NODE:SOCKET).
db0:900e	The connection ID (dstID:srcID).
S:23 A:7	The sequence number (S:23) and the acknowledge number (A:7).
data_t:00	The datastream type: fe - EndOfConnection message was received (SPX_EOC) ff - EndOfConnectionAck message was received (SPX_EOC_ACK) 00-fd - Client Defined
ctrl_t:10	The connection control field.
FORWARD, SPOOF	The status of the registered session.
SPX_EOC, SPX_EOC_ACK	This indicates the message type (End of Connection or End of Connection Acknowledged).

IPX UNIQMAC

This command enables or disables unique MAC address on an IPX port.

Syntax: **IPX UNIQMAC {ENABLE | DISABLE} p.c**

Parameter	Description
p.	IPX port
c	IPX circuit

IPXDEFROUTE CFG

Use this command to display current the Default Route configuration

Syntax: **IPXDEFROUTE CFG**

IPXDEFROUTE {ENABLE | DISABLE}

Use this command to enable or disable the Default Route Mechanism.

Syntax: **IPXDEFROUTE {ENABLE | DISABLE}**

IPXDEFROUTE NETLESS SRV {ENABLE | DISABLE}

Use this command to enable or disable the Learning Netless Servers.

Syntax: **IPXDEFROUTE NETLESS SRV {ENABLE | DISABLE}**

IPXDEFROUTE HELP

Use this command to display short help for the console commands related to Default Route Mechanism.

Syntax: **IPXDEFROUTE HELP**

IPXNETBSTRICT {ENABLE | DISABLE}

The following commands enables and disables dropping IPX NetBIOS frames with non-zero unused padding in field were traversed networks are stored.

Syntax: **IPXNETBSTRICT {ENABLE | DISABLE}**

Parameter	Description
ENABLE	Frames with the non-zero traversed network numbers are dropped.
DISABLE	IPX Router does not check the frames for 0x0 or 0xffffffff traversed network numbers and, in result, does not drop such frames. This option is a default.

20. ISDN Commands

ISDN SET INTERFACE MODE

Sets the mode of operation for ISDN on a specific interface.

Syntax: ISDN SET INTERFACE i MODE {MONO | DUAL}

Parameter	Description
i	The number of the ISDN interface.
MONO	Creates a single virtual circuit (64000 bps) on the specified interface.
DUAL	Creates two virtual circuits (64000 bps) on the specified interface.

ISDN SET INTERFACE SERV

Sets the switch service type for ISDN.

Syntax: ISDN SET INTERFACE i SERV {5E | EU | DM | GR | N1}

Parameter	Description
i	The number of the ISDN interface.
5E	5ESS switch (only with firmware for North America)
EU	EuroISDN/ NET3 switch (including French Delta) (only with firmware for Europe)
DM	DMS100 switch (only with firmware for North America)
1T	1TR6 switch (only with firmware for Europe)
N1	US National 1 switch (only with firmware for North America)

ISDN SET VC ON and ISDN SET VC OFF

Sets the operational state of ISDN virtual circuits.

Syntax: **ISDN SET VC i c {ON | OFF}**

Parameter	Description
i	The number of the ISDN interface.
c	The number of the ISDN virtual circuit defined on that interface.
ON	Activates the virtual circuit.
OFF	Deactivates the virtual circuit.

ISDN SET VC NCA

Sets the number of attempts allowed to reestablish the connection over an ISDN link.

Syntax: **ISDN SET VC i c NCA {value | PERMANENT}**

Parameter	Description
i	The number of the ISDN interface.
c	The number of the ISDN virtual circuit defined on that interface.
value	The number of attempts allowed to reestablish the connection over an ISDN link. Range: 1..255, or PERMANENT (which means retries will be persistent).

ISDN SET VC RI

This command defines the number of seconds that must elapse between subsequent call retries.

Syntax: **ISDN SET VC i c RI value**

Parameter	Description
i	The number of the ISDN interface.
c	The number of the ISDN virtual circuit defined on that interface.
value	The number of seconds that must elapse between subsequent call retries. Range: 1..255.

ISDN SET VC ACF

This command determines the method the virtual circuit accepts an incoming call.

Syntax: **ISDN SET VC i c ACF {ALL | SELECTED | NONE}**

Parameter	Description
i	The number of the ISDN interface.
c	The number of the ISDN virtual circuit defined on that interface.
ALL	Accepts all calls.
SELECTED	Accepts only incoming calls from numbers that match one of the security numbers. This option is available only when “Connect to CrossComm/ Olicom ISDN SIM” option is enabled (commandISDN SET VC CCSIM {ON | OFF} on page 350). The list of security numbers can be defined using command ISDN SET VC SEC on page 346.
NONE	Accepts none of the incoming calls

ISDN SET VC FPH

Sets the telephone number of the remote (far–end) ISDN interface that is intended to be called.

Syntax: **ISDN SET VC i c FPH phn [vc]**

Parameter	Description
i	The number of the ISDN interface.
c	The number of the ISDN virtual circuit defined on that interface.
phn	The remote (far–end) telephone number. Maximum: 20 digits
vc	The VC number that identifies virtual circuit (VC) on the remote interface to which the call is sent. If not specified, the first free virtual circuit is used. Range: 1..2

ISDN SET VC FPH DEL

This command deletes the telephone number of the remote (far–end) ISDN interface that is intended to be called.

Syntax: **ISDN SET VC i c FPH DEL**

Parameter	Description
i	The number of the ISDN interface.
c	The number of the ISDN virtual circuit defined on that interface.
DEL	Deletes the remote (far–end) telephone number.

ISDN SET VC MPH

Sets the telephone number of the local (own) ISDN interface.

Syntax: **ISDN SET VC i c MPH phone**

Parameter	Description
i	The number of the ISDN interface.
c	The number of the ISDN virtual circuit defined on that interface.
phone	The telephone number of the local ISDN interface. Maximum: 20 digits

ISDN SET VC MPH DEL

This command deletes the telephone number of the local (own) ISDN interface.

Syntax: **ISDN SET VC i c MPH DEL**

Parameter	Description
i	The number of the ISDN interface.
c	The number of the ISDN virtual circuit defined on that interface.
DEL	Deletes the local (own) telephone number.

ISDN SET VC SPID

(Applicable only to U.S. ISDN standards US-N1 and DMS-100) Establishes the Service Profile Identification (SPID) for the ISDN virtual circuit. There are two SPIDs and two telephone numbers per ISDN line/interface (each SPID is assigned to a telephone number).

Syntax: **ISDN SET VC i c SPID spid**

Parameter	Description
i	The number of the ISDN interface.
c	The number of the ISDN virtual circuit defined on that interface.
spid	The Service Profile Identification assigned to the specified ISDN virtual circuit. The telephone number assigned to this SPID must be defined as the local phone number for the Virtual Circuit (VC).

Most Virtual Circuit parameters can be changed while the interface is active (as long as the VC state is off), but you must cycle the interface if you change the SPID or if you use ISDN with SPID and you change a local phone number.

ISDN SET VC SPID DEL

This command deletes the telephone number of the local (own) ISDN interface.

Syntax: **ISDN SET VC i c SPID DEL**

Parameter	Description
i	The number of the ISDN interface.
c	The number of the ISDN virtual circuit defined on that interface.
DEL	Deletes the Service Profile Identification. Usually, all Virtual Circuit parameters can be changed when the VC state is off. You do not need to stop the interface. However, when you delete the ISDN SPID you must stop the ISDN interface first and then delete the SPID.

ISDN SET VC SEC

This command creates a new security telephone number. Security telephone numbers are valid only while the Call Acceptance Mode is set to **SELECTED**. They indicate the remote (far–end) telephone numbers from which calls are acceptable.

Syntax: **ISDN SET VC i c SEC phone [vc]**

Parameter	Description
i	The number of the ISDN interface.
c	The number of the ISDN virtual circuit defined on that interface.
phone	The remote (far–end) telephone number from which calls are accepted on the local interface. Maximum: 20 digits
vc	The vc number for the remote device. Range: 1..2

ISDN SET VC DELS

This command deletes a security telephone number.

Syntax: **ISDN SET VC i c DELS id**

Parameter	Description
i	The number of the ISDN interface.
c	The number of the ISDN virtual circuit defined on that interface.
id	The security telephone number to be deleted. Use the SHOW command to display it.

ISDN SHOW CONFIG

This command displays all the configuration parameters of a specific ISDN interface and the related virtual circuits. It can also be used to display the configuration parameters of a specific ISDN virtual circuit only.

Syntax: **ISDN SHOW CONFIG i [c]**

Parameter	Description
i	The number of the ISDN interface.
c	Specifies the virtual circuit to be shown. If omitted, this means to show the interface configuration.

ISDN SET INTERFACE DLOAD

Enables and disables code auto-download to the specified SIM. Auto-download uses ISDN firmware from storage (router's Internal Flash or External Feature Pack) that router was booted from.

Syntax: **ISDN SET INTERFACE i DLOAD {ENABLE | DISABLE}**

Parameter	Description
i	The number of the ISDN interface.
ENABLE	Enables auto-download.
DISABLE	Disables auto-download.

ISDN SET INTERFACE TFTPDLOAD

Enables and disables code TFTP-download to the specified SIM. TFTP-download can be proceeded e.g. from IMS

Syntax: **ISDN SET INTERFACE i TFTPDLOAD {ENABLE | DISABLE}**

Parameter	Description
i	The number of the ISDN interface.
ENABLE	Enables TFTP-download.
DISABLE	Disables TFTP-download.

PROTECT ISDNSIMS

Protects all ISDN SIMs from being written using TFTP-download.

Syntax: PROTECT ISDNSIMS

ISDN SET VC PROT {CCPP | PPP}

This command allows you to choose the protocol to be used by ISDN. In versions previous to 6.0 only the CCPP protocol was available and it was used by default. For the interoperability with other vendors

When you are using PPP over ISDN, you must disable CCSIM option on a VC to have interoperability with devices from vendors other than Olicom.

For interoperability with devices from vendors other than Olicom, you must disable CCSIM option on a VC when using PPP over ISDN

Syntax: ISDN SET VC i c PROT {CCPP | PPP}

Field	Description
i	The number of the ISDN interface.
c	The number of the ISDN virtual circuit defined on that interface.
CCPP	CrossComm Point-to-Point protocol. It is the only protocol available in versions prior to 6.0
PPP	standard point-to-point protocol. When you choose this option, you must disable CCSIM on a VC to achieve interoperability with the devices from vendors other than Olicom.

ISDN SET VC RATE {56K | 64K}

This command selects the rate of B-channel for the outgoing calls.

Syntax: ISDN SET VC i c RATE {56K | 64K}

Parameter	Description
i	The number of the ISDN interface.
c	The number of the ISDN virtual circuit defined on that interface.

ISDN SET VC AUTODIAL {ON | OFF}

This command is used to enable or disable 'Auto dial after start' option on VC.

Syntax: **ISDN SET VC i c AUTODIAL {ON | OFF}**

Parameter	Description
i	The number of the ISDN interface.
c	The number of the ISDN virtual circuit on which autodial is used.
ON / OFF	Enables/disables autodial. When autodial is enabled and remote phone number is defined, the VC will dial automatically as soon as the VC or the interface is switched ON.

Note: It is recommended to enable this option if ISDN VC is used for Dial on Demand.

ISDN SET VC AUTOREC {ON | OFF}

This command is used to enable or disable autoreconnect option on VC.

If an active connection is broken while this option is enabled, the such connection will be reestablished by the VC that originated the connection.

Syntax: **ISDN SET VC i c AUTOREC {ON | OFF}**

Parameter	Description
i	The number of the ISDN interface.
c	The number of the ISDN virtual circuit on which autoreconnect is used.
ON / OFF	Enables/disables autoreconnect. When this option is enabled on the VC, connections originated by this VC will be reestablished if they break.

ISDN SET VC CCSIM {ON | OFF}

This command is used to connect or disconnect a VC to CrossComm/Olicom ISDN SIM.

Syntax: **ISDN SET VC i c CCSIM {ON | OFF}**

Parameter	Description
i	The number of the ISDN interface.
c	The number of the ISDN virtual circuit to be connected or disconnected to CrossComm/Olicom ISDN SIM.
ON / OFF	Enables/disables the “Connect to CrossComm/Olicom ISDN SIM” option. When connected: - full information about the called and calling VCs (including the phone and VC numbers of both sides) is exchanged between the two sides of the connection after the connection is established; - in configurations where both VCs have the same local phone number (My Phone Number), connecting to CrossComm/Olicom ISDN SIM makes it possible to distinguish between VCs (an ISDN switch knows about phone numbers but not about logical ports - VCs - created on an XL router).

Note: This command can be enabled only for the connections where both ends are CrossComm/Olicom ISDN SIMs. The setting ON or OFF must be the same on both ends.

ISDN DIAL

This command is used to originate a call manually.

Syntax: **ISDN DIAL i c**

Parameter	Description
i	The number of the ISDN interface.
c	The number of the ISDN virtual circuit where call is originated.

ISDN DISC

This command is used to terminate a call manually (disconnect command).

Syntax: **ISDN DISC i c**

Parameter	Description
i	The number of the ISDN interface.
c	The number of the ISDN virtual circuit which terminates the connection.

ISDN SHOW STATS

This command is used to display ISDN VC statistics.

Syntax: **ISDN SHOW STATS i c**

Parameter	Description
i	The number of the ISDN interface.
c	The number of the ISDN virtual circuit.

21. LAN Emulation Commands

LAN Emulation provides a simple means for running existing LAN applications in an ATM environment. In general, the LAN Emulation software enables PCs, workstations, and network servers to access an ATM network via protocol stacks, such as IPX and NetBIOS, as if they were running over traditional LANs. The applications running on these devices, either connected to an Ethernet or Token Ring network, do not have to be modified to connect to an ATM network. For these devices, LAN Emulation provides the necessary protocol conversion to allow them to connect to an ATM network.

In the case of the XLT–F, LAN Emulation permits the XLT–F to efficiently bridge and route data in legacy LAN packets, such as Ethernet and Token Ring, to its high–speed ATM port by mapping a legacy LAN MAC address to an ATM address. In addition, multiple instances of the XLT–F LAN Emulation Client (LEC, pronounced “leck”) can be created on a single XLT–F. Each of these LECs represent a port to an emulated LAN.

Entering LEC Commands

Most LEC commands have the following

LEC SET 1 MaxRegRetry 10

Where:

LEC is the token indicating a LEC command

SET is the action to be taken

1 is the number of the interface to act upon

MaxRegRetry is the parameter to act upon

10 is the value to give to the parameter names and values are shown in both uppercase and lowercase to improve readability. You can enter any command and parameter value in either uppercase of lowercase. The XL console accepts both as input.

Many of the LEC console commands accept two equivalent names for a particular parameter. For example, the **LEC SET <n> {ELANName | C5} <string>** command can be entered in either of the following ways:

LEC SET <n> ELANName <string>

LEC SET <n> C5 <string>

C5 is simply an abbreviation for **ELANName**. Each of the above examples sets the value for the emulated LAN name, **ELANName** or **C5**, for the specified LEC interface number <**n**>.

Example:

LEC SET 1 C5 FIRST INTERFACE

Where:

- LEC is the token indicating a LEC command
- SET is the action to be taken
- 1 is the number of the interface to act upon
- C5 is the parameter to act upon
- FIRST INTERFACE is the name string given to an interface

HELP LEC

Lists all LEC console commands.

Syntax: **HELP LEC**

Command line abbreviations and their meaning:

Abbreviation	Meaning
<idx>	The number of the specified LEC interface
{parm}	Global or specific LEC interface parameter
<val>	Value for a specified LEC interface parameter

LEC CREATE

Creates a new LEC interface with all parameters (except LES ATM address) set to default values. The new LEC interface becomes visible to the console and ClearSight. If you specify a unique LEC interface identifier, or LEC index number, that number is assigned to the new LEC interface. If you do not specify a unique LEC index number, the first unused LEC index number is assigned to the new LEC interface. In addition, if you do not specify a LAN type, an unspecified LAN type is set for the new LEC interface.

Syntax: **LEC CREATE [n] [8023 | 8025]**

Parameters:	Description
n (optional)	Specifies a number for the new LEC interface (0-31)
8023 (optional)	Creates an 802.3 LEC interface
8025 (optional)	Creates an 802.5 LEC interface

Example:

```
XL> LEC CREATE
LEC interface 1 created. Assigned to port 19.
XL>
```

LEC DELETE

Deletes a LEC interface. Once you delete a LEC interface, it is no longer visible to the console or ClearSight.

Syntax: LEC DELETE <n>

Parameter:	Description
n	Number of the LEC interface to be deleted (0-31)

Example:

```
XL> LEC DELETE 2
LEC interface 2 deleted.
XL>
```

LEC ENABLE

Enables a LEC interface.

Syntax: LEC ENABLE <n>

Parameter:	Description
n	Number of the LEC interface to be enabled (0-31)

Example:

```
XL> LEC ENABLE 1
Port 18: State changed to Active
XL>
```

LEC DISABLE

Disables a LEC interface.

Syntax: LEC DISABLE <n>

Parameter:	Description
n	Number of the LEC interface to be disabled (0-31)

Example:

```
XL> LEC DISABLE 1
Port 18: State changed to Inactive
XL>
```

LEC CYCLE

Disables and then enables a LEC interface. If the LEC interface is already disabled, this command enables it.

Syntax: **LEC CYCLE <n>**

Parameter:	Description
n	Number of the LEC interface to be cycled (0-31)

Example:

```
XL> LEC CYCLE 1
Port 18: State changed to Inactive
Port 18: State changed to Active
XL>
```

LEC SET MaxConn

Sets the maximum number of Switched Virtual Circuit (SVC) connections all LECs can use at a given time.

Syntax: **LEC SET MaxConn <value>**

Parameter:	Description
value	Number of SVC connections. Default: 1038 Maximum: 1038

Example:

```
XL> LEC SET MaxConn 100
XL>
```

Related Commands:

LEC SHOW MaxConn on page 378.

LEC SET ConReqTmo

Sets the duration of the Connection Request Timer.

Syntax: **LEC SET ConReqTmo <value>**

Parameter:	Description
value	Number of seconds. Default: 0 (timer disabled) Maximum: 256

Example:

```
XL> LEC SET ConReqTmo 10
XL>
```

Related Commands:

LEC SHOW ConReqTmo on page 378

LEC SET ConRespTmo

Sets the duration of the Connection Response Timer.

Syntax: **LEC SET ConRespTmo <value>**

Parameter:	Description
value	Number of seconds. Default: 0 (timer disabled) Maximum: 256

Example:

```
XL> LEC SET ConRespTmo 10
XL>
```

Related Commands:

LEC SHOW ConRespTmo on page 379

LEC SET LECSAtmAddr

Sets the ATM address of the LAN Emulation Configuration Server. You must specify a complete ATM address of 20 bytes (40 hex digits).

Syntax: **LEC SET LECSAtmAddr <idx> <atmaddr>**

Parameter:	Description
atmaddr	ATM address of the LAN Emulation Configuration Server.
idx	Index in table of ATM addresses of LAN Emulation Servers. Range: 0..3

Example:

```
XL> LEC SET LECSAtmAddr
          3902030405060708091011121314151617618190
XL>
```

Related Commands:

LEC SHOW LECSAtmAddr on page 380

LEC DELETE LECSAtmAddr on page 358

LEC DELETE LECSAtmAddr

Deletes the ATM address of the LAN Emulation Configuration Server from the table of ATM addresses (for LAN Emulation Configuration Servers) configured in battram.

Syntax: **LEC DELETE SET LECSAtmAddr <idx>**

Parameter:	Description
idx	ATM addresses table index of the LAN Emulation Servers. Range: 0..3

Example:

```
XL> LEC DELETE LECSAtmAddr 0
XL>
```

Related Commands:

LEC SHOW LECSAtmAddr on page 380

LEC DELETE SET LECSAtmAddr <idx> on page 358

LEC SET PDD

Enables or disables Persistent Data Direct Vcc feature (PDD VCC) for specified LEC. Requested state is set in battram and LEC reads it during the initial phase.

Syntax: **LEC SET <n> PDD {ENABLE | DISABLE}**

Parameters:	Description
n	Number of the LEC interface Range: 0..31
ENABLE	Enables PDD VCC feature
DISABLE	Disables PDD VCC feature

Example:

```
XL> LEC SET 1 PDD Enable
XL>
```

Related Commands:

LEC SHOW ALL on page 381

LEC SET NOTRGTNARP

Enables or disables Target-Less-NARP feature for specified LEC. Requested state is set in battram and LEC reads it during the initial phase.

Syntax: **LEC SET <n> NOTRGTNARP <value>**

Parameters:	Description
n	Number of the LEC interface Range: 0..31
ENABLE	Enables Target-Less-NARP feature
DISABLE	Disables Target-Less-NARP feature

Example:

```
XL> LEC SET 1 NOTRGTNARP Enable
XL>
```

Related Commands:

LEC SHOW NARP on page 382

LEC SET LineRate

Sets the LEC interface line rate, which is used as the Peak Cell Rate (PCR) in virtual connections established by the LEC.

Syntax: **LEC SET <n> LineRate <value>**

Parameters:	Description
n	Number of the LEC interface Range: 0..31
value	Cells per second. OC3 default: 370370. DS3 default: 100663 0 (the value is set automatically depending on the speed of the ATM interface) Range: 1..232. cells per second

Example:

```
XL> LEC SET 1 LineRate 370370
XL>
```

Related Commands:

LEC SHOW LineRate on page 385

LEC SET JoinReqTmo

Sets the Join Request Timer value, which is used to limit the time a LEC waits for a Join Response after a Join Request has been sent to the LAN Emulation Server (LES).

Syntax: **LEC SET <n> JoinReqTmo <value>**

Parameters:	Description
n	Number of the LEC interface. Range: 0..31
value	number of seconds Default: 3 Range: 3..300 and 0(timer disabled)

Example:

```
XL> LEC SET 1 JoinReqTmo 10
XL>
```

Related Commands:

LEC SHOW JoinReqTmo on page 383

LEC SET ArpLastUseTr

Sets the time threshold to delete an unused ARP entry.

Syntax: **LEC SET <n> ArpLastUseTr <value>**

Parameters:	Description
n	Number of the LEC interface. Range: 0..31
value	Number of seconds. Default: 1200 seconds. 0 (disables the timer) Range: 1..232-1/100

Example:

```
XL> LEC SET 1 ArpLastUseTr 1000
XL>
```

Related Commands:

LEC SHOW ArpLastUseTr on page 383

LEC SET <n> MaxRegRetry

Sets the maximum number of retries for Register/Unregister Requests.

Syntax: **LEC SET <n> MaxRegRetry <value>**

Parameters:	Description
n	Number of the LEC interface. Range: 0..31
value	Number of attempts. Default: 2 Range: 0..65535

Example:

```
XL> LEC SET 1 MaxRegRetry 10
XL>
```

Related Commands:

LEC SHOW MaxRegRetry on page 384

LEC SET <n> McastFwdTmo

Sets the value for the Multicast Forward Timer, which is used by the LEC when waiting for the Multicast Forward Virtual Channel Connection (VCC) to be established by the Broadcast and Unknown Server (BUS).

Syntax: **LEC SET <n> McastFwdTmo <value>**

Parameters:	Description
n	Number of the LEC interface. Range: 0..31
value	Number of seconds. Default: 120 Range: 10..300

Example:

```
XL> LEC SET 1 McastFwdTmo 10
XL>
```

Related Commands:

LEC SHOW McastFwdTmo on page 384

LEC SET Mode

Determines whether the LEC interface uses the LAN Emulation Server (LES) for auto–configuration during startup.

Syntax: **LEC SET <n> Mode <AUTO | MANUAL>**

Parameters:	Description
n	Number of the LEC interface. Range: 0..31
AUTO	Obtain all configuration variable values during LEC interface.startup from the LECS (default value).
MANUAL	Obtain all configuration variable values during LEC interface startup from the internal configuration database.

Example:

```
XL> LEC SET 1 Mode MANUAL
XL>
```

Related Commands:

LEC SHOW Mode on page 385

LEC SET LECAtmAddr or LEC SET C1

Sets the LEC interface's primary ATM address, which is used in SVCs established by the LEC interface and which must be known before the Configuration and Join phases can begin.

Syntax: **LEC SET <n> {LECAtmAddr | C1} <atmaddr>**

Parameters:	Description
n	Number of the LEC interface. Range: 0..31
atmaddr	Primary ATM address of the LEC interface. You can enter 1, 7, or 20 bytes:
1	(2 hex digits) If you specify only 1-byte (the selector), the system assumes that the network prefix of this address is the network prefix received from the ATM switch. The ESI portion of the address is the bridge MAC address.
7	(14 hex digits) If you specify a 7-byte ATM address, the system assumes that the network prefix of this address is the network prefix received from the ATM switch.
20	(40 hex digits). If you specify a 20-byte (complete) ATM address, no system assumptions are used.

Example:

```
XL> LEC SET 1 C1 3902030405060708090101112131415161717181902
```

XL>

Related Commands:

LEC SHOW <n> {LECAtmAddr | C1} on page 386

LEC SET LANType or LEC SET C2

Sets the LAN type for LEC interface.

Syntax: **LEC SET <n> {LANType | C2} <8023 | 8025 | AUTO>**

Parameters:	Description
n	Number of the LEC interface. Range: 0..31
8023	Sets LAN type to 802.3
8025	Sets the LAN type to 802.5
AUTO	Sets the LAN type to unspecified (default value)

Example:

```
XL> LEC SET 1 C2 AUTO
```

XL>

Related Commands:

LEC SHOW <n> {LANType | C2} on page 387.

LEC SET MaxDataFrameSize or LEC SET C3

Sets the maximum data frame size for the LEC interface.

Syntax: **LEC SET <n> {MaxDataFrameSize | C3} <1516 | 4544 | 9234 | 18190 | AUTO>**

Parameters:	Description
n	Number of the LEC interface. Range: 0..31
1516	Sets the Maximum Data Frame Size to 1516 bytes (default value for 802.3 ELAN)
4544	Sets the Maximum Data Frame Size to 4544 (default value for 802.5 ELAN)
9234	Sets the Maximum Data Frame Size to 9234
18190	Sets the Maximum Data Frame Size to 18190
AUTO	Sets The LEC interface to accept the Maximum Data Frame Size sent by the LES during the Join Phase (default value).

Example:

```
XL> LEC SET 1 C3 AUTO
XL>
```

Related Commands:

LEC SHOW <n> {MaxDataFrameSize | C3} on page 388.

LEC SET ELANName or LEC SET C5

Sets the LEC interface name for the LEC interface.

Syntax: **LEC SET <n> {ELANName | C5} <string>**

Parameters:	Description
n	Number of the LEC interface. Range: 0..31
string	LEC interface name, Maximum: 32 characters

Example:

```
XL> LEC SET 1 C5 FIRST INTERFACE
XL>
```

Related Commands:

LEC SHOW <n> {ELANName | C5} on page 389.

LEC SET ControlTmo or LEC SET C7

Sets the number of seconds for timing out most Request/Response Control Frame interactions and the Reg/Unreg Timer.

Syntax: **LEC SET <n> {ControlTmo | C7} <value>**

Parameters:	Description
n	Number of the LEC interface. Range: 0..31
value	Number of seconds. Default: 120 Range: 10..300

Example:

```
XL> LEC SET 1 C7 120
XL>
```

Related Commands:

LEC SHOW <n> {ControlTmo | C7} <value> on page 390.

LEC SET LESAtmAddr or LEC SET C9

Sets the LAN Emulation Server (LES) ATM address, which the LEC interface will use the next time the LEC interface starts in Manual Configuration Mode.

Syntax: **LEC SET <n> {LESAtmAddr | C9} <atmaddr>**

Parameters:	Description
n	Number of the LEC interface. Range: 0..31
atmaddr	Complete ATM address (20 bytes, or 40 hex digits).

Example:

```
XL> LEC SET 1 C9 3902030405060708090101112131415161717181902
XL>
```

Related Commands:

LEC SHOW <n> {LESAtmAddr | C9} <value> on page 391.

LEC SET MaxUnknownFrameCount or LEC SET C10

Sets the threshold for the maximum Unknown Frame Count, thereby limiting the number of frames sent to the Broadcast and Unknown Server (BUS) for a given LAN destination.

Syntax: **LEC SET <n> {MaxUnknownFrameCount | C10} <value>**

Parameters:	Description
n	Number of the LEC interface. Range: 0..31
value	The number of unknown frames. Default: 1 Range: 1..10

Example:

```
XL> LEC SET 1 C10 10
XL>
```

Related Commands:

LEC SHOW <n> {MaxUnknownFrameCount | C10} on page 392.

LEC SET MaxUnknownFrameTime or LEC SET C11

Sets the threshold for the Maximum Unknown Frame Time Threshold, which is the amount of time the calculation of the number of frames sent to the Broadcast and Unknown Server (BUS) is performed.

Syntax: **LEC SET <n> {MaxUnknownFrameTime | C11} <value>**

Parameters:	Description
n	Number of the LEC interface. Range: 0..31
value	Number of seconds. Default: 1 Range: 1..60

Example:

```
XL> LEC SET 1 C11 1
XL>
```

Related Commands:

LEC SHOW <n> {MaxUnknownFrameTime | C11} on page 392.

LEC SET VCCTmo or LEC SET C12

Sets the length of time after which an inactive Data Direct SVC should be closed.

Syntax: **LEC SET <n> {VCCTmo | C12} <value>**

Parameters:	Description
n	Number of the LEC interface. Range: 0..31
value	Number of seconds. 0 (disables the timer) Default: 1200 Minimum: 1

Example:

```
XL> LEC SET 1 C12 1200
XL>
```

Related Commands:

LEC SHOW <n> {VCCTmo | C12} on page 393.

LEC SET MaxRetryCount or LEC SET C13

Sets the Maximum ARP Retry Count, which limits the number of Address Resolution Requests that can be issued for a given data frame's LAN destination (MAC address or Route Designator).

Syntax: **LEC SET <n> {MaxRetryCount | C13} <value>**

Parameters:	Description
n	Number of the LEC interface. Range: 0..31
value	Number of retries. Default: 2 retries Range: 0..2

Example:

```
XL> LEC SET 1 C13 1
XL>
```

Related Commands:

LEC SHOW <n> {MaxRetryCount | C13} on page 393.

LEC SET AgingTime or LEC SET C17

Sets the LAN Emulation ARP Aging Time, which is the maximum amount of time the LEC interface maintains an entry in its LAN Emulation ARP Cache without verification of that entry.

Syntax: **LEC SET <n> {AgingTime | C17} <value>**

Parameters:	Description
n	Number of the LEC interface. Range: 0..31
value	Number of seconds. Default: 300 Range: 10..300, should be greater than Forward Delay Time (C18).

Example:

```
XL> LEC SET 1 C17 300
XL>
```

Related Commands:

LEC SHOW <n> {AgingTime | C17} on page 396

LEC SET ForwardDelayTmo or LEC SET C18

Sets the Forward Delay Time, which is the maximum amount of time the LEC interface maintains an entry in its LAN Emulation ARP Cache for a non–local MAC address without verification of that entry.

Syntax: **LEC SET <n> {ForwardDelayTmo | C18} <value>**

Parameters:	Description
n	Number of the LEC interface. Range: 0..31
value	Number of seconds. Default: 15 Range: 4..30, should be less than LAN Emulation ARP Aging Time (C17).

Example:

```
XL> LEC SET 1 C18 15
XL>
```

Related Commands:

LEC SHOW <n> {ForwardDelayTmo | C18} on page 397

LEC SET ArpRespTmo or LEC SET C20

Sets the maximum period of time the LAN Emulation ARP Request and ARP Reply cycle is to complete. It is used for retries and verifications.

Syntax: **LEC SET <n> {ArpRespTmo | C20} <value>**

Parameters:	Description
n	Number of the LEC interface. Range: 0..31
value	Number of seconds. Default: 1 Range: 1..30

Example:

```
XL> LEC SET 1 C20 1
XL>
```

Related Commands:

LEC SHOW <n> {ArpRespTmo | C20} on page 398

LEC SET FlushTmo or LEC SET C21

Sets the Flush Timeout, which limits the time interval in which the LEC waits to receive a LAN Emulation Flush Response after a LAN Emulation Flush Request has been sent.

Syntax: LEC SET <n> {FlushTmo | C21} <value>

Parameters:	Description
n	Number of the LEC interface. Range: 0..31
value	Number of seconds. Default: 1 Range: 1..4

Example:

```
XL> LEC SET 1 C21 1
XL>
```

Related Commands:

LEC SHOW <n> {FlushTmo| C21} on page 398

LEC SET LocalSegmentID or LEC SET C23

Sets the 802.5 emulated LAN Local Segment ID. The Local Segment ID is used in Source/Route bridging.

Syntax: LEC SET <n> {LocalSegmentID | C23} <value>

Parameters:	Description
n	Number of the LEC interface. Range: 0..31
value	Local Segment ID, 2 bytes (4 hex digits) in length

Example:

```
XL> LEC SET 1 C23 0304
XL>
```

Related Commands:

LEC SHOW <n> {LocalSegmentID | C23} on page 399

LEC SET McastSendVccType or LEC SET C24

Sets the type of service (best–effort or variable bit rate) the LEC interface requests when establishing the Multicast Send VCC.

Syntax: **LEC SET <n> {McastSendVccType | C24} <BEST | VAR>**

Parameters:	Description
n	Number of the LEC interface. Range: 0..31
BEST	Sets type of service to best–effort (default value)
VAR	Sets type of service to variable bit rate

Example:

```
XL> LEC SET 1 C24 VAR
```

XL>

Related Commands:

LEC SHOW <n> {McastSendVccType | C24} on page 399

LEC SET McastSendSCR or LEC SET C25

Sets the forward and backward sustained cell rate that the LEC requests when setting up the Multicast Send VCC and requesting the variable bit rate type of service.

Syntax: **LEC SET <n> {McastSendSCR | C25} <value>**

Parameters:	Description
n	Number of the LEC interface. Range: 0..31
value	Cells per second. Default: 0. When a zero is used, the cells-per-second rate setting is automatically set depending on the speed of the ATM interface. Range: 1..232-1

Example:

```
XL> LEC SET 1 C25 100000
XL>
```

Related Commands:

LEC SHOW <n> {McastSendSCR | C25} on page 400

LEC SET McastSendPCR or LEC SET C26

Sets the forward and backward peak cell rate the LEC requests when setting up the Multicast Send VCC and requesting the variable bit rate type of service.

Syntax: **LEC SET <n> {McastSendPCR | C26} <value>**

Parameters:	Description
n	Number of the LEC interface. Range: 0..31
value	Cells per second. Default: 0 (the cells per second are automatically set depending on the speed of the ATM interface). Range: 1..232-1

Example:

```
XL> LEC SET 1 C26 100000
XL>
```

Related Commands:

LEC SHOW <n> {McastSendPCR | C26} on page 400

LEC SET ConnCompTmo or LEC SET C28

Sets the Connection Complete Timer, which is used during connection establishment to limit the amount of time data, or a READY_IND message, takes to arrive from the called LEC.

Syntax: **LEC SET <n> {ConnCompTmo | C28} <value>**

Parameters:	Description
n	Number of the LEC interface. Range: 0..31
value	Number of seconds. Default: 4 Range: 1..10 and 0 (timer disabled)

Example:

```
XL> LEC SET 1 C28 4
XL>
```

Related Commands:

LEC SHOW <n> {ConnCompTmo | C28} on page 401

LEC SHOW GLOBAL

Displays all global LEC interface parameters, including:

- Maximum number of connections
- Connection Request Timer
- Connection Response Timer
- LEC interface address

Syntax: **LEC SHOW GLOBAL**

Example:

```
XL> LEC SHOW 1 GLOBAL
LEC interface list: 0 1 2
Maximum Number of Connections => 128
Connection Request Timeout => 10 s
Connection Request Timeout => 10 s
LECS ATM Address => 47000000000000000000000.004000980000.01
XL>
```

LEC SHOW LIST

Displays the current.LEC interface IDs on all of the LEC interfaces.

Syntax: **LEC SHOW LIST**

Example:

```
XL> LEC SHOW LIST
LEC interface list: 0 1
XL>
```

LEC SHOW MaxConn

Displays the maximum number of connections for the LEC interfaces.

Syntax: **LEC SHOW MaxConn**

Example:

```
XL> LEC SHOW MaxConn
Maximum Number of Connections => 128
XL>
```

Related Commands:

LEC SET MaxConn <value> on page 356

LEC SHOW ConReqTmo

Displays the Connection Request Timer.

Syntax: **LEC SHOW ConReqTmo**

Example:

```
XL> LEC SHOW ConReqTmo
Connection Request Timeout => 10 s
XL>
```

Related Commands:

LEC SET ConReqTmo <value> on page 357o

LEC SHOW ConRespTmo

Displays the Connection Request Timer.

Syntax: LEC SHOW ConRespTmo

Example:

```
XL> LEC SHOW ConRespTmo
Connection Response Timeout => 10 s
XL>
```

Related Commands:

LEC SET ConReqTmo <value> on page 357

LEC SHOW LECSAtmAddr

Displays the list of ATM addresses configured in the LAN Emulation Configuration Servers battram and the list of currently used ATM addresses of LAN Emulation Configuration Servers for the LEC interface.

Syntax: **LEC SHOW LECSAtmAddr**

Example:

```
XL> LEC SHOW LECSAtmAddr
LECS ATM addresses stored in battram:

                    0-> 0102030405060708091011121З.141516171819.20
1-> ----------------- not set ---------------

2-> ----------------- not set ---------------

3-> ----------------- not set ---------------
0 LECS ATM addresses in run-time structures:
0-> ----------------- not set ---------------

1-> ----------------- not set ---------------

2-> ----------------- not set ---------------

3-> ----------------- not set ---------------
XL>
```

Related Commands:

LEC DELETE SET LECSAtmAddr <idx> on page 358

LEC DELETE SET LECSAtmAddr <idx> on page 358

LEC SHOW ALL

The LEC SHOW ALL command displays the parameter values for each LEC interface. It also informs you whether PDD VCC feature will be or will not be activated on this interface.

Syntax: **LEC SHOW <n> ALL**

Parameter:	Description
n	Number of the LEC interface. Range: 0..31

Example:

```
XL> LEC SHOW 1 ALL
This LEC interface is system port 18
Admin state: ENABLED
State of protocol machine: LEC Active
Config Mode => Auto
LECS Addr:  4700790000000000000000000000A03E00000100
Join Request Timeout => 3 s
Multicast Fwd VCC Timeout => 120 s
ARP Last Use Threshold => 1200 s
Max Registration Retry => 2
LEC interface Primary ATM Address =>
    Config: 01
    Actual: 39000000000000000000000001000098949AF001
LAN Type (C2) => Config: 802.3/Ethernet  Actual: 802.3/Ether-
          net
Max Data Frame Size (C3) => Config: 1516  Actual: 1516
Proxy Flag (C4) => PROXY
ELAN Name (C5) =>
   Config: 'ELAN #1, PORT #19'
   Actual: 'CCC_VLAN0'
Control Timeout (C7) => 120 s
LES ATM Address (C9) =>
   Actual: 470079000000000000000000000020D400068002
Max Unknown Frame Count (C10) => 3
Max Unknown Frame Time (C11) => 1 s
VCC Timeout Period (C12) => 1200 s
Max ARP Retry Count (C13) => 2
LEC ID (C14) => Actual: 6
Aging Time (C17) => 300 s
Forward Delay Time (C18) => 15 s
Expected ARP Response Time (C20) => 1 s
```

Flush Timeout (C21) => 1 s
Mcast Send Average Rate (C25) => 0
Mcast Send Peak Rate (C26) => 0
Connection Complete Timer (C28) => 4 s
PDD Vcc Actual State => Inactve
PDD Vcc WILL BE ACTIVATEDPDD Vcc Config State => Enabled (1)
TARGETLESS Narp Actual State => Disabled
TARGETLESS Narp Config State => Disabled
XL>

Related Commands:

various set commands

LEC SHOW NARP

Displays actual and configured in battram state of Target-Less-NARP feature for specified LEC.

Syntax: **LEC SHOW <n> NARP**

Parameters:	Description
n	Number of the LEC interface Range: 0..31

Example:

```
XL> LEC SHOW 1 NARP
TARGETLESS Narp Actual State => Disabled
TARGETLESS Narp Config State => Disabled
XL>
```

Related Commands:

LEC SET <n> NOTRGTNARP <value> on page 359

LEC SHOW JoinReqTmo

Displays the LEC interface Request Timeout value, which is the time in which a LAN Emulation Join Response is received from the LAN Emulation Server (LES).

Syntax: **LEC SHOW <n> JoinReqTmo**

Parameter:	Description
n	Number of the LEC interface. Range: 0..31

Example:

```
XL> LEC SHOW 1 JoinReqTmo
Join Request Timeout => 5 s
XL>
```

Related Commands:

LEC SET <n> JoinReqTmo <value> on page 361

LEC SHOW ArpLastUseTr

Displays the time after which an unused ARP entry is deleted from the address table. This command should be used in conjunction with the AgingTime (C17) command.

Syntax: **LEC SHOW <n> ArpLastUseTr**

Parameter:	Description
n	Number of the LEC interface. Range: 0..31

Example:

```
XL> LEC SHOW 1 ArpLastUseTr
ARP Last Use Threshold => 1200 s

XL>
```

Related Commands:

LEC SET <n> ArpLastUseTr <value> on page 361

LEC SHOW MaxRegRetry

Displays the maximum number of retries for Register/Unregister requests for the LEC interface.

Syntax: **LEC SHOW <n> MaxRegRetry**

Parameter:	Description
n	Number of the LEC interface. Range: 0..31

Example:

```
XL> LEC SHOW 1 MaxRegRetry
Max Registration Retry => 3
XL>
```

Related Commands:

LEC SET <n> MaxRegRetry <value> on page 362

LEC SHOW McastFwdTmo

Displays the specified Multicast Forward VCC Timeout for the LEC interface, which is the time period in which the Multicast Forward VCC is to be received from the Broadcast and Unknown Server (BUS).

Syntax: **LEC SHOW <n> McastFwdTmo**

Parameter:	Description
n	Number of the LEC interface. Range: 0..31

Example:

```
XL> LEC SHOW 1 McastFwdTmo
Multicast Fwd VCC Timeout => 10 s
XL>
```

Related Commands:

LEC SET <n> McastFwdTmo <value> on page 362

LEC SHOW LineRate

Displays the Forward and Backward Peak Cell Rate used in the virtual connections initiated from the LEC interface.

Syntax: **LEC SHOW <n> LineRate**

Parameter:	Description
n	Number of the LEC interface. Range: 0..31

Example:

```
XL> LEC SHOW 1 LineRate
LineRate => 10000
XL>
```

Related Commands:

LEC SHOW <n> LineRate on page 385

LEC SHOW Mode

Shows if the LEC interface uses the LAN Emulation Configuration Server for auto–configuration.

Syntax: **LEC SHOW <n> Mode**

Parameter:	Description
n	Number of the LEC interface. Range: 0..31

Example:

```
XL> LEC SHOW 1 Mode
Config Mode => AUTO
XL>
```

Related Commands:

LEC SHOW <n> Mode on page 385

LEC SHOW CfgSrc

Shows whether the LEC interface used the LAN Emulation Configuration Server for auto–configuration, and if so, the method used to establish the Configuration Direct VCC.

Syntax: **LEC SHOW CfgSrc**

The possible returned values include:

- “Got LECS Address Via ILMI”
- “Used LECS Well Known Address”
- “Used LECS PVC”
- “Did Not Use LECS”

Example:

```
XL> LEC SHOW CfgSrc
Config Source => "Got LECS Address Via ILMI"
XL>
```

LEC SHOW LECAtmAddr or LEC SHOW C1

Displays the LEC interface's primary ATM address.

Syntax: **LEC SHOW <n> {LECAtmAddr | C1}**

- The primary ATM address the LEC interface uses the next time it enters the Initial State is labelled **Config**.
- The current primary ATM address of the LEC interface is labelled **Actual**. The ATM address is registered to a switch.

Parameter:	Description
n	Number of the LEC interface. Range: 0..31

Example:

```
XL> LEC SHOW 1 C1
LEC Interface Primary ATM Address (C1) =>
     Config: 01020304050607080910111213.141516171819.20
     Actual: 01020304050607080910111213.141516171819.20
XL>
```

Related Commands:

LEC SET LECSAtmAddr <idx> <atmaddr> on page 358

LEC SHOW LANType or LEC SHOW C2

The LEC SHOW LANType (C2) command displays the LAN type of the LEC interface.

Syntax: LEC SHOW <n> {LANType | C2}

- The LAN type the LEC interface uses the next time it enters the Initial State is labelled **Config**.
- The LAN type currently configured for the LEC interface is labelled **Actual**.

Parameter:	Description
n	Number of the LEC interface. Range: 0..31

Example:

```
XL> LEC SHOW 1 LANType
LAN Type (C2) => Config: 802.5/Ethernet   Actual: 802.3/
          Ethernet
XL>
```

Related Commands:

LEC SET <n> {LANType | C2} <8023 | 8025 | AUTO> on page 365

LEC SHOW MaxDataFrameSize or LEC SHOW C3

Displays the maximum data frame size for the LEC interface.

Syntax: **LEC SHOW <n> {MaxDataFrameSize | C3}**

- The maximum data frame size the LEC interface uses the next time it enters the Initial State is labelled **Config**.
- The current maximum data frame size for the LEC interface is labelled **Actual**.

Parameter:	Description
n	Number of the LEC interface. Range: 0..31

Example:

```
XL> LEC SHOW 1 MaxDataFrameSize
Max Data Frame Size (C3) => Config: 1516  Actual: 1516
XL>
```

Related Commands:

LEC SET <n> {MaxDataFrameSize | C3} <1516 | 4544 | 9234 | 18190 | AUTO> on page 366

LEC SHOW ELANName or LEC SHOW C5

Displays the LEC interface name.

- The name the LEC interface uses the next time it enters the Initial State is labelled **Config**.
- The current name of the LEC interface is labelled **Actual**.

Syntax: LEC SHOW <n> {ELANName | C5}

Parameter:	Description
n	Number of the LEC interface. Range: 0..31

Example:

```
XL> LEC SHOW 1 ELANName
ELAN NAME (C5) =>
    Config: 'Emulated LAN type 802.3:   'big'
    Actual: 'Emulated LAN type 802.3: 'small'
XL>
```

Related Commands:

LEC SET <n> {ELANName | C5} <string> on page 367

LEC SHOW ControlTmo or LEC SHOW C7

Displays the LEC interface Control Timeout value, which is used for timing out most Request/Response Control Frame interactions and the Register/Unregister Timeout value. The Timeout value defines the period of time a LAN Emulation Register Response is expected from the LAN Emulation Server (LES).

Syntax: **LEC SHOW <n> {ControlTmo | C7} <value>**

Parameter:	Description
n	Number of the LEC interface. Range: 0..31

Example:

```
XL> LEC SHOW 1 ControlTmo
Control Timeout (C7)  +> 10 s
XL>
```

Related Commands:

LEC SET <n> {ControlTmo | C7} <value> on page 367

LEC SHOW LESAtmAddr or LEC SHOW C9

Displays the Emulation Server ATM address for the specified LEC interface.

- The LAN Emulation Server address the LEC interface uses the next time it enters the Initial State is labelled **Config**.
- The current LAN Emulation Server ATM address of the LEC interface is labelled **Actual**.

Syntax: **LEC SHOW <n> {LESAtmAddr | C9} <value>**

Parameter:	Description
n	Number of the LEC interface. Range: 0..31

Example:

```
XL> LEC SHOW 1 LESAtmAddr
LES ATM Address (C9) =>
     Config: 0102030405060708091011213.141516171819.20
     Actual: 0102030405060708091011213.141516171819.20
XL>
```

Related Commands:

LEC SET <n> {LESAtmAddr | C9} <atmaddr> on page 368

LEC SHOW MaxUnknownFrameCount or LEC SHOW C10

Displays the LEC interface Maximum Unknown Frame Count, which limits the number of frames sent to the Broadcast and Unknown Server (BUS) for a given LAN destination.

Syntax: **LEC SHOW <n> {MaxUnknownFrameCount | C10}**

Parameter:	Description
n	Number of the LEC interface. Range: 0..31

Example:

```
XL> LEC SHOW 1 C10
Max Unknown Frame Count (C10)  => 1
XL>
```

Related Commands:

LEC SET <n> {MaxUnknownFrameCount | C10} <value> on page 368

LEC SHOW MaxUnknownFrameTime or LEC SHOW C11

Displays the LEC interface Maximum Unknown Frame Time, the time in which the number of frames coming from an unresolved MAC address to the Broadcast and Unknown Server (BUS) is performed.

Syntax: **LEC SHOW <n> {MaxUnknownFrameTime | C11}**

Parameter:	Description
n	Number of the LEC interface. Range: 0..31

Example:

```
XL> LEC SHOW 1 C11
Max Unknown Frame Time (C11)  => 1 s

XL>
```

Related Commands:

LEC SET <n> {MaxUnknownFrameTime | C11} <value> on page 369

LEC SHOW VCCTmo or LEC SHOW C12

Displays the VCC timeout period, which specifies the length of time after which an inactive Data Direct SVC should close.

Syntax: **LEC SHOW <n> {VCCTmo | C12}**

Parameter:	Description
n	Number of the LEC interface. Range: 0..31

Example:

```
XL> LEC SHOW 1 VCCTmo
VCC Timeout Period (C12)  +> 1200 s
XL>
```

Related Commands:

LEC SET <n> {VCCTmo | C12} <value> on page 369

LEC SHOW MaxRetryCount or LEC SHOW C13

Displays the Maximum ARP Retry Count, which limits the number of LAN Emulation ARP Requests that can be issued for a given data frame's LAN destination (MAC address or Router Designator).

Syntax: **LEC SHOW <n> {MaxRetryCount | C13}**

Parameter:	Description
n	Number of the LEC interface. Range: 0..31

Example:

```
XL> LEC SHOW 1 MaxRetryCount
Max ARP Retry Count (C13)  => 1
XL>
```

Related Commands:

LEC SET <n> {MaxRetryCount | C13} <value> on page 370

LEC SHOW LECID or LEC SHOW C14

Displays the LEC interface ID, a number that uniquely identifies the LEC in an emulated LAN.

Syntax: **LEC SHOW <n> {LECID | C14}**

Parameter:	Description
n	Number of the LEC interface. Range: 0..31

Example:

```
XL> LEC SHOW 1 LECID
LEC ID (C14)  => 12
XL>
```

Displaying the LAN Emulation ARP Cache (C16)

The LEC SHOW Cache (C16) command displays the LEC interface MAC address ARP Table and the RD ARP Table. The entries in each table establish a relationship between a LAN destination external to the LEC interface and the ATM address to which data frames for that LAN destination are sent.

Syntax: **LEC SHOW <n> {Cache | C16}**

Parameters:	Description
n	Number of the LEC interface. Range: 0..31

Example:

```
XL> LEC SHOW 1 Cache
MAC ARP table on LEC interface 0
--MAC ADDR--  --------------ATM ADDRESS--------------- -STATE-
000098133570  39111111111111111111111111200009834185003 ACTIVE
080009786384  39111111111111111111111111200009834185003 ACTIVE
000098d336b0  39111111111111111111111111200009834185003 ACTIVE
0000985336b0  39111111111111111111111111200009834185003 ACTIVE
0000983336b0  39111111111111111111111111200009834185003 ACTIVE
0000981336b0  39111111111111111111111111200009834185003 ACTIVE
000098f336b0  39111111111111111111111111200009834185003 ACTIVE
00009813a600  39111111111111111111111111200009834185003 ACTIVE
00009853c860  39111111111111111111111111200009834185003 ACTIVE
08000983e3dc  39111111111111111111111111200009834185003 ACTIVE
000098d31880  39111111111111111111111111200009834185003 ACTIVE
0000981359a0  39111111111111111111111111200009834185003 ACTIVE
0000c0d51030  39111111111111111111111111200009834185003 ACTIVE
000098149970  39111111111111111111111111200009834185003 ACTIVE
000098138040  39111111111111111111111111200009834185003 ACTIVE
08000979cbd7  39111111111111111111111111200009834185003 ACTIVE
0000981441e0  39111111111111111111111111200009834185003 ACTIVE
0000980034b2  39111111111111111111111111200009834185003 ACTIVE
0ac064c00060  39111111111111111111111111200009834185003 ACTIVE
0ac064e00060  39111111111111111111111111200009834185003 ACTIVE
3600980042df  39111111111111111111111111200009834185003 ACTIVE
000098000225  39111111111111111111111111200009834185003 ACTIVE
00009813e450  39111111111111111111111111200009834185003 ACTIVE
00009814b3c0  39111111111111111111111111200009834185003 ACTIVE
08000949a99c  39111111111111111111111111200009834185003 ACTIVE
0000c10008b4  47000580FFE1000000F21514F10000C10008B400 ACTIVE
0000980034b2  39111111111111111111111111200009834185003 ACTIVE
```

```
0ac064c00060  3911111111111111111111111200009834185003 ACTIVE
0ac064e00060  3911111111111111111111111200009834185003 ACTIVE
3600980042df  3911111111111111111111111200009834185003 ACTIVE
000098000225  3911111111111111111111111200009834185003 ACTIVE
00009813e450  3911111111111111111111111200009834185003 ACTIVE
00009814b3c0  3911111111111111111111111200009834185003 ACTIVE
08000949a99c  3911111111111111111111111200009834185003 ACTIVE
0000c1000846  47000580FFE1000000F21514F10000C100084600 ACTIVE
```

LEC SHOW AgingTime or LEC SHOW C17

Displays the ARP Aging Time, which is the maximum amount of time the LEC maintains an entry in its LAN Emulation ARP Cache without verification of that entry. The value should always be higher than the value of the Forward Delay Time (C18).

Syntax: **LEC SHOW <n> {AgingTime | C17}**

Parameter:	Description
n	Number of the LEC interface. Range: 0..31

Example:

```
XL> LEC SHOW 1 AgingTime
Aging Time (C17)  => 300 s
XL>
```

Related Commands:

LEC SET <n> {AgingTime | C17} <value> on page 371

LEC SET <n> {ForwardDelayTmo | C18} <value> on page 372

LEC SHOW <n> {ForwardDelayTmo | C18} on page 397

LEC SHOW ForwardDelayTmo or LEC SHOW C18

Displays the Forward Delay Time, which is the maximum amount of time the LEC maintains an entry in its LAN Emulation ARP Cache for a non–local MAC address without verification of that entry. The value should always be lower than the value of the LAN Emulation ARP Aging Time.

Syntax: **LEC SHOW <n> {ForwardDelayTmo | C18}**

Parameter:	Description
n	Number of the LEC interface. Range: 0..31

Example:

```
XL> LEC SHOW 1 ForwardDelayTmo
Forward Delay Time (C18)  => 15 s
XL>
```

Related Commands:

LEC SET <n> {ForwardDelayTmo | C18} <value> on page 372

LEC SET <n> {AgingTime | C17} <value> on page 371

LEC SHOW <n> {AgingTime | C17} on page 396

LEC SHOW ArpRespTmo or LEC SHOW C20

Displays the LEC interface expected ARP Response Time, which is the maximum period of time the LAN Emulation ARP Request and Reply cycle takes to complete. It is used for retries and verifications.

Syntax: **LEC SHOW <n> {ArpRespTmo | C20}**

Parameter:	Description
n	Number of the LEC interface. Range: 0..31

Example:

```
XL> LEC SHOW 1 ArpRespTmo
Expected ARP Response Time (C20)  => 1 s
XL>
```

Related Commands:

LEC SET <n> {ArpRespTmo | C20} <value> on page 372

LEC SHOW FlushTmo or LEC SHOW C21

Displays the LEC interface Flush Timeout, which limits the time interval in which the LEC interface waits to receive a LAN Emulation Flush Response after a LAN Emulation Flush Request has been sent.

Syntax: **LEC SHOW <n> {FlushTmo| C21}**

Parameter:	Description
n	Number of the LEC interface. Range: 0..31

Example:

```
XL> LEC SHOW 1 FlushTmo
Flush Timeout (C21)  +> 4 s
XL>
```

Related Commands:

LEC SET <n> {FlushTmo | C21} <value> on page 373

LEC SHOW LocalSegmentID or LEC SHOW C23

Displays LEC interface 802.5 emulated LAN Local Segment ID, which is used in Source/Route bridging.

Syntax: **LEC SHOW <n> {LocalSegmentID | C23}**

Parameter:	Description
n	Number of the LEC interface.

Range: 0..31

Example:

```
XL> LEC SHOW 1 LocalSegmentID
Local Segment ID (C23)  +> 0xFA
XL>
```

Related Commands:

LEC SET <n> {LocalSegmentID | C23} <value> on page 373

LEC SHOW McastSendVccType or LEC SHOW C24

Displays the type of service (best–effort or variable bit rate) the LEC interface requests when establishing the Multicast Send VCC.

Syntax: **LEC SHOW <n> {McastSendVccType | C24}**

Parameter:	Description
n	Number of the LEC interface. Range: 0..31

Example:

```
XL> LEC SHOW 1 McastSendVccType
Mcast Send VCC Type (C24)  => BEST
XL>
```

Related Commands:

LEC SET <n> {McastSendVccType | C24} <BEST | VAR> on page 374

LEC SHOW McastSendSCR or LEC SHOW C25

Displays the forward and backward sustained cell rate the LEC interface requests when setting up the Multicast Send VCC, and requesting the variable bit rate type of service.

Syntax: **LEC SHOW <n> {McastSendSCR | C25}**

Parameter:	Description
n	Number of the LEC interface. Range: 0..31

Example:

```
XL> LEC SHOW 1 McastSendSCR
Mcast Send Average Rate (C25)  => 10000
XL>
```

Related Commands:

LEC SET <n> {McastSendSCR | C25} <value> on page 375

LEC SHOW McastSendPCR or LEC SHOW C26

Displays the forward and backward peak cell rate the LEC interface requests when setting up the Multicast Send VCC, and requesting the variable bit rate type of service.

Syntax: **LEC SHOW <n> {McastSendPCR | C26}**

Parameter:	Description
n	Number of the LEC interface. Range: 0..31

Example:

```
XL> LEC SHOW 1 McastSendPCR
Mcast Send Peak Cell Rate (C26)  => 10000
XL>
```

Related Commands:

LEC SET <n> {McastSendPCR | C26} <value> on page 376

LEC SHOW ConnCompTmo or LEC SHOW C28

Displays the LEC interface Connection Complete Timer, which is used during connection establishment to limit the amount of time the LEC waits for data, or a READY_IND message, from the called LEC.

Syntax: **LEC SHOW <n> {ConnCompTmo | C28}**

Parameter:	Description
n	Number of the LEC interface. Range: 0..31

Example:

```
XL> LEC SHOW 1 ConnCompTmo
Connection Complete Timer (C28)  => 4 s
XL>
```

Related Commands:

LEC SET <n> {ConnCompTmo | C28} <value> on page 377

LEC SHOW STATS

Displays the list of statistical counters for the LEC interface. These counters provide statistics on the activity of the LAN Emulation Protocol for the specified emulated LAN.

Syntax: **LEC SHOW <n> STATS**

Parameter:	Description
n	Number of the LEC interface. Range: 0..31

Example:

```
ILAN/XL(9)>ILAN/XL(9)>lec show 0 stats
Statistics for LEC interface 0:
  ARP Requests Out...................1
  ARP Replies In.....................1
  ARP Requests In....................0
  ARP Replies Out....................0
  Total number of Control Frames Out.51
  Total number of Control Frames In..5
  Multicast Packets Out..............52
  Multicast Packets In...............0
  Unicast Packets Out................0
  Unicast Packets In.................0
  Packets discarded on transmission..0
  Packets discarded on reception.....0
  SVC Failures.......................0
 XL>
```

LEC SHOW LastFailureCode

Displays the status code from the last failed Configure Response or Join Response.

Syntax: **LEC SHOW <n> LastFailureCode**

Parameter:	Description
n	Number of the LEC interface. Range: 0..31

Failed responses are those for which the LE_CONFIGURE_RESPONSE / LE_JOIN_RESPONSE frame contains a non–zero code, or fails to arrive within a timeout period. If none of the LEC interface's requests have failed, this command displays 'none'.

Possible returned values include:

"none"
"timeout"
"undefined error"
"version not supported"
"invalid request parameters"
"duplicate LAN destination"
"duplicate ATM address"
"insufficient resources"
"access denied"
"invalid requester ID"
"invalid LAN destination"
"invalid ATM address"
"no Configuration"
"LE Configure Error"
"insufficient information"

Example:

```
XL> LEC SHOW 0 LastFailureCode
Last Failure Response Code => "invalid LAN destination"
XL>
```

LEC SHOW LastFailureState

Displays the state the LEC interface was in at the time of the lastFailureRespCode update.

Syntax: **LEC SHOW <n> LastFailureState**

Parameter:	Description
n	Number of the LEC interface. Range: 0..31

Possible returned values include:

"initial state"
"LECS connect"
"configure"
"join"
"initial registration"
"BUS connect"
"operational"

Example:

```
XL> LEC SHOW 0 LastFailureState
Last Failure State => "initial state"
XL>
```

LEC SHOW STATE

Displays the information stored in the dynamical structures of the LEC interface.

Syntax: **LEC SHOW <n> STATE**

Parameter:	Description
n	Number of the LEC interface. Range: 0..31

Example:

```
XL> LEC SHOW 1 STATE
State of LEC interface 1:
Admin state: ENABLED
Bind state: Bound to port 21
Proxy Client: Yes
Config Mode:  Auto
Protocol: 1  Version: 1
State of protocol machine: Initial State
LEC Addr:   39000000000000000000000001000098A49AF002
LEC ID    =
lanName   = 'CCC_VLAN0'
LAN Type  = 802.3/Ethernet
Max Frame = 1516 bytes
lineRate  = 370370 cps
Topology Change: FALSE
LECS Addr:  47007900000000000000000000A03E00000100
LES Addr:
Config Direct VCC:
Control Distribute VCC:
Multicast Send VCC:
Multicast Forward VCC:
XL>
```

LEC SET {FORCEREG | NOFORCEREG}

This command enables or disables removal of old registration entry and registering a new one by XLES. Enabling speeds up CSP switching.

Normally there is no need to enable this feature on XLES - XLES will always know how to service register frame with additional TLV. If the XL code with 'registration forcing' is loaded to XL previously running earlier version of XL 7.0 (or 6.0, etc.), this feature will be DISABLED (the code will behave as previously loaded code - TLV will not be added to register request). In such case enable this feature using console command. When a new code is loaded and HBOOT is performed, the feature will be ENABLED after HBOOT.

Syntax: **LEC SET {FORCEREG | NOFORCEREG}**

LEC SHOW FORCEREG

This command displays the state of forced registration (whether it is enabled or disabled).

Syntax: **LEC SHOW FORCEREG**

22. LNM Agent Commands

HELP LNM

This command displays the available LNM Agent console commands.

Syntax: **HELP LNM**

LNM SHOW PORT

This command displays the LNM port configuration parameters.

Syntax: **LNM SHOW PORT [n]**

Parameter	Description
n	The number of an LNM port whose parameters you want to display.

LNM SHOW BRIDGE

This command displays a specific entry of the advertised bridge tables. If the argument is omitted, all the entries display.

Syntax: **LNM SHOW BRIDGE [n]**

Parameter	Description
n	The number of the advertising bridges entry table. Range: 1..8

LNM SET VPSEG

This command sets the secondary (alternate) LAN segment number on a specified port.

Syntax: **LNM SET VPSEG n x**

Parameter	Description
n	The number of an LNM port you want to set a secondary number for.
x	The segment number (the range is from 1 to FFF).

LNM SET VSEG

This command sets the secondary (alternate) LAN segment number on all ports.

Syntax: **LNM SET VSEG x**

Parameter	Description
x	The segment number. Range: 1..FFF

LNM SER ADDR

This command sets the secondary Media Access Control (MAC) Address on a specified LNM port.

Syntax: **LNM SER ADDR n xx–xx–xx–xx–xx–xx**

Parameter	Description
n	The number of an LNM port you want to set the secondary address for.
xx–xx–xx–xx–xx–xx	The MAC address.

LNM SET PERTHRS

This command sets the Percent Frames Lost Threshold on a specified LNM port.

Syntax: **LNM SET PERTHRS n x**

Parameter	Description
n	The number of the LNM port for which you want set the Percent Frames Lost Threshold.
x	The Percent Frames Lost Threshold. Range: 0..9999

LNM SET TELTHRS

This command sets the Telecommunication Link Error Threshold on a specified port.

Syntax: **LNM SET TELTHRS n x**

Parameter	Description
n	The number of the LNM port for which you want set the Telecommunications Link Error Threshold.
x	The Telecommunication Link Error Threshold. Range: 0 to 9999

LNM SET BRIDGE

This command defines a bridge advertising its presence on the integrated network. The advertising bridges are automatically linked by Token Ring Manager (Madge).

Syntax: **LNM SET BRIDGE [p1] [p2]**

Parameter	Description
p1	The number of the LNM port whose address (primary or secondary) you want to use in the definition of the bridge. Range: 0P 7P (primary address is used in the definition) 0S 7S (secondary address is used in the definition)
p2	The number of the LNM port whose address (primary or secondary) you want to use in the definition of the bridge. Range: 0P 7P (primary address is used in the definition) 0S 7S (secondary address is used in the definition

LNM SET DFLTBRI

This command defines default bridges that advertise their presence on the integrated network.

Syntax: **LNM SET DFLTBRI**

LNM DEL BRIDGE

This command removes a specified entry in the advertised bridges table, or all entries if the optional argument is omitted.

Syntax: **LNM DEL BRIDGE [n]**

Parameter	Description
n	The number of the entry. Range: 1..8

23. OSPF Commands

Information

- One OSPF instance is supported.
- OSPF router IDs must be unique, and any change of router ID requires restarting OSPF router.
- For stub areas, it is necessary to configure stub metrics on the stub Area Border Router to make the router advertise into the area a default exit route.
- For Virtual Links, configure Virtual Links only between directly connected routers.
- To learn other protocol routes or configured static routes (to import them from the routing table and advertise throughout OSPF's routing domain), OSPF router has to be an Autonomous System Boundary Router.
- LOCAL networks (directly connected) are advertised by OSPF only when OSPF is running on an associated port. LOCAL routes are always better than RIP routes. When there is a directly connected network, and on this port only RIP is running, OSPF will not learn this RIP route (because there is a better, LOCAL route in the routing table). To make this route advertised by OSPF, you must define OSPF on this port (there will be no OSPF neighbours on this port, and this route will be advertised in the OSPF Router LSA, not in the OSPF ASE LSA). All other RIP routes (not directly connected to the router) will be learned by OSPF and advertised by OSPF as ASE throughout the OSPF routing domain.
- OSPF learns RIP routes with a RIP (hop-)metric.

OSPF INSTANCE NEW and OSPF INSTANCE DEL

Create an OSPF protocol instance:

Syntax: **OSPF INSTANCE NEW instance_id ASE_interval ASE_limit LSDB_limit**

Parameter	Description
instance_id	This is the number which identifies the new OSPF instance.
ASE_interval	This is the time interval OSPF router, when configured to be an ASBR, is scanning the routing table to import routing information into OSPF’s database and advertise it throughout OSPF’s routing domain as Autonomous System External (ASE) advertisements (see also ASE_limit).
ASE_limit	This is the number of routing table entries OSPF router can import every ASE_interval.
LSDB_limit	This is the limit of ASE LSAs that can be contained in the ASE Link Status DataBase (LSDB).

To reverse this command (delete an OSPF instance):

Syntax: **OSPF INSTANCE DEL instance_id**

OSPF RTRID

After creating an instance, set its Router ID:

Syntax: **OSPF RTRID router_id**

Example:

```
OSPF RTRID 10.0.0.10
```

Parameter	Description
router_id	This is the router identifier (32-bit value). It has the same format as an IP address but identifies the router independent of its IP address.

- A router’s ID should not be changed while the OSPF process is running. Disable the OSPF process before changing a Router’s ID.
- The default value is 10.0.0.0.
- One possible strategy for choosing the router ID would be to use the smallest IP interface address belonging to the router.

OSPF AREA NEW and OSPF AREA DEL

Create an OSPF area in which the router will work:

Syntax: OSPF AREA NEW area_id area_type

Parameter	Description
area_id	This is the area identifier (a user-supplied 32-bit value). It has the same format as an IP address.
area_type	This is the area type. The possible values are: *TRANS*, *STUB*, *STUBNS* or *NSSA* as outlined below.

- A TRANS (transit) area is the only non-backbone area that can carry data traffic that neither originates nor terminates in the area itself. It can be used to pass information from hosts outside this area to other hosts outside this area.
- A STUB area, by definition, is an area into which AS external advertisements are not flooded; routing to AS external destinations in these areas is based on a (per-area) default only; a STUB area cannot be used as a transit area for information between outside hosts, but only for directed information flow to hosts inside this area or to hosts outside this area.

  All routers working in a stub area must be defined as such.

  When there is a net range set for a stub area, the border router propagates the summarized advertisements from that area to the backbone.

  External advertisements are not propagated in a stub area, which reduces protocol traffic and routing information exchange. To reduce protocol traffic and routing table size even more, it is also possible to configure the border router so that it doesn’t advertise network advertisements into a stub area; routing to AS external and inter-area destinations is then based on a per-area default route advertised by the stub area border router.
- A STUBNS area’s border router does not originate or propagate summary LSAs into the *STUB* area and the routers working in this area rely entirely on border router’s default route.
- An NSSA is a new optional type of OSPF area, sometimes referred to as a “not-so-stubby” area. NSSAs are similar to stub areas but they have the additional capability of importing AS external routes in a limited fashion (see RFC1587).

To reverse this command (delete an area):

Syntax: OSPF AREA DEL area_id

Example:
OSPF AREA NEW 1.1.1.1 TRANS

OSPF AREA SCOST and OSPF AREA SCOST DEL

(Applies to stub areas only.) Set the cost of the default external route that will be advertised into the stub area:

Syntax: OSPF AREA SCOST area_id cost [N]

Parameter	Description
cost	This is the cost metric.
N	This parameter is optional. If included, it means that the metric value is not comparable with other OSPF metrics. This should only be used for an NSSA area.

After setting the cost for the default external route, the border router will advertise the IP address 0.0.0.0 with IP mask 0.0.0.0 + Stub Metric into the area. This tells hosts working in this area where to send information (to the border router) when they don’t know the addressee.

Note: It is absolutely necessary to configure the cost, or else the border router will not advertise the default route throughout the stub area.

To reverse this command (delete a cost for the default external route):

Syntax: OSPF AREA SCOST DEL area_id

OSPF AREA ENABLE and OSPF AREA DISABLE

After creating a new area, enable it:

Syntax: OSPF AREA ENABLE area_id

Example:

OSPF AREA ENABLE 1.1.1.1

To reverse this command (disable an area):

Syntax: OSPF AREA DISABLE area_id

OSPF AREA TYPE

Each area can be set to use authentication (passwords) or to allow unrestricted communication among all routers.

Setting authentication is performed in two steps:

- enable authentication per-area,
- define authentication key, per OSPF interface, to be used while exchanging routing information.

All routers on a particular LAN/WAN segment have to have the same authentication keys or they will not accept each other.

Setting an area to require passwords requires that you then set a password on each router working in the area. That is discussed later, under *Setting the Authentication Key for an Interface*.

The following command defines the type and authentication requirement of an area.

Syntax: OSPF AREA TYPE area_id area_type authentication_type

Parameter	Description
area_type	The possible values are (as discussed before):

TRANS	Transitive
STUB	Stub
STUBNS	Stub No Summary
NSSA	NSSA

authentication_type

The authentication type, which determines whether routers in the area require authentication before communication:

NONE	No passwords required
PSWD	Communication among routers requires setting a simple password

OSPF RANGE NEW and OSPF RANGE DEL

Use this command to add a net range to an area. Remember that you must disable an area (using the command OSPF AREA DISABLE area_id on page 414) before you can define net ranges for it.

Syntax: OSPF RANGE NEW area_id ip_address ip_mask [N]

Parameter	Description
area_id	This is the area identifier to which you want to add a Net Range.
ip_address	This is the IP address of the net range.
ip_mask	This is the IP mask associated with the IP address.
N	This parameter is optional. If included, it means that the net range is an NSSA range.

Adding a net range to an area aggregates information advertised by the border router across an area boundary. When defined, the aggregate route will be advertised across an area border only when there are active routes in the routing table falling into the aggregate net range.

Example:

In area 1.0.0.0, there are the following IP networks:

128.100.1.0/255.255.255.0
128.100.2.0/255.255.255.0
128.100.3.0/255.255.255.0
128.100.4.0/255.255.255.0
Without net ranges defined, the area border router advertises all these networks into OSPF's backbone area (0.0.0.0) and then into other areas.

To reduce the routing information exchanged (and routing tables sizes), configure the following net range

OSPF RANGE NEW 1.0.0.0 128.100.0.0 255.255.0.0, or
OSPF RANGE NEW 1.0.0.0 128.100.0.0 255.255.248.0

With this net range configured, the area border router will advertise only one (aggregate) network across the area border and then into other areas.

To reverse this command (delete a net range):

Syntax: OSPF RANGE DEL area_id ip_address ip_mask [N]

OSPF ENABLE and OSPF DISABLE

After an instance and area are created and the router's parameters are set, activate the OSPF protocol:

Syntax: **OSPF ENABLE**

To reverse this command (disable OSPF):

Syntax: **OSPF DISABLE**

OSPF INTF NEW and OSPF INTF DEL

This command identifies the interface as an OSPF interface.

Syntax: **OSPF INTF NEW interface_number area_id**

Example:

OSPF INTF NEW 1 1.1.1.1

Parameter	Description
interface_number	This identifies the interface.
area_id	This is the area identifier (a user-supplied 32-bit value; IP address format) to which the interface is connected.

To reverse this command (delete an OSPF interface):

Syntax: **OSPF INTF DEL interface_number**

OSPF INTF ENABLE and OSPF INTF DISABLE

This command enables an OSPF interface.

Syntax: **OSPF INTF ENABLE interface_number**

To reverse this command (disable an OSPF interface):

Syntax: **OSPF INTF DISABLE interface_number**

Each network has a Designated Router (DR) which controls synchronization of the Link State Databases of all routers in the area (all of them must have the same LSDB).

There is also a Backup Designated Router (BDR) in the network. If the DR fails, the BDR becomes the DR and a new BDR is chosen.

When a new router appears in the network it synchronizes its LSDB with the databases of the DR and BDR. (The DR controls synchronization with all router databases, and the BDR will do so if the DR fails.)

Immediately after starting OSPF, all routers exchange information about themselves to learn the network topology. After that, topology information is exchanged only if the topology changes or if the LS Refresh Timer expires.

OSPF INTF COST

Set the cost of the OSPF interface:

Syntax: **OSPF INTF COST interface_number cost**

Parameter	Description
cost	This is the cost metric you want to set for the interface. One suggested strategy for assigning metrics is to base them on interface type. Th table below describes the metrics to be advertised for a specified interface; the assumed default value based on bandwidth is: Metric = 10^8 / ifSpeed Network type/bit rateMetric >= 100 MBPS1 Ethernet/802.310 E148 T1 (ESF)65 64 KBPS1562 56 KBPS1785 19.2 KBPS5208 9.6 KBPS10416

Note: When configuring OSPF metrics for a network topology where OSPF exchanges its routing information with other protocols, note that:

- when RIP imports an OSPF route, it sets the metric to 1
- when BGP imports an OSPF route, it uses the OSPF metric
- when OSPF imports a RIP route, it uses the RIP metric
- OSPF and RIP do not import BGP routes by default

OSPF INTF PRIOR

Set the router's priority. This priority is used in the Designated Router (DR) election process.

Syntax: **OSPF INTF PRIOR interface_number prior**

Parameter	Description
prior	This is the priority in the range from 0 to 255. The value 0 means that the router is not eligible to become the DR on this network.

The router with the highest priority wins the election process, which happens only if the currently active DR fails, and becomes the new DR. If the current DR continues to work, adding a router with a higher priority will not make the new router the DR because only a DR failure triggers a DR election.

OSPF INTF AUTHKEY

If you have set the area to require authentication (with **OSPF AREA TYPE** ***area_id area_type*** PSWD), you must set the *authentication key* (essentially a password) for all OSPF interfaces to that area.

Syntax: **OSPF INTF AUTHKEY interface_number [auth_key]**

Parameter	Description
auth_key	The authentication key consist of up to eight hexadecimal codes (in the range 0..FF) separated by spaces.

OSPF INTF RXMT

(Optional) This command sets the *retransmission interval*, which is the number of seconds between link state advertisement retransmissions for adjacencies belonging to this interface. This value is also used when retransmitting database description and link state request packets.

Syntax: **OSPF INTF RXMT interface_number interval**

Parameter	Description
interval	This is the interval in seconds.

OSPF INTF TRANS

(Optional) This command sets the *transit delay interval*, which is the number of seconds it takes to transmit a link state update packet over this interface. Link state advertisements contained in the Link State Update packet will have their age incremented by this amount before transmission.

Syntax: **OSPF INTF TRANS interface_number interval**

Parameter	Description
interval	Must be greater than zero.

OSPF INTF HELLO

(Optional) This command sets the *hello interval*, which is the number of seconds the router waits between sending Hello packets on this interface. This value must be the same for all routers attached to a common network.

Syntax: **OSPF INTF HELLO interface_number interval**

OSPF INTF DEAD

(Optional) This command sets the *dead interval*, which is the number of seconds that a router will wait to receive a hello packet from its neighbor before it declares the neighbor router to be down. This should be some multiple of the *hello interval* and must be the same for all routers attached to a common network.

Syntax: **OSPF INTF DEAD interface_number interval**

OSPF INTF POLL

(Optional) This command sets the *poll interval*, which is the number of seconds between hello packets being sent to an inactive non-broadcast multi-access neighbor.

Syntax: **OSPF INTF POLL interface_number interval**

Configuration of an OSPF Virtual Interface

Use this procedure to set OSPF virtual interface parameters from the console port.

Communication through the backbone has to be dependable: if the backbone area is disconnected or partitioned, some IP destinations become unreachable. To establish and maintain connectivity of the backbone, virtual links can be configured through non-backbone transit areas.

The endpoints of a virtual link are area border routers. To create a virtual link, create two virtual interfaces, one on each of the two border routers that the virtual link will connect.

A virtual interface works like a normal OSPF unnumbered point-to-point interface, and belongs by definition to the backbone.

Note: When one, or both, of the virtual endpoints connect to transit area via an unnumbered point-to-point link, virtual link will not become operational, because it is impossible to calculate the virtual neighbour's IP address.

Virtual links can not be configured through stub areas.

OSPF VINTF NEW and OSPF VINTF DEL

Create a virtual interface:

Syntax: **OSPF VINTF NEW nbr area_id**

Parameter	Description
nbr	This is the router identifier of the virtual neighbor. For each router this is an identifier of the second router from the pair for which the Virtual Link is being established.
area_id	This is the area identifier (a user-supplied 32-bit value; IP address format) of the transit area.

To reverse this command (delete a virtual interface):

Syntax: **OSPF VINTF DEL nbr area_id**

OSPF VINTF ENABLE and OSPF VINTF DISABLE

Enable the virtual interface:

Syntax: OSPF VINTF ENABLE nbr area_id

To reverse this command (disable a virtual interface):

Syntax: OSPF VINTF DISABLE nbr area_id

OSPF VINTF AUTHKEY

(Applies only to areas with the authentication type set to simple password.) Set the *authentication key* for the virtual interface:

Syntax: OSPF VINTF AUTHKEY nbr area_id [auth_key]

Parameter	Description
auth_key	The authentication key consist of up to eight hexadecimal codes (in the range 0..FF) separated by spaces.

Optionally you can also set the timer parameters described below, but in most cases you should leave them set to the default values. If you do change them, be sure to make the Hello and Dead intervals consistent across all directly connected OSPF routers.

OSPF VINTF RXMT

(Optional) Sets the *retransmission interval*, which is the number of seconds between link state advertisement retransmissions for adjacencies belonging to this virtual interface. This value is also used when retransmitting a database description and link state request packets.

Syntax: OSPF VINTF RXMT nbr area_id interval

Parameter	Description
interval	This is the interval in seconds.

OSPF VINTF TRANS

(Optional) Sets the *transit delay interval*, which is the number of seconds it takes to transmit a link state update packet over this interface. Link state advertisements contained in the Link State Update packet will have their age incremented by this amount before transmission.

Syntax: **OSPF VINTF TRANS nbr area_id interval**

Parameter	Description
interval	Must be greater than zero.

OSPF VINTF HELLO

(Optional) Sets the *hello interval*, which is the number of seconds the router waits between sending Hello packets on this virtual interface. This value must be the same for both virtual neighbors.

Syntax: **OSPF VINTF HELLO nbr area_id interval**

OSPF VINTF DEAD

(Optional) Sets the *dead interval*, which is the number of seconds that a router will wait to receive a hello packet from its neighbor before it declares the router to be down. This should be some multiple of the *hello interval* and must be the same for both virtual neighbors.

Syntax: **OSPF VINTF DEAD nbr area_id interval**

OSPF INSTANCE LOCATE

There may be several OSPF instances. This command sets the current OSPF instance. All commands are associated with the current OSPF instance.

Syntax: **OSPF INSTANCE LOCATE instance_id**

Parameter	Description
instance_id	This is the instance identifier of the instance you want to set as the current instance.

Note: Currently, only one instance of OSPF protocol is supported

OSPF RANGE {HIDE | ADVERTISE}

This command changes the status of a net range.

Syntax: **OSPF RANGE {HIDE | ADVERTISE} area_id ip_address ip_mask [N]**

Parameter	Description
HIDE	If the *HIDE* option is selected, the net range will not be advertised.
ADVERTISE	If the *ADVERTISE* option is selected, the net range will be advertised.

OSPF HOST NEW and OSPF HOST DEL

This command adds a new host.

Syntax: **OSPF HOST NEW area_id ip_address cost**

Parameter	Description
area_id	This is the area identifier of the area in which the host resides.
ip_address	This is the IP address of the host.
cost	This is the cost metric you want to set for the host.

To delete information for a host, use:

Syntax: **OSPF HOST DEL area_id ip_address**

OSPF IMPORT DEFAULT

This command sets the import policy default. If the parameters are omitted, this command will display the default preferences. Before entering this command, disable the OSPF instance.

Syntax: **OSPF IMPORT DEFAULT [class_0 class_1 class_2]**

Parameter	Description
class_0	This sets the preferences for class 0 routes.
class_1	This sets the preferences for class 1 routes.
class_2	This sets the preferences for class 2 routes.

OSPF IMPORT ENABLE and OSPF IMPORT DISABLE

This command enables the import policy.

Syntax: **OSPF IMPORT ENABLE**

This command disables the import policy.

Syntax: **OSPF IMPORT DISABLE**

OSPF IMPORT NEW and OSPF IMPORT DEL

This command adds a new entry to the import policy table.

Syntax: **OSPF IMPORT NEW address mask pref**

Parameter	Description
address mask	The address and the mask specify a net range for imported routes.
pref	This is the preference for imported routes.

This command deletes an entry from the import policy table.

Syntax: **OSPF IMPORT DEL address mask**

OSPF IMPORT RESET

This command resets the import policy table.

Syntax: **OSPF IMPORT RESET**

OSPF EXPORT ENABLE and OSPF EXPORT DISABLE

This command enables the export policy.

Syntax: **OSPF EXPORT ENABLE**

This command disables the export policy.

Syntax: **OSPF EXPORT DISABLE**

OSPF EXPORT NEW and OSPF EXPORT DEL

This command adds a new entry to the export policy table.

Syntax: **OSPF EXPORT NEW proto spec1 spec2 address {E|B} metric tag [key_bits]**

Parameter	Description
proto	This specifies the protocol type of the route to be exported. The possible values are REMOTE and RIP.
	Spec1 and Spec2 are dependent on the protocol. These fields have the following meaning:
spec1	REMOTE Preference IP address. RIP IP address of interface.
spec2	REMOTE IP Mask. RIP Next hop IP address.
address	This is the network address of the exported route.
E	When this is selected, it means the route is exported.
B	When this is selected, it means the route is blocked.
metric	This is the metric value for the exported route. If you want to use the original metric, enter PROTO.
tag	This is the tag for the exported route. You may enter a decimal number, EGPAS, AS or NONE.
key_bits	This indicates which keys are used when comparing.

To delete an entry from the export policy table, use:

Syntax: **OSPF EXPORT DEL proto spec1 spec2 address**

OSPF EXPORT RESET

This command resets the export policy table.

Syntax: **OSPF EXPORT RESET**

OSPF NBMA NEW and OSPF NBMA DEL

This command creates a neighbor entry for the non-broadcast, multi-access interface.

Syntax: OSPF NBMA NEW intf ip_address prior

Parameter	Description
intf	This identifies the non-broadcast, multi-access interface.
ip_address	This is the IP address of the neighbor.
prior	This is the neighbor's priority used in the designated router election process.

This command deletes a neighbor entry for the non-broadcast, multi-access interface.

Syntax: OSPF NBMA DEL intf ip_address spec1

OSPF DBSIZE

This command sets the default sizes of the Link State DataBase (LSDB) hash tables. Each new OSPF instance creates has tables using the values that are set.

Syntax: OSPF DBSIZE stub rtr net sumnet sumasb ase mc nssa

Parameter	Description
stub	This changes the size of the hash table for stub network information.
rtr	This changes the size of the hash table for router information.
net	This changes the size of the hash table for network information.
sumnet	This changes the size of the hash table for summary network information.
sumasb	This changes the size of the hash table for Autonomous System Boundary router information.
ase	This changes the size of the hash table for Autonomous System External information.
mc	This changes the size of the hash table for multicast information.
nssa	This changes the size of the hash table for NSSA advertisements.

- Changing the size of the hash tables can affect performance. Care must be taken before changing these values
- The changes to the LSDB hash tables will take affect after the router is restarted.
- All hash tables must have the same configured size.

OSPF SHOW GEN [DETAILED]

To display general information about the OSPF Router enter the command:

Syntax: **OSPF SHOW GEN [DETAILED]**

Example:

OSPF SHOW GEN
Rtr ID: 3.3.3.0Instance ID: 1
Status: Disabled
OSPF Version: 2ABR: Off ASBR: On TOS Support: OffLS ASE Count: 0
ASE Cksum sum: Ox0LSA Orig Count: 0 Rx LSA Count: 0LSDB Limit: 1000 MC Support: 0

When **DETAILED** is specified, the following additional information is displayed:

ASE Limit: 100 ASE Interval: 10
Sizes of LSDB hash tables:

STUB-	3
RTR -	3
NET -	3
SUMNET-	3
SUMASB-	3
ASE -	3
MC -	3
NSSA-	3

Display Field	Description
Rtr ID	This is the router identifier. It has the same format as an IP address but identifies the router independent of its IP address.
Instance ID	This is the OSPF instance identifier.
Status	This will display *Enabled* if the OSPF process is active and *Disabled* if it is inactive.
OSPF Version	This is the version number of the OSPF protocol.
ABR	This will display *on* if the router is an Area Border Router (ABR) and *off* it if not an ABR.
ASBR	This will display *on* if the router is an Autonomous System Boundary Router (ASBR) and *off* if it is not an ASBR.
TOS Support	This will display *on* if the Type of Service (TOS) routing is supported and *off* if it is not supported.
LS ASE Count	This is the number of external (LS type 5) link state advertisements in the Link State DataBase (LSDB).

ASE Cksum sum
: This is the sum of the Link State checksums for external Link State Advertisements (LSAs) contained in the Link State DataBase (LSDB). This sum can be used to determine if there has been a change in the router's LSDB or to compare the LSDB of two routers.

LSA Orig Count
: This is the number of new Link State Advertisements (LSAs) that have been originated.

Rx LSA Count
: This is the number of Link State Advertisements (LSAs) received.

LSDB Limit
: This is the maximum number of ASE LSAs that can be originated by this OSPF instance.

MC Support
: This indicates whether multicast of IP DATAGRAMs is supported. 0 means that it is not supported; 1 means that it is supported.

ASE Limit
: This is the number of ASE LSAs searched every ASE interval.

ASE Interval
: This is the interval for scanning ASE LSAs.

Sizes of LSDB hash tables
: This indicates the number of hash table entries for each type of advertisement.

OSPF SHOW INSTANCES

This command displays the status of all the OSPF instances that are defined.

Syntax: **OSPF SHOW INSTANCES**

Display Field	Description
Instance ID	This identifies the OSPF instance.
Router ID	This is a 32 bit number assigned to each router running the OSPF protocol which uniquely identifies the router within the AS.
Status	This is the status of the instance. It is displayed as *Enabled* or *Disabled*.

Example:

OSPF SHOW INSTANCES

Instance ID	Router ID	Status
1	10.0.0.0	Enabled
2	10.0.0.0	Disabled

OSPF SHOW INTFS

This command displays OSPF specific information about the router's interfaces.

Syntax: **OSPF SHOW INTFS**

Display Field	Description
INTF	This is the IP address of the interface.
Port	This is the IP port description.
ENABLED or DISABLED	ENABLED is displayed if the interface is enabled for the OSPF process and disabled is displayed if the interface is disabled for the OSPF process.
Area	This is the area identifier to which the interface is connected.
Type	This is the type of interface. The possible values are: *BCAST, NBMA* or *PTOP.*
State	This is the interface state. The possible values are: *Down*, *Loopback*, *Waiting, P to P, DR*, *BackupDr,* or *DR Other*).
Prior	This is the priority of the interface. It is used in the designated router election.
Events	This is the number of times this interface has changed its state.
Dly	This is the value of the *InfTransDelay* parameter in seconds.
Retrans	This is the value of the *RxmtInterval* parameter in seconds.
Hello	This is the value of the *HelloInterval* parameter in seconds.
Poll	This is the value of the *PollInterval* parameter in seconds.
Dead	This is the value of the *RouterDeadInterval* parameter in seconds.
DR	This is the IP address of the Designated Router.
BDr	This is the IP address of the Backup Designated Router.

Example:

```
OSPF SHOW INTFS
INTF: 2.2.2.2  Port: 0  ENABLED
                    Area: 0.0.0.0  Type: BC    State: DR  Prior: 5  Events: 2
                    Dly: 1 Retrans: 5 Hello: 10 Poll: 0  Dead: 40
                    DR: 2.2.2.2  BDr: 0.0.0.0
INTF: 128.100.1.1  Port: 3  ENABLED
                    Area: 1.1.1.1  Type: BC    State: DR  Prior: 5  Events: 2
                    Dly: 1 Retrans: 5 Hello: 10 Poll: 0  Dead: 40
                    DR: 128.100.1.1  BDr: 128.100.1.2
INTF: 128.101.1.1  Port: 2  ENABLED
                    Area: 0.0.0.0  Type: BC    State: DR  Prior: 5  Events: 2
                    Dly: 1 Retrans: 5 Hello: 10 Poll: 0  Dead: 40
                    DR: 128.101.1.1  BDr: 128.101.1.2
```

OSPF SHOW VINTFS

This command displays information about configured virtual interfaces.

Syntax: OSPF SHOW VINTFS

Display Field	Description
Transit Area	This identifies the transit area.
Neighbor	This is the router ID of the virtual neighbor.
State	This is the interface state. The possible values are: *Down*, *Loopback*, *Waiting*, *P to P*, *DR*, *BackupDr*, or *DR Other*).
Dly	This is the value of the *InfTransDelay* parameter in seconds.
Retrans	This is the value of the *RxmtInterval* parameter in seconds.
Hello	This is the value of the *HelloInterval* parameter in seconds.
Dead	This is the value of the *RouterDeadInterval* parameter in seconds.
Events	This is the number of times this interface has changed its state.

Example:

```
OSPF SHOW VINTFS
Transit Area: 1.1.1.1  Neighbor: 130.130.130.130  State: P To P
                        Dly: 1  Retrans: 5  Hello: 10  Dead: 40  Events: 1
```

OSPF SHOW AREAS

This command displays information about the router's attached areas.

Syntax: **OSPF SHOW AREAS**

Display Field	Description
Area ID	This is the area identifier.
Auth	This is the authentication type. The possible types are *NONE* or *PSWD* (simple password).
Type	This is the area's support for importing Autonomous System External Link State Advertisements (ASE LSAs). The possible types are Type 5 (which stands for transit area), Stub or NSSA.
Spf Runs	This is the number of times that the intra-area route table has been calculated using this area's Link State DataBase (LSDB).
Summary	This indicates whether summaries are advertised into a stub area. ON means that summaries are advertised; OFF means that they are not advertised.
ABRs	This is the number of Area Border Routers (ABRs) that are reachable in this area.
ASBRs	This is the number of Autonomous System Boundary Routers (ASBRs) that are reachable in this area.
Intra LSAs	This is the total number of Link State Advertisements (LSAs) in this areas Link State DataBase (LSDB) excluding the Autonomous System External Link State Advertisements (ASE LSAs).
Cksum sum	This is the sum of the Link State checksums contained in this area's Link State DataBase (LSDB) excluding the Autonomous System External (Type 5) Link State Advertisements (ASE LSAs). This sum can be used to determine if there has been a change in the router's LSDB or to compare the LSDB of two routers.

Example:

OSPF SHOW AREAS

Area ID	Auth	Type	Spf Runs	Sum-mary	ABRs	ASBRs	Intra LSAs	Cksum sum
0.0.0.0	NONE	Type 5	8	on	2	2	5	0x0003191d
1.1.1.1	NONE	Type 5	5	on	2	2	9	0x00043074

OSPF SHOW NBRS

This command displays information about the router's non-virtual neighbors.

Syntax: **OSPF SHOW NBRS**

Display Field	Description
IP Address	This is the IP address of the neighbor.
N	This is port or logical link associated with this interface.
Router ID	This is the router ID of the neighbor.
Opt	This is a bit pattern that describes the OSPF neighbor options.
Prior	This is the priority of the neighbor in the designated router election algorithm. 0 signifies that the neighbor is not eligible to become the designated router.
State	This is the state of the neighbor. The possible values are: *Down*, *Attempt*, *Ini*t, *2 Way*, *ExStart*, *Exchange*, *Loading*, or *Full*).
Events	This is the number of times the neighbor has changed state or an error has occurred.
QLen	This the current length of the retransmission queue.
Status	This indicates the status of the neighbor router. *Dynamic* means that the router was learned by the OSPF process. *Permanent* means that the router was defined as static.

Example:

OSPF SHOW NBRS

IP Address	N	Router ID	Opt	Prior	State	Events	QLen	Status
128.100.1.2	3	130.130.130.130	0002	5	Full	6	0	Dynamic
128.101.1.2	2	130.130.130.130	0002	5	Full	6	0	Dynamic

OSPF SHOW VNBRS

This command displays information about the router's virtual neighbors.

Syntax: **OSPF SHOW VNBRS**

Display Field	Description
Transit Area	This is the transit area's ID.
Neighbor ID	This is the router ID of the virtual neighbor.
Neighbor address	This is the address of the neighbor.
Opt	This is a bit pattern that describes the OSPF virtual neighbor options.
State	This is the state of the neighbor. The possible values are: *Down, Attempt, Init*, *2 Way*, *ExStart*, *Exchange*, *Loading*, or *Full*).
Events	This is the number of times the neighbor has changed state or an error has occurred.
QLen	This the current length of the retransmission queue.

Example:

OSPF SHOW VNBRS

Transit Area	Neighbor ID	Neighbor Addr	Opt	State	Events	Qlen
0.0.0.2	33.0.0.0	128.200.33.4	0002	Full	41	0

OSPF SHOW LSDB [DETAILED]

This command displays the router's Link State DataBase (LSDB), excluding Autonomous System External Link State Advertisements (ASE LSAs) for all attached areas. If the area ID is provided, only information for the specified area is displayed.

Only one page is displayed at a time (maximum 24 lines).Re-type the command to display next page.

If you type the command with new parameters, new information will be displayed, starting from first page.

To always break printing continuation of LSDB use FIRST option.

Syntax: **OSPF SHOW LSDB [area_id] [type] [LS_ID ls_id] [ADV_RTR adv_rtr] [FIRST] [DETAILED]**

Syntax: **OSPF SHOW LSDB [area_id] [DETAILED]**

Parameter	Description
area_id	Area Id of the area to which the LSAs belong.
type	Type of LSAs. Possible values are: *RTR, NET, SUMNET, SUMASB, ASE, NSSA*.
ls_id	Link State identifier of LSAs.
adv_rtr	Router ID of the router which originated LSAs.

Display Field	Description
Area ID	Identifies the area to which the LSA belongs.
Type	This is the type of LSA. The possible values are: STUB, *RTR, NET, SUMNET, SUMASB, ASE, MC, NSSA*., *PRI*
LS ID	This is the Link State identifier; this field identifies the portion of the internet environment described by the advertisement. When this parameter is specified, the command displays only the matching entries. Depending on the advertisement's LS type, it takes the following values: RTR: The originating router's Router ID NET: The IP interface address of the network's Designated Router SUMNET: The destination network's IP address SUMASB: The Router ID of the described AS boundary router ASE: The destination network's IP address NSSA: The destination networks IP address

Adr Rtr	This is the Router ID of the originating router. When this parameter is specified, the command displays only the matching entries.
Age	This is the age of the LSA (seconds since the link state advertisement was originated).
Cksum hex	This is the checksum of the LSA, not including the age field.
Seq hex	This is the sequence number of the LSA.

Common Display Field	Description
Area ID	This identifies the area to which this LSA belongs.
LS type	This is the type of LSA. The possible values are: *RTR, NET, SUMNET, SUMASB, ASE, NSSA.*
LS ID	This is the Link State identifier; this field identifies the portion of the internet environment described by the advertisement. Depending on the advertisement's LS type, it takes the following values: RTR: The originating router’s Router ID NET: The IP interface address of the network's Designated Router SUMNET: The destination network’s IP address SUMASB: The Router ID of the described AS boundary router ASE: The destination network’s IP address NSSA: The destination network's IP address
Adr Rtr	This is the Router ID of the originating router.
Age	This is the age of the LSA (seconds since the link state advertisement was originated).
Len	This is the length in bytes of the LSA including the 20 byte LSA header.
Seq #	This is the sequence number of the LSA in hex.
Checksum	This is the checksum of the LSA, not including the age field.
Options	This is a bit pattern that indicates the optional capabilities supported by the described portion of the routing domain.

RTR

Display Field	Description
ASB:	When on, the router is advertised as an ASBR.
AB:	When on, the router is advertised as an Area Border router.
Virtual:	When on, router is an end-point of a virtual link.
Area WC:	When on, the Inter-Area multicast extension of OSPF is enabled.
AS WC:	When on, the NSSA area border router translates from type 7 to type 5 Link State Advertisements.

Link ID and data are dependent on type of described router link. These fields have the following meaning:

type: Router (stands for point-to-point connection to another router)
When the type is point-to-point connection to another router, the *link id* is the neighboring router's router ID and the *link data* is the IP interface address (for numbered) or the index (for unnumbered).

type: Transit net
When the type is a transit network, the *link id* is the IP address of the Designated Router and the *link data* is IP interface address.

type: Stub net When the type is a stub network, the *link id* is the IP network or subnetwork number and the *link data* is the network's IP address mask.

type: Virtual When the type is a virtual link, the *link id* is the neighboring router's router ID and the *link data* is the IP interface address.

metric This is the value of the metric for this link.

Net

Display Field	Description
Net mask:	This is the network mask.
Attached router:	Router IDs of all routers that are attached to this network and fully adjacent to the Designated Router. Designated Router includes itself in this list.

SUMNET

Display Field	Description
Net mask:	This is the network mask.
Tos:	Type of Service is not implemented in this version.
metric:	This is the metric (cost) of this route.

SUMASB

Display Field	Description
Tos:	Type of Service is not implemented in this version.
metric:	This is the metric (cost) of this route.

Example (when DETAILED is not specified)

OSPF SHOW LSDB

Area ID	Type	LS ID	Adr Rtr	Age	Cksum hex	Seq hex
0.0.0.0	RTR	2.2.2.2	2.2.2.2	38	ca8b	80000004
1.1.1.1	NET	128.100.1.1	2.2.2.2	42	c395	80000002
0.0.0.1	SUMNET	111.30.1.1	36.0.0.0	802	1333	80000001
0.0.0.1	SUMASB	33.0.0.0	36.0.0.0	802	af65	80000001

Example (when DETAILED is specified)

the following additional information is displayed:

```
OSPF SHOW LSDB DETAILED
Area ID: 1.1.1.1  LS type: RTR  LS ID: 2.2.2.2  Adv rtr: 2.2.2.2  Age: 0
                  Len: 36  Seq #: 80000003  Checksum: Ox4927  Options: 2
                  Capabilities: ASB: On AB: On Virt: Off Area WC: Off AS WC: Off
                  link id: 128.100.1.1  data: 128.100.1.1  type: Transit net metric: 1
Area ID: 0.0.0.0  LS type: NET  LS ID: 128.101.1.1  Adv rtr: 2.2.2.2  Age: 0
                  Len: 32  Seq #: 80000002  Checksum: Oxb7a0  Options: 1
                  Net mask: 255.255.255.0
                  Attached router: 2.2.2.2
                  Attached router: 130.130.130.130
Area ID: 0.0.0.0  LS type: SUMNET  LS ID: 128.100.1.0  Adv rtr: 2.2.2.2  Age: 0
                  Len: 28  Seq #: 80000001  Checksum: Ox115f  Options: 0
                  Net mask: 255.255.255.0
                  Tos 0 metric: 1
Area ID: 0.0.0.1  LS type: SUMASB  LS ID: 33.0.0.0  Adv rtr:  36.0.0.0  Age:  33
                  Len: 28  Seq #:  80000001  Checksum:  0xaf65  Options:  0
                  Tos 0 metric:4
```

OSPF SHOW EXTLSDB [DETAILED]

This command displays the part of the router's Link State DataBase (LSDB) which contains Autonomous System External Link State Advertisements (ASE LSAs).

Only one page is displayed at a time (maximum 24 lines).Re-type the command to display next part of external link advertisements.

If you type the command with new parameters, new information will be displayed, starting from first page.

To always break printing continuation of links use FIRST option.

Syntax: **OSPF SHOW EXTLSDB [LS_ID ls_id] [ADV_RTR adv_rtr] [DETAILED]**

Syntax: **OSPF SHOW EXTLSDB [DETAILED]**

Parameter	Description
ls_id	Link State identifier of LSAs.
adv_rtr	Router ID of the router which originated LSAs.

Display Field	Description
Type	This is the type of LSA.
LS ID	The Link State identifier of the network (here, the destination network's IP address). When this parameter is specified, the command displays only the matching entries.
Adv Rtr	This is the Router ID of the originating router. When this parameter is specified, the command displays only the matching entries.
Age	This is the age of the LSA (seconds since the LSA was originated).
Cksum hex	This is the checksum of the LSA, not including the age field.
Seq hex	This is the sequence number of the LSA.

(fields below are displayed with DETAILED parameter)	
LS type	This is the type of LSA.
LS ID	This is the Link State identifier (here, the destination network's IP address).
Adv rtr	This is the Router ID of the originating router.
Age	This is the age of the LSA in seconds.

Len	This is the length in bytes of the LSA including the 20 byte LSA header.
Seq #	This is the sequence number of the LSA in hex.
Checksum	This is the checksum of the LSA, not including the age field.
Options	This is a bit pattern that indicates the optional capabilities supported by the described portion of the routing domain.
Net mask	This is the network mask for the network being advertised.
Tos	Currently not used.
metric	This is the cost of the route.
External type	This determines how the cost stored in the routing table will be calculated. 1 indicates that the intra route cost will be added to the external route cost. 2 indicates that only the external route cost is stored.
Forwarding address	This is the address of the network link through which the external link is accessed. If 0.0.0.0 is entered, the external link will be reached through the router which originated the advertisement.
Tag	Currently not used.

Example (when DETAILED is not specified)

```
OSPF SHOW EXTLSDB
 Type    LS ID      Adv Rtr    Age    Cksum hex   Seq hex
 ASE     1.0.0.0    10.0.0.0   41     42c2        80000001
 ASE     2.0.0.0    10.0.0.0   11     c770        80000001
```

Example (when DETAILED is specified)

```
OSPF SHOW EXTLSDB DETAILED
LS type: ASE  LS ID:  123.123.0.0  Adv rtr:  33.0.0.0  Age:  5
                Len: 36  Seq #:  8000000b  Checksum:  0x50c  Options:  0
                Net mask:  255.255.0.0  Tos  0  Metric:  64   External type: 1
                Forwarding Address  128.199.199.1  Tag:  d0000000
```

OSPF SHOW RANGES

This command displays the configured net ranges for a router's attached areas.

Syntax: **OSPF SHOW RANGES**

Display Field	Description
Area ID	This is the area identifier in which the net range is found.
Type	This is the net range type. The possible values are: *SUM* or *NSSA*.
Net	This is the IP address of the subnet.
Mask	This is the IP mask associated with the IP address.
Status	This indicates whether network information is advertised between areas. *Advertise* means that it is advertised; *Hide* means that it is not advertised.

Example:

OSPF SHOW RANGES

Area ID	Type	Net	Mask	Status
0.0.0.2	SUM	128.200.0.0	255.255.0.0	Advertise

OSPF SHOW HOSTS

This command displays information and metrics for hosts directly attached to the router.

Syntax: **OSPF SHOW HOSTS**

Display Field	Description
Area ID	This is the area identifier in which the host is found.
Address	This is the IP address of the host.
TOS	This is the type of service associated with this metric.
Cost	This is the metric value.

Example:

OSPF SHOW HOSTS

Area ID	Address	TOS	Cost
0.0.0.0	128.101.2.199	0	11
0.0.0.0	128.101.2.200	0	200

OSPF SHOW IMPORT

This command displays the router's import policy. By default, all static routers are not learned by the OSPF process.

Syntax: **OSPF SHOW IMPORT**

Display Field	Description
Net	This is the IP network.
Mask	This is the mask associated with the network.
Preference	This is the preference for imported route.

Example:

OSPF SHOW IMPORT

```
 Net            Mask            Preference
 1.0.0.0        255.0.0.0       90
```

OSPF SHOW EXPORT

This command displays the router's export policy.

Syntax: **OSPF SHOW EXPORT**

Display Field	Description
Protocol	This is the origin of the route.

Specific 1 and Specific 2 are dependent on the protocol. These fields have the following meaning:

Specific 1	REMOTE Preference IP address. RIP IP address of interface.
Specific 2	REMOTE IP Mask. RIP Next hop IP address.
Net	This is the network number.
FB	The first character of this flag is *E* if the route is exported and *B* is the export is blocked. The second character displays policy key bits in hex.
Metric	This is the metric associated with the route. If the original metric is used, protocol will be displayed.
Tag	This is the tag used in OSPF LSAs when advertising the route. If there is no tag, *NONE* will be displayed and if the tag is an AS id, *AS* will be displayed.

Example:

OSPF SHOW EXPORT

Protocol	Specific 1	Specific 2	Net	FB	Metric	Tag
REMOTE	0.0.0.90	255.0.0.0	1.0.0.0	Ef	protocol	0x00000000

OSPF SHOW STUBAREAS

This command displays metrics that are advertised by a default Area Border Router into a stub area.

Syntax: **OSPF SHOW STUBAREAS**

Display Field	Description
Area ID	This is the area identifier.
Metric Type	This is the metric type. The possible types are *OSPF, Type 1* or *Type 2*.
Metric	This is the metric value.
TOS	This is the type of service associated with the metric.

Example:

OSPF SHOW STUBAREAS

Area ID	Metric Type	Metric	TOS
1.0.0.0	OSPF	123	0

OSPF SHOW METRICS

This command displays metrics for all the router's interfaces.

Syntax: **OSPF SHOW METRICS**

Display Field	Description
IP Address	This is the IP address of this interface.
Port	This is port or logical link associated with this interface. If the IP address is 0.0.0.0, the port is the index number of the interface. If the IP address is not 0.0.0.0, the port is not available.
TOS	This is the type of service associated with this metric.
Metric	This is the value of the metric.

Example:

OSPF SHOW METRICS

IP Address	Port	TOS	Metric
0.0.0.0	LL0	0	0
0.0.0.0	LL1	0	0
128.101.3.156	n/a	0	1

OSPF TRACE

This command sets tracing dup entries that were not inserted.

Syntax: **OSPF TRACE intf <intf_number> que 2**

To enable tracing use OSPF TRACE ENABLE on page 447.

OSPF TRACE ENABLE

This command enables OSPF tracing.

Syntax: **OSPF TRACE ENABLE**

24. PCMCIA Modem Commands

PCMCIA HELP

This command displays available PCMCIA commands. It can be used on XLA routers with PCMCIA interface.

Syntax: **PCMCIA HELP**

PCMCIA RESET

This command performs a master reset on the PCMCIA modem. This command cannot be entered when the modem is active (that is, when a connection is established). You must stop the interface first.

Syntax: **PCMCIA RESET**

PCMCIA WAN

This command sets the PCMCIA modem to be a WAN interface.

Syntax: **PCMCIA WAN**

PCMCIA CONSOLE

This command sets the PCMCIA modem to be a console. You cannot change the modem into a console if the PCMCIA is working as a WAN interface and is not stopped

Syntax: **PCMCIA CONSOLE**

25. PIR Commands

SET BRIDGE MODE

This command is used to select one of the Protocol Independent Routing modes.

Syntax: **SET BRIDGE MODE {DSPF/T | DSPF/SR | DSPF/SRT}**

Parameter	Description
DSPF/T	When DSPF/Transparent mode is selected, a Olicom router does not process, modify, or interpret the Routing Information Field. All user data messages are transmitted transparently through the PIR network, regardless of whether they contain Source Routing information or not.
DSPF/SR	When DSPF/Source Routing is selected, only Source Routing frames are forwarded by the Olicom router. Non–Source Routing frames are filtered. The entire PIR cloud is a virtual segment and a single hop in the RIF.
DSPF/SRT	When DSPF/Source Routing Transparent is selected, source routed frames are forwarded as described in DSPF/SR mode and non–Source Routed frames are forwarded transparently.

SET PORT PIR CONNECT and SET PORT PIR NOTCONNECT

This command allows you to define the LAN connected to a router running PIR. If more than one router running PIR is connected to the LAN, the PIR status of all of them must be set to `Connect' for all relevant ports.

Syntax: **SET PORT n PIR [CONNECT | NOTCONNECT}**

Parameter	Description
n	the port number.
CONNECT	Connect should be selected if more than one router running PIR is connected to the LAN.
NOTCONNECT	When NOTCONNECT is selected, the sending of router service messages to the port is inhibited.

SET PORT PIR DBKP and SET PORT PIR NODBKP

This command allows you to define the Dial Backup connected to a router running PIR. Both sides of Dial Backup must set this flag.

Syntax: **SET PORT n PIR {DBKP | NODBKP}**

Parameter	Description
n	the WAN port number.
DBKP	It should be selected if the WAN port is a Dial Backup.
NODBKP	NODBKP informs PIR that this port is not a Dial Backup port.

SET PIR RUNNING and SET PIR STOPPED

This command enables and disables the DSPF algorithm.

Syntax: **SET PIR {RUNNING | STOPPED}**

Parameter	Description
RUNNING	Running enables the DSPF algorithm.
STOPPED	Stopped disables the DSPF algorithm.

SET PIR GROUPID

This command is used to set the LAN Segment Group ID used for the virtual segment. This value is used in DSPF/SR and DSPF/SRT modes, and must be unique across the entire network.

Syntax: **SET PIR GROUPID x**

Parameter	Description
x	The Group SR ID is a hexadecimal value in the range from 0x0 to 0xFFF. The default value is 0xFFF.

SET PIR UPDATE

This command is used to set a value for the Routing Update Interval parameter. The frequency of routing updates is used to measure delay through the network.

Syntax: **SET PIR UPDATE value**

Parameter	Description
value	The routing update interval is in the range from 1 to 60 seconds. The default value is 18 seconds. The value must be the same on all Olicom routers in the network running PIR.

SET PIR RECOVERY

This command is used to set a value for the Recovery Update Interval parameter. After detection of an interface failure, if the failed link is part of the path to some destination segment, a router running PIR will initiate an extra routing update process. The parameter defines the settling time for this update before traffic can be routed over the new path.

Syntax: **SET PIR RECOVERY value**

Parameter	Description
value	The recovery update interval is in the range from 1 to 19 seconds. The default value is 2 seconds. The value must be the same on all Olicom routers in the network running PIR.

SET PIR AGING

This command is used to set a value for the Address Aging Timer parameter. PIR associates a LAN segment number with every MAC address. Once this association is made, it will not be changed even if a packet is received that indicates that the station is no longer on the segment. If, however, a message is not received from the workstation (on the associated segment) within the time specified by the Address Aging Timer, the segment association will be considered to be stale and a new segment can then be associated with the MAC address.

Syntax: **SET PIR AGING value**

Parameter	Description
value	The Address Aging Timer value is in the range from 30 to 255 seconds. The default value is 180 seconds.

SET PIR SEQUENCE

This command is used to set a value for the Sequence Time parameter.
The Sequence Time is the maximum interval between packets. As long as the time between packets does not exceed the specified Sequence Time, the packets will be routed along the same path, thereby assuring correct sequencing of packets. This command applies to ILAN only.

Syntax: **SET PIR SEQUENCE value**

Parameter	Description
value	The Sequence Time is in the range from 100 to 1499 msecs. The default value is 150 msecs.

SET PIR MINMETRIC

This command is used to set a value for the Minimum Metric for a WAN Line. This value is not added to the delay (metric) value. It is a minimum, meaning that the metric calculation cannot fall below this value.

Syntax: **SET PIR MINMETRIC value**

Parameter	Description
value	The Minimum WAN Metric is in the range from 0 to 99 metric units. The default value is 5 metric units.

SET PIR THRESHOLD

This command is used to set a value for the Metric Threshold parameter.
The Metric Threshold is implemented to adjust the sensitivity level during routing changes. A path change is avoided if the delay difference between the new and old paths does not exceed the Metric Threshold. This command applies to ILAN only.

Syntax: **SET PIR THRESHOLD value**

Parameter	Description
value	The Metric Threshold is in the range from 0 to 999 metric units. The default value is 4 metric units.

SET PIR CORRELATION

This command is used to set a value for the Metric Correlation parameter. The Metric Correlation provides a smoothing effect on changes in the delay metric. This command applies to ILAN only.

Syntax: SET PIR CORRELATION value

Parameter	Description
value	The Metric Correlation is in the range from 0% to 99%. The default value is 0%.

SET PIR STRATEGY

This command allows you to choose additional options for PIR.

Syntax: SET PIR STRATEGY n

Parameter	Description
n	is a value defining the Metric Strategy which represents an option or combination of options listed below. We recommend that, whenever possible, you use 56 (the default) or 60.

a. Treat bus as WAN (1).
b. Enhanced filtering for Token Ring frames (2).
c. Support duplicate physical addresses (4).
d. Service messages acknowledges (8).
e. Traffic delayed after tree reconfiguration (16).
f. Static paths (32).
g. Transmitting long packets over Ethernet (64).
h. Compound service messages (128).
i. Enhanced analysis of LNM frames (256).
j. Disable FAST RESET algorithm (512).

The numbers in brackets are the bit's values matching proper strategic. The Metric Strategy is the option or the sum of the options listed above.

The default strategy (56) is: *Service messages acknowledges* (8) + *Traffic delayed after tree reconfiguration* (16) + *Static paths* (32).

SHOW PIR SEGMENTS

This command allows you to view the contents the PIR routing table for a specified tree.

Syntax: **SHOW PIR SEGS [n]**

or

Syntax: **SHOW PIR SEGMENTS [n]**

or

Syntax: **SHSEGS [n]**

for an ILAN

Parameter	Description
n	is the tree number. If the tree number is not entered, all table entries for the current active tree are displayed.

SHOW PIR NEIGHBORS

This command allows you to view the contents of a PIR neighbor table for a specified tree.

Syntax: **SHOW PIR NEIGHBORS [n]**

Parameter	Description
n	is the tree number. If the tree number is not entered, all table entries for the current active tree are displayed.

SHOW PIR MONITORS

This command allows you to view the MAC and(or) IP addresses of DSPF Monitors known by PIR (currently active in the network).

Syntax: **SHOW PIR MONITORS**

26. PPP Commands

SET INTERFACE PPP

This command enables PPP on a specified interface.

Syntax: **SET INTERFACE n PPP**

Parameter	Description
n	The interface number.

PPP MAGIC

This command enables/disables the magic number negotiation ability of the specified device.

Syntax: **PPP n MAGIC {ENABLE | DISABLE}**

Parameter	Description
n	The interface number.
Enable	The local node will attempt to perform magic number negotiation with the remote node.
Disable	No magic number negotiation will be attempted by the local node.

Setting the MRU

This command sets the initial maximum receive unit (MRU).

Syntax: **PPP n MRU number**

Parameter	Description
n	The interface number.
number	The value of the MRU that the local PPP entity will advertise to the remote entity. The value range is from 1500 to 1900 bytes. The default value is 0. If the MRU is not negotiated a default value of 1500 is taken.

PPP IPCP

This command enables/disables the Internet Protocol Control Protocol (IPCP) negotiation ability of the specified device.

Syntax: PPP n IPCP {ENABLE | DISABLE}

Parameter	Description
n	The interface number.
ENABLE	Enables IPCP negotiation on the indicated device.
DISABLE	Disables IPCP negotiation on the indicated device.

PPP IPCP COMPRESSION

This command sets the initial type of Transmission Control Protocol (TCP) compression.

Syntax: PPP n IPCP COMPRESSION {NONE | VJ-TCP}

Parameter	Description
n	The number of the interface on which you want to set the TCP compression type.
NONE	Indicates that the local node will not attempt to negotiate any IP Compression options.
VJ-TCP	Indicates that the local node will attempt to negotiate the Van Jacobson TCP/IP (VJ-TCP) compression mode.

PPP SHOW STAT

This command displays the PPP statistics for a specified interface.

Syntax: PPP n SHOW STAT

Parameter	Description
n	The number of the interface whose statistics you want to display.

PPP SHOW INIT

This command displays the PPP initial options for a specified interface.

Syntax: **PPP n SHOW INIT**

Parameter	Description
n	The number of the interface whose initial options you want to display.

PPP SHOW NEG

This command displays the PPP negotiated options.

Syntax: **PPP n SHOW NEG**

Parameter	Description
n	The number of the interface whose negotiated options you want to display.

27. Parallel Port Commands

Abbreviations

PP = parallel port

PPM = parallel port member

Related commands: BonD Console Commands on page 122.

PP CREATE

This command creates a parallel port without member ports. The new parallel port will be invisible to all applications (including ClearSight) until you add at least one member port to it.

Syntax: **PP CREATE**

To add member ports to it, use PP pp ATTACH ppm prot on page 460.

To reverse this command, use PP DELETE pp on page 458.

PP DELETE

This command deletes a specified parallel port and makes all of its member ports available to applications again.

Syntax: **PP DELETE pp**

Parameter	Description
pp	The number of the parallel port you want to delete.

PP SHP

To list all parallel ports in the module, use:

Syntax: **PP SHP**

To see information about just one parallel port, use the number of the parallel port:

Syntax: **PP SHP pp**

Parameter	Description
pp	The number of the parallel port you want to delete. If you do not use this parameter, all parallel ports will be listed.

Example 1

```
ILAN/XL(1)>pp shp
Total number Parallel Ports: 2
Port 18
                        Total Number of Members: 1
                          Parallel Port Members:
                                   Port 3 - BRG
Port 19
                        Total Number of Members: 1
                          Parallel Port Members:
                                   Port 2 - BRG
```

Example 2

```
ILAN/XL(1)>pp shp 19
Port 19
                        Total Number of Members: 1
                          Parallel Port Members:
                                   Port 2 - BRG
```

PP ATTACH

This command attaches a port to the parallel port and specifies what protocols will be forwarded on it.

Syntax: **PP pp ATTACH ppm prot**

Check your work with PP SHP on page 459.

To reverse this command, use PP pp DETACH ppm on page 461.

Parameter	Description
pp	The number of the parallel port to which you want to attach a member port.
ppm	The number of the port you want to attach to parallel port pp.
prot	The protocols that should be forwarded on this port. Possible prot values: BRG to forward Bridge packets on this member port. IP to forward IP packets on this member port. IPX to forward IPX packets on this member port. ALL to forward all available protocol types on this member port. This is the same as specifying a prot of IP IPX BRG.

Example 1

```
ILAN/XL(1)>pp 19 attach 2 ip ipx
 Parallel Port: port 2 successfully attach to Parallel Port 19
ILAN/XL(1)>
```

(makes port 2 a member of parallel port 19 and specifies that this member will forward both IP and IPX packets.)

Example 2

```
ILAN/XL(1)>pp 19 attach 2 all
 Parallel Port: port 2 successfully attach to Parallel Port 19
ILAN/XL(1)>
```

(makes port 2 a member of parallel port 19 and specifies that this member will forward all available types of packets.)

PP DETACH

This command detaches a member port from a parallel port, thus returning the member port to normal use and making it directly available to applications.

Syntax: **PP pp DETACH ppm**

Check your work with PP SHP on page 459.

To reverse this command, use PP pp ATTACH ppm prot on page 460.

Parameter	Description
pp	The number of the parallel port from which you want to detach a member port.
ppm	The number of the parallel port member you want to detach from parallel port pp.

Example

ILAN/XL(1)>pp 19 detach 2
(removes member port 2 from parallel port 19.)

PP BRGSPLIT

This command specifies the traffic splitting mode for bridged traffic on a parallel port. Only one mode can be specified.

Syntax: **PP pp BRGSPLIT {DA | SA | BL}**

Parameter	Description
pp	The number of the parallel port for which you want to specify the traffic splitting mode for bridged traffic.
DA	This distribution is safe for SNA and NetBIOS because it does not changed the order of packets. The low-order four bits of the destination address of each message are used as an index into a table of parallel port members. Destination MAC address distribution is most useful when forwarding from one or more LANs with few end stations to one or more LANs with many end stations.
SA	This distribution is safe for SNA and NetBIOS because it does not changed the order of packets. The low-order four bits of the source address of each message are used as an index into a table of parallel port members assigned to the Bridge protocol. Source MAC address distribution is most useful when forwarding from one or more LANs with many end stations to one or more LANs with few end stations.
BL	This distribution is *not* safe for SNA and NetBIOS because it may change the order of packets. Use it only for the IP and IPX routing. (Balance Load can be used for SNA when DLSw is applied.) This traffic splitting procedure tracks the load and line speed of each parallel port member within a PP. When there is a packet to transmit, it is sent on the parallel port member with the shortest delay.

If there is congestion on the parallel port member with the shortest delay, the packet is sent on the first active parallel port member assigned to current protocol.

If a parallel port member becomes inactive, its traffic is distributed on the rest of the parallel port members.

Use shorter packets to take greater control of latency and to make smarter use of bandwidth. To control IP and IPX packet sizes, set the MTU on the PP. For the Bridge protocol, you can control the packet size only for SR Bridge (globally for all ports on module).

Example

ILAN/XL(1)>PP 19 BRGSPLIT DA
(specifies the Destination Address traffic splitting mode for bridged traffic on parallel port 19.)

28. Proprietary CHAP Commands

Console commands for the proprietary Challenge Authentication Protocol (CHAP).

Note: Proprietary CHAP does not work on ports with disabled IP router.

CHAP HOSTNAME

Sets the name of the host device.

Syntax: **CHAP HOSTNAME <hostname>**

Parameter	Description
hostname	Device's name (ASCII character string). Delimit these strings with white space or quotes (single or double). The delimiter characters can themselves be used within a secret if, on the command line, each is preceded by a backslash (\) character as shown in the examples below. The asterisk symbol (*) is a reserved character and cannot be used within secrets or names.

Examples

CHAP HOSTNAME Jane1290Lucy
(The hostname is set to **Jane1290Lucy**.)

CHAP HOSTNAME "Bobo was mine"
(The hostname is set to **Bobo was mine**. The string is preceded by a double quote, so all text until the next double quote, including the spaces, is taken as part of the secret string.)

CHAP HOSTNAME "Tom\"Mary 86"
(The hostname is set to **Tom"Mary 86**. A double quote usually marks the beginning or end of a secret string but, because the backslash indicates that you want to use the next character literally and not as a delimiter, the double quote between Tom and Mary becomes part of the secret string.)

CHAP SHOW

Displays the hostname of the device and all pairs of hosts which have secrets.

Syntax: **CHAP SHOW**

CHAP p SHOW

Displays all CHAP settings for the specified port.

Syntax: **CHAP p SHOW**

Parameter	Description
p	The number of the port to which this command applies.

CHAP p AUTH

Sets to on or off (toggles) CHAP authentication on this port. By default, authentication is disabled. You can check the current setting with the **CHAP p SHOW** command.

Syntax: **CHAP p AUTH**

Parameter	Description
p	Number of the port to which this command applies.

CHAP p RETRY retries

Sets the number of challenge retries sent before giving up and closing the link.

Syntax: **CHAP p RETRY retries**

Parameter	Description
p	Number of the port to which this command applies.
r	Number of challenge retries to make before giving up and closing the link. Default: 5 Range: 0..19

CHAP p RECHAL

Sets the number of seconds to wait before rechallenging a peer.

Syntax: **CHAP p RECHAL s**

Parameter	Description
p	Number of the port to which this command applies.
s	Seconds to wait before rechallenging. Default: 0 (rechallenge disabled)

CHAP p RESTART

Sets the number of seconds to wait before the specified port is restarted after a failed authentication. If this is set to 0, the link will restart only with operator intervention.

Syntax: **CHAP p RESTART s**

Parameter	Description
p	Number of the port to which this command applies.
s	Seconds before restarting the port. Default: 30 Range: 0..30000, where 0 disables auto-restart

CHAP ADD

Adds a secret between the specified pair of hosts. Note the optional use of an asterisk as a wildcard to indicate “all authenticators” or “all peers”.

Syntax: **CHAP ADD <client/peer> <server/authenticator> <secret>**

Parameter	Description
client/peer	The peer hostname (set with CHAP HOSTNAME). Using an asterisk here will add the specified secret string to all specified peers. Delimit these strings with white space or quotes (single or double). The delimiter characters can also be used within a secret if each is preceded by a backslash (\) character as shown in the examples below. The asterisk symbol (*) is a reserved character and cannot be used within secrets or names. Length: 1..50 ASCII characters
server/authenticator	The authenticator’s hostname. Using an asterisk here will add the specified secret string to all authenticators. Length: 1..50 ASCII characters
secret	The secret string to associate with the specified pair of hosts. Delimit these strings with white space or quotes (single or double). The delimiter characters can also be used within a secret if each is preceded by a backslash (\) character as shown in the examples below. The asterisk symbol (*) is a reserved character and cannot be used within secrets or names. Length: 1..50 ASCII characters; we recommend that you use an unpredictable string of at least 16 characters.

Example

CHAP ADD Carrie Ben “AR12BR23 5 6 ALA”
(Adds secret **AR12BR23 5 6 ALA** between peer Carrie and authenticator Ben.)

CHAP ADD Carrie * “AR74KL35 8 6 MOPS”
(Adds secret **AR74KL35 8 6 MOPS** between peer Carrie and all authenticators.)

CHAP ADD * * “75 BA 5 62 LON 94”
(Adds secret **75 BA 5 62 LON 94** between all peers and all authenticators.)

CHAP DEL

Deletes the secret between the specified pair of hosts (peer and authenticator). Note the optional use of an asterisk as a wildcard to indicate “all authenticators” or “all peers”.

Syntax: CHAP DEL <client/peer> <server/authenticator>

Parameter	Description
client/peer	The peer hostname. Using an asterisk here will add the specified secret string to all peers. Length: 1..50 ASCII characters
server/authenticator	The authenticator hostname. Using an asterisk here will add the specified secret string to all authenticators. Length: 1..50 ASCII characters

Examples

CHAP DEL Bambo Telly
(Deletes the secret between peer Bambo and the authenticator Telly. When you delete secrets, you don’t need to specify the secret strings themselves because there is only one secret between any two hosts. You just have to make clear which hosts you have on mind.)

CHAP DEL Bambo *
(Deletes the secrets between peer Bambo and all the authenticators.)

CHAP DEL * *
(Deletes the secrets between all peers and all the authenticators.)

29. SLCS Commands

SHOW SLCS SESS

The following command displays information about all defined SLCS sessions, including local and remote MAC addresses and SAPs, and SDLC addresses.

Syntax: **SHOW SLCS SESS (or SHSS)**

SET SLCS UP and SET SLCS DOWN

The following command starts and stops the SLCS subsystem.

Syntax: **SET SLCS {UP | DOWN}**

SHOW SLCS session_id

This command is used to display the LLC/SDLC parameter settings for a SLCS session.

Syntax: **SHOW SLCS {Sess_Id} {Parameters}**

Variation	Description

SHOW SLCS sess_id ALL
Displays the values of all parameters for the specified session.

SHOW SLCS sess_id ACC_TYPE
Displays the type of session (0–Ethernet, 2– Token Ring, 5 – SDLC).

SHOW SLCS sess_id DEVI_MAC
Displays the MAC address of the session partner.

SHOW SLCS sess_id DEVI_SAP
Displays the SAP of the session partner.

SHOW SLCS sess_id SLCS_MAC
Displays the MAC address of SLCS.

SHOW SLCS sess_id SLCS_SAP
Displays the SAP of SLCS.

SHOW SLCS sess_id NODE_ID
Displays the Node ID of the secondary station (IDBLK & IDNUM).

SHOW SLCS sess_id SDLC_ADDR
Displays the SDLC address.

SHOW SLCS sess_id SDLC_PORT
Displays the SDLC port number (ILAN SDLC Port #: 0,1,2,3,4 etc.).

SHOW SLCS sess_id SDLC_ROLE
Displays the SDLC role (1 - primary, 2- secondary. The next two are only valid for PU 2.1 sessions: 3 - negotiable, 7 - negotiable/no broadcast).

SHOW SLCS sess_id NET_ID
Optional - valid for PU 2.1 sessions. Displays the network name of a defined SNA device on SDLC. NET ID has up to eight characters and includes a country code, an enterprise code and a network suffix. NET IDs should be registered at IBM to ensure uniqueness. The NET ID is used with the CP Name (Control Point Name) to uniquely identify an SNA session.

SHOW SLCS sess_id CP_NAME
Optional - valid for PU 2.1 session. It displays the CP Name of an SNA device on SDLC. The CP Name is used with the NET ID to uniquely name an SNA device.

SHOW SLCS sess_id T1_REPLY
Displays the T1 Reply timer (in 1/10 seconds).

SHOW SLCS sess_id TI_INACT
Displays the Ti Inactivity timer (in 1/10 seconds).

SHOW SLCS sess_id T2_RECV
Displays the T2 Receiver Acknowledgment (in 1/10 seconds).

SHOW SLCS sess_id N2_TRANS
Displays the N2 Maximum of Retransmissions.

SHOW SLCS sess_id G_POLL
Displays the Group Poll Address.

SHOW SLCS sess_id BUFF_SIZE
Displays the buffer size.

SHOW SLCS sess_id WINDOW
Displays the window size.

SHOW SLCS sess_id SIDE_A_FIRST
Valid for PU 2.0 sessions. It displays which side is connected first (Side A or Side B).

SHOW SLCS sess_id DLC_STAT [1|23]
Show a session DLC-level statistics. If no more arguments are used, all statistics are displayed. Otherwise, portion 1, 2 or 3 of the statistics is made visible.

SHOW SLCS NULL_DLC_STAT [1|23]
Show a null-SAP session DLC-level statistics. If no more arguments are used, all statistics are displayed. Otherwise, portion 1, 2 or 3 of the statistics is made visible.

SET SLCS sess_id

The following command changes SLCS session parameters.

Note: Prior to changing any parameters, the SLCS session must be set to OFF. After the parameter(s) have been modified, the session can be set to ON.

Syntax: **SET SLCS sess_id <option>**

Option	Description
ON	This parameter starts the specified session.
OFF	This parameter stops the specified session.
XID3_BLOCK	This parameter blocks the sending of SDLC broadcast XIDs during session establishment after a cutoff of 12 XIDs is reached. Blocking broadcast XIDs prevents a broadcast storm.
XID3_NOTBLOCK	This parameter turns off the blocking of SDLC XIDs during session establishment. (It turns off the XID3_BLOCK command.)
DEL	This parameter deletes the specified session. The session must first be defined, stopped, or invalid.
PU21	This parameter puts the SLCS session into PU type 2.1 mode. In this mode, neither side is connected first: both sides wait for incoming connections and the SDLC role of the SDLC side (primary or secondary) is negotiated.
PU10	This parameter puts the SLCS session into PU type 1.0 mode. This mode is similar to PU 2.1 mode except the XID format differs. See the Olicom Reference Guide.
FORCE	This parameter causes an unconditional stop of the session, regardless of the type of the state of the session. It is an abnormal stop and all state variables are reset.
TR_RECON	This parameter sets the reconnect timer (in 1/10 seconds).

SET SLCS sess_id SIDE_A_FIRST

Valid only for PU 2.0 sessions. It connects either side A or side B first. In most cases, the downstream device from the SLCS ILAN should be connected first.

Syntax: **SET SLCS {Sess_Id} SIDE_A_FIRST {ON | OFF}**

SET SLCS session_id SIDE

The following command will allow you to define or modify one or more SLCS session parameters for either side (SDLC and/or LLC) of a SLCS session.

Syntax: SET SLCS session_id SIDE {A|B} <option>

Parameter	Description
A, B	This identifies the side of the session for which parameters are being defined

Option	Description

ACC_TYPE <type>
Sets the type of session (0–Ethernet, 2– Token Ring, 5 – SDLC).

DEVI_MAC <xxxxxxxxxxxx>
Sets the MAC address of the session partner.

DEVI_SAP <xx>
Sets the SAP of the session partner.

SLCS_MAC <xxxxxxxxxxxx>
Sets the MAC address of SLCS.

SLCS_SAP <xx>
Sets the SAP of SLCS.

NODE_ID <xxxxxxxx>
Sets the Node ID of the SLCS (IDBLK & IDNUM).

SDLC_ADDR <address>
Sets the SDLC address.

SDLC_PORT <port>
Sets the SDLC port number (ILAN SDLC Port #: 0,1,2,3,4 etc.).

SDLC_ROLE <role>
Sets the SDLC role (1– primary, 2 – secondary; There are two more parameters valid only for PU 2.1 sessions: 3- negotiable, 7- negotiable but no broadcast.).

NET_ID <xxxxxxxx>
This optional parameter is only valid for PU 2.1 sessions. It sets the eight character network name (the SNA Net ID) for the SDLC side of the session

CP_NAME <xxxxxxxx>
This optional parameter is only valid for PU 21. sessions. It sets the Control Point Name for the SDLC side of the session.

T1_REPLY <time>
Sets the T1 Reply timer (in 1/10 seconds).

TI_INACT <time>
Sets the Ti Inactivity timer (in seconds).

T2_RECV <time>
Sets the T2 Receiver Acknowledgment (in 1/10 seconds).

N2_TRANS <number>
Sets the N2 Maximum of Transmission.

G_POLL <address>
Sets the Group Poll Address.

BUFF_SIZE <size>
Sets the buffer size.

WINDOW <size>
Sets the window size.

TN_NONC <timer>
Sets the non-context timer (in seconds).

SHOW SLCS NV

The following command is used to display NetView session parameters.

Syntax: **SHOW SLCS NV**

SET SLCS NV

The following command defines or modifies NetView session parameters.

Note: When modifying or defining a NVW SLCS session, the NVW Session must first be set to OFF. In order to take effect after the changes are made, SLCS has to be cycled (set down and up again).

Syntax: **SET SLCS NV <option>**

Option	Description
SET SLCS NV ON	This option enables a NetView session.
SET SLCS NV OFF	This option disables a NetView session.
SET SLCS NV ACC_TYPE <d>	Sets the type of session (0–Ethernet, 2– Token Ring, 5 – SDLC).
SET SLCS NV HOST_MAC <xxxxxxxxxxxx>	Sets the MAC address of the Host.
SET SLCS NV HOST_SAP <xx>	Sets the SAP of Host.
SET SLCS NV SLCS_MAC <xxxxxxxxxxxx>	Sets the MAC address of SLCS.
SET SLCS NV SLCS_SAP <xx>	Sets the SAP of SLCS.
SET SLCS NV SLCS_ADDR <xx>	Sets the SDLC address.
SET SLCS NV SDLC_PORT <d>	Sets the SDLC port number.
SET SLCS NV RES_NAME <xxxx>	Sets the resource name.
SET SLCS NV NODE_ID <xxxxxxxx>	Sets the Node ID of the NetView Agent (IDBLK & IDNUM).

SHOW SLCS NV_DLC_STAT

This command shows NetView session DLC-level statistics. If no more arguments are used, all statistics are displayed. Otherwise, portion 1, 2, or 3 of the statistics is made visible.

Syntax: **SyntaxSHOW SLCS NV_DLC_STAT {1 | 2 3}**

SET SLCS BMA_LIMIT

The following command sets the memory limit (XL heap). XL heap can be allocated as buffer memory area and the limit becomes maximum value for the area. This command is available for XLP, and XLT/XLT-F QWAN.

Syntax: **SET SLCS BMA_LIMIT n**

Parameter	Description
n	Memory limit value. Range: 102400…8388608 bytes Default value: 716800 or 700 kB of heap

SHOW SLCS BMA_LIMIT

The following command displays the memory limit (XL heap). This command is available for XLP, and XLT/XLT-F QWAN.

Syntax: **SHOW SLCS BMA_LIMIT**

SET SLCS ILAN_COMPATIBLE {OFF | ON}

Sets the compatibility between the SLCS Token Ring Session traffic and SLCS on ILAN router.

Syntax: **SETSLCS ILAN_COMPATIBLE {OFF | ON}**

Option	Description
ON	SLCS is able to establish a session with the partner on ILAN router over WAN links.
OFF	SLCS Token Ring Session traffic over WAN links (CrossComm Point to Point, Frame Relay, X.25) is not compatible with SLCS on ILAN router. It is, however, faster than in previous XL versions due to eliminated CRC calculating. This option is a default.

SHOW SLCS ILAN_COMPATIBLE

Displays the compatibility (whether it is ON or OFF) between the SLCS Token Ring Session traffic and SLCS on ILAN router.

Syntax: **SHOW SLCS ILAN_COMPATIBLE**

SET SLCS TR_FORMAT {RING | INTERNAL}

The following command selects the format to be used in building SLCS frames.

Syntax: **SET SLCS TR_FORMAT {RING | INTERNAL}**

Option	Description
RING	SLCS builds ring frames in normal ring format. This option provides slightly faster service on Frame Relay links.
INTERNAL	SLCS builds Token Ring frames in Olicom internal format which is used on the WAN links and enables forwarding Ring frames over WAN without CRC field. This format may be used only between two XL routers. It is a default option.

SHOW SLCS TR_FORMAT

The following command displays the format to be used in building SLCS frames (RING or INTERNAL).

Syntax: **SHOW SLCS TR_FORMAT**

QSLCS ACP

This command is used to switch control between ACP 0 and ACP 1. When SLCS is on QWMA module, you can switch control only to ACP.

Syntax: **QSLCS ACP *n***

Parameter	Description
n	Possible values: 1 (switches control to ACP 0), 2 (switches control to ACP 1)

Example 1:

```
ILAN/XL(1)>qslcs acp n
ACP[n] is not supporting SLCS
```

Example 2:

```
ILAN/XL(1)>qslcs acp n
ACP[n] is now supporting SLCS
```

30.SMDS Commands

Address Formats

The SMDS architecture is designed with the following assumption:

Only one individual SMDS address exists on an interface, and therefore that only one port is related with one interface.

SMDS Addresses

To work with SMDS you have to know what address format to use. Olicom uses SMDS addresses in E.164 format (8 bytes - 16 digit). First digit is C (four bits 1100b 0xC) for an individual address (unicast), or E (four bits 1110b 0xE) for a group address (multicast).

Address Formats for Console Commands

SMDS Address - Console Format

Individual address (unicast):

CXXXXXXXXXXXXXXX

Example:

```
C4491810790031FF
```

Group address (multicast):

EXXXXXXXXXXXXXXX

Example:

```
E4491818998234FF
```

Digits X...X represent telephone number digits which are coded in BCD (Binary Coded Decimal) format. If you do not specify all 15 digits, the rest of the address is padded with F (1111b 0xF) digits.

IP Address - Console Format

SMDS console commands require IP addresses in the format:

XXX.XXX.XXX.XXX

where X is a decimal digit.

Example:

128.101.71.3

IPX Address - Console Format

SMDS console commands require IPX addresses in the format:

XXXXXXXX XXXXXXXXXXXX

where X is a hexadecimal digit.

Example:

A20 160098002345

An IPX has a net number (the first 8 digits) and a node number (the last 12 digits).

MAC Address - Console Format

SMDS console commands require MAC addresses in the format:

XX-XX-XX-XX-XX-XX

where X is a hexadecimal digit.

Example:

00-00-98-01-14-07

SET INTERFACE SMDS

This command sets an interface to SMDS mode.

Syntax: **SET INTERFACE x SMDS**

Parameter	Description
x	The number of the interface which you want to set to SMDS mode.

SET INTERFACE HBPERIOD

This command sets DXI Heartbeat Period on an interface.

Syntax: **SET INTERFACE x HBPERIOD = p**

Parameter	Description
x	The number of the interface on which you want to set DXI heartbeat period
p	The period between sending heartbeat frames. When a heartbeat period is set to 0 no heartbeat frames are sent. Range: 1 to 32,000 sec Default: 0

Heartbeat frames are used to determine whether the connection to the switch or DSU/CSU works correctly. The default value is 0, which disables the transmission of heartbeat frames. If heartbeat frames are necessary, the recommended period is 10 seconds.

SET INTERFACE HBTHRES

This command sets the DXI Heartbeat Threshold on an interface.

Syntax: **SET INTERFACE x HBTHRES = t**

Parameter	Description
x	The number of the interface on which you want to set DXI Heartbeat Threshold
t	The number of unacknowledged heartbeat frames, which determines the local disconnect state on the DXI interface

When a DXI interface is sending heartbeat frames, each of these frames must be acknowledged by the DSU/CSU or the switch. If the number of unacknowledged heartbeat frames is greater than the heartbeat threshold, the DXI interface enters the local disconnect state.

SMDS SET IA

This command sets the SMDS Individual Address on a port.

Syntax: **SMDS SET x IA c**

Parameter	Description
x	The number of the port on which you want to set SMDS Individual Address
c	The individual address

SMDS SET BRGA

This command sets the Bridge Group Address.

Syntax: **SMDS SET x BRGA e**

Parameter	Description
x	The number of the port on which you want to set the bridge group address
e	The bridge group address.

This group address creates a virtual LAN on SMDS. This is an SMDS group address, so it must start with hexadecimal digit E in conformance with the CCITT E.164 numbering format.

Bridging is always enabled on SMDS so this address must always be set.

SMDS SET SRBRTIMEOUT

This command sets the SR Bridge Timeout.

Syntax: **SMDS SET x SRBRTIMEOUT e**

Parameter	Description
x	The number of the port on which you want to set the SR bridge timeout
e	The SR bridge timeout value.This is the amount of time after which the entry in the SR Bridge address resolution cache is removed.

SMDS SET IPLISGA and SMDS SET IPARPRA

This command sets the SMDS Group Address (LIS_GA) that identifies a member of a logical IP subnetwork.

Syntax: **SMDS SET x IPLISGA e**

This command sets the SMDS ARP Request Address that represents address to which ARP requests are sent.

Syntax: **SMDS SET x IPARPRA e**

Parameter	Description
x	The number of the port.
e	The address.

These parameters are required only when IP routing is enabled on this port.

Note: In the current version of SMDS the address LIS_GA must be equal to SMDS ARP Request Address.

Configure SMDS for IPX Router

The following group addresses must be set for IPX router:

Address	Purpose
GLOBAL_GA	Allows ARP broadcasts within a multiprotocol Virtual Private Network (VPN). In IPX-only VPN: GLOBAL_GA = IPX_GA
IPX_GA	Allows IPX broadcasts within VPN.
IPX_ARP_GA	Allows dedicated ARP servers within a VPN. When no dedicated ARP servers are used, IPX_ARP_GA = GLOBAL_GA
IPX_NLSP_GA	Allows NLSP broadcasts within a VPN. Typically, IPX_NLSP_GA = IPX_GA
IPX_SAP_GA	Allows SAP broadcast. Permissible setting: IPX_SAP_GA = IPX_GA

Note: In the current version of SMDS all IPX group addresses must be equal (GLOBAL_GA = IPX_GA = IPX_ARP_GA = IPX_NLSP_GA = IPX_SAP_GA).

The following commands set these group addresses:

Syntax: SMDS SET x IPXGLGA e

Syntax: SMDS SET x IPXGA e

Syntax: SMDS SET x IPXARPGA e

Syntax: SMDS SET x IPXNLSPGA e

Syntax: SMDS SET x IPXSAPGA e

Parameter	Description
x	The number of the port on which you want to set parameters
e	The group address

The following command sets the ARP Time-out for IPX. This is the time after which the entry in the IPX address resolution cache is removed.

Syntax: SMDS SET x IPXTIMEOUT n

Parameter	Description
x	The number of the port on which you want to set Time-out
n	The age time (in seconds) Default:7200 seconds

These parameters are required only when IPX routing is enabled on the port.

SET INTERFACE NOSMDS

The following command disables SMDS on an interface.

Syntax: **SET INTERFACE x NOSMDS**

Parameter	Description
x	The number of the interface on which you want to disable SMDS.

HELP SMDS

The following command displays the console help where all SMDS commands are described.

Syntax: **HELP SMDS**

SMDS SHC

This command shows SMDS configuration on a port (individual address, group addresses, and IPX ARP time-out)

Syntax: **SMDS SHC x**

Parameter	Description
x	The port number.

SMDS SHSTAT

This command shows SMDS statistics on a port (SIP Level 3 statistics and DXI statistics)

Syntax: **SMDS SHSTAT x**

Parameter	Description
x	The port number.

SMDS SHARP

The following commands show all ARP tables on port (bridge, IP and IPX).

Syntax: **SMDS SHARP x**

Syntax: **orSMDS SHARP x all**

Parameter	Description
x	The port number

The ARP tables of IP and IPX are displayed only when these routers are enabled.

SMDS SHARP BRIDGE

The following command shows the address resolution table for a bridge:

Syntax: **SMDS SHARP x BRIDGE**

Parameter	Description
x	The port number for which you want to see the address resolution table for a bridge

SMDS SHARP SR

The following command shows the address resolution table for the SR bridge:

Syntax: **SMDS SHARP x SR**

Parameter	Description
x	The port number for which you want to see the address resolution table for the SR bridge

SMDS SHARP IP

The following command shows the address resolution table for an IP router:

Syntax: **SMDS SHARP x IP**

Parameter	Description
x	The port number for which you want to see the address resolution table for an IP router

SMDS SHARP IPX

The following command shows the address resolution table for an IPX router:

Syntax: **SMDS SHARP x IPX**

Parameter	Description
x	The port number for which you want to see the address resolution table for an IPX router

Note: Address resolution tables are located on QWMA adapter, while the “show” commands (SMDS SHARP...) display copies of these tables, which are located on ICP and updated every 20 seconds. With this update delay, it is therefore possible that the QWMA has an address in its table that the “show” command does not display until the end of the 20-second update cycle.

SMDS CLRARP

The following command removes all entries from all ARP cache tables (MAC, IP, IPX).

Syntax: **SMDS CLRARP x**

Parameter	Description
x	The port number on which you want to remove all entries from all ARP cache tables (MAC, IP, IPX)

SMDS IPCLR

The following commands enable you to remove a particular entry from an ARP table:

Syntax: **SMDS IPCLR x ip_adr**

Parameter	Description
x	The port number for which you want to remove one particular entry from an ARP table
ip_adr	The IP address to be removed from the IP ARP table

This command removes IP address *ip_adr* from the IP ARP table.

SMDS IPXCLR

The following command removes IPX address *ipx_net ipx_node* from the IPX ARP table.

Syntax: **SMDS IPXCLR x ipx_net ipx_node**

Parameter	Description
x	The port number for which you want to remove one particular entry from the ARP table
ipx_net	The IPX net number to be removed from the IPX ARP table
ipx_node	The IPX node number to be removed from the IPX ARP table

SMDS MACCLR

The following command removes MAC address *mac_adr* from the bridge address resolution table:

Syntax: **SMDS MACCLR x mac_adr**

Parameter	Description
x	The port number for which you want to remove one particular entry from the ARP table
mac_adr	The MAC address to be removed from the bridge address resolution table

SMDS SRCLR

The following command removes Route Descriptor *rd* from the SR bridge address resolution table:

Syntax: **SMDS SRCLR x rd**

Parameter	Description
x	The port number for which you want to remove one particular entry from the ARP table
rd	The Rout Descriptor to be removed from the SR bridge address resolution table

SMDS SRSET

The following command adds static Route Descriptor *rd* to the SR bridge address resolution table.

Syntax: **SMDS SRSET x smds_adr rd**

Parameter	Description
x	The port number on which you want to set static address
smds_adr	The SMDS address which must be related with Route Descriptor
rd	The Route Descriptor to be put into the SR bridge address resolution table

Note: Maximum 128 static entries for the entire module can be stored in a nonvolatile memory.

SMDS IPSET

The console commands below manually add entries to an address resolution table. Such entries are called static entries, and they are not removed by the aging process.

The following commands can be used to set static addresses.

Syntax: **SMDS IPSET x smds_adr ip_adr**

Parameter	Description
x	The port number on which you want to set static addresses
smds_adr	The SMDS address which must be related with an IP address
ip_adr	The IP address to be put into the IP ARP table

This command adds static IP address *ip_adr* to the IP ARP table on port *x* and relates it to SMDS address *smds_adr.*

Note: Maximum 128 static entries for the entire module can be stored in a nonvolatile memory.

SMDS IPXSET

The following command adds static IPX net and node *ipx_net ipx_node* to the IPX ARP table on port *x* and relates it to SMDS address *smds_adr.*

Syntax: **SMDS IPXSET x smds_adr ipx_net ipx_node**

Parameter	Description
x	The port number on which you want to set static addresses
smds_adr	The SMDS address which must be related with an IPX address
ipx_net	The IPX net number to be put into the IPX ARP table
ipx_node	The IPX node number to be put into the IPX ARP table

The pair *ipx_net* and *ipx_node* determines one particular entry in the IPX ARP table.

Note: Maximum 128 static entries for the entire module can be stored in a nonvolatile memory.

SMDS MACSET

The following command adds static MAC address *mac_adr* to the bridge address resolution table.

Syntax: **SMDS MACSET x smds_adr mac_adr**

Parameter	Description
x	The port number on which you want to set static addresses
smds_adr	The SMDS address which must be related with MAC address
mac_adr	The MAC address to be put into the bridge address resolution table

Note: Maximum 128 static entries for the entire module can be stored in a nonvolatile memory.

31. Session Capture Commands

SET SCAP {ENABLE | DISABLE}

This command enables and disables the Session Capture feature.

Syntax: **SET SCAP {ENABLE | DISABLE} [password]**

Field	Description
password	If the password has been set the user is required to enter the correct password. By default Session Capture is enabled and no password is set.

SET SCAP PASSWORD

This command sets the password for Session Capture protection.

Syntax: **SET SCAP PASSWORD [old password] [new password]**

Field	Description
old password	Specifying this field deletes the password protection.
new password	By default there is no password set. Specifying this field sets the password protection.

SHOW SCAP

This command displays information about the state of the Session Capture feature.

Syntax: **SHOW SCAP**

32. Standard CHAP over PPP commands

Standard CHAP over PPP uses the same Secret Database as the Proprietary CHAP. Only the port commands are different from the Proprietary CHAP console commands.

PPP p SHOW

Displays all PPP settings for the specified port.

Syntax: **PPP p SHOW**

Parameter	Description
p	The number of the port to which this command applies.

PPP p AUTH ACTAS PEER

Enables/disables acting as a peer on specified port. By default, acting as a peer is disabled and any authentication requests are rejected.

Syntax: **PPP p AUTH ACTAS PEER {ENABLE | DISABLE}**

Parameter	Description
p	Number of the port to which this command applies.

PPP p AUTH ACTAS AUTH

Enables/disables acting as an authenticator on specified port. By default, acting as an authenticator is disabled. We do not send any authentication requests

Syntax: **PPP p AUTH ACTAS AUTH {ENABLE|DISABLE}**

Parameter	Description
p	Number of the port to which this command applies.

PPP p AUTH CHAP

Enables/disables negotiation of CHAP protocol on specified port. By default negotiation of CHAP protocol is disabled

Syntax: **PPP p AUTH CHAP {ENABLE | DISABLE}**

Parameter	Description
p	Number of the port to which this command applies.

CHAP HOSTNAME

Sets the name of the host device.

Syntax: **CHAP HOSTNAME <hostname>**

Parameter	Description
hostname	Device’s name (ASCII character string). Delimit these strings with white space or quotes (single or double). The delimiter characters can themselves be used within a secret if, on the command line, each is preceded by a backslash (\) character as shown in the examples below. The asterisk symbol (*) is a reserved character and cannot be used within secrets or names.

Examples

CHAP HOSTNAME Jane1290Lucy
(The hostname is set to **Jane1290Lucy**.)

CHAP HOSTNAME “Bobo was mine”
(The hostname is set to **Bobo was mine**. The string is preceded by a double quote, so all text until the next double quote, including the spaces, is taken as part of the secret string.)

CHAP HOSTNAME “Tom\"Mary 86”
(The hostname is set to **Tom"Mary 86**. A double quote usually marks the beginning or end of a secret string but, because the backslash indicates that you want to use the next character literally and not as a delimiter, the double quote between Tom and Mary becomes part of the secret string.)

CHAP SHOW

Displays the hostname of the device and all pairs of hosts which have secrets.

Syntax: **CHAP SHOW**

CHAP p SHOW

Displays the state of CHAP on a specified port.

Note: This command additionally displays information about proprietary CHAP.

Syntax: **CHAP p SHOW**

Parameter	Description
p	The number of the port to which this command applies. Range: 0..19 Default: 0 (rechallenge disabled)

CHAP ADD

Adds a secret between the specified pair of hosts. Note the optional use of an asterisk as a wildcard to indicate “all authenticators” or “all peers”.

Syntax: **CHAP ADD <client/peer> <server/authenticator> <secret>**

Parameter	Description
client/peer	The peer hostname (set with CHAP HOSTNAME). Using an asterisk here will add the specified secret string to all specified peers. Delimit these strings with white space or quotes (single or double). The delimiter characters can also be used within a secret if each is preceded by a backslash (\) character as shown in the examples below. The asterisk symbol (*) is a reserved character and cannot be used within secrets or names. Length: 1..50 ASCII characters
server/authenticator	The authenticator’s hostname. Using an asterisk here will add the specified secret string to all authenticators. Length: 1..50 ASCII characters
secret	The secret string to associate with the specified pair of hosts. Delimit these strings with white space or quotes (single or double). The delimiter characters can also be used within a secret if each is preceded by a backslash (\) character as shown in the examples below. The asterisk symbol (*) is a reserved character and cannot be used within secrets or names. Length: 1..50 ASCII characters; we recommend that you use an unpredictable string of at least 16 characters.

Example

CHAP ADD Carrie Ben “AR12BR23 5 6 ALA”
(Adds secret **AR12BR23 5 6 ALA** between peer Carrie and authenticator Ben.)

CHAP ADD Carrie * “AR74KL35 8 6 MOPS”
(Adds secret **AR74KL35 8 6 MOPS** between peer Carrie and all authenticators.)

CHAP ADD * * “75 BA 5 62 LON 94”
(Adds secret **75 BA 5 62 LON 94** between all peers and all authenticators.)

CHAP DEL

Deletes the secret between the specified pair of hosts (peer and authenticator). Note the optional use of an asterisk as a wildcard to indicate “all authenticators” or “all peers”.

Syntax: **CHAP DEL <client/peer> <server/authenticator>**

Parameter	Description
client/peer	The peer hostname. Using an asterisk here will add the specified secret string to all peers. Length: 1..50 ASCII characters
server/authenticator	The authenticator hostname. Using an asterisk here will add the specified secret string to all authenticators. Length: 1..50 ASCII characters

Examples

CHAP DEL Bambo Telly
(Deletes the secret between peer Bambo and the authenticator Telly. When you delete secrets, you don’t need to specify the secret strings themselves because there is only one secret between any two hosts. You just have to make clear which hosts you have on mind.)

CHAP DEL Bambo *
(Deletes the secrets between peer Bambo and all the authenticators.)

CHAP DEL * *
(Deletes the secrets between all peers and all the authenticators.)

33. TCP Commands

HELP TCP

Use this command to display the list of available TCP commands.

Syntax: **HELP TCP**

TCP SHOW

Use this command to show TCP connections

Syntax: **TCP SHOW [n]**

Parameter	Description
n	The socket number

TCP STAT

Use this command to dump TCP statistics and display the summary of all TCBs.

Syntax: **TCP STAT**

TCP WINDOW

Use this command to set default window size.

Syntax: **TCP WINDOW n**

Parameter	Description
n	The window size value (in bytes)

TCP MSS

Use this command to set default maximum segment size (in bytes)

Syntax: **TCP MSS n**

Parameter	Description
n	The maximum segment size value (in bytes)

TCP DISC

Use this command to set the disconnect timeout for TCP connection.

Syntax: **TCP DISC n**

Parameter	Description
n	The disconnect timeout value (in seconds). Do not use this timer for n=0.

TCP IRTT

Use this command to set initial round trip time for new connections.

Syntax: **TCP IRTT n**

Parameter	Description
n	The round trip time (in milliseconds)

TCP SYNDATA {ENABLE | DISABLE}

Use this command to enable and disable TCP syn+data piggybacking.

Syntax: **TCP SYNDATA {ENABLE | DISABLE}**

TCP RTT

Use this command to set smoothed round trip time for specified socket.

Syntax: **TCP RTT m n**

Parameter	Description
n	The smoothed round trip time (in milliseconds)
m	The socket number

TCP SOCKCONN

Use this command to connect with remote port and IP address.

Syntax: **TCP SOCKCONN m n o [p]**

Parameter	Description
m	The remote port
n	The remote IP address
o	The local port
p	The local IP address

TCP SOCKLIS {SER | PAS}

Use this command to set ‘listen socket’ in server mode or passive mode.

Syntax: **TCP SOCKLIS {SER | PAS} m n o [p]**

Parameter	Description
SER	The server mode
PAS	The passive mode
m	The remote port
n	The remote IP address
o	The local port
p	The local IP address

TCP SOCKACCEPT

Use this command to accept TCP socket

Syntax: **TCP SOCKACCEPT n**

Parameter	Description
n	The socket number

TCP SOCKCLOSE

Use this command to close TCP socket in a ‘graceful’ way. Graceful close means that all the data in the outcoming packets queue will be sent before closing TCP connection. No new data is accepted during the closing process.

Syntax: **TCP SOCKCLOSE n**

Parameter	Description
n	The socket number

TCP SOCKSHUT

Use this command to ‘suddenly’ shut down TCP socket. Contrary to ‘graceful’ TCP close, shutting down results in losing the data contained in the outcoming packets queue.

Syntax: **TCP SOCKSHUT n {0|1|2}**

Parameter	Description
n	The socket number
0|1|2	0 - no more receives 1 - no more sends 2 - no more receives or sends. This is the default value, use it to hard reset TCP connection.

TCP SOCKSHOW

Use this command to display socket status

Syntax: **TCP SOCKSHOW**

TCP SOCKKICK

Use this command to enforce TCP retransmission

Syntax: **TCP SOCKKICK n**

Parameter	Description
n	The socket number

TCP MAX_RTO

Sets the maximum RTO (retransmission time-out) for the session. The time-out takes effect only after backoff parameter has reached its maximum value. Therefore, setting timeout alone may not result in decreased retransmission time.

Syntax: **TCP MAX_RTO n**

Parameter	Description
n	The RTO time in milliseconds. Range: MIN_RTO…120000. Default value: 120000

TCP MIN_RTO

Sets the minimum RTO (retransmission time-out) for the session.

Syntax: **TCP MIN_RTO n**

Parameter	Description
n	The RTO time in milliseconds. Range: 100…MAX_RTO. Default value: 500

TCP MAX_BACKOFF

Sets the maximum backoff value.

In TCP protocol *exponential backoff* parameter value increases after every retransmission. After the frame retransmission *backoff* is used to determine the time-out (the time-out for next retransmission enlarges in proportion to *backoff*). Therefore, by limiting this parameter, you can control TCP frames retransmission time.

Syntax: **TCP MAX_BACKOFF n**

Parameter	Description
n	The backoff value Range: 2…16 Default: 16

TCP BF_INC_TRSH

Sets the frequency of backoff increase. Note that increase of the backoff value causes increase in the time-out value for the retransmitted frame.

Syntax: **TCP BF_INC_TRSH n**

Parameter	Description
n	The frequency of backoff increase (it takes place every n-th retransmission) Range: 1…100 Default: 1

34. UNI Commands

Getting Started

The UNI commands are governed by the following

(Object) (Verb) (Locator) {Parameter} {Value}

Locators and parameters can include one or two words, separated by spaces.

1 The first word, or token, in a command line is the command object. The command object is a category of related commands. All UNI commands start with **UNI**. The Command Line User Interface (CLI) facilitates this by offering context sensitive help. At the CLI prompt, typing the command object followed by a question mark (?) generates a list of all the commands in the category.

2 The second token in the command line is a verb. It defines the action to be performed by the command. The allowable verbs are **SET**, **SHOW**, **ENABLE**, and **DISABLE**.

3 The third token in the command line is a locator. A locator further defines the object, specifying which interface, device, or other entity is to be acted upon. The allowable locators are:

SET	**SHOW**
QSAAL	ILMI
SWITCH	STATS
ROLE	
STATUS	
TIMER	
SIGNAL	
ILMI	
RETRY	
RESTART	
TX BUFF	
RX BUFF	
MAX	

4 The final tokens in the command line are parameters and values. Typing the parameter followed by a question mark (?) provides context sensitive help showing what value is expected.

The following example enables the UNI environment.

XL> UNI ENABLE SIGNAL

The UNI console commands are shown here in uppercase to improve readability, but you can enter any command in either uppercase or lowercase. The XL console accepts both as input.

Console Help

Type **HELP UNI** to view basic UNI help.

UNI Commands Roadmap

- UNI ENABLE {SIGNAL | ILMI | nothing implies both}
- UNI DISABLE {SIGNAL | ILMI | nothing implies both}
- UNI SET commands include:
- UNI SET QSAAL {PASSIVE | ACTIVE}
- UNI SET SWITCH {NNI | UNI 3.0 | UNI 3.1}
- UNI SET INTERFACE {USER | NETWORK}
- UNI SET TIMER {T303 | T308 | T310 | T313 | T316 | T316c | T322 | T309 | T398 | T399 | DISCONNECT | RECONNECT | UME_TOUT | POLL | KEEP ALIVE | NO RESP | CONTROL | IDLE} <value>
- UNI SET SIGNAL VPI <value>
- UNI SET SIGNAL VCI <value>
- UNI SET ILMI VPI <value>
- UNI SET ILMI VCI <value>
- UNI SET RETRY <value>
- UNI SET RESTART ENABLE
- UNI SET RESTART DISABLE
- UNI SET TX BUFF <value>
- UNI SET RX BUFF <value>
- UNI SET MAX STAT <value>
- UNI SET MAX CC <value>
- UNI SET MAX PD <value>
- UNI SHOW ILMI
- UNI SHOW STATS
- UNI SHOW STATUS
- UNI SHOW CONFIG [QSAAL | ILMI | SIGNAL]

UNI ENABLE

The UNI ENABLE command enables the UNI environment. By default, both Signaling and ILMI are enabled. You can specify only Signaling or ILMI.

Syntax: **UNI ENABLE {SIGNAL | ILMI | default}**

You must specify an interface number when using an XLX.

Examples:

XL(1)> UNI ENABLE
XL(1)> UNI ENABLE 1
(*Where* 1 is the interface number on the XLX.)

UNI DISABLE

The UNI DISABLE command disables the UNI environment. By default, both Signaling and ILMI are disabled. You can also specify only Signaling or ILMI.

Syntax: **UNI DISABLE {SIGNAL | ILMI | default}**

You must specify an interface number when using an XLX.

Examples:

XL(1)> UNI DISABLE
XL(1)> UNI DISABLE 1
(*Where* 1 is the interface number on the XLX.)

UNI SET QSAAL

The UNI SET QSAAL command actively establishes the SSCOP connection, or passively awaits the remote side of the connection to setup the connection.
The default value is active. The change does not take effect until the UNI is cycled.

Syntax: **UNI SET QSAAL {PASSIVE | ACTIVE}**

You must specify an interface number when using an XLX.

Examples:

XL(1)> UNI SET QSAAL ACTIVE
XL(1)> UNI SET QSAAL ACTIVE 1
(*Where*: 1 is the interface number on the XLX.)

UNI SET RX BUFF

The UNI SET RX BUFF command sets the number of buffers available for receiving Q.SAAL messages.

Syntax: **UNI SET RX BUFF <value>**

Parameter	Description
<value>	The number of receive buffers.

You must specify an interface number when using an XLX.

Examples:

XL(1)> UNI SET RX BUFF 24
XL(1)> UNI SET RX BUFF 1 24
(*Where*: 1 is the interface number on the XLX.)

UNI SET TX BUFF

The UNI SET TX BUFF command sets the number of buffers available for transmitting Q.SAAL messages.

Syntax: **UNI SET TX BUFF <value>**

Parameter	Description
<value>	The number of transmit buffers.

You must specify an interface number when using an XLX.

Examples:

XL(1)> UNI SET TX BUFF 24
XL(1)> UNI SET TX BUFF 1 24
(*Where* 1 is the interface number on the XLX.)

UNI SET SWITCH

The UNI SET SWITCH command sets the interface protocol version. Only UNI 3.0 and UNI 3.1 are valid on the XLT–F. All versions are valid on the XLX. The change does not take effect until the UNI is cycled.

Syntax: **UNI SET SWITCH {NNI | UNI 3.0 | UNI 3.1}**

You must specify an interface number when using an XLX.

Examples:

XL(1)> UNI SET SWITCH UNI 3.1
XL(1)> UNI SET SWITCH NNI 1
(*Where*: 1 is the interface number on the XLX.)

UNI SET INTERFACE

The UNI SET INTERFACE command enables the UNI interface, either User or Network, as described in the ATM Forum Specifications. The NETWORK option is allowed on both the XLT–F and the XLX. However on the XLT–F, it should only be used for testing purposes. The change does not take effect until UNI is cycled.

Syntax: **UNI SET INTERFACE {USER | NETWORK}**

You must specify an interface number when using an XLX.

Examples:

XL(1)> UNI SET INTERFACE USER
XL(1)> UNI SET INTERFACE USER 1
(*Where* 1 is the interface number on the XLX.)

UNI SET TIMER

Sets the following UNI timers: CONTROL, DISCONNECT, IDLE., KEEP ALIVE, NO RESP, POLL, RECONNECT, T303, T308, T309, T310, T313, T316, T316c, T322, T398, T399, UME_TOUT. Timers not documented below are documented in the ATM Forum UNI Specification. The UNI must be cycled before any new values are used. A zero value for any timer means it is disabled.

Syntax: **UNI SET TIMER timer_name i s**

Parameter	Description
timer_name	One of the timers as listed above
i	Interface number is required for an XLX only. Otherwise, do **not** use an interface number, and instead just enter UNI SET TIMER followed by the timer name and then by the number of seconds to set for that timer.
s	Number of seconds to set for the specified timer.

Timers	Description
DISCONNECT	Seconds (s) to wait before disconnecting from the Q.SAAL layer.
RECONNECT	Seconds (s) to wait before reattempting to connect to the Q.SAAL layer.
UME_TOUT	Seconds (s) to wait for ILMI messages.
POLL	Seconds (s) between Q.SAAL POLL messages with data waiting.
KEEP ALIVE	Seconds (s) between Q.SAAL POLL messages with no data.
CONTROL	Seconds (s) between sending BGN, END, or RS PDUs during an inactive state.
IDLE	SSCOP Idle Timer as defined for UNI 3.1.

Examples:

XL(1)> UNI SET TIMER RECONNECT 10
XL(1)> UNI SET TIMER RECONNECT 1 10

(*Where* 1 is the interface number on the XLX, and 10 sets the reconnect timer to 10 seconds.)

UNI SET SIGNAL VPI

The UNI SET SIGNAL VPI command configures the VPI used for the Signaling PVC. The UNI must be disabled before executing this command. The default value is 0.

Syntax: **UNI SET SIGNAL VPI <value>**

Parameter	Description
<value>	The VPI assigned to the Signaling PVC.

You must specify an interface number when using an XLX.

Examples:

XL(1)> UNI SET SIGNAL VPI 4
XL(1)> UNI SET SIGNAL VPI 1 4
(*Where*: 1 is the interface number on the XLX.)

UNI SET SIGNAL VCI

The UNI SET SIGNAL VCI command sets the VCI used for the Signaling PVC. The UNI must be disabled before executing this command. The default value is 5.

Syntax: **UNI SET SIGNAL VCI <value>**

Parameter	Description
<value>	The VCI assigned to the Signaling PVC.

You must specify an interface number when using an XLX.

Examples:

XL(1)> UNI SET SIGNAL VCI 45
XL(1)> UNI SET SIGNAL VPI 1 45
(Where 1 is the interface number on the XLX.)

UNI SET ILMI VPI

The UNI SET ILMI VPI command sets the VPI used for the ILMI PVC. The UNI Managed Entity (UME) must be disabled before executing this command.
The default value is 0.

Syntax: UNI SET ILMI VPI <value>

Parameter	Description
<value>	The VPI assigned to the ILMI PVC.

You must specify an interface number when using an XLX.

Examples:

XL(1)> UNI SET ILMI VPI 1
XL(1)> UNI SET ILMI VPI 1 1
(*Where* 1 is the interface number on the XLX.)

UNI SET ILMI VCI

The UNI SET ILMI VCI command sets the VCI used for the ILMI PVC. ILMI must be disabled before executing this command. The default value is 16.

Syntax: UNI SET ILMI VCI <value>

Parameter	Description
<value>	The VCI assigned to the ILMI PVC.

You must specify an interface number when using an XLX.

Examples:

XL(1)> UNI SET ILMI VCI 32
XL(1)> UNI SET ILMI VCI 1 32
(*Where* 1 is the interface number on the XLX.)

UNI SET RETRY

The UNI SET RETRY command sets the number of times the ILMI sends a message before declaring the link is down.

Syntax: **UNI SET RETRY <value>**

Parameter	Description
<value>	The number of ILMI retries.

You must specify an interface number when using an XLX.

Examples:

XL(1)> UNI SET RETRY 5
XL(1)> UNI SET RETRY 1 5
(*Where* 1 is the interface number on the XLX.)

UNI SET RESTART

The UNI SET RESTART command sets whether or not to send a RESTART message upon link startup.

Syntax: **UNI SET RESTART {ENABLE | DISABLE}**

You must specify an interface number when using an XLX.

Examples:

XL(1)> UNI SET RESTART ENABLE
XL(1)> UNI SET RESTART ENABLE 1
(*Where* 1 is the interface number on the XLX.)

UNI SET MAX STAT

The UNI SET MAX STAT command sets the maximum number of elements allowed in a SSCOP STAT message.

Syntax: **UNI SET MAX STAT <value>**

Parameter	Description
<value>	The number of elements in the STAT message.

You must specify an interface number when using an XLX.

Examples:

XL(1)> UNI SET MAX STAT 67
XL(1)> UNI SET MAX STAT 1 67
(*Where* 1 is the interface number on the XLX.)

UNI SET MAX CC

The UNI SET MAX CC command sets the upper limit for the SSCOP variable VT(CC).

Syntax: **UNI SET MAX CC <value>**

Parameter	Description
<value>	The limit of variable VT(CC).

You must specify an interface number when using an XLX.

Examples:

XL(1)> UNI SET MAX CC 4
XL(1)> UNI SET MAX CC 1 4
(*Where* 1 is the interface number on the XLX.)

UNI SET MAX PD

The UNI SET MAX PD command sets the upper limit for the SSCOP variable VT(PD).

Syntax: **UNI SET MAX PD <value>**

Parameter	Description
<value>	The limit of variable VT(PD).

You must specify an interface number when using an XLX.

Examples:

XL(1)> UNI SET MAX PD 25
XL(1)> UNI SET MAX PD 1 25
(*Where* 1 is the interface number on the XLX.)

UNI SHOW ILMI

The UNI SHOW ILMI command displays the negotiated parameters using Interim Layer Management Interface (ILMI) and remote parameters.

Syntax: **UNI SHOW ILMI**

You must specify an interface number when using an XLX.

Examples:

XL(1)> UNI SHOW ILMI
XL(1)> UNI SHOW ILMI 1
(*Where* 1 is the interface number on the XLX.)

UNI SHOW CONFIG

The UNI SHOW CONFIG command displays the current UNI parameters. You can add the UNI protocol name to display only the parameters from its section.

Syntax: **UNI SHOW CONFIG [QSAAL | ILMI | SIGNAL]**

You must specify an interface number when using an XLX.

Examples:

XL(1)> UNI SHOW CONFIG
XL(1)> UNI SHOW CONFIG 1
(*Where* 1 is the interface number on the XLX.)

UNI SHOW STATS

The UNI SHOW STATS command displays statistics for the received and transmitted Signaling frames.

Syntax: **UNI SHOW STATS**

You must specify an interface number when using an XLX.

Examples:

XL(1)> UNI SHOW STATS
XL(1)> UNI SHOW STATS 1
(*Where* 1 is the interface number on the XLX.)

UNI SHOW STATUS

The UNI SHOW STATUS command displays the current status for Signaling and ILMI. It also displays the total active connections and total connections since the UNI has been active.

Syntax: **UNI SHOW STATUS**

You must specify an interface number when using an XLX.

Examples:

XL(1)> UNI SHOW STATUS
XL(1)> UNI SHOW STATUS 1
(*Where* 1 is the interface number on the XLX.)

35. WAN Line Monitor Commands

Note: The interface number used in the WAN Line Monitor console commands is internal to WAN Line Monitor, and is not the same as the interface number used when displaying or configuring WAN interfaces from the console or through ClearSight. The IDENTIFY command will display the interface type and SNMP interface number for the specified WAN Line Monitor interface number.

WLM START

This command is used to enable WAN Line Monitor.

Syntax: **WLM START**

WLM STOP

This command is used to disable WAN line Monitor

Syntax: **WLM STOP**

WLM HELP

This command is used to display the available WAN Line Monitor commands.

Syntax: **WLM HELP**

WLM INTERFACE

This command is used to set the default interface for all subsequent commands. Once you have used this command, it is not necessary to specify an internal WAN Line Monitor interface number for all subsequent commands; they will default to the interface number you have specified in this command.

Syntax: **WLM INTERFACE interface**

Parameter	Description
interface	Internal WAN Line Monitor interface number to which you want all subsequent commands to default.

WLM IDENTIFY

This command is used to display the interface type and the SNMP interface number for the specified internal WAN Line Monitor interface number.

Syntax: **WLM IDENTIFY interface**

Parameter	Description
interface	Internal WAN Line Monitor interface number for which you want to display the SNMP interface number.

WLM ENABLE and WLM DISABLE

This command is used to enable or disable sampling for the specified interface. This command only applies to the interface specified.

Syntax: **WLM {ENABLE | DISABLE} [interface]**

Parameter	Description
interface	Internal WAN Line Monitor interface number of the WAN interface for which you want to enable or disable sampling.
ENABLE	Enables sampling for the specified interface.
DISABLE	Disables sampling for the specified interface.

WLM INTERVAL

This command is used to set the sampling interval for the interface.

Syntax: **WLM INTERVAL [interface] seconds**

Parameter	Description
interface	this is the internal WAN Line Monitor interface number for which you want to set the sampling interval.
seconds	this is the number of seconds you want to sample the interface.

WLM REPORT

This command displays samples for the interface as they are collected.

Syntax: **WLM REPORT [interface]**

Parameter	Description
interface	this is the internal WAN Line Monitor interface number for which you want to display samples.

The report displays the following information:

Field	Description
n1	This is the internal WAN Line Monitor interface number for which you are displaying samples.
n2	This is the index number of the sample that is being displayed. When WAN Line Monitor is started, it stores samples in a buffer beginning with sample `1'.
DSR:n3	n3 is the Data Set Ready modem signal status. The possible values are 0 or 1 for low or high signal.
DCD:n4	n4 is the Data Carrier Device modem signal status. The possible values are 0 or 1 for low or high signal.
CTS:n5	n5 is the Clear to Send modem signal status. The possible values are 0 or 1 for low or high signal.
RI:n6	n6 is the Ring Indicator modem signal status. The possible values are 0 or 1 for low or high signal.
n7	This indicates if there were any transitions in DSR during the most recent interval. The value will be 0 if there were no transitions and 1 if there were transitions.
n8	This indicates if there were any transitions in DCD during the most recent interval. The value will be 0 if there were no transitions and 1 if there were transitions.
n9	This indicates if there were any transitions in CTS during the most recent interval. The value will be 0 if there were no transitions and 1 if there were transitions.
n10	This indicates if there were any transitions in RI during the most recent interval. The value will be 0 if there were no transitions and 1 if there were transitions.

n11	This indicates if there were any transitions in the Receive Date (RXD) during the most recent interval. The value will be 0 if there were no transitions and 1 if there were transitions.
n12	This indicates if there were any transitions in Receive Clock (RXC) during the most recent interval. The value will be 0 if there were no transitions and 1 if there were transitions.
n13	This indicates if there were any transitions in Transmit Clock (TXC) during the most recent interval. The value will be 0 if there were no transitions and 1 if there were transitions.
Err:n14	n14 is the number of physical errors detected during the sampling period.
n15	n15 is the number of state changes during the sampling period.
state	This is the state of the interface when the sample was taken.
n16	This is the offered load in the range of 0 to 255%. The offered load is the percent of the maximum line utilization that was offered to the transmit routine. The offered load includes all packets given to the driver, including those that were dropped due to congestion.
n17	This is the transmitted load in the range of 0 to 255%. The transmitted load is the percent of the maximum line utilization that was actually transmitted, not just queued.
n18	This is the congestion drop rate in the range of 0 to 255%. The congestion drop rate is the percentage of the maximum line utilization that was dropped during this period.
n19	This is the current queue depth which is the number of kilobytes queued to the interface when the sample was taken.
n20	This is the maximum queue depth with is the maximum number of kbytes queued during the sampling period.

WLM SAMPLE

This command is used to display a specific sample in the buffer. The **WLM SAMPLE** command displays information in the same format as the **WLM REPORT** command (see above).

Syntax: **WLM SAMPLE [interface] sample**

Parameter	Description
interface	This is the internal WAN Line Monitor interface number for which you want to display a sample.
sample	This is the number of the sample which you want to display. For example, if you want to display the 10th sample taken since WAN Line Monitor has been started, the value of this parameter is 10.

WLM STATUS

This command is used to display WAN Line Monitor status for the specified interface.

Syntax: **WLM STATUS [interface]**

Parameter	Description
interface	This is the internal WAN Line Monitor interface number for which you want to display status.

The report displays the following information:

Display Field	Description
n1	This is the interface number for which you are displaying status information.
n2	This is the index number of the oldest sample in the buffer.
n3	This is the index number of the latest sample in the buffer.
n4	This is the number of samples the buffer will hold.
n5	This is the sampling interval is seconds.
hh:mm	This is the time stamp of the oldest sample in the buffer in hours and minutes.
state	This is the state of the interface when the sample was taken. The following states can be displayed: Up and Running - samples are taken Initializing - interface is initializing No resources - resources do not exist to obtain samples Dead Interface - hardware failure Unsupported Interface - bad firmware Halted - sampling halted after interface was shutdown Disabled - sampling disabled from console

36. X.25 Commands

General Information

It is possible to abbreviate commands. All X.25 commands to set parameters start with:

X25 SET INTERFACE ...

but you can use

X25 SET IFC ...

or even

X25 STIFC ...

to do the same thing. Likewise, all X.25 commands to display parameters start with:

X25 SHOW INTERFACE ...

but you can use

X25 SHOW IFC ...

or even

X25 SHIFC ...

X25

This command enables or disables the X.25 console commands (it acts as a toggle).

Syntax: **X25**

After you enter the command, a message appears on the console that lets you know whether the X.25 commands are enabled or disabled.

Note: X.25 commands are disabled after each reboot.

X25 SET INTERFACE

This command sets the parameters of the X.25 interface.

Syntax: **X25 SET INTERFACE n <option> [<value>]**

or

Syntax: **X25 SET IFC n <option> [<value>]**

or

Syntax: **X25 STIFC n <option> [<value>]**

Parameter	Description
n	The interface number for which you want to set parameters. The number must refer to an existing WAN interface on which an X.25 interface was created.
option	The parameter that you want to set for the specified X.25 interface. All options are listed below in the command variations table.
value	A parameter associated with the selected option. Not all options have associated values.

Variation Description

X25 SET INTERFACE n DTE

Sets logical addressing to the Data Terminal Equipment (DTE).
Value range: no value accepted with this option

X25 SET INTERFACE n DCE

Sets logical addressing to the Data Communications Equipment (DCE).
Value range: no value accepted with this option

X25 SET INTERFACE n VCN value

Assigns specified number of Virtual Channels (VCs) for given X.25 interface.
Value range: 1..32

X25 SET INTERFACE n LAD value

Local DTE Address is the X.121 address of the interface in the X.25 protocol.
Value range: up to 15 decimal digits

X25 SET INTERFACE n FADD value

Full Addressing option.
If value = Y, the Local DTE address will be inserted into CALL REQUEST packets beside Remote DTE address.
If value = N, the Local DTE address will not be inserted into CALL REQUEST packet. This is required for certain X.25 networks (switches).
Value range: Y or N
Default: N

X25 SET INTERFACE n DBIT value

D-bit sending option.
If value = Y, the Delivery Bit will be sent in outgoing packets
If value = N, the Delivery Bit will not be sent in outgoing packets. This may be required for certain X.25 networks.
Value range: Y or N
Default: N

X25 SET INTERFACE n ALS value

Active Link Setup is a High–Level Data Link Control (HDLC) parameter.
If value = Y, the X.25 interface will be sending a SABM frame periodically to set up the link.
If value = N, the X.25 interface will wait for the DCE to initiate the link.
Value range: Y or N
Default: Y

X25 SET INTERFACE n PB0 value

Poll Bit 0 is an HDLC parameter.
If value = Y, RR/RNR/IREJ commands (frames) with the Poll Bit set to 0 will be rejected.
If value = N, RR/RNR/REJ commands (frames) with Poll Bit set to 0 will be ignored.
Value range: Y or N
Default: Y

X25 SET INTERFACE n EFF value

Extended Frame Format denotes how HDLC are numbered.
If value = Y, frames are numbered modulo 128 (Extended Format).
If value = N, frames are numbered modulo 8 (Basic Format).
Value range: Y or N
Default: N

X25 SET INTERFACE n K value

Link Level Window size is the maximum outstanding HDLC frames allowed.
Value range (basic format): 0..7
Value range (extended format): 0..127
Default: 7

X25 SET INTERFACE n EPF value

Extended Packet Format denotes how packets are numbered.
If value = Y, packets are numbered modulo 128 (Extended Format).
If value = N, packets are numbered modulo 8 (Basic Format).
Value range: Y or N
Default: N

X25 SET INTERFACE n MPW value

Maximum Packet–level Window sets the maximum window size for X.25 packets that can be accepted under the Window Size Negotiation Facility.
Value range: 0..7 (basic format)
Value range: 0..127 (extended format)
Default: 7

X25 SET INTERFACE n DPW value

Default Packet–level Window establishes the maximum number of outstanding X.25 packets allowed.
Value range: 0..7 (basic format)
Value range: 0..127 (extended format)
Default: 2

X25 SET INTERFACE n MPS value

Maximum Packet Size is the maximum value for packet length that can be accepted under the packet Size Negotiation Facility.
Value range: 64, 128, 256, 512, 1024, 2048, 4096
Default: 1024

X25 SET INTERFACE n DPS value

Default Packet Size is the X.25 packet length normally sent to the network.
Value range: 64, 128, 256, 512, 1024, 2048, 4096
Default: 128

X25 SET INTERFACE n N2 value

The maximum number of frame retransmissions at the link level.
Value range: 0..99
Default: 10

X25 SET INTERFACE n N3 value

The maximum number of retransmissions at the packet level.
Value range: 0..99
Default: 3

X25 SET INTERFACE n SEQ value

Sequential VC assigning.
If value = Y, the X.25 interface automatically assigns logical channel numbers to VCs.
If value = N, the starting numbers of logical channels must be assigned manually for each type of VC.
Value range: Y or N
Default: Y

X25 SET INTERFACE n PVS value

Permanent Virtual Circuit Starting number (the lowest logical channel number for PVCs).
Value range: 1..4095

X25 SET INTERFACE n IVS value

Incoming–only Virtual Circuit Starting number (the lowest logical channel number for IVCs).
Value range: 1..4095

X25 SET INTERFACE n TVS value

Two–way Virtual Circuit Starting number (the lowest logical channel number for TVCs).
Value range: 1..4095

X25 SET INTERFACE n OVS value

Outgoing–only Virtual Circuit Starting number (the lowest logical channel number for OVCs).
Value range: 1..4095

X25 SET INTERFACE n T1 value

The delay (in ms) between Replay Timer expiration and start of frame retransmission.
Value range: 200..9999 ms
Default: 3000 ms

X25 SET INTERFACE n T2 value

The Receiver Acknowledgment Timer value indicates the maximum amount of ms that can elapse before sending acknowledgments from the receiver. Note that the value for T2 must be less than the value for T1.
Value range: 0 to 9999 ms
Default: 200 ms

X25 SET INTERFACE n T3 value

The Idle Probe Timer detects inoperative conditions on the link. Note that the value for T3 must be significantly greater than the value for T1.
Value range: 0 to 99999 ms
Default: 15000 ms

X25 SET INTERFACE n T20 value

The Restart Supervisor Timer denotes the maximum amount of time between issuance of a RESTART INDICATION packet and a RESTART CONFIRMATION packet. When this timer expires, a RESTART packet is retransmitted.
Value range: 0 to 999 s
Default: 180 seconds

X25 SET INTERFACE n T21 value

The Call Supervisor Timer denotes the maximum amount of time that can elapse between CALL REQUEST packets and CALL CONFIRMATION packets. When this timer expires, a CALL will be cleared.
Value range: 0 to 999 s
Default: 200 seconds

X25 SET INTERFACE n T22 value

The Reset Supervisor Timer denotes the maximum amount of time that can elapse between RESET REQUEST packets and RESET CONFIRMATION packets. When this timer expires, a RESET packet is retransmitted.
Value range: 0 to 999 s
Default: 180 seconds

X25 SET INTERFACE n T23 value

The Clear Supervisor Timer denotes the maximum amount of time that can elapse between CLEAR REQUEST packets and CLEAR CONFIRMATION packets.
Value range: 0 to 999 s
Default: 180 seconds

X25 SET INTERFACE n OLD ILAN ENCAP {ON | OFF} value

Enables/disables the old way of token ring frames encapsulation. ILAN /XL must be connected to ILAN 386.
Value range: 0 to 999 s
Default: 180 seconds

X25 SET INTERFACE n QUEUE {LONG | NORM} value

Sets the limit to X.25 VC queue length (buffer size).
LONG sets the limit to 64 kB. Use it when you transmit very long datagrams over the VC. Before choosing LONG make sure there is enough RAM.
NORM sets the limit to 32 kB.
Value range: 0 to 999 s
Default: 180 seconds

X25 SHOW INTERFACE

This command allows you to display all or selected parameters of an X.25 interface.

Syntax: **X25 SHOW INTERFACE n <option>**

or

Syntax: **X25 SHOW IFC n <option>**

or

Syntax: **X25 SHIFC n <option>**

Parameter	Description
n	The interface number for which you want to display the parameters. This number must refer to an existing WAN interface on which the X.25 was created.
option	The parameter that you want to display for the specified X.25 interface. To display all the parameters, use the **ALL** option. Otherwise, to see just one setting, use one of the same **options** used for the preceding command (X25 SET INTERFACE n <option> [<value>] on page 520) but do not use a value because in this case you do not want to set a value, you want the system to return the current value. But there are some exceptions: - instead of the **DCE** and **DTE** options used in the SET command, use the **DXE** option in the SHOW command to display whether the interface is set to DCE or DTE. - instead of the **ALS** option used in the SET command, use the **LS** option in the SHOW command to display the Active Link Setup setting. - instead of the **EFF** and **EPF** options used in the SET command, use the **FF** and **PF** options in the SHOW command to display whether the interface is using Extended Frame Format or Extended Packet Format.

X25 SHOW CONFIG

This command displays the parameters of all X.25 interfaces created on an XL device.

Syntax: **X25 SHOW CONFIG**

or

Syntax: **X25 SHOW CFG**

or

Syntax: **X25 SHC**

X25 SET INTERFACE VC

This command sets the parameters for a single Virtual Circuit (VC).

Syntax: **X25 SET INTERFACE n VC <i> <option> [<value1>] [<value2>]**

or

Syntax: **X25 SET IFC n VC <i> <option> [<value1>] [<value2>]**

or

Syntax: **X25 STIFC n VC <i> <option> [<value1>] [<value2>]**

Parameter	Description
n	The interface number. This number must refer to an existing WAN interface on which the X.25 was created.
i	The VC number on a specified interface (described by n) that you want to set parameters.
option	The parameter that you want to set for the specified VC. See the list that follows this command for a description of these options and their associated values.
value1, value2	Parameters that are associated with the selected option. See the list that follows this command for a description of these values.

The following table describes the options and associated values you can use when setting a Virtual Circuit.

Option	Description
VCT	Use Virtual Circuit Type P for PVCs. Use Virtual Circuit Type I for IVCs. Use Virtual Circuit Type T for TVCs. Use Virtual Circuit Type O for OVCs value1 range: P, I, T, O
RAD	Allows you to set the Remote DTE address in the Address Book. You can define as many as five Remote DTE addresses for each VC. Value1 defines the address index in the Address Book. **value1** range: 1..5 **value2** range: an X.121 address
FAC	Use this option to select facilities. The value is a string of hexadecimal numbers. **value1** range: up to 28 hex characters

CRE — Sets the maximum number of CALL retries for each Remote DTE Address defined for this VC. A value of zero sets it for no CALLs, and a null value (no numeric parameter) puts it in endless mode.
value1 range: 0..9999
Default: 20

REI — Sets the Retry Interval value for a specified VC. This parameter defines the time interval between successive CALLs.
value1 range: 0..9999
Default: 15 seconds

LRE — Sets the Loop Retry Counter. It denotes how many times the Address Book will be repeated. A 0 indicates that the Address Book will be processed only once.
value1 range: 0..9
Default: 0

CYCLE — Performs a STOP followed by a START on a specified VC.
value1 range: no value1 accepted

STOP — Sets the VC operator state to OFF. This stops communication on a specified VC.
value1 range: no value1 accepted

START — Sets the VC operator state to ON. This starts VC activity.
value1 range: no value1 accepted

RECON — Auto Reconnect option. If set to Y, VC will always try to re-establish a disconnected link. If set to N, VC will never try to re-establish a disconnected link.
value1 range: Y, N
Default: Y

ENCAP — Sets the encapsulation type for the VC. The possible encapsulation types are:
- ILANMakes possible connections to Olicom devices only.
- RFC 1356standard encapsulation which gives the possibility of connecting to different devices (not only Olicom devices).

value1 range: ILAN, RFC1356
Default: ILAN

PROTO — Determines what kind of traffic can be transmitted over the VC when RFC1356 encapsulation type is set:
value1description
MULTIAll kinds of traffic can be transmitted over the X.25 VC.
IP The VC can transmit only IP frames and no IP SNAP header is added to the Call Request packet during connection establishment.

SNAP_IP — The VC can transmit only IP frames and during connection establishing an IP SNAP header is added to the Call Request packet.

SNAP_IPX	The VC can transmit only IPX frames and IPX SNAP header is added to the Call Request packet during connection establishing.**value1** range: MULTI, IP, SNAP_IP, SNAP_IPX Default: MULTI

X25 SHOW IFC VC

This command allows you to display all or selected parameters of an X.25 VC.

Syntax: **X25 SHOW INTERFACE n VC <i> <option> [<value1>] [<value2>]**

or

Syntax: **X25 SHOW IFC n VC <i> <option>**

or

Syntax: **X25 SHIFC n VC <i> <option>**

Parameter	Description
n	The interface number. The number must refer to an existing WAN interface on which the X.25 was created.
i	The VC number on a specified interface (described by n) whose parameters you want to display.
option	The parameter that you want to display for a specified VC. You can use the options **ALL**, **CONFIG**, or **CFG** to display all parameters.

SET INTERFACE X25

This command allows you to create the X.25 mode on a specified WAN interface.

Syntax: **SET INTERFACE n X25**

Parameter	Description
n	The interface number.

SET INTERFACE NOPASS

This command allows you to terminate the X.25 mode on a specified WAN interface.

Syntax: **SET INTERFACE n NOPASS**

Parameter	Description
n	The interface number.

X25 SET INTERFACE VC START

This command starts the VC.

Syntax: **X25 SET INTERFACE n VC m START**

Parameter	Description
n	This is the interface number.
m	This is the VC number.

Example:

X25 SET INTERFACE 1 VC 3 START
(to start interface 1, virtual circuit 3)

X25 SET INTERFACE VC STOP

This command stops the VC.

Syntax: **X25 SET INTERFACE n VC m STOP**

Parameter	Description
n	This is the interface number.
m	This is the VC number.

Example:

X25 SET INTERFACE 1 VC 3 STOP
(to stop interface 1, virtual circuit 3)

X25 PKTFSM

This command enables and disables packet level tracing.

Syntax: **X25 PKTFSM**

X25 FRMFSM

This command enables and disables frame level tracing (tracing the incoming and outgoing frames).

Syntax: **X25 FRMFSM**

37. XLX Commands

The XLX commands use the following

Class Verb <Locator> <Parameter> <Value>

Note: Defining class and verb is mandatory. Defining parameter and value is optional.

Field	Description
class	Defines an object of the command
verb	Action to be performed, e.g. show or set
locator	Further defines the class or object
parameter	A parameter followed by a quotation mark provides context sensitive help showing what value is expected
value	The value of the parameter

HUNTGROUP SET IP ADDRESS

This command allows the Network Administrator to set the ARP Server IP address for a specific hunt group.

Syntax: **huntgroup <n> set_arp_server ip_address <ip>**

Parameter	Description
n	Specifies the hunt group number (1 through 4)
ip	Specifies the ARP Server IP address

Example:

XLX/1> huntgroup 1 set_arp_server ip_address 128.100.00.00
Huntgroup 1 ARP server ip address set to 128.100.00.00

HUNTGROUP SET ATM ADDRESS

This command allows the Network Administrator to set the ARP Server IP address for a specific hunt group.

Syntax: **huntgroup <n> set_arp_server ip_address <atm>**

Parameter	Description
n	Specifies the hunt group number (1 through 4)
atm	Specifies the ARP Server atm address

Example:

XLX/1> huntgroup 1 set_arp_server atm_address
3911111111111111111111111200009834185003

Huntgroup 1 ARP server ATM address set to
3911111111111111111111111200009834185003

HUNTGROUP ENABLE

This command allows the Network Administrator to enable a specific hunt group or all hunt groups.

Syntax: **huntgroup {n | all} enable**

Parameter	Description
n	Specifies the port number of the hunt group
all	Specifies all hunt groups

Example:

XLX/1> huntgroup 1 enable

HUNTGROUP DISABLE

This command allows the Network Administrator to disable a specific hunt group or all hunt groups. Disabling a hunt group or all hunt groups releases all virtual channels to the endpoints. These released endpoints are then free to connect to the ARP server; however, unless changed the endpoints will all have the same IP address, which may create an error trying to register duplicate IP addresses with the same ARP server.

Syntax: **huntgroup <n | all> disable**

Parameter	Description
n	Specifies the port number of the hunt group
all	Specifies all hunt groups

Example:

XLX/1> huntgroup 1 disable

HUNTGROUP ADD PORT

This command allows the Network Administrator to add a specific port to a specific hunt group. Up to 16 ports can be added to a single hunt group.

Syntax: **huntgroup <n> add_port <p>**

Parameter	Description
n	Specifies the number of the hunt group
p	Specifies the port number to be added to the Hunt Group

Example:

XLX/1> huntgroup 1 add_port 5
Huntgroup 1 now includes port 5

HUNTGROUP REMOVE PORT

This command allows the Network Administrator to remove a specific port from a specific hunt group. All secondary ports must be removed before the primary port can be removed.

Syntax: **huntgroup <n> remove_port <p>**

Parameter	Description
n	Specifies the number of the hunt group
p	Specifies the port number to be removed from the Hunt Group

Example:

XLX/1> huntgroup 1 remove_port 5
Port 5 removed from huntgroup 5

HUNTGROUP SHOW

This command allows the Network Administrator to display the current configuration for a specific Hunt Group or all Hunt Groups.

Syntax: **huntgroup <n | all> show**

Parameter	Description
n	Specifies the number of the Hunt Group
all	Specifies all Hunt Groups

Example:

```
XLX/1> huntgroup 1 show

Huntgroup 1 configured as follows:
ATM address:                    39333233343536373839303030000009894d2e00
ARP server IP:        128.100.000.00
ARP server address    39111111111111111111111111200009834185003
State: Enabled

Port              Role             Admin State        Oper State
                  - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
9                 primary   Up                 Up
10                secondaryUp                  Up

XLX/1>
```

SOFTPVC CREATE SPVC

This command allows the Network Administrator to connect two PVCs with an SVC, thereby creating a “Soft PVC”. Note that the ATM create spvc command performs the same function.

Syntax: **softpvc create <ifc> <vpi> <vci> <ATM address>**

Syntax: **<remote vpi> <remote vci> [<retry interval> <limit>]**

Parameter	Description
ifc	Specifies the port number on the XLX switch
vpi	Specifies the virtual path identifier
vci	Specifies the virtual channel identifier
ATM address	Specifies the ATM address of the interface connecting the remote station
retry interval	Specifies the number of seconds elapsed between attempts to use the spvc (optional parameter with a default of 10 seconds)
limit	Specifies the number of retries (optional parameter with a default of infinity)

Example:

```
XLX/1> softpvc create 1 2 33 391111111111111111111111112000098341850031 1 19
Created VC: 1: 2/33 (Up)<
```

SOFTPVC DELETE

This command allows the Network Administrator to delete an existing SPVC. Note that the ATM delete spvc command performs the same function.

Syntax: **softpvc delete <ifc><vpi><vci>**

Parameter	Description
ifc	Specifies the port number on the XLX switch
vpi	Specifies the virtual path identifier
vci	Specifies the virtual channel identifier

Example:

```
XLX/1> softpvc delete spvc 1 2 33
Delete VC: 1: 2/33 OK
```

SOFTPVC SHOW CIRCUIT

This command provides information about specific soft PVCs. This information is shown in the example below.

Syntax: **softpvc show circuit <ifc> <vpi> <vci>**

Parameter	Description
ifc	Specifies the port number on the XLX switch
vpi	Specifies the virtual path identifier
vci	Specifies the virtual channel identifier

Example:

XLX/1> Softpvc show circuit 1 2 33
XLX(1)> Local PVC: 1/2/33, state: INACTIVE
Remote PVC address: 39111111111111111111112000098341850031, VPI: 1, VCI: 19
SVC state: NOT CONNECTED
Last RELEASE cause: 3; Last RELEASE diagnostics: ff.ff.00.00.2c.00.00.00

Retry Interval: 10; timer: 10; threshold: 0, failures: 17346, limit: 0

SOFTPVC SHOW LIST

This command allows the Network Administrator to display a list of all Soft Permanent Virtual Channels.

Syntax: **softpvc show list**

SOFTPVC DIAG

This command allows the Network Administrator to turn soft PVC diagnostic routines on or off on the switch. Diagnostics information on the status of soft PVCs configured on the switch are displayed on the console when diagnostics are turned on. This information is displayed as it becomes available.

Syntax: **softpvc diag <ON | OFF>**

OAM SEND SEGMENT LOOPBACK VP

This command allows the Network Administrator to test the ATM-layer connectivity on the virtual path between the XLX and the next hop device.

Syntax: **OAM Send segment loopback VP <interface> <vpi>**

Parameter	Description
interface	The number of the interface
vpi	Specifies the virtual path identifier

Example:

XLX/1> OAM send segment loopback VP 1 2

OAM SEND SEGMENT LOOPBACK VC

This allows the Network Administrator to test the ATM-layer connectivity on the virtual channel between the XLX and the next hop device.

Syntax: **OAM Send segment loopback VC <interface> <vpi> <vci>**

Parameter	Description
interface	The number of the interface
vpi	Specifies the virtual path identifier
vci	Specifies the virtual channel identifier

Example:

XLX/1> OAM send segment loopback VC 1 2 33

OAM SEND END TO END LOOPBACK VP

This command allows the Network Administrator to test the ATM-layer connectivity on the virtual path between the XLX and the end devices. Note that the results of an end-to-end loopback test are not received by the XLX. The end station receives the OAM cell.

Syntax: **OAM Send end-to-end loopback VP <interface> <vpi>**

Parameter	Description
interface	The number of the interface
vpi	Specifies the virtual path identifier

Example:

XLX/1> OAM send end-to-end loopback VP 1 1

OAM SEND END TO END LOOPBACK VC

This command allows the Network Administrator to test the ATM-layer connectivity on the virtual channel between the XLX and the end devices.

Syntax: **OAM Send end-to-end segment loopback VC <interface> <vpi> <vci>**

Parameter	Description
interface	The number of the interface
vpi	Specifies the virtual path identifier
vci	Specifies the virtual circuit identifier

Example:

XLX/1> OAM send segment loopback VC 1 1 15

ATM CREATE VP

This command allows the Network Administrator to create a virtual path.

Syntax: **ATM create VP <ifc> <vpi> <trfidx>**

Parameter	Description
ifc	Specifies the port number on the XLX switch
vpi	Specifies the virtual path identifier
trfidx	Specifies a traffic profile which sets the carrying capacity of the path and future logical port

Example:

XLX/1> ATM create vp 1 44 traffic 6
Created VP: 1: 2 (UP)

ATM SET VP TUNNELING ON

This command allows the Network Administrator to turn on the tunneling feature for a specific virtual path within a specific interface. This creates a logical port associated with the tunneled VP. Note that signaling and UME functions of this new logical port will not function until the system is rebooted.

Syntax: **ATM set VP <ifc> <vpi> tunneling on**

Parameter	Description
ifc	Specifies the interface number on the XLX switch
vpi	Specifies the virtual path identifier

Example:

XLX/1> ATM set vp 1 2 tunneling on
IFC: 1020 added, IFC: 2020 added,
To support this tunneled VP, the XLX will need to be rebooted. Before rebooting, configure all logical AMT ports needed.

IFC 1020: OperSts (UP)
Tunneled VP 1:2 bound to logical ATM Port: 20
XLX(1)

ATM SET VP TUNNELNG OFF

This command allows the Network Administrator to turn off the tunneling feature for a specific virtual path within a specific interface.

Syntax: ATM set VP <ifc> <vpi> tunneling off

Parameter	Description
ifc	Specifies the interface number on the XLX switch
vpi	Specifies the virtual path identifier

Example:

```
XLX/1> ATM set vp 1 2 tunneling off
IFC 1020: OperSts (DOWN)
IFC: 2020 deleted, IFC: 1020 Deleted, VP 1:2 has removed its previous assigned Logical
        ATM Port.
XLX(1)>
```

ATM SHOW VP

This command allows the Network Administrator to display detailed information for a specific Virtual Path. This command lists all VPs and shows which VPs are being tunneled.

Syntax: ATM show VP

Example:

```
XLX/1> ATM show VP
ATM - Virtual Path Summary    MON JAN 13 14:51:38 1997
Port: 1 MAX Xmt:366792 Rcv:366792 AVL Xmt:319632 Rcv:319632
Port VPI Stt Type   Owner        Xmt        Rcv     Connection Name
1:   7 +/+ Perm     Tunnel: 20   3:2358     3:2358  Connection Name
```

ATM SHOW INTERFACE

This command allows the Network Administrator to display detailed information for a specific ATM interface number. This interface could be a physical ATM port, internal ATM Port - Network Side, internal ATM Port - User Side, Logical ATM port - tunnel.

Syntax: **ATM show interface <ifc>**

Parameter	Description
ifc	Specifies the interface number on the XLX switch

SIGNALING SET PROXY_USER

The following command allows the Network Administrator to define an interface as a proxy user interface to existing ATM networks and assign an end station interface to use the proxy user interface as a connection to the network.

Syntax: **Signaling set proxy_user <end station interface> <proxy user interface>**

Example:

XLX/1> signaling set proxy_user 5 6

The following command allows the Network Administrator to remove proxy user configuration from an interface and set the interface back to its normal state. This command toggles an end station interface between enabling and disabling usage of the proxy interface.

Syntax: **Signaling delete proxy_user <end station interface>**

Example:

XLX/1> signaling delete proxy_user 5

Procedures

1. X.25 Procedures

To configure an X.25 interface

1 Enable X.25 Commands
X25 on page 519

2 Stop the interface
STOP n on page 15

3 Set Interface Parameters
SET INTERFACE n intf_type
SET INTERFACE n clock_type
SET INTERFACE n INVERT on page 33
SET INTERFACE n SPEED = x on page 34

4 Set X.25 Protocol
SET INTERFACE n X25 on page 528

5 Set Local Address
X25 SET INTERFACE n LAD value on page 520

6 Set Full Addressing
X25 SET INTERFACE n FADD value on page 521

7 Set Additional Parameters

7.1. FRAME FORMAT {basic|extended}
X25 SET INTERFACE n EFF value on page 521

7.2. MAXIMUM FRAME WINDOW SIZE
X25 SET INTERFACE n K value on page 521

7.3. DEFAULT PACKET SIZE
X25 SET INTERFACE n DPS value on page 522

7.4. MAXIMUM PACKET SIZE
X25 SET INTERFACE n MPS value on page 522

7.5. PACKET FORMAT {basic|extended}
X25 SET INTERFACE n EPF value on page 522

7.6. DEFAULT PACKET WINDOW SIZE
X25 SET INTERFACE n DPW value on page 522

7.7. MAXIMUM PACKET WINDOW SIZE
X25 SET INTERFACE n MPW value on page 522

8 View Interface Configuration
X25 SHOW INTERFACE n VC <i> <option> [<value1>] [<value2>] on page 528

To configure an X.25 virtual circuit

1 Set X.25 VC Parameters
X25 SET INTERFACE n VCN value on page 520

2 Stop VCs
X25 SET INTERFACE n VC m STOP on page 529

3 Set the VC Type
X25 SET IFC n VC <i> <option> [<value1>] [<value2>] on page 526
use VCT for <option>.

4 Set VC Encapsulation Type
X25 SET IFC n VC <i> <option> [<value1>] [<value2>] on page 526
use ENCAP for <option>.
If RFC 1356 encapsulation is chosen, it is also possible to set the proper VC protocol type:

4.1. Setting VC Protocol Type
X25 SET IFC n VC <i> <option> [<value1>] [<value2>] on page 526
use PROTO for <option>.

5 Set Calling Parameters

5.1. Setting Call Retries
X25 SET IFC n VC <i> <option> [<value1>] [<value2>] on page 526
use CRE for <option>.

5.2. Setting Loop Retries
X25 SET IFC n VC <i> <option> [<value1>] [<value2>] on page 526
use LRE for <option>.

5.3. Setting Retry Interval
X25 SET IFC n VC <i> <option> [<value1>] [<value2>] on page 526
use REIfor <option>.

6 Set Remote Address
X25 SET IFC n VC <i> <option> [<value1>] [<value2>] on page 526
use RADfor <option>.

7 Start the VC
X25 SET INTERFACE n VC m START on page 529

8 View VC Configuration
X25 SHOW IFC n VC <i> <option> on page 528
use ALL or parameter_name for <option>.

2. SMDS Procedures

To configure an SMDS interface

1 Stop the Interface
STOP n on page 15

2 Configure General Interface Parameters
Set general interface parameters as required by the SMDS DSU/CSU or SMDS switch (interface type X.21, V35; noinvert, etc.).

3 Set Interface to SMDS Mode
SET INTERFACE x SMDS on page 480

4 Configure DXI Interface

4.1. Set DXI Heartbeat Period:
SET INTERFACE x HBPERIOD = p on page 480

4.2. Set DXI Heartbeat Threshold:
SET INTERFACE x HBTHRES = t on page 480

5 Start the Interface
START n on page 16

To configure an SMDS port

1 Set SMDS Individual Address on Port
SMDS SET x IA c on page 481

2 Set Bridge Group Address
SMDS SET x BRGA e on page 481

3 Configure SMDS for IP Router
SMDS SET x IPLISGA e on page 482
SMDS SET x IPARPRA e on page 482

4 Configure SMDS for IPX Router

4.1. Set Group Addresses
SMDS SET x IPXGLGA e on page 483
SMDS SET x IPXGA e on page 483
SMDS SET x IPXARPGA e on page 483
SMDS SET x IPXNLSPGA e on page 483
SMDS SET x IPXSAPGA e on page 483

4.2. Set ARP Time-out
SMDS SET x IPXTIMEOUT n on page 483

3. SLCS Procedures

To delete a SLCS session

1 Stop the session:
SET SLCS sess_id <option> on page 471
use OFF for <option>.

There is one more way to stop the session, regardless of the type of the state of the session. It is an abnormal stop and all state variables are reset. To perform this unconditional stop, use:
SET SLCS sess_id <option> on page 471
use FORCE for <option>.

2 Delete the session:

SET SLCS session_id DEL
SET SLCS sess_id <option> on page 471
use DEL for <option>.
After entering this command the session setup will be removed from the non-volatile ILAN parameter memory.

To configure a SLCS session

1 If the session you want to change the parameters for is started, stop it:

SET SLCS sess_id <option> on page 471
use OFF or FORCE for <option>.

2 Set the PU type. There are three possibilities:
PU 2.0 - in this mode one side connects first. In most cases, the downstream device from the SLCS ILAN should be connected first. Select the side which connects first:
SET SLCS {Sess_Id} SIDE_A_FIRST {ON | OFF} on page 471

PU 2.1 - in this mode, neither side is connected first: both sides wait for incoming connections and the SDLC role of the SDLC side (primary or secondary) is negotiated:
SET SLCS sess_id <option> on page 471
use PU21 for <option>.

PU 1.0 - this mode is similar to PU 2.1 mode except the XID format differs:
SET SLCS sess_id <option> on page 471
use PU10 for <option>.

3 On SDLC, sending broadcast XIDs during session establishment can lead to broadcast storms. To prevent this from happening, you can block them after 12 have been sent:

SET SLCS sess_id <option> on page 471
use XID3_BLOCK for <option>.

To reverse this command (to allow XIDs during session establishment), use:
SET SLCS sess_id <option> on page 471
use XID3_NOTBLOCK for <option>

4 Set any required session-side parameters. For details see: To configure SLCS session-side parameters on page 549.

5 Start the specified session.
SET SLCS sess_id <option> on page 471
use ON for <option>.

To configure SLCS session-side parameters

1 Set the type of session:
SET SLCS session_id SIDE {A|B} <option> on page 472
use ACC_TYPE n for <option>. (0–Ethernet, 2– Token Ring, 5 – SDLC)

2 Set the buffer size:
SET SLCS session_id SIDE {A|B} <option> on page 472
use BUFF_SIZE n for <option>.

3 Set the window size:
SET SLCS session_id SIDE {A|B} <option> on page 472
use WINDOW n for <option>.

4 Set the reconnect timer:
SET SLCS sess_id <option> on page 471
use TR_RECON for <option>.

The remaining parameters depend on whether it is either an Ethernet or Token Ring session, or whether it is an SDLC session. Decide whether you want:
To configure Ethernet or Token Ring SLCS session-side parameters on page 550
To configure SLCS session-side parameters on page 549.

To configure Ethernet or Token Ring SLCS session-side parameters

1 Set the MAC address and the SAP of the session partner:
SET SLCS session_id SIDE {A|B} <option> on page 472
use DEVI_MAC n for <option>.

SET SLCS session_id SIDE {A|B} <option> on page 472
use DEVI_SAP n for <option>

2 Set the MAC address and the SAP of SLCS:
SET SLCS session_id SIDE {A|B} <option> on page 472
Use SLCS_MAC n for <option>.

SET SLCS session_id SIDE {A|B} <option> on page 472
use SLCS_SAP n for <option>.

3 Set the node ID of the secondary station:
SET SLCS session_id SIDE {A|B} <option> on page 472
use NODE_ID n for <option>.

4 Set the T1 reply timer (in 1/10 seconds):
SET SLCS session_id SIDE {A|B} <option> on page 472
use T1_REPLY n for <option>.

5 Set the TI inactivity timer (in 1/10 seconds):
SET SLCS session_id SIDE {A|B} <option> on page 472
use TI_INACT n for <option>.

6 Set the N2 maximum of retransmissions:
SET SLCS session_id SIDE {A|B} <option> on page 472
use N2_TRANS n for <option>.

7 Set the T2 receiver acknowledgment (in 1/10 seconds):
SET SLCS session_id SIDE {A|B} <option> on page 472
use T2_RECV n for <option>.

To configure SDLC SLCS session-side parameters

If it is an SDLC session:

1. Set the SDLC address and ILAN port number of the interface put into SLCS Pass Through mode:
   SET SLCS session_id SIDE {A|B} <option> on page 472
   use SDLC_ADDR n for <option>.

   SET SLCS session_id SIDE {A|B} <option> on page 472
   use SDLC_PORTn for <option>.

2. Set the SDLC role.
   For PU 2.0, it can be 1 or 2:
   1 - primary
   2 - secondary

   For PU 2.1, it can be 1, 2, 3, or 7:
   1 - primary
   2 - secondary
   3 - negotiable
   7 - negotiable but no broadcast (SDLC address will be used in XID frames)

   SET SLCS session_id SIDE {A|B} <option> on page 472
   use SDLC_ROLE n for <option>.

   Optional If you are working with PU 2.1 sessions, set the eight character network name and the Control Point name for the SDLC side of the session:
   SET SLCS session_id SIDE {A|B} <option> on page 472
   use NET_ID n for <option>.

   SET SLCS session_id SIDE {A|B} <option> on page 472
   use CP_NAME n for <option>.

3. If the SDLC role is primary:

Set the T1 reply timer (in 1/10 seconds):
SET SLCS session_id SIDE {A|B} <option> on page 472
use T1_REPLY n for <option>.

Set the TI inactivity timer (in 1/10 seconds):
SET SLCS session_id SIDE {A|B} <option> on page 472
use TI_INACT n for <option>

Set the N2 maximum of retransmissions:
SET SLCS session_id SIDE {A|B} <option> on page 472

use N2_TRANS n for <options>.

4 Set the group poll address:
SET SLCS session_id SIDE {A|B} <option> on page 472
use G_POLL n for <options>.

5 Set the non-context timer (in seconds):
SET SLCS session_id SIDE {A|B} <option> on page 472
use TN_NONC n for <options>.

To configure NetView session parameters

1 Disable the NV session. It must be done whenever you modify or define a NV SLCS session:
SET SLCS NV <option> on page 474
use OFF for <option>.

2 Choose the type of session (0 - Ethernet, 2 - Token Ring, 5 - SDLC):
SET SLCS NV <option> on page 474
use ACC_TYPE n for <option>.

3 For Ethernet or Token Ring set the following parameters:
Set the MAC address and the SAP of the host:
SET SLCS NV <option> on page 474
use HOST_MAC n for <option>.

SET SLCS NV <option> on page 474
use HOST_SAP n for <option>.

Set the MAC address and the SAP of SLCS:
SET SLCS NV <option> on page 474
use SLCS_MAC n for <option>.
and
SET SLCS NV <option> on page 474
use SLCS_SAP n for <option>.

Set the node ID of the NetView Agent:
SET SLCS NV <option> on page 474
use NODE_ID n for <option>.

4 For SDLC set the SDLC address and ILAN port number of the interface put into SLCS Pass Through mode:
SET SLCS NV <option> on page 474
use SDLC_ADDR n for <option>.
and
SET SLCS NV <option> on page 474
use SDLC_PORT n for <option>.

5 Set the resource name:
SET SLCS NV <option> on page 474
use RES_NAME n for <option>.

6 Enable the NV session:
SET SLCS NV <option> on page 474
use ON n for <option>.
To start the NV session you should cycle the SLCS using the commands SET SLCS {UP | DOWN} on page 468.

4. OSPF Procedures

To configure an OSPF router

Note: To avoid useless network state changes during router configuration, you should configure OSPF on an inactive router.

1 Configure an IP Router

1.1. Set the port IP address:
IPR ADDRESS n ipaddress on page 234

1.2. Set the port IP mask:
IPR MASK n ipmask on page 234

1.3. Enable the port:
IPR PORT {ENABLE | DISABLE} n on page 238
use the ENABLE option

2 Create an OSPF protocol instance:
OSPF INSTANCE NEW instance_id ASE_interval ASE_limit LSDB_limit on page 412

3 Set Parameters for the Instance

Set the Router's Identifier
OSPF RTRID router_id on page 412

4 Create an Area
OSPF AREA NEW area_id area_type on page 413

5 Set cost for the Default External Route, when area is stub
OSPF AREA SCOST area_id cost [N] on page 414

6 Enable an Area
OSPF AREA ENABLE area_id on page 414

7 Set Area Authentication Requirement
OSPF AREA TYPE area_id area_type authentication_type on page 415

8 Add a Net Range
OSPF RANGE NEW area_id ip_address ip_mask [N] on page 416

9 Enable an OSPF Protocol
OSPF ENABLE on page 417

To configure an OSPF interface

1 Create the interface
OSPF INTF NEW interface_number area_id on page 417

2 Enable the interface
OSPF INTF ENABLE interface_number on page 418

3 Optional Set the cost of the interface:
OSPF INTF COST interface_number cost on page 419

4 Optional Set the router's priority:
OSPF INTF PRIOR interface_number prior on page 420

5 Optional Set the authentication key:
OSPF INTF AUTHKEY interface_number [auth_key] on page 420

6 Optional Set the retransmission interval:
OSPF INTF RXMT interface_number interval on page 420

7 Optional Set the transit delay interval:
OSPF INTF TRANS interface_number interval on page 421

8 Optional Set the hello interval:
OSPF INTF HELLO interface_number interval on page 421

9 Optional Set the dead interval:
OSPF INTF DEAD interface_number interval on page 421

10Optional Set the poll interval:
OSPF INTF POLL interface_number interval on page 421

To configure an OSPF virtual interface

1 Create the virtual interface:
OSPF VINTF NEW nbr area_id on page 422

2 Enable the virtual interface:
OSPF VINTF ENABLE nbr area_id on page 423

3 Optional Set the authentication key:

Applies only to areas with the authentication type set to simple password
OSPF VINTF AUTHKEY nbr area_id [auth_key] on page 423

4 Optional Set the retransmission interval:
OSPF VINTF RXMT nbr area_id interval on page 423

5 Optional Set the transit delay interval:
OSPF VINTF TRANS nbr area_id interval on page 424

6 Optional Set the hello interval:
OSPF VINTF HELLO nbr area_id interval on page 424

7 Optional Set the dead interval:
OSPF VINTF DEAD nbr area_id interval on page 424

5. ISDN Procedures

To configure general ISDN parameters

1 Set the mode of operation
ISDN SET INTERFACE i MODE {MONO | DUAL} on page 341

2 Set the switch service type
ISDN SET INTERFACE i SERV {5E | EU | DM | GR | N1} on page 341

To configure ISDN VC parameters

1 Deactivate the virtual circuit
ISDN SET VC i c {ON | OFF} on page 342
use the OFF option

2 Set the number of attempts allowed to reestablish the connection
ISDN SET VC i c NCA {value | PERMANENT} on page 342

3 Set the retry interval
ISDN SET VC i c RI value on page 342

4 Set the call acceptance mode
ISDN SET VC i c ACF {ALL | SELECTED | NONE} on page 343

5 Set the telephone numbers of the remote ISDN interface (you want to make calls) and the local ISDN interface
ISDN SET VC i c FPH phn [vc] on page 343
and
ISDN SET VC i c MPH phone on page 344

6 Establish the Service Profile Identification (SPID) for the ISDN virtual circuit
ISDN SET VC i c SPID spid on page 345

7 Create a new security telephone number
ISDN SET VC i c SEC phone [vc] on page 346

8 Choose the encapsulation protocol for ISDN VC. Default encapsulation is CCPP

For compatibility with previous implementations of ISDN (versions earlier than 6.0) choose CCPP encapsulation.
ISDN SET VC i c PROT {CCPP | PPP} on page 348

9 Activate the virtual circuit
ISDN SET VC i c {ON | OFF} on page 342
use the ON option

6. Frame Relay Procedures

To configure an interface to Frame Relay

1 Stop the interface
STOP n on page 15

2 Set the clock source
SET INTERFACE n RECOVER on page 33

3 Set the line speed
SET INTERFACE n SPEED = x on page 34

4 Set the interface to No Data Inversion
SET INTERFACE n NOINVERT on page 33

5 Set the interface type to Frame Relay
SET INTERFACE n FR on page 33

6 Restart the interface
START n on page 16

To configure a Frame Relay interface

1 Stop Interface
STOP n on page 15

2 Set Interface Name
FR SET INTERFACE n LINKNAME name on page 193

3 Set Correct Link Management Protocol for Switch
FR SET INTERFACE n LMI {NONE | LMI | STRATACOM | ANNEXD} on page 190

4 Set Required Injection Management Type
FR SET INTERFACE n INJECT {STANDARD | FORCED} on page 197

5 Complete FR Interface Setup
START n on page 16

To create a Frame Relay port

1. Stop the interface on which the port will reside
   STOP n on page 15

2. Create the port
   FR CREATE PORT n portname on page 195

3. Restart the interface
   START n on page 16

To check whether a VC was learned (when LMI is enabled)

1. Display FR VCs on Interface
   FR SHOW VC i on page 208
2. All VCs learned from the switch should be listed as VC UNASSIGNED.

To create a VC manually (when LMI is disabled)

1. Stop the interface
   STOP n on page 15
2. Create the virtual circuit
   FR CREATE VC n c on page 194
3. Restart the interface
   START n on page 16

To map a VC to a port

1. Stop the interface
   STOP n on page 15

2. Check the port number
   FR SHOW PORT [n] on page 203

3. Map the VC to the port
   FR MAP VC n c p on page 195

4. Restart the interface
   START n on page 16

7. BGP Procedures

To create a BGP instance

1 Create the new instance:
BGP AS as_number on page 106

2 Set the router ID:
BGP RTRID router_id on page 107

3 Optional Set the default metric:
BGP METRIC metric on page 108

4 Optional Set the default preference:
BGP PREF pref on page 107

5 Enable the instance:
BGP ENABLE on page 106

To specify a BGP peer

1 Create a peer:
BGP PEER NEW peer_addr as_number on page 115
Define BGP policies
IPR IMPORT policy-id1 [BEFORE policy-id2] FROM scope on page 264
IPR EXPORT policy-id1 [BEFORE policy-id2] TO scope on page 265
BGP [DONT] IMPORT ROUTES [option] on page 111
BGP [DONT] EXPORT protocol ROUTES [option] on page 113

Optional BGP AGGREGATE net mask [OSPF_TAG tag] [BGP_AS as_number] on page 110

Optional BGP ASWEIGHT as_number {weight | INFINITY | DEFAULT} on page 109

2 Optional Set the local address of the connection:
BGP PEER LADDR peer_addr local_addr on page 118

3 Optional Set the multi-exit discriminator:
BGP PEER MED {ENABLE | DISABLE} peer_addr on page 120

4 Optional Set the local preference option:
BGP PEER USEPREF {ENABLE | DISABLE} peer_addr on page 121
(This applies to peers from the same AS only.)

5 Optional Set the peer connection type:
BGP PEER {ACTIVE | PASSIVE} peer_addr on page 116

6 Optional Set the peer's timers:
BGP PEER TIMERS peer_addr <keepalive> <holdtime> [<connretry> <min-orig> <minadver>] on page 117

7 Enable the peer:
BGP ENABLE on page 106

To define BGP policies

1 Set the import policy:
IPR IMPORT policy-id1 [BEFORE policy-id2] FROM scope on page 264
BGP [DONT] IMPORT ROUTES [option] on page 111

2 Set the export policy:
IPR EXPORT policy-id1 [BEFORE policy-id2] TO scope on page 265
BGP [DONT] EXPORT protocol ROUTES [option] on page 113

3 Optional Specify the aggregate routes:
BGP AGGREGATE net mask [OSPF_TAG tag] [BGP_AS as_number] on page 110

4 Optional Set the AS weights:
BGP ASWEIGHT as_number {weight | INFINITY | DEFAULT} on page 109

8. PPP Procedures

To configure a PPP interface on ordinary WAN lines (like RS232, V35, etc.)

1. Stop the Interface
   STOP n on page 15
2. Configure General Interface Parameters
   Set general interface parameters as required by the PPP DSU/CSU (interface type X.21, V35, RS232; noinvert, etc.).
3. Set Interface to PPP Mode
   SET INTERFACE n PPP on page 455
4. Start the Interface
   START n on page 16
5. Look at the default and negotiated parameters of PPP interface
   PPP n SHOW STAT on page 456
6. If you change some PPP parameters, you have to re-establish PPP connection
   CYCLE n on page 15

To enable PPP over ISDN

What module are you using?

XLT or XLTF. See To enable PPP over ISDN for XLT or XLTF module on page 570

XLP or XLA. See To enable PPP over ISDN for XLP or XLA module on page 571

To enable PPP over ISDN for XLT or XLTF module

For the mono option an interface has only one virtual circuit and therefore only one port. If the option is dual, each interface has two virtual circuits. They can be using different protocols. Every circuit needs to be defined separately.

1. Disable virtual circuit
   ISDN SET VC i c {ON | OFF} on page 342
   use the OFF option.

2. Choose the protocol to be used by the circuit
   ISDN SET VC i c PROT {CCPP | PPP} on page 348

3. Enable virtual circuit
   ISDN SET VC i c {ON | OFF} on page 342
   use the ON option.

To enable PPP over ISDN for XLP or XLA module

For the mono option an interface has only one virtual circuit and therefore only one port. If the option is dual, each interface has two virtual circuits. Both circuits must use the same protocol. When you chose the protocol for one circuit, the other one is automatically set to use the same protocol.

1 Stop the interface
STOP n on page 15

2 Choose the protocol to be used by the circuit
ISDN SET VC i c PROT {CCPP | PPP} on page 348

3 Start the interface
START n on page 16

9. Proprietary CHAP Procedures

CHAP is used to authenticate branch offices from a central office. To achieve this you must configure CHAP in both the branch offices and the central office.

Note: Proprietary CHAP does not work on ports with disabled IP router.

To configure a CHAP central office interface

1 Assign a name to the Central Office:
CHAP HOSTNAME <hostname> on page 463

2 Create an entry in CHAP Secret Database:
CHAP ADD <client/peer> <server/authenticator> <secret> on page 466

3 Check your work on the CHAP Secret Database and Hostname by using:
CHAP SHOW on page 463

4 Set the authentication request on the port:
CHAP p AUTH on page 464

5 Check the state of CHAP on specified port:
CHAP p SHOW on page 464

To configure a CHAP branch office interface

1. Assign a name to the Branch Office:
   CHAP HOSTNAME <hostname> on page 463
2. Create an entry in CHAP Secret Database (just like for a Central Office):
   CHAP ADD <client/peer> <server/authenticator> <secret> on page 466
3. Check your work on the CHAP Secret Database and Hostname by using:
   CHAP SHOW on page 463

Example proprietary CHAP configuration

Assume that you have an XL in a central office in Houston and another XL in a branch office in London, and that you want the Houston XL to authenticate connections established by the London XL. Here is how you should proceed:

Configure the central office XL

1. Assign a name to the central office:
   CHAP HOSTNAME COHOUSTON
2. Create an entry for London in the Houston CHAP Secret Database
   CHAP ADD BOLONDON COHOUSTON DUCK1968DUFFY1999
3. Check your work on the CHAP Secret Database and Hostname by using:
   CHAP SHOW
4. Set the authentication request on the port:
   CHAP p AUTH
5. Check the state of CHAP on specified port:
   CHAP pp SHOW

Configure the branch office XL

1. Assign a name to the branch office:
   CHAP HOSTNAME BOLONDON
2. Create an entry for Houston in the London CHAP Secret Database:
   CHAP ADD BOLONDON COHOUSTON DUCK1968DUFFY1999
   This entry is identical to the entry made in step 2 of the Houston procedure above.
3. Check your work on the CHAP Secret Database and Hostname by using:
   CHAP SHOW

10. Standard CHAP over PPP Procedures

Standard CHAP over PPP is used to authenticate branch offices from a central office. To achieve this you must configure CHAP in both the branch offices and the central office.

To configure a Standard CHAP over PPP central office interface

1 Assign a name to the Central Office:
CHAP HOSTNAME <hostname> on page 492

2 Create an entry in CHAP Secret Database:
CHAP ADD <client/peer> <server/authenticator> <secret> on page 494

3 Check your work on the CHAP Secret Database and Hostname by using:
CHAP SHOW on page 492

4 Configure the PPP interface. See:
To configure a PPP interface on ordinary WAN lines (like RS232, V35, etc.) on page 568
To enable PPP over ISDN on page 569

5 Set the act as authenticator on the PPP port:
PPP p AUTH ACTAS AUTH {ENABLE|DISABLE} on page 491
use the ENABLE option

6 Set the act as peer on the PPP port if we allow to authenticate ourselves.
PPP p AUTH ACTAS PEER {ENABLE | DISABLE} on page 491
use the ENABLE option

7 Enable Standard CHAP protocol on the PPP port
PPP p AUTH CHAP {ENABLE | DISABLE} on page 492
use the ENABLE option

8 Start the PPP port. See:
START n on page 16
ISDN SET VC i c {ON | OFF} on page 342
use the ON option

9 Check the state of CHAP on specified port:
CHAP p SHOW on page 464

Note: This command additionally displays information about proprietary CHAP.

To configure a CHAP branch office interface

1. Assign a name to the Branch Office:
   CHAP HOSTNAME <hostname> on page 463
2. Create an entry in CHAP Secret Database (just like for a Central Office):
   CHAP ADD <client/peer> <server/authenticator> <secret> on page 466
3. Check your work on the CHAP Secret Database and Hostname by using:
   CHAP SHOW on page 463
4. Configure the PPP interface. See:
   To configure a PPP interface on ordinary WAN lines (like RS232, V35, etc.) on page 568
   To enable PPP over ISDN on page 569
5. Set the act as peer on the PPP port if we allow to authenticate ourselves.
   PPP p AUTH ACTAS PEER {ENABLE | DISABLE} on page 491
   use the ENABLE option
6. Set the act as authenticator on the PPP port:
   PPP p AUTH ACTAS AUTH {ENABLE|DISABLE} on page 491
   use the ENABLE option
7. Enable Standard CHAP protocol on the PPP port
   PPP p AUTH CHAP {ENABLE | DISABLE} on page 492
   use the ENABLE option
8. Start the PPP port. See:
   START n on page 16
   ISDN SET VC i c {ON | OFF} on page 342
   use the ON option
9. Check the state of CHAP on specified port:
   CHAP p SHOW on page 464

Note: This command additionally displays information about proprietary CHAP.

Example standard CHAP configuration

Assume that you have an XL in a central office in Houston and another XL in a branch office in London, and that you want the Houston XL to authenticate connections established by the London XL. Here is how you should proceed:

Configure the central office XL

1 Assign a name to the central office:
CHAP HOSTNAME COHOUSTON

2 Create an entry for London in the Houston CHAP Secret Database
CHAP ADD BOLONDON COHOUSTON DUCK1968DUFFY1999

3 Check your work on the CHAP Secret Database and Hostname by using:
CHAP SHOW

4 Configure the PPP interface (See: Configuring PPP interface and Configuring PPP over ISDN)

5 Set the act as peer on the PPP port.
PPP p AUTH ACTAS AUTH ENABLE

6 Enable Standard CHAP protocol on the PPP port
PPP p AUTH CHAP ENABLE

7 Start the PPP port (look Configuring PPP interface and Configuring PPP over ISDN)

8 Check the state of CHAP on specified port:
PPP p SHOW

Configure the branch office XL

1 Assign a name to the branch office:
CHAP HOSTNAME BOLONDON

2 Create an entry for Houston in the London CHAP Secret Database:
CHAP ADD BOLONDON COHOUSTON DUCK1968DUFFY1999
This entry is identical to the entry made in step 2 of the Houston procedure above.

3 Check your work on the CHAP Secret Database and Hostname by using:
CHAP SHOW

4 Configure the PPP interface (See: Configuring PPP interface and Configuring PPP over ISDN)

5 Set the act as peer on the PPP port.
PPP p AUTH ACTAS PEER ENABLE

6 Enable Standard CHAP protocol on the PPP port
PPP p AUTH CHAP ENABLE

7 Start the PPP port (See: Configuring PPP interface and Configuring PPP over ISDN)

8 Check the state of CHAP on specified port:
PPP p SHOW

11. Parallel Port Procedures

To create a parallel port

1 Choose the ports that will become members of the parallel port.

2 Activate the future member ports. If you are connecting X25 or Frame Relay ports, set them to ILAN Compatibility Mode. Be sure to set their costs (speed, CIR, etc.) before to attach them to the parallel port.

3 Create the parallel port:
PP CREATE on page 458

The number of the newly created port will be displayed.

4 For each port you selected in step 1, issue the following command to attach it to the parallel port:
PP pp ATTACH ppm prot on page 460

PP pp ATTACH ppm prot

5 Set the splitting mode for the ports that forward bridged traffic:
PP pp BRGSPLIT {DA | SA | BL} on page 462

6 To see information about the ports and check your work, use:
PP SHP on page 459

To change the parameters of a parallel port member

1. From the parallel port, detach the member port whose parameters you want to change:
   PP pp DETACH ppm on page 461
2. Change the parameters: the type, speed, or cost of the port.
3. Reattach the member port to the parallel port:
   PP pp ATTACH ppm prot on page 460

To troubleshoot a parallel port

For a parallel port to function properly, the configuration of the parallel port members must be symmetrical, so that the parallel port members on both routers have identical type, speed, and cost.

1. For each side of the connection, check the parameter settings to see if they match:
   PP SHP pp on page 459
2. If some of the member parameters don't match, modify them with the procedure To change the parameters of a parallel port member on page 579.

12. Broadcast Resolution Procedures

To enable or disable TCP/IP Broadcast Resolution globally

SET BRES TCPIP {ON | OFF} on page 129

If you disable Broadcast Resolution globally, after enabling globally the Broadcast Resolution feature on the particular ports remains as it was before disabling globally.

To enable TCP/IP Broadcast Resolution on a specified port

1. Enable TCP/IP Broadcast Resolution globally:
   SET BRES TCPIP {ON | OFF} on page 129
   use the ON option

2. Enable TCP/IP Broadcast Resolution on the port:
   SET BRES TCPRES {ON | OFF} n on page 129

   use the ON option

3. Enable learning of IP addresses on the port:
   SET BRES TCPLRN {ON | OFF} n on page 129

   use the ON option

To enable NetBIOS Broadcast Resolution globally

1. To enable NetBios Broadcast resolution globally, use:
   SET BRES NETBIOS {ON | OFF} on page 129
   use the ON option
   If you disable Broadcast Resolution globally, the port settings are not lost. If you re-enable Broadcast Resolution globally, any previous port settings will be restored.

To enable NetBIOS Broadcast Resolution on a specified port

1 Enable NetBIOS Broadcast Resolution globally:
SET BRES NETBIOS {ON | OFF} on page 129
use the ON option

2 Enable NetBIOS Broadcast Resolution on the port:
SET BRES NETBRES {ON | OFF} n on page 130

use the ON option

3 Enable learning of NetBIOS addresses on the port:

SET BRES NETBLRN {ON | OFF} n on page 130
use the ON option

To enable or disable NetBIOS name learning

1 To enable or disable the learning of NetBIOS names from ADD_NAME_QUERY frames:
SET BRES ADDNAME {ON | OFF} on page 130

To manage NetBIOS name length parameters

The default NetBIOS name comparison is 15 bytes.

1 To enable/disable 16-byte NetBIOS name comparison:
SET BRES FULLNAME {ON | OFF} on page 131

2 To display the number of characters in a NetBIOS name that are distinguished during the learning process:
SHOW BRES CHAR on page 132

3 To change the number displayed in step 2:
SET BRES CHAR n on page 131

To set the maximum number of learned NetBIOS names

1. Check the maximum number of NetBIOS names that can be learned:
   SHOW BRES MAXNAMES on page 132

2. Change the setting:
   SET BRES MAXNAMES n on page 132

3. Check your work:
   SHOW BRES MAXNAMES on page 132

Broadcast Resolution Troubleshooting

After using the command SET BRES ADDNAME {ON | OFF} on page 130 (with the ON option) in the internetwork with duplicate NetBIOS names, the connectivity may be lost. If this happens, you will need to change names or wait for the address timeout in one of the names, or timeout it yourself. If the names have different 16th character, use SET BRES FULLNAME {ON | OFF} on page 131 (with the ON option) to differentiate them.

13. IPX Routing Procedures

To configure IPX routing

1 Set the network number on all relevant ports:
IPXLOCALNET p[.c] {net_adr | 0} on page 285

2 Make sure that all ports have proper IPX routing state. By default, IPX routing is enabled on all ports.
To change the state:
IPXPORT {ENABLE | DISABLE} p [.c] on page 287

3 Make sure that the IPX frame type selected on port matches the type used by other devices.
To check current frame type:
IPXPORTCFG p[.c] on page 317

To set the IPX frame type to be processed on the specified IPX circuit:
IPXFT {TSNAP | ESNAP | T8022| E8022 | E8023 | PORTABLE} p[.c] [protocol_type] on page 297

4 If more than one IPX frame type is used in parallel on a single LAN segment, it is necessary to have one IPX circuit for each frame type used.
To create circuit:
IPXPORT CREATE p[.c] {type} on page 296

5 Delete circuit:
IPXPORT DELETE p[.c] on page 297

6 Check whether or not Source Routing should be used on the port (it affects only Token Ring ports).
To enable IPX Source Routing mode on the IPX circuit:
IPXSR {ENABLE | DISABLE} p[.c] on page 288
use the ENABLE option

7 Make sure that on point-to-point connections, where RIP/SAP reduced advertising can be used, RIP/SAP state is set consistently on both sides of a link.
See the commands IPXPORTRIPSM {OFF | OLD | NEW} p[.c] on page 290 and IPXPORTSAPSM {OFF | OLD | NEW} p[.c] on page 291.

8 For group mode Frame Relay ports that are not fully meshed RIP/SAP split horizon must be disabled.
To disable IPX RIP split horizon:
IPX RIPSPLITHORIZON {ON|OFF} p [.c] on page 303
use the OFF option.
To disable IPX SAP split horizon:
IPX SAPSPLITHORIZON {ON|OFF} p [.c] on page 303

use the OFF option.

Optional To improve performance, you can disable Smart Filters and Address Filters:
IPXFILT {SMON | SMOFF | ADDRON | ADDROFF} on page 303
use the SMOFF and ADDOFF options.

9 Enable IPX router:
IPXROUTER {ENABLE | DISABLE} on page 287
use the ENABLE option

14. Dial on Demand Procedures

To configure Dial on Demand

1 Enable Dial on Demand on both ports separately:
DOD p ENABLE on page 182

2 Optional Set additional parameters for all call types (Internal X.25, Internal ISDN, External/DTR, PCMCIA):
DOD p IDLETIME value on page 182
DOD p HOLDUPDATETIME value on page 183

3 Optional Enable or disable piggyback option on a port:
DOD p PIGGYBACKON on page 183
DOD p PIGGYBACKOFF on page 183

4 Display new configuration parameters on a port:
DOD p CONFIG on page 184

15. IP Router Procedures

To configure an IP port

1 Set an IP address for the specified port
IPR ADDRESS n ipaddress on page 234

2 Set an IP routing mask for the specified port
IPR MASK n ipmask on page 234

3 Enable IP routing on the specified port
IPR PORT {ENABLE | DISABLE} n on page 238
use the ENABLE option

4 Enable IP routing globally
IPR ROUTER {ENABLE | DISABLE} on page 243
use the ENABLE option

To assign a secondary IP address

1. It is advised that you assign and register a unique network number portion to each network. To do so, contact the Network Information Center (NIC). This step is necessary if you are planning to connect to Internet.

2. Set an IP address for the specified port:
   IPR ADDRESS n ipaddress on page 234

3. Set an IP routing mask for the specified port:
   IPR MASK n ipmask on page 234

4. Create a new secondary address:
   IPR SECADD n addr mask on page 259
   Optional To change the secondary port into a primary port:
   IPR SECPRI n addr mask on page 259
   If you use this command, the previous primary port automatically becomes secondary.

16. DLSw Procedures

To configure DLSw

1 Set the general DLSw parameters:
DLSW SET parameter value on page 162

IP address of your DLSw router: DLSW SET NETNAME

Virtual ring number (Optional: may be set for Source Routed Token Ring configurations to include additional DLSw hop in RIF): DLSW SET VRN

Bridge number (Optional: may be set for Source Routed Token Ring configurations to include additional DLSw hop in RIF): DLSW SET BRIDGE

Maximum size of the BTU (Optional: may be adjusted for saving router memory): DLSW SET MAX_BTU

Heap size (Optional: in very small and very large DLSw configurations may require adjustment): DLSW SET HEAP

2 Set the LLC DLSw parameters.:
DLSW SET LLC parameter value on page 164

The media type (**Note:** It is recommended to leave this setting on default Token Ring even if only Ethernet interfaces are used.): DLSW SET LLC MAC_TYPE

The maximum buffer size: DLSW SET LLC FRAME_SIZE

3 Define the DLSw partners:
DLSW SET PARTNER address on page 167

4 Start DLSw.
DLSW UP on page 167

Note: It is recommended to leave this setting on default Token Ring even if only Ethernet interfaces are used.

17. GEN Procedures

To perform the testing using GEN

1 Initialise the system.

2 Set the generator to IDLE state:
GEN INIT on page 211

Optional At this point you may terminate your project:
GEN DEL [A] on page 211

3 Start the advertising process:
GEN BEGIN on page 212

Optional At this point you may terminate your project and return to idle state:
GEN CLEAR [A] on page 214

4 Set generator's parameters and synchronize the settings of the test modules:
GEN PAR seconds [tics [packets [pkt_len]]] on page 215

5 Set the number of test repeats and a duration of pause between the tests:
GEN REPEAT times [pause] on page 215

6 Start the test:
GEN START [L] on page 216

7 Perform the test. Use the commands of your choice:
GEN PAR seconds [tics [packets [pkt_len]]] on page 215
GEN SRF [A] on page 216
GEN TRANSP [A] on page 217

8 Return to the INIT_DONE state
GEN STOP [L] on page 216

9 Terminate the task:
GEN DEL [A] on page 211

18. Asynchronous Interface Procedures

To configure an asynchronous interface

1 Stop the interface
STOP n on page 15

2 Enable asynchronous mode on the interface
SET INTERFACE ASYNC on page 32

3 List supported modem types.
SHOW MODEM [i] on page 25
omit the [i] parameter.

4 Using a console command select modem type number from the list.
SET ADV INTERFACE n MODEM=i on page 18

5 Set the interface parameters. You cansee the parameters to be set on The interface parameters list on page 598.

6 Add the phone number to the Phone book
SET ADV INTERFACE n INSPHN i phn on page 21

7 Start the interface
START n on page 16

To manage the Phone Book

I want to:

Insert a phone number at the i-th position:
See SET ADV INTERFACE n INSPHN i phn on page 21.

Remove a phone number from the book:
SET ADV INTERFACE n DELPHN i on page 22.

Set the phone number at the i-th position:
SET ADV INTERFACE n SETPHN i phn on page 21

Shift i-th phone number up or down:
SET ADV INTERFACE n {UP | DOWN} i on page 22.

Clear the entire phone book:
SET ADV INTERFACE n CLRALL on page 22.

The interface parameters list

1 UART speed
SET ADV INTERFACE n UARTSPEED=i on page 18

2 Parity bit type
SET ADV INTERFACE n PARITY=<EVEN | ODD | NONE> on page 18

3 Stop bits per character
SET ADV INTERFACE n STOP=<1 | 2 | 1.5> on page 19

4 Call retry interval
SET ADV INTERFACE n RETRYINTV=i on page 19
or call retry number

SET ADV INTERFACE n CALLRETRY=i on page 19

5 Phone book retry number
SET ADV INTERFACE n LOOPRETRY=i on page 19

6 Waiting time for establishing call
SET ADV INTERFACE n TIMEOUT=i on page 20

7 Call mode
SET ADV INTERFACE n mode on page 20

8 Dial mode
SET ADV INTERFACE n {TONE | PULSE} on page 20

9 Autoreconnection
SET ADV INTERFACE n {RECON | NORECON} on page 21

10Strings:
Mode initialize string
SET ADV INTERFACE n INIT str on page 23

Dial mode string
SET ADV INTERFACE n {TONEPREF | PULSEPREF} str on page 23

Suffix string
SET ADV INTERFACE n SUFFIX str on page 23

Hang up command string
SET ADV INTERFACE n HANGUP str on page 24

Answer string
SET ADV INTERFACE n {ANSON | ANSOFF} str on page 24

19. Asynchronous Modem Support Procedures

How to configure User Define Modem

User Define Modem is an option for the customer who wants to use a modem which is not on the list of supported modems. To display the list use SHOW MODEM [i] on page 25 (omit the [i] parameter). This option can be used for PCMCIA and external modems. However, we cannot guarantee that such modem will work correctly even if the configuration strings are correct.

Choose the way to configure the modem:
To manually configure User Define Modem on page 600
To configure User Define Modem using a template on page 601

To manually configure User Define Modem

The commands shown below may be different for your modem. Refer to the in modem manual.

All the strings except Dial Tone Prefix and Dial Pulse Prefix must have ^M character at the end.

1 Start the initialization string (usually **AT** command).

2 Restore factory default settings (usually **&F** command).
Do not perform &F command for PCMCIA -- it is always done by PCMCIA asynchronous driver.

3 Disable escape codes (usually you do it by writing a value from 128 to 255 to S2 register, for example S2=255).

4 Set the waiting time to the greatest possible value (usually you do it by writing a number of seconds into S7 register, for example S7=255).

5 Make sure the modem returns result codes in verbal form. If it does not, correct modem settings (usually you do it by using **V1Q0** command).

6 Make sure the modem echoes the characters from DCE in command mode. If it does not, correct modem settings using **E1** command.

7 Make sure the CD signal tracks the presence of the carrier. It is often a default setting. If it is not, correct modem settings (usually you do it by using **&C1** command).

8 Make sure that when DTR line enters OFF state, it causes the modem to hang up and return to the command state.

9 Make sure the modem controls DSR signal and DSR is ON when the modem is ready accept data. If it is not, correct modem settings (usually you do it by using **&S1** command).

10Make sure CTS line controls data flow. If it does not, correct modem settings (usually you do it by using **&F1** command).

11If possible, modem should return information about speed between modems by sending CONNECTION messages. If it does not, correct modem settings(usually you do it by using **W2** command).

12End the initialization string with ^M character.

To configure User Define Modem using a template

1. Display the list of supported modems Use:
   SHOW MODEM [i] on page 25
   omit the [i] parameter
2. Decide what modem will be the template. Remember its number.
3. Display settings for the modem to be used as a template. Use
   SHOW MODEM [i] on page 25
4. Use the displayed settings as an example to configure your modem.

How to connect a remote terminal

A module can be remotely accessed using a modem. To attach an external modem you have to perform the two procedures below:

1 To make physical connection on page 603

2 To configure the modem on page 604

To make physical connection

1. Connect the single-pronged end of the console cable to the interface named Console.
2. Connect the other end of the console cable to a null modem connector.
3. Connect the null modem connector to the external modem.

To configure the modem

1 Configure the modem line settings:
baud rate: 9,600
data bits: 8
stop bits: 1
parity: none

2 Set the modem functions. Check whether the modem has DIP switches:
If yes, use the procedure To configure a modem using DIP switches on page 605
If no, use the procedure To configure a modem which does not have DIP switches on page 606.

To configure a modem using DIP switches

Refer to your modem manual and follow its guidelines to achieve the following results:

ignoring Data Terminal Ready (DTR) signal: ON
verbal (word) results: OFF
suppressing result code display: OFF
suppressing Command Mode Local echo: OFF
enabling Auto Answer: ON
enabling Carrier Detect (CD): OFF
loading a generic template from Read Only Memory (ROM): OFF
disabling Command Set Recognition: ON

To configure a modem which does not have DIP switches

Modems which do not have DIP Switches must be configured by AT commands from a terminal.

1 Connect the modem to the terminal.

2 Send a configuration string to the modem. The speed between the terminal and the modem must be the same as between the XL and the modem. Configure the modem in the following way:
enable Auto Answer must be enabled.
disable character echo in command state.
disable return result codes.
disable local flow control.
set the modem to ignore DTR signal. It must assume that DTR is always ON.
See Example configuration string on page 607.

3 Store current configuration in modem profile.

4 Connect modem to XL console.

Example configuration string

Example 1

HAYES ACCURA 336 configuration string: *AT&FS0=1&K0E0Q1&W0*

Example 2

MOTOROLA LIFESTYLE 288 configuration string:*AT&FS0=1&D\QEQ1&W*

Example 3

ZYXEL 2864 configuration string: *AT&FS0=1&D0&H0E0Q1&W0Z0*

- The Zyxel 2864 and UsRobotics Sportster do not work together for a console (when Zyxel 2864 is connected to XL console and UsRobotics Sportster is connected to terminal on remote side or vice versa). They work correctly with other modems for a console.

Example 4

LASAT Safire 336 configuration string: *AT&FS0=1&D0&K0E0Q1&W0&Y0*

Example 5

LASAT Safire 228 configuration string: *AT&FS0=1&D0&K0E0Q1&W0&Y0*

To connect PCMCIA modem as a Console to XLA modules.

1. Make sure your PCMCIA modem is on the list of modems supported as console in XL version 6.0:
   Olicom GoCard Trn/Modem 336
   Olicom GoCard Eth/Modem 336
   Lasat Credit 288
   Hayes Optima 336
   Megahertz XJ1288
   Megahertz XJ4288
   Megahertz XJ1144
2. Use the following command to set the console mode for PCMCIA:
   PCMCIA CONSOLE on page 448

The console mode can also be set from ClearSight.

20. ClearSession Protocol (CSP) Procedures

To configure the CSP for IP Routing

1 Enable CSP feature for IP Routing
CSP IP ENABLE on page 139

2 Optional: Set a GAP time if you want to change default value
CSP IP GAP gap_t on page 140

3 Create CSP IP group with virtual IP address
CSP IP port group_id CREATE [IP ip_addr] on page 140

4 Set a priority for the router if you want to change default value
CSP IP port group_id PRIO prio on page 141

5 Set hello timer and hold timer if you want to change default values
CSP IP port group_id TIMERS hello_t hold_t on page 141

6 Set UDP port if you want to change default value
CSP IP UDPPORT udp_port on page 143

7 Define traced port and decrement priority if you want to track some port availability
CSP IP port group_id TRACE tr_port [d_prio] on page 142

8 Enable CSP for defined group
CSP IP port group_id ENABLE on page 139

To configure the CSP for Source Route Bridging

1 Enable CSP feature SR Bridging
CSP SR ENABLE on page 151

2 Optional: Set a GAP time if you want to change default value
CSP SR GAP gap_t on page 152

3 Create CSP SR group and define traced port
CSP SR port group_id tr_port CREATE on page 153

4 Set a priority for the bridge if you want to change default value
CSP SR port group_id PRIO prio on page 153

5 Set hello timer and hold timer if you want to change default values
CSP SR port group_id TIMERS hello_t hold_t on page 154

6 Enable CSP for defined group
CSP SR port group_id ENABLE on page 151