613-000656 Rev.A 070328

TELESYN® Series Command Handbook Release 8.0 Issue 1

Introduction to the Command Handbook

Congratulations on your purchase of a Telesyn™ Series Multiservice Access Platform product. This product is part of a family of products that leverages Ethernet switching technology to offer service providers a range of services, including video over xDSL.

Who Should Read This Handbook?

This document is for those who perform all types of tasks for Telesyn products and need a complete reference for all commands that can be issued for the Telesyn products.

About this Handbook

This Handbook includes provides all commands and parameters that can be applied to the Telesyn products. Commands are listed to help the user find a specific command quickly by organizing them in various ways. There is also a complete description of parameters as well as specific notes on what a parameter means in the context of a particular command.

- Section 1 provides an overview of the Command System and a description of the syntax symbols.
- Section 2 lists the commands by Product and Feature, and includes whether a command has been added to the release or modified since the previous release.
- Sections 3 lists the commands by syntax and is a quick way to find a specific command. The number of the command assigned here matches the number of the command description in the next Section.
- Section 4 lists the commands and parameters. This list is organized by syntax as in Section 3 and includes a description of the command and the parameters, as well as any special notes on how the parameter is used for that specific command.
- Section 5 is a complete reference of parameters.

Table of Contents

1. Overview of Command System

1.1 Command Syntax

The syntax rules for a Command and its parameters use the following conventions throughout this document:

- All upper case = Key Word
- | = Option (OR)
- [] = Optional
- { = Choice of until }

1.1.1 Editing Functions, Keystrokes, and Abbreviations

The Telesyn Series product supports line editing, line recall, and abbreviations, so that command line input and editing can be done very quickly once command syntax and the line editing commands are learned. These are described in Section 3 of the Telesyn User Guide.

Note: Throughout this document all syntax will use complete words, with verbs and parameters in upper case and the pairing of parameters and values with equal (=) signs.

Table 1-1 lists the terminal editing and keystroke functions most commonly used.

TABLE 1-1 Terminal Editing Functions and Keystrokes

Action	Key Sequence
Move cursor within command line	left and right arrow
Delete character to left of cursor	[Delete] or [Backspace]
Clear command line	[Ctrl/U]
Recall previous command in command history	CTRL/P or up arrow
Recall next command in command history	CTRL/N or down arrow
Automatically complete a partially entered command keyword	[Tab] or [Ctrl/I]

1.2 Security Levels

The security levels required for the management interface follows these rules:

- Security Officers can add, remove, or modify other user accounts.
- Users can only change the attributes of their own accounts.
- Managers can control various aspects of a User’s account, such as showing all active sessions or showing statistics.

For all command listings in this document, the security level is included.

1.3 Control of CLI command confirmation

CLI commands that may result in destructive actions will warn the user by responding to the input of such commands with a prompt asking the user to confirm the requested action with a ‘YES or Y” or “NO or N”. The user must respond with either a ‘YES or Y” or “NO or N”. The system will continue to prompt for this response until the user inputs a correct response. This provides the system a certain level of protection from unwanted destructive events.

Note: It is recommended that confirmation prompting be enabled.

CLI Confirmation can be disabled if the user requires it. Disabling is especially useful when executing command scripts on the system. Scripts are discuss in detail in the Telesyn User Guide, section 14.

The user disables confirmation by:

```
> DISABLE CONFIRMATION
```

The user enables confirmation by:

```
> ENABLE CONFIRMATION
```

1.4 Using Online Help

Online help is available for all Telesyn product commands. There are two types of online help:

1. For command string help, type in the start of a command and enter a space and a “?” at the end of the line. The Telesyn product will display a list of possible parameters. After entering a parameter and a “?”, online help provides an explanation of the parameter. Entering a “?” alone will display all of the verbs available.
2. For complete online help, type HELP and the command. If the command is incomplete, there is an error message. Entering a space and a “?” will show the next valid parameter. When the command is complete, a complete description of the command is displayed.

2. Command Updates

2.1 Overview

This document includes commands used by all Telesyn products. The commands can be organized as follows:

- Common - These commands apply to all Telesyn series products. For this release, the product series includes the Telesyn 7000 and Telesyn 9000.
- Product - These commands apply to a specific product, such as the Telesyn 7400. In many cases, the command is product specific because of a component that applies only to that product.

Within any of these, commands may be used to support a feature, such as Link Aggregation Group (LAG).

The commands listed in this Section are organized into these categories as explained in 2.3.

2.2 Deprecated Commands / Parameters

In release 7.0, many commands and parameters that involve PORT are deprecated. Following is the list:

- SHOW ALARMS PORT (just the PORT keyword)
- ENABLE PORT
- DISABLE PORT
- SHOW PORT
- SET PORT PROFILE
- SET PORT ADSL
- SET PORT SHDSL
- SET PORT POTS
- SET PORT DS1
- SET PORT E1
- SET PORT GE
- SET PORT XE
- SET PORT FX
- SET PORT FE

- SHOW CARD PORTS
- SET INTERFACE PMONALERT ATUC (replaced by SET INTERFACE PMONALERT ADSL ATUC)
- SET INTERFACE PMONALERT ATUR (replaced by SET INTERFACE PMONALERT ADSL ATUR)

2.3 Commands Listed by Feature, and Change

The following table lists the commands using these attributes:

- **Change** - A command can either be **Added** or **Modified** for a release. A command can also be deleted, and where possible this is shown.
- **Feature** - These are the hardware and software features that allow users to group commands into tasks. Refer to the User Guide for a description of how the products are divided into features and feature sets.
- **Syntax** - This is the complete syntax of the command following the conventions described in Section 1.
- **Reason for Change** - If a command has been modified or deleted, the reason for the update is provided.

Using this table allows the user to immediately spot the changes that have occurred in a command for the release and the product and feature that is affected.

Command Listing Ordered by Change, Feature, and Syntax – Section 2

No.	***Feature***	***Change***	***Syntax***	***Reason for Change***
1	IGMP	Modified	ADD IGMPSNOOPING INTERFACE={ type:id-range | id-range | ifname-list | ALL } MACADDRESS={ macaddress-list | partial-macaddress-list }	id, interface, and mac can have list, can use partial macaddress
2	IGMP	Modified	DELETE IGMPSNOOPING INTERFACE={ type:id-range | id-range | ifname-list | ALL } MACADDRESS={ macaddress-list | partial-macaddress-list | ALL }	id, interface, and mac can have list, can use partial macaddress
3	IGMP	Modified	SET IGMPSNOOPING { CARD={ slot-list | ALL } MCASTGROUPLIMIT=1..512 | INTERFACE={ type:id-range | id-range | ifname-list | ALL } SNOOPINGMODE={ INTERNAL | EXTERNAL | MCPASSTHROUGH } | [FLOODUNKNOWNS={ ON | OFF }] [ROUTERAGEINGTIMER=10..1200] [GENQUERYTIMER=5..120] [DUPREPORTTIMER=5..120] }	DUPREPORTTIMER range is 1..120 or OFF
4	Interface_Mgmt_SHDSL	Modified	SET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } SHDSL [MAXCONNECTRATE=72..2312] [MINCONNECTRATE=72..2312] [TARGETSNRMARGIN=0..10] [LINEQUALITYMONITOR={ LOW | MEDIUM | HIGH }] [VPI=0..4095] [VCI=32..65535] [DESCRIPTION=description]	WIREMODE added in Release 7.2
5	PortRateLimiting	Modified	CREATE EGRESSLIMITER=limitername RATE=bits-per-second BURSTSIZE={ 4KB | 8KB | 16KB | 32KB | 64KB | 128KB | 256KB | 512KB | 1MB | 2MB | 4MB | 8MB | 16MB | 32MB | 64MB }	Higher rates (in MB)
6	PortRateLimiting	Modified	SET EGRESSLIMITER=limitername [RATE=bits-per-second] [BURSTSIZE={ 4KB | 8KB | 16KB | 32KB | 64KB | 128KB | 256KB | 512KB | 1MB | 2MB | 4MB | 8MB | 16MB | 32MB | 64MB }]	Higher rates (in MB)
7	QOS	Modified	CREATE TRAFFICDESCRIPTOR=tdname RATE=bits-per-second BURSTSIZE={ 4KB | 8KB | 16KB | 32KB | 64KB | 128KB | 256KB | 512KB | 1MB | 2MB | 4MB | 8MB | 16MB | 32MB | 64MB }	Higher rates (in MB)
8	QOS	Modified	SET TRAFFICDESCRIPTOR=tdname-list [RATE=bits-per-second] [BURSTSIZE={ 4KB | 8KB | 16KB | 32KB | 64KB | 128KB | 256KB | 512KB | 1MB | 2MB | 4MB | 8MB | 16MB | 32MB | 64MB }]	Higher rates (in MB)
9	Interface_Mgmt_EPON	New	CREATE PROFILE=name EPONPORT [ADMINSTATE={ UP | DOWN }] [IPMCVLAN={ vlanname | vid }] [IPADDRESS=ipaddress]	
10	Interface_Mgmt_EPON	New	SET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } EPON [IPMCVLAN={ vlanname | vid }] [IPADDRESS=ipaddress] [DESCRIPTION=description]	
11	Interface_Mgmt_EPON	New	SET PROFILE=name EPONPORT [ADMINSTATE={ UP | DOWN }] [IPMCVLAN={ vlanname | vid }] [IPADDRESS=ipaddress]	
12	Interface_Mgmt_GE	New	CREATE PROFILE=name XEPORT [AUTONEGOTIATION={ ON | OFF }] [FLOWCONTROL={ AUTONEGOTIATE | ON | OFF }] [ADMINSTATE={ UP | DOWN }]	
13	Interface_Mgmt_GE	New	SET PROFILE=name XEPORT [AUTONEGOTIATION={ ON | OFF }] [FLOWCONTROL={ AUTONEGOTIATE | ON | OFF }] [ADMINSTATE={ UP | DOWN }]	
14	Interface_Mgmt_GE	New	SHOW PROFILE [={ name-list | NAMES | ALL }] { XE1 | XEPORT } [FULL]	

No.	Feature	Change	Syntax	Reason for Change
15	Interface_Mgmt_VDSL	New	CREATE PROFILE=name VDSLPORT [MODE={ VDSL2 | GLITE | GDMT | T1.413 | ADSL2 | ADSL2+ | AUTO | AUTO2 | ADSL2M | ADSL2+M }] [LINETYPE={ FAST | INTERLEAVE }] [MAXUPSTREAMRATE=32..14848] [MINUPSTREAMRATE=32..14848] [MAXDOWNSTREAMRATE=32..51200] [MINDOWNSTREAMRATE=32..51200] [TARGETSNRMARGIN=snr-margin-dB] [MAXSNRMARGIN={ OFF | snr-margin-dB }] [MINSNRMARGIN={ OFF | snr-margin-dB }] [MAXRECEIVEPOWER={ OFF | value }] [BANDPLAN={ 997 | 998 }] [OPTUPSTREAMBAND={ ON | OFF }] [RFIBAND={ { 30M | 40M | 80M | 160M } [,...] | NONE | ALL }] [MAXINTERLEAVEDELAY=0..255] [MINIMPULSENOISEPROTECTION UPSTREAMMININP={ 0 | 0.5 | 1 | 2 | 4 | 8 | 16 } DOWNSTREAMMININP={ 0 | 0.5 | 1 | 2 | 4 | 8 | 16 }] [DEPLOYMENT={ CABINET | CENTRALOFFICE }] [PSDMASK UPSTREAMPSDMASK={ MASK1 | MASK2 } DOWNSTREAMPSDMASK={ MASK1 | MASK2 }] [DATABOOST={ ON | OFF }] [LINEQUALITYMONITOR={ LOW | MEDIUM | HIGH }] [VPI=0..4095] [VCI=32..65535] [ADMINSTATE={ UP | DOWN }]	For future release
16	Interface_Mgmt_VDSL	New	SET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } VDSL [MODE={ VDSL2 | GLITE | GDMT | T1.413 | ADSL2 | ADSL2+ | AUTO | AUTO2 | ADSL2M | ADSL2+M }] [LINETYPE={ FAST | INTERLEAVE }] [MAXUPSTREAMRATE=32..14848] [MINUPSTREAMRATE=32..14848] [MAXDOWNSTREAMRATE=32..51200] [MINDOWNSTREAMRATE=32..51200] [TARGETSNRMARGIN=snr-margin-dB] [MAXSNRMARGIN={ OFF | snr-margin-dB }] [MINSNRMARGIN={ OFF | snr-margin-dB }] [MAXRECEIVEPOWER={ OFF | value }] [BANDPLAN={ 997 | 998 }] [OPTUPSTREAMBAND={ ON | OFF }] [RFIBAND={ { 30M | 40M | 80M | 160M } [,...] | NONE | ALL }] [MAXINTERLEAVEDELAY=0..255] [MINIMPULSENOISEPROTECTION [UPSTREAMMININP={ 0 | 0.5 | 1 | 2 | 4 | 8 | 16 }] [DOWNSTREAMMININP={ 0 | 0.5 | 1 | 2 | 4 | 8 | 16 }]] [DEPLOYMENT={ CABINET | CENTRALOFFICE }] [PSDMASK UPSTREAMPSDMASK={ MASK1 | MASK2 } DOWNSTREAMPSDMASK={ MASK1 | MASK2 }] [DATABOOST={ ON | OFF }] [LINEQUALITYMONITOR={ LOW | MEDIUM | HIGH }] [VPI=0..4095] [VCI=32..65535] [DESCRIPTION=description]	For future release
17	Interface_Mgmt_VDSL	New	SET PROFILE=name VDSLPORT [MODE={ VDSL2 | GLITE | GDMT | T1.413 | ADSL2 | ADSL2+ | AUTO | AUTO2 | ADSL2M | ADSL2+M }] [LINETYPE={ FAST | INTERLEAVE }] [MAXUPSTREAMRATE=32..14848] [MINUPSTREAMRATE=32..14848] [MAXDOWNSTREAMRATE=32..51200] [MINDOWNSTREAMRATE=32..51200] [TARGETSNRMARGIN=snr-margin-dB] [MAXSNRMARGIN={ OFF | snr-margin-dB }] [MINSNRMARGIN={ OFF | snr-margin-dB }] [MAXRECEIVEPOWER={ OFF | value }] [BANDPLAN={ 997 | 998 }] [OPTUPSTREAMBAND={ ON | OFF }] [RFIBAND={ { 30M | 40M | 80M | 160M } [,...] | NONE | ALL }] [MAXINTERLEAVEDELAY=0..255] [MINIMPULSENOISEPROTECTION [UPSTREAMMININP={ 0 | 0.5 | 1 | 2 | 4 | 8 | 16 }] [DOWNSTREAMMININP={ 0 | 0.5 | 1 | 2 | 4 | 8 | 16 }]] [DEPLOYMENT={ CABINET | CENTRALOFFICE }] [PSDMASK UPSTREAMPSDMASK={ MASK1 | MASK2 } DOWNSTREAMPSDMASK={ MASK1 | MASK2 }] [DATABOOST={ ON | OFF }] [LINEQUALITYMONITOR={ LOW | MEDIUM | HIGH }] [VPI=0..4095] [VCI=32..65535] [ADMINSTATE={ UP | DOWN }]	For future release
18	Interface_Mgmt_XE	New	SET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } XE [AUTONEGOTIATION={ ON | OFF }] [FLOWCONTROL={ AUTONEGOTIATE | ON | OFF }] [DESCRIPTION=description]	

No.	Feature	Change	Syntax	Reason for Change
19	Interface_Mgmt_XE	New	SET PORT={ port-list | ALL } XE [WITH LAG=lagname] [AUTONEGOTIATION={ ON | OFF }] [FLOWCONTROL={ AUTONEGOTIATE | ON | OFF }] [DESCRIPTION=description]	
20	LLDP	New	ADD LLDP INTERFACE={ type:id-range | id-range | ifname-list | ALL } OPTIONS [PORTDESC] [SYSNAME] [SYSDESC] [SYSCAP] [PORTVLAN] [VLANNAME] [PROTOVLAN] [PROTOCOL] [MACPHYCONFIGSTATUS] [POWERVIAMDI] [LINKAGGREGATION] [MAXFRAMESIZE] [EPSR] [UCP] [ALL]	
21	LLDP	New	DELETE LLDP INTERFACE={ type:id-range | id-range | ifname-list | ALL } OPTIONS [PORTDESC] [SYSNAME] [SYSDESC] [SYSCAP] [PORTVLAN] [VLANNAME] [PROTOVLAN] [PROTOCOL] [MACPHYCONFIGSTATUS] [POWERVIAMDI] [LINKAGGREGATION] [MAXFRAMESIZE] [EPSR] [UCP] [ALL]	
22	LLDP	New	RESET LLDP COUNTER [INTERFACE={ type:id-range | id-range | ifname-list | ALL }]	
23	LLDP	New	SET LLDP [TXINTERVAL=5..32768] [TXHOLD=2..10] [TXDELAY=1..8192] [REINITDELAY=1..10] [NOTIFYINTERVAL=5..3600]	
24	LLDP	New	SET LLDP INTERFACE={ type:id-range | id-range | ifname-list | ALL } [MODE={ TX | RX | BOTH | OFF }] [NOTIFY={ ON | OFF }]	
25	LLDP	New	SETDEFAULTS LLDP [TXINTERVAL] [TXHOLD] [TXDELAY] [REINITDELAY] [NOTIFYINTERVAL]	
26	LLDP	New	SETDEFAULTS LLDP INTERFACE={ type:id-range | id-range | ifname-list | ALL } [MODE] [NOTIFY]	
27	LLDP	New	SHOW LLDP [INTERFACE [={ type:id-range | id-range | ifname-list | ALL }] [FULL]]	
28	LLDP	New	SHOW LLDP COUNTER [INTERFACE={ type:id-range | id-range | ifname-list | ALL }] [FULL]	
29	NetworkMonitoring	New	SET INTERFACE={ type:id-range | id-range | ifname-list | ALL } PMONALERT VDSL { VTUC [LOFS=0..900] [LOSS=0..900] [LPRS=0..900] [ES=0..900] [SES=0..900] [UAS=0..900] [LOLS=0..900] [FAILEDFASTRETRAIN=threshold] | VTUR [LOFS=0..900] [LOSS=0..900] [LPRS=0..900] [ES=0..900] }	For future release
30	ONU	New	CREATE ONU=onuname ONUID=0..15 INTERFACE={ type:id | id | ifname } MACADDRESS=macaddress	
31	ONU	New	DESTROY ONU={ onuname-list | ALL } [INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL }] [FORCE]	
32	ONU	New	RENAME ONU=onuname TO=onuname	
33	ONU	New	SET ONU=onuname MACADDRESS=macaddress	
34	ONU	New	SHOW ONU [={ onuname-list | ALL }] [ONUID={ 0..15 | ALL }] [INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL }] [MACADDRESS={ macaddress | ALL }] [FULL]	
35	QOSPolicy	New	ADD QOSPOLICY=policyname INTERFACE={ type:id-range | id-range | ifname-list } { BRUUM | IPMC | BIDIRECTIONAL VLAN={ vlanname-list | vid-range | ALL } }	

No.	Feature	Change	Syntax	Reason for Change
36	QOSPolicy	New	CREATE QOSPOLICY=policyname [DESCRIPTION=text] [MAXUPSTREAMRATE={ bits-per-second | MAX }] [MAXDOWNSTREAMRATE={ bits-per-second | MAX }] [MINUPSTREAMRATE={ bits-per-second | MIN }] [MINDOWNSTREAMRATE={ bits-per-second | MIN }] [UPBURSTSIZE={ 1..256 | MAX }] [DOWNBURSTSIZE={ 1..256 | MAX }] [UPDELAYSENSITIVITY={ SENSITIVE | TOLERANT }] [DOWNDELAYSENSITIVITY={ SENSITIVE | TOLERANT }]	
37	QOSPolicy	New	DELETE QOSPOLICY={ policyname-list | ALL } INTERFACE={ type:id-range | id-range | ifname-list | ALL } { BRUUM | IPMC | BIDIRECTIONAL VLAN={ vlanname-list | vid-range | ALL } | ALL }	
38	QOSPolicy	New	DESTROY QOSPOLICY={ policyname-list | ALL } [FORCE]	
39	QOSPolicy	New	RENAME QOSPOLICY=policyname TO=policyname	
40	QOSPolicy	New	SET QOSPOLICY={ policyname-list | ALL } [DESCRIPTION=text] [MAXUPSTREAMRATE={ bits-per-second | MAX }] [MAXDOWNSTREAMRATE={ bits-per-second | MAX }] [MINUPSTREAMRATE={ bits-per-second | MIN }] [MINDOWNSTREAMRATE={ bits-per-second | MIN }] [UPBURSTSIZE={ 1..256 | MAX }] [DOWNBURSTSIZE={ 1..256 | MAX }] [UPDELAYSENSITIVITY={ SENSITIVE | TOLERANT }] [DOWNDELAYSENSITIVITY={ SENSITIVE | TOLERANT }]	
41	QOSPolicy	New	SHOW QOSPOLICY [={ policyname-list | ALL }] [INTERFACE={ type:id-range | id-range | ifname-list | ALL }] [{ BRUUM | IPMC | BIDIRECTIONAL [VLAN={ vlanname-list | vid-range | ALL }] | ALL }] [FULL]	
42	System	New	SET SYSTEM POWERINPUT={ -48VDC | -60VDC }	

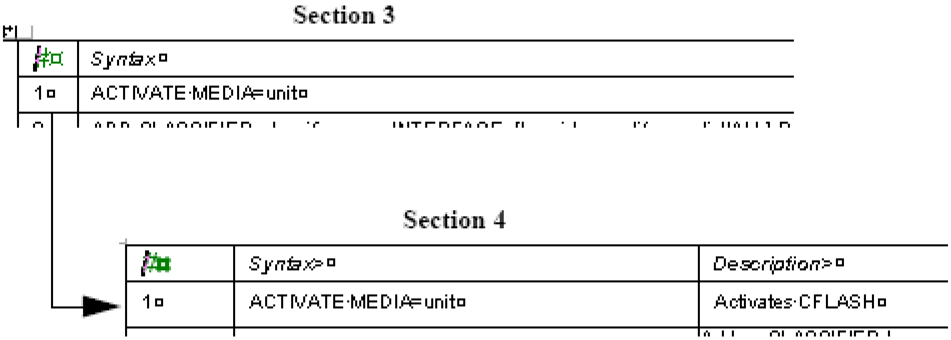
3. Commands Listed By Syntax

3.1 Overview

When inputting commands, the user “builds” a command starting with the verb and then adds a noun, keywords, and parameters. At each stage of building the command, the user can use the help prompt (?) to see what options are available. Listing the commands by syntax follows this building process and allows the user to locate the reference material quickly.

3.2 Commands Listed by Syntax

The following table lists the commands only by syntax and allows the user to easily find a command with the complete syntax. The first column of the table is a record number, which provides a reference number for the command in the next section, which has a description of the command, and a brief description of the parameters. Refer to Figure 3-1.



#	*Syntax*
1	ACTIVATE MEDIA=unit

#	*Syntax>*	*Description>*
1	ACTIVATE MEDIA=unit	Activates CFLASH

FIGURE 3-1 Referencing from Section 3 to Section 4

No.	Level	Syntax
1	Sec_Off	ACTIVATE MEDIA=unit FORCE
2	Manager	ADD CLASSIFIER=classifiername INTERFACE={ type:id-range | id-range | ifname-list | ALL } PRECEDENCE=1..255
3	Manager	ADD DHCPRELAY={ dhcpname | MAIN } VLAN={ vlanname-list | vid-range | ALL }
4	Manager	ADD DHCPRELAY={ dhcpname-list | MAIN | ALL } SERVER=ipaddress-list
5	Manager	ADD EGRESSLIMITER=limitername INTERFACE={ type:id-range | id-range | ifname-list | ALL }
6	Manager	ADD EPSR=epsrdomain INTERFACE={ type:id-range | id-range | ifname-list } [TYPE={ PRIMARY | SECONDARY }]
7	Manager	ADD EPSR=epsrdomain VLAN={ vlanname | vid } [TYPE={ CONTROL | DATA }]
8	Manager	ADD HVLAN={ hvlanname | vid } INTERFACE={ type:id-range | id-range | ifname-list | ALL } [FRAME={ UNTAGGED | TAGGED }]
9	Manager	ADD IGMPSNOOPING FLOODING { ALLSTANDARD | DVMRP | OSPFALL | OSPFDESIGNATED | RIP2 | IGRP | DHCPRELAY | PIM | RSVP | CBT | VRRP | DXCLUSTER | CISCONHAP | HSRP | MDNS | CUSTOM=groupname GROUPADDRESS=ipaddress }
10	Manager	ADD IGMPSNOOPING INTERFACE={ type:id-range | id-range | ifname-list | ALL } MACADDRESS={ macaddress-list | partial-macaddress-list }
11	Manager	ADD INTERFACE={ type:id-range | id-range | ifname-list | ALL } RMONALERT { DROPEVENTS | OCTETS | PACKETS | BROADCAST | MULTICAST | UNDERSIZE | OVERSIZE | CRCALIGN | FRAGMENTS | JABBERS | COLLISIONS | PKTS64OCTETS | PKTS65TO127OCTETS | PKTS128TO255OCTETS | PKTS256TO511OCTETS | PKTS512TO1023OCTETS | PKTS1024TO1518OCTETS } { ABSOLUTE | CHANGE } { INTERVAL=2..3600 RISINGTHRESHOLD=threshold FALLINGTHRESHOLD=threshold }
12	Manager	ADD IP INTERFACE={ MGMT | type:id } IPADDRESS=ipaddress SUBNETMASK=mask [CARD={ slot | ACTCFC }] [IFNAME=ifname] [GATEWAY=ipaddress] [DOMAINNAME=name] [DNS=ipaddress-list]
13	Manager	ADD LAG=lagname INTERFACE={ type:id-range | id-range | ifname-list }
14	Manager	ADD LLDP INTERFACE={ type:id-range | id-range | ifname-list | ALL } OPTIONS [PORTDESC] [SYSNAME] [SYSDESC] [SYSCAP] [PORTVLAN] [VLANNAME] [PROTOVLAN] [PROTOCOL] [MACPHYCONFIGSTATUS] [POWERVIAMDI] [LINKAGGREGATION] [MAXFRAMESIZE] [EPSR] [UCP] [ALL]
15	Manager	ADD MLPPP=mlpppname INTERFACE={ type:id-range | id-range | ifname-list } [FORCE]
16	Manager	ADD PPP INTERFACE={ type:id-range | id-range | ifname-list } [RESTARTINTERVAL=seconds] [MAXTERMINATE={ value | CONTINUOUS }] [MAXCONFIGURE=value] [MAXFAILURE={ value | CONTINUOUS }] [ECHOREQUEST={ seconds | OFF }]
17	Manager	ADD PROTECTIONGROUP=groupname INTERFACE={ type:id-range | id-range | ifname-list }
18	Manager	ADD QOSPOLICY=policyname INTERFACE={ type:id-range | id-range | ifname-list } { BRUUM | IPMC | BIDIRECTIONAL VLAN={ vlanname-list | vid-range | ALL } }
19	Sec_Off	ADD RADIUS SERVER={ ipaddress-list | hostname-list } SECRET=secret [AUTHPORT=1..65535] [ACCTPORT=1..65535] [RETRIES=0..10] [TIMEOUT=1..60] [AUTHENTICATION={ ON | OFF }] [ACCOUNTING={ ON | OFF }]
20	Manager	ADD STP INSTANCE={ stpname | mstid } VLAN={ vlanname | vid-range }
21	Sec_Off	ADD TACPLUS SERVER={ ipaddress-list | hostname-list } KEY=key [PORT=1..65535] [RETRIES=0..10] [TIMEOUT=1..60] [AUTHENTICATION={ ON | OFF }] [AUTHORIZATION={ ON | OFF }] [ACCOUNTING={ ON | OFF }]
22	Manager	ADD TRACE EPSR [={ epsrdomain-list | ALL }] MESSAGETYPE={ HEALTH | RINGUPFLUSH | RINGDOWNFLUSH | LINKDOWN | ALL } [INTERFACE={ type:id-range | id-range | ifname-list | ALL }]

<table>
<tr><th>No.</th><th>Level</th><th>Syntax</th></tr>
<tr><td>23</td><td>Manager</td><td>ADD TRACE IGMPSNOOPING MESSAGETYPE={ REPORTV1 | REPORTV2 | LEAVE | GENERALQUERY | LASTMEMBERQUERY | ALL } [INTERFACE={ type:id-range | id-range | ifname-list | ALL }] [MACADDRESS={ macaddress | ALL }] [GROUPADDRESS={ ipaddress | ALL }]</td></tr>
<tr><td>24</td><td>Manager</td><td>ADD TRACE PPP [EVENT={ PORT | LCP | BCP | ECHO | FRAME | TIMER | ERRPROTO | MAIN | ALL }] [INTERFACE={ type:id-range | id-range | ifname-list | ALL }]</td></tr>
<tr><td>25</td><td>Manager</td><td>ADD TRACE VOICECALL [EVENT={ OPENLOOP | CLOSELOOP | MGCPOFFHOOK | MGCPONHOOK | MODEMDETECT | ALL }] [INTERFACE={ type:id-range | id-range | ifname-list | ALL }]</td></tr>
<tr><td>26</td><td>Sec_Off</td><td>ADD USER=login-name PASSWORD=password [FORMAT={ CLEARTEXT | MD5 }] [DESCRIPTION=description] [PRIVILEGE={ USER | MANAGER | SECURITYOFFICER }] [LOGIN={ TRUE | FALSE | ON | OFF | YES | NO }] [TELNET={ YES | NO }] [PWDAGEING={ OFF | 0 | 1..365 }] [DEACTIVATE={ OFF | yyyy-mm-dd }]</td></tr>
<tr><td>27</td><td>Sec_Off</td><td>ADD USER=login-name PASSWORD=password [FORMAT={ CLEARTEXT | MD5 }] [DESCRIPTION=description] [PRIVILEGE={ USER | MANAGER | SECURITYOFFICER }] [LOGIN={ TRUE | FALSE | ON | OFF | YES | NO }] [TELNET={ YES | NO }] [SSH={ YES | NO } [PUBLICKEY=key-name]] [PWDAGEING={ OFF | 0 | 1..365 }] [DEACTIVATE={ OFF | yyyy-mm-dd }]</td></tr>
<tr><td>28</td><td>Manager</td><td>ADD VC=vcid INTERFACE={ type:id-range | id-range | ifname-list } VPI=0..255 VCI=32..65535 [TXPEAKCELLRATE={ 150..65535 | MAX }]</td></tr>
<tr><td>29</td><td>Manager</td><td>ADD VLAN={ vlanname | vid } INTERFACE={ type:id-range | id-range | ifname-list | ALL } [FRAME={ UNTAGGED | TAGGED }] [TRANSLATE={ 1..4094 }] [FORWARDING={ PRIMARYUPSTREAM | SECONDARYUPSTREAM | DOWNSTREAM | STP | UCP }]</td></tr>
<tr><td>30</td><td>Manager</td><td>ADD VLANTUNNELMAP VLAN={ vlanname-list | vid-range } HVLAN={ hvlanname | vid } [INTERFACE={ type:id-range | id-range | ifname-list }]</td></tr>
<tr><td>31</td><td>Manager</td><td>ADD ACCESSLIST=accesslistname INTERFACE={ type:id-range | id-range | ifname-list }</td></tr>
<tr><td>32</td><td>Manager</td><td>ADD ACCESSLIST=accesslistname RULE { PERMIT | DENY } [IPSOURCE={ ipaddress| ANY } [SOURCEMASK=mask]] [IPDEST={ ipaddress | ANY } [DESTMASK=mask]] [MACSOURCE={ macaddress | ANY }] [MACDEST={ macaddress | ANY }] [APPLICATION={ DHCPSERVER | DHCPCLIENT | NETBIOS | FUM | TELNET | SSH | SNMP| FTP | TFTP }] [TCPPORTDEST={ tcp-port-list | ANY }] [TCPPORTSOURCE={tcp-port | ANY }] [UDPPORTDEST={ udp-port-list | ANY }] [UDPPORTSOURCE={ udp-port | ANY }] [PROTOCOL={ IPV4 | IPV6 | protocol-type | ANY }] [IPPROTOCOL={ TCP | UDP | ICMP | IGMP | ipprotocol-type | ANY }] [BEFORE=rulenumber]</td></tr>
<tr><td>33</td><td>Manager</td><td>ADD ACTION CLASSIFIER=classifiername-list { DROP | FORWARD | COUNT |SETVPRIORITY=0..7 | SETIPTOS=0..7 | SETIPDSCP=0..63 | MOVEPRIOTOTOS | MOVETOSTOPRIO }</td></tr>
<tr><td>34</td><td>Manager</td><td>ADD CLASSIFIER=classifiername PORT={port-list|ALL} PRECEDENCE=1..255</td></tr>
<tr><td>35</td><td>Manager</td><td>ADD INTERFACE={ type:id-range | id-range | ifname-list | ALL } COUNTER HISTORY INTERVAL=interval-list [BUCKETS=1..2700]</td></tr>
<tr><td>36</td><td>User</td><td>ADD LOG FILTER={filterid-list|ALL} OUTPUT=outputid</td></tr>
<tr><td>37</td><td>Sec_Off</td><td>ADD SNMP COMMUNITY=name [TRAPHOST=ipaddress-list] [V2CTRAPHOST=ipaddress-list] [MANAGER=ipaddress-list]</td></tr>
<tr><td>38</td><td>Manager</td><td>ADD SNTP SERVER={ipaddress|hostname}</td></tr>
<tr><td>39</td><td>Manager</td><td>ADD TRAFFICDESCRIPTOR=tdname CLASSIFIER=classifiername-list {NCDROP | NCFORWARD} [NCCOUNT={ON|OFF}]</td></tr>
<tr><td>40</td><td>User</td><td>AUDIT FILES</td></tr>
<tr><td>41</td><td>Sec_Off</td><td>BACKUP CONFIG FILE={ destinationfile | unit:destinationfile }</td></tr>
<tr><td>42</td><td>Sec_Off</td><td>BACKUP DATABASE FILE={ destinationfile | unit:destinationfile | serverpath/destinationfile } [{ TFTP SERVER={ ipaddress | hostname } | ZMODEM | FTP SERVER={ ipaddress | hostname } USER=userid PASSWORD=password }]</td></tr>
</table>

<table>
<tr><th>No.</th><th>Level</th><th>Syntax</th></tr>
<tr><td>43</td><td>Manager</td><td>CLEAR ALARMS CARD={ slot-list | ALL } MCASTGROUPLIMIT</td></tr>
<tr><td>44</td><td>Manager</td><td>CLEAR ALARMS PROTECTIONGROUP={ groupname-list | ALL }</td></tr>
<tr><td>45</td><td>Manager</td><td>CLEAR DHCPRELAY INTERFACE={ type:id-range | id-range | ifname-list | ALL } { [IPADDRESS={ ipaddress-list | ALL }] | [MACADDRESS={ macaddress | ALL }] }</td></tr>
<tr><td>46</td><td>Manager</td><td>CLEAR DIAGNOSTICS [FORCE]</td></tr>
<tr><td>47</td><td>Manager</td><td>CLEAR IP ARP [={ ipaddress-list | ALL }] [INTERFACE={ type:id-range | ifname-list | MGMT | ALL }] [FORCE]</td></tr>
<tr><td>48</td><td>Manager</td><td>CLEAR TRACE [FORCE]</td></tr>
<tr><td>49</td><td>Manager</td><td>CLEAR SWITCH FDB [INTERFACE={type:id-range|id-range|ifname-list| ALL}] [ADDRESS=macaddress] [HVLAN={hvlanname|vid}]</td></tr>
<tr><td>50</td><td>Manager</td><td>CLEAR SWITCH FDB [INTERFACE={type:id-range|id-range|ifname-list| ALL}] [ADDRESS=macaddress] [VLAN={vlanname|vid}]</td></tr>
<tr><td>51</td><td>Manager</td><td>CONNECT INTERFACE={ type:id | ifname } TO={ type:id | ifname }</td></tr>
<tr><td>52</td><td>Manager</td><td>COPY FILE={ sourcefile | unit:sourcefile } TO={ destinationfile | unit:destinationfile }</td></tr>
<tr><td>53</td><td>Manager</td><td>CREATE ALIAS=aliasname STRING=substitution</td></tr>
<tr><td>54</td><td>Manager</td><td>CREATE CARD=slot CES8 [{ [PREFLOAD=filename] [ADMINSTATE={ UP | DOWN }] [PORTTYPE={ DS1 | E1 }] | PROFILE=name }]</td></tr>
<tr><td>55</td><td>Manager</td><td>CREATE CARD=slot NTE8 [{ [PREFLOAD=filename] [ADMINSTATE={ UP | DOWN }] [PORTTYPE={ DS1 | E1 }] | PROFILE=name }]</td></tr>
<tr><td>56</td><td>Manager</td><td>CREATE CARD=slot SHDSL16 [{ [PREFLOAD=filename] [WETTINGCURRENT={ ON | OFF }] [ANNEXTYPE={ A | B }] [WIREMODE={ NORMAL | BONDED }] [ADMINSTATE={ UP | DOWN }] | PROFILE=name }]</td></tr>
<tr><td>57</td><td>Manager</td><td>CREATE CARD=slot SHDSL24 [{ [PREFLOAD=filename] [WETTINGCURRENT={ ON | OFF }] [ANNEXTYPE={ A | B }] [WIREMODE={ NORMAL | BONDED }] [ADMINSTATE={ UP | DOWN }] | PROFILE=name }]</td></tr>
<tr><td>58</td><td>Manager</td><td>CREATE CONTACTALARM={ 0..2 } STATE={ OPEN | CLOSED } SEVERITY={ CRITICAL | MAJOR | MINOR | INFO } [MESSAGE=text]</td></tr>
<tr><td>59</td><td>Manager</td><td>CREATE DHCPRELAY=dhcpname [AGENT REMOTEID={ remote-id | DEFAULT }] [MODE={ RELAY | SNOOPING }] [SERVER={ ipaddress-list | NONE }] [VLAN={ vlanname-list | vid-range | ALL }]</td></tr>
<tr><td>60</td><td>Manager</td><td>CREATE EGRESSLIMITER=limitername RATE=bits-per-second BURSTSIZE={ 4KB | 8KB | 16KB | 32KB | 64KB | 128KB | 256KB | 512KB | 1MB | 2MB | 4MB | 8MB | 16MB | 32MB | 64MB }</td></tr>
<tr><td>61</td><td>Manager</td><td>CREATE EPSR=epsrdomain { TRANSIT | MASTER [HELLOTIME=value] [FAILOVERTIME=value] [RINGFLAPTIME=value] }</td></tr>
<tr><td>62</td><td>Manager</td><td>CREATE HVLAN=hvlanname VID=2..4094 [TYPE={ PORTTUNNEL | VLANTUNNEL }]</td></tr>
<tr><td>63</td><td>Manager</td><td>CREATE LOG OUTPUT=outputid [{ CLI [FORMAT={ FULL | MSGONLY | SUMMARY }] | CONSOLE [FORMAT={ FULL | MSGONLY | SUMMARY }] | SYSLOG SERVER={ ipaddress | hostname } | FILE=unit:filename [FORMAT={ FULL | MSGONLY | SUMMARY }] }]</td></tr>
<tr><td>64</td><td>Manager</td><td>CREATE MLPPP=mlpppname ID=8..15 INTERFACE={ type:id-range | id-range | ifname-list } [SEGMENTSIZE={ 64..1526 }] [SEQUENCENUMBERBITS={ 12 | 24 }] [FORCE]</td></tr>
<tr><td>65</td><td>Manager</td><td>CREATE ONU=onuname ONUID=0..15 INTERFACE={ type:id | id | ifname } MACADDRESS=macaddress</td></tr>
</table>

<table>
<tr><th>No.</th><th>Level</th><th>Syntax</th></tr>
<tr><td>66</td><td>Manager</td><td>CREATE PROFILE=name ADSLPORT [MODE={ GLITE | GDMT | T1.413 | ADSL2 | ADSL2+ | AUTO | AUTO2+ | ADSL2M | ADSL2+M }] [BITMAPMODE={ FBM | DBM }] [LINETYPE={ FAST | INTERLEAVE }] [INTERLEAVEDELAY=1..64] [ECHOCANCELLATION={ ON | OFF }] [DATABOOST={ ON | OFF }] [MAXUPSTREAMRATE=32..3072] [MINUPSTREAMRATE=32..3072] [MAXDOWNSTREAMRATE=32..26624] [MINDOWNSTREAMRATE=32..26624] [TARGETSNRMARGIN=0..15] [MAXSNRMARGIN={ OFF | 1..30 }] [LINEQUALITYMONITOR={ LOW | MEDIUM | HIGH }] [VPI=0..4095] [VCI=32..65535] [ADMINSTATE={ UP | DOWN }]</td></tr>
<tr><td>67</td><td>Manager</td><td>CREATE PROFILE=name cardtype [PREFLOAD=filename] [ADMINSTATE={ UP | DOWN }]</td></tr>
<tr><td>68</td><td>Manager</td><td>CREATE PROFILE=name DS1PORT [ADMINSTATE={ UP CREATE PROFILE=name DS1PORT [ADMINSTATE={ UP | DOWN }] [TIMINGREFERENCE={ SELF | CONNECTION | CARD }] [LINEENCODING={ B8ZS | AMI }] [LINEBUILDOUT { LONGHAUL={ 0.0DB | -7.5DB | -15.0DB | -22.5DB } | SHORTHAUL={ 133FT | 266FT | 399FT | 533FT | 655FT } }] [FRAMING={ UNFRAMED | SF | ESF | STANDARD }] | DOWN }] [TIMINGREFERENCE={ SELF | CONNECTION | CARD }] [LINEBUILDOUT { LONGHAUL={ 0.0DB | -7.5DB | -15.0DB | -22.5DB } | SHORTHAUL={ 133FT | 266FT | 399FT | 533FT | 655FT } }] [LINEENCODING={ B8ZS | AMI }] [LOOPBACK={ NONE | INWARD | LINE }]</td></tr>
<tr><td>69</td><td>Manager</td><td>CREATE PROFILE=name E1PORT [ADMINSTATE={ UP | DOWN }] [TIMINGREFERENCE={ SELF | CONNECTION | CARD }] [LINEENCODING={ HDB3 | AMI }] [FRAMING={ UNFRAMED | E1 | E1CRC | STANDARD }]</td></tr>
<tr><td>70</td><td>Manager</td><td>CREATE PROFILE=name EPONPORT [ADMINSTATE={ UP | DOWN }] [IPMCVLAN={ vlanname | vid }] [IPADDRESS=ipaddress]</td></tr>
<tr><td>71</td><td>Manager</td><td>CREATE PROFILE=name FEPORT [ADMINSTATE={ UP | DOWN }] [AUTONEGOTIATION={ ON | OFF }] [SPEED={ AUTONEGOTIATE | 10 | 100 }] [DUPLEX={ AUTONEGOTIATE | FULL | HALF }] [FLOWCONTROL={ AUTONEGOTIATE | ON | OFF }]</td></tr>
<tr><td>72</td><td>Manager</td><td>CREATE PROFILE=name FXPORT [FLOWCONTROL={ ON | OFF }] [ADMINSTATE={ UP | DOWN }]</td></tr>
<tr><td>73</td><td>Manager</td><td>CREATE PROFILE=name GEPORT [AUTONEGOTIATION={ ON | OFF }] [SPEED={ AUTONEGOTIATE | 10 | 100 | 1000 }] [DUPLEX={ AUTONEGOTIATE | FULL | HALF }] [FLOWCONTROL={ AUTONEGOTIATE | ON | OFF }] [ADMINSTATE={ UP | DOWN }]</td></tr>
<tr><td>74</td><td>Manager</td><td>CREATE PROFILE=name NTE8 [PREFLOAD=filename] [ADMINSTATE={ UP | DOWN }] [PORTTYPE={ DS1 | E1 }]</td></tr>
<tr><td>75</td><td>Manager</td><td>CREATE PROFILE=name POTSPORT [CAPABILITY={ PCMU | G726 | ALL }] [MINPACKETIZATION=10..30] [MAXPACKETIZATION=10..30] [BUFFERDELAY=0..150] [BUFFERMODE={ STATIC | DYNAMIC }] [TXPREECHOGAIN=-9.0..+3.0] [TXPOSTECHOGAIN=-9.0..+3.0] [RXPREECHOGAIN=-9.0..+3.0] [RXPOSTECHOGAIN=-9.0..+3.0] [ECHOCANCELLATION={ ON | OFF }] [VOICEACTIVITYDETECTION={ ON | OFF }] [COMFORTNOISEGENERATION={ ON | OFF }] [PACKETLOSSCONCEALMENT={ ON | OFF }] [ADMINSTATE={ UP | DOWN }]</td></tr>
<tr><td>76</td><td>Manager</td><td>CREATE PROFILE=name SHDSL16 [PREFLOAD=filename] [ADMINSTATE={ UP | DOWN }] [WETTINGCURRENT={ ON | OFF }] [ANNEXTYPE={ A | B }] [WIREMODE={ NORMAL | BONDED }]</td></tr>
<tr><td>77</td><td>Manager</td><td>CREATE PROFILE=name SHDSL24 [PREFLOAD=filename] [ADMINSTATE={ UP | DOWN }] [WETTINGCURRENT={ ON | OFF }] [ANNEXTYPE={ A | B }] [WIREMODE={ NORMAL | BONDED }]</td></tr>
<tr><td>78</td><td>Manager</td><td>CREATE PROFILE=name SHDSLPORT [MAXCONNECTRATE=72..2312] [MINCONNECTRATE=72..2312] [TARGETSNRMARGIN=0..10] [LINEQUALITYMONITOR={ LOW | MEDIUM | HIGH }] [VPI=0..4095] [VCI=32..65535] [ADMINSTATE={ UP | DOWN }]</td></tr>
<tr><td>79</td><td>Manager</td><td>CREATE PROFILE=name VDSLPORT [MODE={ VDSL2 | GLITE | GDMT | T1.413 | ADSL2 | ADSL2+ | AUTO | AUTO2 | ADSL2M | ADSL2+M }] [LINETYPE={ FAST | INTERLEAVE }] [MAXUPSTREAMRATE=32..14848] [MINUPSTREAMRATE=32..14848] [MAXDOWNSTREAMRATE=32..51200] [MINDOWNSTREAMRATE=32..51200] [TARGETSNRMARGIN=snr-margin-dB] [MAXSNRMARGIN={ OFF | snr-margin-dB }] [MINSNRMARGIN={ OFF | snr-margin-dB }] [MAXRECEIVEPOWER={ OFF | value }] [BANDPLAN={ 997 | 998 }] [OPTUPSTREAMBAND={ ON | OFF }] [RFIBAND={ { 30M | 40M | 80M | 160M } [,...] | NONE | ALL }] [MAXINTERLEAVEDELAY=0..255] [MINIMPULSENOISEPROTECTION UPSTREAMMININP={ 0 | 0.5 | 1 | 2 | 4 | 8 | 16 } DOWNSTREAMMININP={ 0 | 0.5 | 1 | 2 | 4 | 8 | 16 }] [DEPLOYMENT={ CABINET | CENTRALOFFICE }] [PSDMASK UPSTREAMPSDMASK={ MASK1 | MASK2 } DOWNSTREAMPSDMASK={ MASK1 | MASK2 }] [DATABOOST={ ON | OFF }] [LINEQUALITYMONITOR={ LOW | MEDIUM | HIGH }] [VPI=0..4095] [VCI=32..65535] [ADMINSTATE={ UP | DOWN }]</td></tr>
<tr><td>80</td><td>Manager</td><td>CREATE PROFILE=name XEPORT [AUTONEGOTIATION={ ON | OFF }] [FLOWCONTROL={ AUTONEGOTIATE | ON | OFF }] [ADMINSTATE={ UP | DOWN }]</td></tr>
</table>

No.	Level	Syntax
81	Manager	CREATE PROTECTIONGROUP=groupname
82	Manager	CREATE PSPAN=pspanname PSPANID=0..127 SATOP { INTERFACE={ VLAN:id | id | ifname } | IPADDRESS=ipaddress } { UDPPORT=49152..65535 } { PEERIPADDRESS=ipaddress } { PEERUDPPORT=49152..65535 } [NUMBYTES=16..1023] [JITTERBUFFER=value] [TIMINGREFERENCE={ SELF | CONNECTION | CARD }] [RTP={ ON | OFF }] [VPRIORITY=0..7] [IPDSCP=0..63]
83	Manager	CREATE QOSPOLICY=policyname [DESCRIPTION=text] [MAXUPSTREAMRATE={ bits-per-second | MAX }] [MAXDOWNSTREAMRATE={ bits-per-second | MAX }] [MINUPSTREAMRATE={ bits-per-second | MIN }] [MINDOWNSTREAMRATE={ bits-per-second | MIN }] [UPBURSTSIZE={ 1..256 | MAX }] [DOWNBURSTSIZE={ 1..256 | MAX }] [UPDELAYSENSITIVITY={ SENSITIVE | TOLERANT }] [DOWNDELAYSENSITIVITY={ SENSITIVE | TOLERANT }]
84	Manager	CREATE STP INSTANCE=stpname MSTID=1..4094 [PRIORITY=0..65535]
85	Manager	CREATE TRAFFICDESCRIPTOR=tdname RATE=bits-per-second BURSTSIZE={ 4KB | 8KB | 16KB | 32KB | 64KB | 128KB | 256KB | 512KB | 1MB | 2MB | 4MB | 8MB | 16MB | 32MB | 64MB }
86	Manager	CREATE ACCESSLIST=accesslistname [RULE { PERMIT | DENY } [IPSOURCE={ipaddress | ANY } [SOURCEMASK=mask]] [IPDEST={ ipaddress | ANY } [DESTMASK=mask]] [MACSOURCE={ macaddress | ANY }] [MACDEST={ macaddress| ANY }] [APPLICATION={ DHCPSERVER | DHCPCLIENT | NETBIOS | FUM | TELNET| SSH | SNMP | FTP | TFTP }] [TCPPORTDEST={ tcp-port-list | ANY }] [TCPPORTSOURCE={ tcp-port | ANY }] [UDPPORTDEST={ udp-port-list | ANY }][UDPPORTSOURCE={ udp-port | ANY }] [PROTOCOL={ IPV4 | IPV6 | protocol-type | ANY }] [IPPROTOCOL={ TCP | UDP | ICMP | IGMP | ipprotocol-type |ANY }]] [INTERFACE={ type:id-range | id-range | ifname-list }]
87	Manager	CREATE CARD=slot card_type [{[PREFLOAD=filename] [ADMINSTATE={UP|DOWN}]| PROFILE=name}]
88	Manager	CREATE CLASSIFIER=classifiername[VID={1..4095|ANY}] [VPRIORITY={0..7|ANY}] [INNERVID={1..4095|ANY}] [INNERVPRIORITY={0..7|ANY}] [ETHFORMAT={802.3|802.3TAGGED|802.3UNTAGGED |ETHII|ETHIITAGGED|ETHIIUNTAGGED |ANY}] [LSAP={NETBIOS|lsap-value|ANY}] [IPDEST={ipaddress-mask|MULTICAST|ANY}] [IPSOURCE={ipaddress-mask|ANY}] [IPDSCP={0..63|ANY}] [IPPROTOCOL={TCP|UDP|ICMP|IGMP| ipprotocol-number|ANY}] [IPTOS={0..7|ANY}] [MACDEST={macaddress|MULTICAST|ANY}] [MACSOURCE={macaddress|ANY}] [PROTOCOL={IPV4|IPV6|protocol-type|ANY}] [TCPPORTDEST={tcp-port-list|ANY}] [TCPPORTSOURCE={tcp-port|ANY}][TCPFLAGS={{URG|ACK|RST|SYN|FIN|PSH}[,...] |ANY}] [UDPPORTDEST={udp-port-list|ANY}] [UDPPORTSOURCE={udp-port|ANY}]
89	Manager	CREATE LAG=lagname [INTERFACE={ type:id-range | id-range | ifname-list }][MODE={ ON | OFF | PASSIVE | ACTIVE }] [SELECT={ MACSRC | MACDEST |MACBOTH | IPSRC | IPDEST | IPBOTH | PORTSRC | PORTDEST }] [ADMINKEY=1..1024]
90	User	CREATE LOG FILTER=filterid [CATEGORY=category] [SEVERITY=[op]{CRITICAL|MAJOR|MINOR|NONE}]
91	User	CREATE LOG OUTPUT=outputid [{CLI [FORMAT={FULL|MSGONLY|SUMMARY}]| CONSOLE [FORMAT={FULL|MSGONLY|SUMMARY}]| SYSLOG SERVER={ipaddress|hostname}}]
92	Sec_Off	CREATE SNMP COMMUNITY=name [ACCESS={READ|WRITE}] [V2CTRAPHOST=ipaddress-list] [TRAPHOST=ipaddress-list] [MANAGER=ipaddress-list]
93	Manager	CREATE VLAN=vlanname VID=2..4094 [FORWARDINGMODE={STD|UPSTREAMONLY}]
94	Manager	DEACTIVATE MEDIA=unit [FORCE]
95	Sec_Off	DEACTIVATE SESSION={session-list|ALL} [{CANCEL|[MESSAGE=message-text][DELAY=1..600]}]
96	Manager	DELETE CLASSIFIER=classifiername-list INTERFACE={ type:id-range | id-range | ifname-list | ALL }
97	Manager	DELETE DHCPRELAY={ dhcpname-list | MAIN | ALL } SERVER={ ipaddress-list | ALL } [FORCE]
98	Manager	DELETE DHCPRELAY={ dhcpname-list | MAIN | ALL } VLAN={ vlanname-list | vid-range | ALL }
99	Manager	DELETE EGRESSLIMITER=limitername INTERFACE={ type:id-range | id-range | ifname-list | ALL }

No.	Level	Syntax
100	Manager	DELETE EPSR={ epsrdomain-list | ALL } INTERFACE={ type:id-range | id-range | ifname-list | ALL }
101	Manager	DELETE EPSR={ epsrdomain-list | ALL } VLAN={ vlanname | vid | ALL }
102	Manager	DELETE FILES={ filename-pattern | unit:filename-pattern } [FORCE]
103	Manager	DELETE HVLAN={ hvlanname | vid } INTERFACE={ type:id-range | id-range | ifname-list | ALL }
104	Manager	DELETE IGMPSNOOPING FLOODING { ALL | ALLSTANDARD | DVMRP | OSPFALL | OSPFDESIGNATED | RIP2 | IGRP | DHCPRELAY | PIM | RSVP | CBT | VRRP | DXCLUSTER | CISCONHAP | HSRP | MDNS | CUSTOM=groupname }
105	Manager	DELETE IGMPSNOOPING INTERFACE={ type:id-range | id-range | ifname-list | ALL } MACADDRESS={ macaddress-list | partial-macaddress-list | ALL }
106	Manager	DELETE INTERFACE={ type:id-range | id-range | ifname-list | ALL } COUNTER HISTORY [INTERVAL={ interval-list | ALL }]
107	Manager	DELETE IP INTERFACE={ MGMT | type:id-range | ifname-list | ALL } [FORCE]
108	Manager	DELETE LLDP INTERFACE={ type:id-range | id-range | ifname-list | ALL } OPTIONS [PORTDESC] [SYSNAME] [SYSDESC] [SYSCAP] [PORTVLAN] [VLANNAME] [PROTOVLAN] [PROTOCOL] [MACPHYCONFIGSTATUS] [POWERVIAMDI] [LINKAGGREGATION] [MAXFRAMESIZE] [EPSR] [UCP] [ALL]
109	Manager	DELETE MLPPP={ mlpppname-list | ALL } INTERFACE={ type:id-range | id-range | ifname-list | ALL } [FORCE]
110	Manager	DELETE PPP INTERFACE={ type:id-range | id-range | ifname-list } [FORCE]
111	Manager	DELETE PROTECTIONGROUP=groupname INTERFACE={ type:id-range | id-range | ifname-list | ALL }
112	Manager	DELETE QOSPOLICY={ policyname-list | ALL } INTERFACE={ type:id-range | id-range | ifname-list | ALL } { BRUUM | IPMC | BIDIRECTIONAL VLAN={ vlanname-list | vid-range | ALL } | ALL }
113	Manager	DELETE STP INSTANCE={ stpname | mstid | ALL } VLAN={ vlanname | vid-range | ALL }
114	Manager	DELETE TRACE EPSR [={ epsrdomain-list | ALL }] [MESSAGETYPE={ HEALTH | RINGUPFLUSH | RINGDOWNFLUSH | LINKDOWN | ALL }] [INTERFACE={ type:id-range | id-range | ifname-list | ALL }]
115	Manager	DELETE TRACE IGMPSNOOPING [MESSAGETYPE={ REPORTV1 | REPORTV2 | LEAVE | GENERALQUERY | LASTMEMBERQUERY | ALL }] [INTERFACE={ type:id-range | id-range | ifname-list | ALL }] [MACADDRESS={ macaddress | ALL }] [GROUPADDRESS={ ipaddress | ALL }]
116	Manager	DELETE TRACE PPP [EVENT={ PORT | LCP | BCP | ECHO | FRAME | TIMER | ERRPROTO | MAIN | ALL }] [INTERFACE={ type:id-range | id-range | ifname-list | ALL }]
117	Manager	DELETE TRACE VOICECALL [EVENT={ OPENLOOP | CLOSELOOP | MGCPOFFHOOK | MGCPONHOOK | MODEMDETECT | ALL }] [INTERFACE={ type:id-range | id-range | ifname-list | ALL }]
118	Manager	DELETE TRAFFICDESCRIPTOR={ tdname-list | ALL } CLASSIFIER={ classifiername-list | ALL }
119	Manager	DELETE VC={ vcid-range | ALL } INTERFACE={ type:id-range | id-range | ifname-list | ALL } [FORCE]
120	Manager	DELETE VLANTUNNELMAP VLAN={ vlanname-list | vid-range | ALL } HVLAN={ hvlanname | vid } [INTERFACE={ type:id-range | id-range | ifname-list | ALL }]
121	Manager	DELETE ACCESSLIST={ accesslistname-list | ALL } INTERFACE={ type:id-range |id-range | ifname-list }
122	Manager	DELETE ACCESSLIST=accesslistname RULE=rulenumber
123	Manager	DELETE ACTION CLASSIFIER=classifiername-list {DROP|FORWARD|COUNT| SETVPRIORITY|SETIPTOS|SETIPDSCP| MOVEPRIOTOTOS|MOVETOSTOPRIO|ALL}
124	Manager	DELETE CLASSIFIER=classifiername-list PORT={port-list|ALL}

No.	Level	Syntax
125	Manager	DELETE INTERFACE={ type:id-range | id-range | ifname-list | ALL } RMONALERT { DROPEVENTS | OCTETS | PACKETS | BROADCAST | MULTICAST | UNDERSIZE | OVERSIZE | CRCALIGN | FRAGMENTS | JABBERS COLLISIONS | PKTS64OCTETS | PKTS65TO127OCTETS | PKTS128TO255OCTETS | PKTS256TO511OCTETS | PKTS512TO1023OCTETS | PKTS1024TO1518OCTETS | ALL }
126	Manager	DELETE LAG=lagname INTERFACE={ type:id-range | id-range | ifname-list | ALL}
127	User	DELETE LOG FILTER={filterid-list|ALL} OUTPUT=outputid
128	Manager	DELETE NONPREFLOADS
129	Sec_Off	DELETE RADIUS SERVER={ ipaddress-list | hostname-list | ALL }
130	Sec_Off	DELETE SNMP COMMUNITY=name [TRAPHOST=ipaddress-list] [V2CTRAPHOST=ipaddress-list] [MANAGER=ipaddress-list]
131	Manager	DELETE SNTP SERVER
132	Sec_Off	DELETE TACPLUS SERVER={ ipaddress-list | hostname-list | ALL }
133	Sec_Off	DELETE USER=login-name
134	Manager	DELETE VLAN={ vlanname | vid } INTERFACE={ type:id-range | id-range |ifname-list | ALL }
135	Manager	DESTROY PROFILE=name cardtype
136	Manager	DESTROY ALIAS={ aliasname-list | ALL }
137	Manager	DESTROY CONTACTALARM={ 0..2 } STATE={ OPEN | CLOSED }
138	Manager	DESTROY DHCPRELAY={ dhcpname-list | ALL } [FORCE]
139	Manager	DESTROY DHCPRELAY={ dhcpname-list | ALL } [FORCE]
140	Manager	DESTROY EPSR={ epsrdomain-list | ALL }
141	Manager	DESTROY MLPPP={ mlpppname-list | ALL } [FORCE]
142	Manager	DESTROY ONU={ onuname-list | ALL } [INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL }] [FORCE]
143	Manager	DESTROY PROFILE=name port_type
144	Manager	DESTROY PROTECTIONGROUP={ groupname-list | ALL } [FORCE]
145	Manager	DESTROY PSPAN [={ pspanname-list | ALL }] [INTERFACE={ type:id-range | ifname-list | ALL }] [FORCE]
146	Manager	DESTROY QOSPOLICY={ policyname-list | ALL } [FORCE]
147	Manager	DESTROY STP INSTANCE={ stpname | mstid | ALL }
148	Manager	DESTROY TRAFFICDESCRIPTOR={ tdname-list | ALL }
149	Manager	DESTROY ACCESSLIST={ accesslistname-list | ALL } [FORCE]
150	Manager	DESTROY CARD=slot-list [FORCE]
151	Manager	DESTROY CLASSIFIER={classifiername-list|ALL}

No.	Level	Syntax
152	Manager	DESTROY EGRESSLIMITER={limitername-list|ALL}
153	Manager	DESTROY HVLAN={hvlanname|vid|ALL}
154	Manager	DESTROY LAG=lagname
155	User	DESTROY LOG FILTER={filterid-list|ALL}
156	User	DESTROY LOG OUTPUT={outputid-list|ALL}
157	Sec_Off	DESTROY SNMP COMMUNITY=name
158	Manager	DESTROY VLAN={vlanname|vid|ALL}
159	Manager	DIAGNOSE INTERFACE={ type:id-range | id-range | ifname-list }
160	Manager	DIAGNOSE CARD={slot-list|ALL} {INSERVICE|OUTOFSERVICE}
161	Manager	DIAGNOSE MEDIA=unit
162	Manager	DISABLE DHCPRELAY={ dhcpname-list | MAIN | ALL } INTERFACE={ type:id-range | id-range | ifname-list | ALL
163	Manager	DISABLE EPSR={ epsrdomain-list | ALL }
164	Manager	DISABLE IGMPSNOOPING [INTERFACE={ type:id-range | id-range | ifname-list | ALL }]
165	Manager	DISABLE INTERFACE={ type:id-range | id-range | ifname-list } [FORCE]
166	Manager	DISABLE IP INTERFACE={ MGMT | type:id | ifname }
167	Manager	DISABLE PSPAN [={ pspanname-list | ALL }] [{ INTERFACE={ type:id-range | ifname-list | ALL } | CARD={ slot-list | ALL } }]
168	Manager	DISABLE STP [{ [INSTANCE={ stpname | mstid | MAIN | ALL } INTERFACE={ type:id-range | id-range | ifname-list | ALL } [TOPOLOGYCHANGE]] | [INTERFACE={ type:id-range | id-range | ifname-list | ALL } [TOPOLOGYCHANGE]] }]
169	Manager	DISABLE TRACE
170	Manager	DISABLE ARPFILTER INTERFACE={type:id-range|id-range|ifname-list|ALL}
171	Manager	DISABLE CARD={slot-list|INACTCFC} [FORCE]
172	User	DISABLE CONFIRMATION
173	Manager	DISABLE FANMODULE
174	Sec_Off	DISABLE FEATURE={ userlabel-list | ALL } [FORCE]
175	User	DISABLE LOG OUTPUT={outputid-list|ALL}
176	User	DISABLE MORE
177	Manager	DISABLE PORT=port-list [FORCE]
178	Sec_Off	DISABLE RADIUS SERVER={ ipaddress-list | hostname-list | ALL }
179	Sec_Off	DISABLE SNMP

No.	Level	Syntax
180	Sec_Off	DISABLE SNMP AUTHENTICATE_TRAP
181	Sec_Off	DISABLE SNMP COMMUNITY=name [TRAP]
182	Manager	DISABLE SNTP
183	Manager	DISABLE STP INTERFACE={ type:id-range | id-range | ifname-list | ALL } [TOPOLOGYCHANGE]
184	Manager	DISABLE SWITCH AGEINGTIMER
185	Manager	DISABLE SWITCH LEARNING
186	Sec_Off	DISABLE TACPLUS SERVER={ ipaddress-list | hostname-list | ALL }
187	Sec_Off	DISABLE TELNET SERVER
188	Sec_Off	DISABLE USER=login-name
189	Manager	DISCONNECT INTERFACE={ type:id-range | ifname-list | ALL }
190	Manager	ENABLE DHCPRELAY={ dhcpname-list | MAIN | ALL } INTERFACE={ type:id-range | id-range | ifname-list | ALL }
191	Manager	ENABLE EPSR={ epsrdomain-list | ALL }
192	Manager	ENABLE IGMPSNOOPING [INTERFACE={ type:id-range | id-range | ifname-list | ALL }]
193	Manager	ENABLE INTERFACE={ type:id-range | id-range | ifname-list }
194	Manager	ENABLE IP INTERFACE={ MGMT | type:id | ifname }
195	Manager	ENABLE PSPAN [={ pspanname-list | ALL }] [{ INTERFACE={ type:id-range | ifname-list | ALL } | CARD={ slot-list | ALL } }]
196	Manager	ENABLE STP [{ [INSTANCE={ stpname | mstid | MAIN | ALL } INTERFACE={ type:id-range | id-range | ifname-list | ALL } [{ TOPOLOGYCHANGE | RSTPCHECK }]] | [INTERFACE={ type:id-range | id-range | ifname-list | ALL } [{ TOPOLOGYCHANGE | RSTPCHECK }]] }]
197	Manager	ENABLE TRACE [OUTPUT={ CLI } [FORMAT={ FULL | SUMMARY }]]
198	Manager	ENABLE ARPFILTER INTERFACE={type:id-range|id-range|ifname-list|ALL}
199	Manager	ENABLE CARD={slot-list|INACTCFC} [NODIAGS] [VERBOSE]
200	User	ENABLE CONFIRMATION
201	Manager	ENABLE FANMODULE
202	Sec_Off	ENABLE FEATURE=userlabel KEY=hexkey
203	User	ENABLE LOG OUTPUT={outputid-list|ALL}
204	User	ENABLE MORE
205	Manager	ENABLE PORT=port-list
206	Sec_Off	ENABLE RADIUS SERVER={ ipaddress-list | hostname-list | ALL }
207	Sec_Off	ENABLE SNMP

<table>
<tr><th>No.</th><th>Level</th><th>Syntax</th></tr>
<tr><td>208</td><td>Sec_Off</td><td>ENABLE SNMP AUTHENTICATE_TRAP</td></tr>
<tr><td>209</td><td>Sec_Off</td><td>ENABLE SNMP COMMUNITY=name [TRAP]</td></tr>
<tr><td>210</td><td>Manager</td><td>ENABLE SNTP</td></tr>
<tr><td>211</td><td>Manager</td><td>ENABLE STP INTERFACE={ type:id-range | id-range | ifname-list | ALL } [{TOPOLOGYCHANGE | RSTPCHECK }]</td></tr>
<tr><td>212</td><td>Manager</td><td>ENABLE SWITCH AGEINGTIMER</td></tr>
<tr><td>213</td><td>Manager</td><td>ENABLE SWITCH LEARNING</td></tr>
<tr><td>214</td><td>Sec_Off</td><td>ENABLE TACPLUS SERVER={ ipaddress-list | hostname-list | ALL }</td></tr>
<tr><td>215</td><td>Sec_Off</td><td>ENABLE TELNET SERVER</td></tr>
<tr><td>216</td><td>Sec_Off</td><td>ENABLE USER=login-name</td></tr>
<tr><td>217</td><td>User</td><td>EXECUTE SCRIPT=filename</td></tr>
<tr><td>218</td><td>Manager</td><td>FORMAT MEDIA=unit</td></tr>
<tr><td>219</td><td>Manager</td><td>GET FILE={ sourcefilename | serverpath/sourcefilename } { TFTP SERVER={ ipaddress | hostname } | ZMODEM | FTP SERVER={ ipaddress | hostname } USER=userid PASSWORD=password } [TO=unit:]</td></tr>
<tr><td>220</td><td>Manager</td><td>GET FILE=filename CARD=slot</td></tr>
<tr><td>221</td><td>Manager</td><td>LOOPBACK INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } { NEAREND | FAREND } { INWARD | PAYLOAD | LINE | PACKET | NONE</td></tr>
<tr><td>222</td><td>User</td><td>PING={ ipaddress | hostname } [FROM { INTERFACE={ type:id | id | ifname } | IPADDRESS=ipaddress }] [DELAY=1..900] [LENGTH=1..8192] [NUMBER={ 1..65535 | CONTINUOUS }] [TIMEOUT=1..900]</td></tr>
<tr><td>223</td><td>Sec_Off</td><td>PURGE DATABASE [FORCE]</td></tr>
<tr><td>224</td><td>Manager</td><td>PURGE LOG</td></tr>
<tr><td>225</td><td>Manager</td><td>PURGE MEDIA=unit</td></tr>
<tr><td>226</td><td>Manager</td><td>PURGE STP</td></tr>
<tr><td>227</td><td>Sec_Off</td><td>PURGE USER</td></tr>
<tr><td>228</td><td>Manager</td><td>PUT FILE={sourcefile|unit:sourcefile} {TFTP SERVER={ipaddress|hostname} | FTP SERVER={ipaddress|hostname} USER=userid PASSWORD=password | ZMODEM} [TO=serverpath]</td></tr>
<tr><td>229</td><td>Manager</td><td>PUT FILE=filenamemCARD={ slot | slot-list }</td></tr>
<tr><td>230</td><td>Manager</td><td>PUT LOG FILE={ destinationfile | unit:destinationfile |serverpath/destinationfile } [{ TFTP SERVER={ ipaddress | hostname } |ZMODEM | FTP SERVER={ ipaddress | hostname } USER=userid PASSWORD=password}] [TYPE={ MGMT | ERROR | TRACE | CRASH }] [CARD={ ACTCFC | INACTCFC }]</td></tr>
<tr><td>231</td><td>Manager</td><td>RENAME DHCPRELAY=dhcpname TO=dhcpname</td></tr>
<tr><td>232</td><td>Manager</td><td>RENAME ONU=onuname TO=onuname</td></tr>
<tr><td>233</td><td>Manager</td><td>RENAME QOSPOLICY=policyname TO=policyname</td></tr>
</table>

No.	Level	Syntax
234	Manager	RENAME STP INSTANCE={ stpname | mstid } TO=stpname
235	Manager	RENAME FILE={ sourcefile | unit:sourcefile } TO={ destinationfile | unit:destinationfile }
236	Manager	RESET CARD={ slot-list | ACTCFC | INACTCFC | ALL } { CPUSTATS }
237	Manager	RESET CLASSIFIER COUNTER INTERFACE={ type:id-range | id-range | ifname-list | ALL }
238	Manager	RESET IGMPSNOOPING COUNTER [{ STANDARD | MESSAGERESPONSE | INTERFACE={ type:id-range | id-range | ifname-list | ALL } | CARD={ slot-list | ALL } }]
239	Manager	RESET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } COUNTER [FORCE]
240	Manager	RESET LLDP COUNTER [INTERFACE={ type:id-range | id-range | ifname-list | ALL }]
241	Manager	RESET MGCP COUNTER [INTERFACE={ type:id-range | id-range | ifname-list | ALL }]
242	Manager	RESET STP [{ INSTANCE={ stpname | mstid | MAIN | ALL } | LEARNCISCODIGEST }]
243	Manager	RESET ACCESSLIST=accesslistname RULE=rulenumber [{ PERMIT | DENY }]
244	Manager	RESET CLASSIFIER COUNTER PORT={port-list|ALL}
245	Manager	RESET CLASSIFIER=classifiername
246	Manager	RESET DHCPRELAY COUNTER INTERFACE={type:id-range|id-range|ifname-list|ALL}
247	Manager	RESET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } FAULTCOUNT [FORCE]
248	Manager	RESET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } QUEUECOUNT [FORCE]
249	Manager	RESET LAG COUNTER={LACPSTATS|MACSTATS|ALL}
250	Manager	RESET SNTP
251	Manager	RESET SWITCH COUNTER [FORCE]
252	Sec_Off	RESET USER[=login-name] [COUNTER[={ALL|GLOBAL|USER}]]
253	Manager	RESTART CARD={ slot-list | INACTCFC | ACTCFC } [COLD] [FORCE]
254	Manager	RESTART SYSTEM [FORCE]
255	Sec_Off	RESTORE CONFIG FILE={ sourcefile | unit:sourcefile } [OUTPUT={ CONSOLE | logfile | unit:logfile }]
256	Sec_Off	RESTORE DATABASE FILE={sourcefile|unit:sourcefile|serverpath/sourcefile} [{TFTP SERVER={ipaddress|hostname}|ZMODEM| FTP SERVER={ipaddress|hostname} USER=userid PASSWORD=password}] [FORCE]
257	User	SEND MESSAGE=message-text SESSION={session-list|ALL}
258	Manager	SET LOG OUTPUT=outputid [{ CLI [FORMAT={ FULL | MSGONLY | SUMMARY }] | CONSOLE [FORMAT={ FULL | MSGONLY | SUMMARY }] | SYSLOG SERVER={ ipaddress | hostname } | FILE=unit:filename [FORMAT={ FULL | MSGONLY | SUMMARY }] }]
259	Manager	SET ALARMS THRESHOLD [MINOR=value] [MAJOR=value] [CRITICAL=value]

No.	Level	Syntax
260	Manager	SET CARD={ slot-list | ACTCFC | INACTCFC } [{ NTE8 [PORTTYPE={ DS1 | E1 }] [TIMINGREFERENCE={ type:id | ifname | INTERNAL }] }] [PREFLOAD={ filename | NONE }] [ALTLOAD={ filename | NONE }] [TEMPLOAD={ filename | NONE }]
261	Manager	SET CARD={ slot-list | ACTCFC | INACTCFC } [{ SHDSL24 [WETTINGCURRENT={ ON | OFF }] [ANNEXTYPE={ A | B }] [WIREMODE={ NORMAL | BONDED }] }] [PREFLOAD={ filename | NONE }] [ALTLOAD={ filename | NONE }] [TEMPLOAD={ filename | NONE }]
262	Manager	SET CARD={ slot-list | ACTCFC | INACTCFC } [SHDSL16 [WETTINGCURRENT={ ON | OFF }] [ANNEXTYPE={ A | B }] [WIREMODE={ NORMAL | BONDED }]] [PREFLOAD={ filename | NONE }] [ALTLOAD={ filename | NONE }] [TEMPLOAD={ filename | NONE }]
263	Manager	SET CONTACTALARM={ 0..2 } STATE={ OPEN | CLOSED } [SEVERITY={ CRITICAL | MAJOR | MINOR | INFO }] [MESSAGE=text]
264	Manager	SET DHCPRELAY AGENT [REMOTEID={ remote-id | DEFAULT }] [CIDFORMAT={ AUTOMATIC | IFDESC | BOTH }]
265	Manager	SET DHCPRELAY INTERFACE={ type:id-range | id-range | ifname-list | ALL } [FILTER={ ON | OFF }] [AGEING={ ON | OFF }]
266	Manager	SET DHCPRELAY={ dhcpname-list | MAIN | ALL } [AGENT REMOTEID={ remote-id | DEFAULT }] [MODE={ RELAY | SNOOPING }] [FORCE]
267	Manager	SET EGRESSLIMITER=limitername [RATE=bits-per-second] [BURSTSIZE={ 4KB | 8KB | 16KB | 32KB | 64KB | 128KB | 256KB | 512KB | 1MB | 2MB | 4MB | 8MB | 16MB | 32MB | 64MB }]
268	Manager	SET EPSR={ epsrdomain-list | ALL } [HELLOTIME=value] [FAILOVERTIME=value] [RINGFLAPTIME=value]
269	Manager	SET EPSR=epsrdomain INTERFACE={ type:id | id | ifname } [TYPE={ PRIMARY | SECONDARY }]
270	Manager	SET HVLAN={ hvlanname | vid } INTERFACE={ type:id-range | id-range | ifname-list | ALL } [FRAME={ UNTAGGED | TAGGED }]
271	Manager	SET IGMPSNOOPING { CARD={ slot-list | ALL } MCASTGROUPLIMIT=1..512 | INTERFACE={ type:id-range | id-range | ifname-list | ALL } SNOOPINGMODE={ INTERNAL | EXTERNAL | MCPASSTHROUGH } | [FLOODUNKNOWNS={ ON | OFF }] [ROUTERAGEINGTIMER=10..1200] [GENQUERYTIMER=5..120] [DUPREPORTTIMER=5..120] }
272	Manager	SET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } ADSL [MODE={ GLITE | GDMT | T1.413 | ADSL2 | ADSL2+ | AUTO | AUTO2+ | ADSL2M | ADSL2+M }] [BITMAPMODE={ FBM | DBM }] [LINETYPE={ FAST | INTERLEAVE }] [INTERLEAVEDELAY=1..64] [ECHOCANCELLATION={ ON | OFF }] [DATABOOST={ ON | OFF }] [MAXUPSTREAMRATE=32..3072] [MINUPSTREAMRATE=32..3072] [MAXDOWNSTREAMRATE=32..26624] [MINDOWNSTREAMRATE=32..26624] [TARGETSNRMARGIN=0..15] [MAXSNRMARGIN={ OFF | 1..30 }] [LINEQUALITYMONITOR={ LOW | MEDIUM | HIGH }] [VPI=0..4095] [VCI=32..65535] [DESCRIPTION=description]
273	Manager	SET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } COUNTER { ON | OFF }
274	Manager	SET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } DS1 [TIMINGREFERENCE={ SELF | CONNECTION | CARD }] [LINEENCODING={ B8ZS | AMI }] [LINEBUILDOUT { LONGHAUL={ 0.0DB | -7.5DB | -15.0DB | -22.5DB } | SHORTHAUL={ 133FT | 266FT | 399FT | 533FT | 655FT } }] [FRAMING={ UNFRAMED | SF | ESF | STANDARD }] [DIRECTION={ NETWORK | CUSTOMER }] [DESCRIPTION=description] [FORCE]
275	Manager	SET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } E1 [TIMINGREFERENCE={ SELF | CONNECTION | CARD }] [LINEENCODING={ HDB3 | AMI }] [FRAMING={ UNFRAMED | E1 | E1CRC | STANDARD }] [DIRECTION={ NETWORK | CUSTOMER }] [DESCRIPTION=description] [FORCE]
276	Manager	SET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } EPON [IPMCVLAN={ vlanname | vid }] [IPADDRESS=ipaddress] [DESCRIPTION=description]
277	Manager	SET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } FE [AUTONEGOTIATION={ ON | OFF }] [SPEED={ AUTONEGOTIATE | 10 | 100 }] [DUPLEX={ AUTONEGOTIATE | FULL | HALF }] [FLOWCONTROL={ AUTONEGOTIATE | ON | OFF }] [DIRECTION={ NETWORK | CUSTOMER } [FORCE]] [DESCRIPTION=description]
278	Manager	SET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } FX [FLOWCONTROL={ ON | OFF }] [DIRECTION={ NETWORK | CUSTOMER } [FORCE]] [DESCRIPTION=description]

No.	Level	Syntax
279	Manager	SET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } GE [AUTONEGOTIATION={ ON | OFF }] [SPEED={ AUTONEGOTIATE | 10 | 100 | 1000 }] [DUPLEX={ AUTONEGOTIATE | FULL | HALF }] [FLOWCONTROL={ AUTONEGOTIATE | ON | OFF }] [DIRECTION={ NETWORK | CUSTOMER }] [DESCRIPTION=description] [FORCE]
280	Manager	SET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } POTS [CAPABILITY={ PCMU | G726 | ALL }] [MINPACKETIZATION=10..30] [MAXPACKETIZATION=10..30] [BUFFERDELAY=0..150] [BUFFERMODE={ STATIC | DYNAMIC }] [TXPREECHOGAIN=-9.0..+3.0] [TXPOSTECHOGAIN=-9.0..+3.0] [RXPREECHOGAIN=-9.0..+3.0] [RXPOSTECHOGAIN=-9.0..+3.0] [ECHOCANCELLATION={ ON | OFF }] [VOICEACTIVITYDETECTION={ ON | OFF }] [COMFORTNOISEGENERATION={ ON | OFF }] [PACKETLOSSCONCEALMENT={ ON | OFF }] [DESCRIPTION=description]
281	Manager	SET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } PROFILE=name
282	Manager	SET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } SHDSL [MAXCONNECTRATE=72..2312] [MINCONNECTRATE=72..2312] [TARGETSNRMARGIN=0..10] [LINEQUALITYMONITOR={ LOW | MEDIUM | HIGH }] [VPI=0..4095] [VCI=32..65535] [DESCRIPTION=description]
283	Manager	SET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } VDSL [MODE={ VDSL2 | GLITE | GDMT | T1.413 | ADSL2 | ADSL2+ | AUTO | AUTO2 | ADSL2M | ADSL2+M }] [LINETYPE={ FAST | INTERLEAVE }] [MAXUPSTREAMRATE=32..14848] [MINUPSTREAMRATE=32..14848] [MAXDOWNSTREAMRATE=32..51200] [MINDOWNSTREAMRATE=32..51200] [TARGETSNRMARGIN=snr-margin-dB] [MAXSNRMARGIN={ OFF | snr-margin-dB }] [MINSNRMARGIN={ OFF | snr-margin-dB }] [MAXRECEIVEPOWER={ OFF | value }] [BANDPLAN={ 997 | 998 }] [OPTUPSTREAMBAND={ ON | OFF }] [RFIBAND={ { 30M | 40M | 80M | 160M } [,...] | NONE | ALL }] [MAXINTERLEAVEDELAY=0..255] [MINIMPULSENOISEPROTECTION [UPSTREAMMININP={ 0 | 0.5 | 1 | 2 | 4 | 8 | 16 }] [DOWNSTREAMMININP={ 0 | 0.5 | 1 | 2 | 4 | 8 | 16 }]] [DEPLOYMENT={ CABINET | CENTRALOFFICE }] [PSDMASK UPSTREAMPSDMASK={ MASK1 | MASK2 } DOWNSTREAMPSDMASK={ MASK1 | MASK2 }] [DATABOOST={ ON | OFF }] [LINEQUALITYMONITOR={ LOW | MEDIUM | HIGH }] [VPI=0..4095] [VCI=32..65535] [DESCRIPTION=description]
284	Manager	SET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } XE [AUTONEGOTIATION={ ON | OFF }] [FLOWCONTROL={ AUTONEGOTIATE | ON | OFF }] [DESCRIPTION=description]
285	Manager	SET INTERFACE={ type:id-range | id-range | ifname-list } DESCRIPTION=description
286	Manager	SET INTERFACE={ type:id-range | id-range | ifname-list | ALL } [ACCEPTABLE={ ALL | VLAN | HVLAN }] [INFILTERING={ OFF | ON }] [TAGALL={ ON | OFF }] [TPID=tpidvalue] [LEARNLIMIT={ 1..64 | OFF }]
287	Manager	SET INTERFACE={ type:id-range | id-range | ifname-list | ALL } ALARM SEVERITY={ NONE | INFO | MINOR | MAJOR | CRITICAL } [FORCE]
288	Manager	SET INTERFACE={ type:id-range | id-range | ifname-list | ALL } COUNTER HISTORY [INTERVAL={ interval-list | ALL }] [BUCKETS=1..2700]
289	Manager	SET INTERFACE={ type:id-range | id-range | ifname-list | ALL } PMONALERT { ATUC [LOFS=0..900] [LOSS=0..900] [LPRS=0..900] [ES=0..900] [SES=0..900] [UAS=0..900] [LOLS=0..900] [FAILEDFASTRETRAIN=threshold] | ATUR [LOFS=0..900] [LOSS=0..900] [LPRS=0..900] [ES=0..900] }
290	Manager	SET INTERFACE={ type:id-range | id-range | ifname-list | ALL } PMONALERT { DS1 | E1 } { NEAREND } { LINE | PATH [FCP=0..32767] [ESAP=0..900] [CSS=0..900] [BES=0..900] [SEFS=0..900] [AISSP=0..900] } [ES=0..900] [SES=0..900] [UAS=0..900] [CV=0..32767]
291	Manager	SET INTERFACE={ type:id-range | id-range | ifname-list | ALL } PMONALERT ADSL { ATUC [LOFS=0..900] [LOSS=0..900] [LPRS=0..900] [ES=0..900] [SES=0..900] [UAS=0..900] [LOLS=0..900] [FAILEDFASTRETRAIN=threshold] | ATUR [LOFS=0..900] [LOSS=0..900] [LPRS=0..900] [ES=0..900] }
292	Manager	SET INTERFACE={ type:id-range | id-range | ifname-list | ALL } PMONALERT PPP [SENTECHOREQUESTS=0..900] [FAILEDECHOREQUESTS=0..900]
293	Manager	SET INTERFACE={ type:id-range | id-range | ifname-list | ALL } PMONALERT PSPAN { SATOP } [ES=0..900] [LOPSS=0..900] [LATEPACKETS=0..230400000] [EARLYPACKETS=0..230400000] [LOSTPACKETS=0..230400000]
294	Manager	SET INTERFACE={ type:id-range | id-range | ifname-list | ALL } PMONALERT PSPAN { SATOP } [ES=0..900] [LOPSS=0..900] [LATEPACKETS=0..230400000] [EARLYPACKETS=0..230400000] [LOSTPACKETS=0..230400000]

No.	Level	Syntax
295	Manager	SET INTERFACE={ type:id-range | id-range | ifname-list | ALL } PMONALERT SHDSL [LOSWS=0..900] [CRCANOMALIES=0..900] [ES=0..900] [SES=0..900] [UAS=0..900]
296	Manager	SET INTERFACE={ type:id-range | id-range | ifname-list | ALL } PMONALERT VDSL { VTUC [LOFS=0..900] [LOSS=0..900] [LPRS=0..900] [ES=0..900] [SES=0..900] [UAS=0..900] [LOLS=0..900] [FAILEDFASTRETRAIN=threshold] | VTUR [LOFS=0..900] [LOSS=0..900] [LPRS=0..900] [ES=0..900] }
297	Manager	SET IP INTERFACE={ MGMT | type:id-range | ifname-list | ALL } [IPADDRESS=ipaddress] [SUBNETMASK=mask] [IFNAME=ifname] [GATEWAY=ipaddress] [DOMAINNAME=name] [DNS=ipaddress-list]
298	Manager	SET LLDP [TXINTERVAL=5..32768] [TXHOLD=2..10] [TXDELAY=1..8192] [REINITDELAY=1..10] [NOTIFYINTERVAL=5..3600]
299	Manager	SET LLDP INTERFACE={ type:id-range | id-range | ifname-list | ALL } [MODE={ TX | RX | BOTH | OFF }] [NOTIFY={ ON | OFF }]
300	Sec_Off	SET LOGINBANNER { FILE=filename | STRING=string } [{ USER | MANAGER | SECURITYOFFICER | ALL }]
301	Manager	SET MGCP INTERFACE={ type:id-range | id-range | ifname-list | ALL } [CALLAGENT={ domain | domain:udp-port | localname@domain | localname@domain:udp-port }] [CALLAGENTPROFILE={ GENERIC | GENBAND | METASWITCH | ASTERISK }] [DISCONNECTTHRESHOLD=number] [SUSPICIONTHRESHOLD=number] [INITIALRETRANSMITDELAY=100..4000] [MAXRETRANSMITDELAY=100..4000] [IPDSCP=0..63] [UDPPORT=udp-port] [VPRIORITY=0..7]
302	Manager	SET MLPPP={ mlpppname-list | ALL } [SEGMENTSIZE={ 64..1526 }] [SEQUENCENUMBERBITS={ 12 | 24 }] [FORCE]
303	Manager	SET ONU=onuname MACADDRESS=macaddress
304	Manager	SET PORT={ port-list | ALL } ADSL [attributes]
305	Manager	SET PORT={ port-list | ALL } DS1 [DS1 attributes]
306	Manager	SET PORT={ port-list | ALL } E1 [E1 attributes]
307	Manager	SET PORT={ port-list | ALL } FE [FE attributes]
308	Manager	SET PORT={ port-list | ALL } FX [FX attributes]
309	Manager	SET PORT={ port-list | ALL } GE [GE attributes]
310	Manager	SET PORT={ port-list | ALL } POTS [POTS attributes]
311	Manager	SET PORT={ port-list | ALL } SHDSL [SHDSL Attributes]
312	Manager	SET PORT={ port-list | ALL } XE [WITH LAG=lagname] [AUTONEGOTIATION={ ON | OFF }] [FLOWCONTROL={ AUTONEGOTIATE | ON | OFF }] [DESCRIPTION=description]
313	Manager	SET PPP INTERFACE={ type:id-range | id-range | ifname-list } [RESTARTINTERVAL=seconds] [MAXTERMINATE={ value | CONTINUOUS }] [MAXCONFIGURE=value] [MAXFAILURE={ value | CONTINUOUS }] [ECHOREQUEST={ seconds | OFF }]
314	Manager	SET PROFILE=name ADSLPORT [MODE={ GLITE | GDMT | T1.413 | ADSL2 | ADSL2+ | AUTO | AUTO2+ | ADSL2M | ADSL2+M }] [BITMAPMODE={ FBM | DBM }] [LINETYPE={ FAST | INTERLEAVE }] [INTERLEAVEDELAY=1..64] [ECHOCANCELLATION={ ON | OFF }] [DATABOOST={ ON | OFF }] [MAXUPSTREAMRATE=32..3072] [MINUPSTREAMRATE=32..3072] [MAXDOWNSTREAMRATE=32..26624] [MINDOWNSTREAMRATE=32..26624] [TARGETSNRMARGIN=0..15] [MAXSNRMARGIN={ OFF | 1..30 }] [LINEQUALITYMONITOR={ LOW | MEDIUM | HIGH }] [VPI=0..4095] [VCI=32..65535] [ADMINSTATE={ UP | DOWN }] [MODE={ GLITE | GDMT | T1.413 | ADSL2 | ADSL2+ | AUTO | AUTO2+ }] [BITMAPMODE={ FBM | DBM }] [LINETYPE={ FAST | INTERLEAVE }] [INTERLEAVEDELAY=1..64] [ECHOCANCELLATION={ ON | OFF }] [MAXUPSTREAMRATE=32..1024] [MINUPSTREAMRATE=32..1024] [MAXDOWNSTREAMRATE=32..26624] [MINDOWNSTREAMRATE=32..26624] [TARGETSNRMARGIN=0..15] [LINEQUALITYMONITOR={ LOW | MEDIUM | HIGH }] [VPI=0..255] [VCI=32..65535] [ADMINSTATE={ UP | DOWN }]

No.	Level	Syntax
315	Manager	SET PROFILE=name CES8 [PREFLOAD=filename] [ADMINSTATE={ UP | DOWN }] [PORTTYPE={ DS1 | E1 }]
316	Manager	SET PROFILE=name DS1PORT [ADMSET PROFILE=name DS1PORT [ADMINSTATE={ UP | DOWN }] [TIMINGREFERENCE={ SELF | CONNECTION | CARD }] [LINEENCODING={ B8ZS | AMI }] [LINEBUILDOUT { LONGHAUL={ 0.0DB | -7.5DB | -15.0DB | -22.5DB } | SHORTHAUL={ 133FT | 266FT | 399FT | 533FT | 655FT } }] [FRAMING={ UNFRAMED | SF | ESF | STANDARD }]INSTATE={ UP | DOWN }] [TIMINGREFERENCE={ SELF | CONNECTION | CARD }] [LINEBUILDOUT { LONGHAUL={ 0.0DB | -7.5DB | -15.0DB | -22.5DB } | SHORTHAUL={ 133FT | 266FT | 399FT | 533FT | 655FT } }] [LINEENCODING={ B8ZS | AMI }] [LOOPBACK={ NONE | INWARD | LINE }]
317	Manager	SET PROFILE=name E1PORT [ADMINSTATE={ UP | DOWN }] [TIMINGREFERENCE={ SELF | CONNECTION | CARD }] [LINEENCODING={ HDB3 | AMI }] [FRAMING={ UNFRAMED | E1 | E1CRC | STANDARD }]
318	Manager	SET PROFILE=name EPONPORT [ADMINSTATE={ UP | DOWN }] [IPMCVLAN={ vlanname | vid }] [IPADDRESS=ipaddress]
319	Manager	SET PROFILE=name FEPORT [ADMINSTATE={ UP | DOWN }] [AUTONEGOTIATION={ ON | OFF }] [SPEED={ AUTONEGOTIATE | 10 | 100 }] [DUPLEX={ AUTONEGOTIATE | FULL | HALF }] [FLOWCONTROL={ AUTONEGOTIATE | ON | OFF }]
320	Manager	SET PROFILE=name FXPORT [FLOWCONTROL={ ON | OFF }] [ADMINSTATE={ UP | DOWN }]
321	Manager	SET PROFILE=name GEPORT [AUTONEGOTIATION={ ON | OFF }] [SPEED={ AUTONEGOTIATE | 10 | 100 | 1000 }] [DUPLEX={ AUTONEGOTIATE | FULL | HALF }] [FLOWCONTROL={ AUTONEGOTIATE | ON | OFF }] [ADMINSTATE={ UP | DOWN }]
322	Manager	SET PROFILE=name NTE8 [PREFLOAD=filename] [ADMINSTATE={ UP | DOWN }] [PORTTYPE={ DS1 | E1 }]
323	Manager	SET PROFILE=name POTSPORT [CAPABILITY={ PCMU | G726 | ALL }] [MINPACKETIZATION=10..30] [MAXPACKETIZATION=10..30] [BUFFERDELAY=0..150] [BUFFERMODE={ STATIC | DYNAMIC }] [TXPREECHOGAIN=-9.0..+3.0] [TXPOSTECHOGAIN=-9.0..+3.0] [RXPREECHOGAIN=-9.0..+3.0] [RXPOSTECHOGAIN=-9.0..+3.0] [ECHOCANCELLATION={ ON | OFF }] [VOICEACTIVITYDETECTION={ ON | OFF }] [COMFORTNOISEGENERATION={ ON | OFF }] [PACKETLOSSCONCEALMENT={ ON | OFF }] [ADMINSTATE={ UP | DOWN }]
324	Manager	SET PROFILE=name SHDSLPORT [MAXCONNECTRATE=72..2312] [MINCONNECTRATE=72..2312] [TARGETSNRMARGIN=0..10] [LINEQUALITYMONITOR={ LOW | MEDIUM | HIGH }] [VPI=0..4095] [VCI=32..65535] [ADMINSTATE={ UP | DOWN }]
325	Manager	SET PROFILE=name VDSLPORT [MODE={ VDSL2 | GLITE | GDMT | T1.413 | ADSL2 | ADSL2+ | AUTO | AUTO2 | ADSL2M | ADSL2+M }] [LINETYPE={ FAST | INTERLEAVE }] [MAXUPSTREAMRATE=32..14848] [MINUPSTREAMRATE=32..14848] [MAXDOWNSTREAMRATE=32..51200] [MINDOWNSTREAMRATE=32..51200] [TARGETSNRMARGIN=snr-margin-dB] [MAXSNRMARGIN={ OFF | snr-margin-dB }] [MINSNRMARGIN={ OFF | snr-margin-dB }] [MAXRECEIVEPOWER={ OFF | value }] [BANDPLAN={ 997 | 998 }] [OPTUPSTREAMBAND={ ON | OFF }] [RFIBAND={ { 30M | 40M | 80M | 160M } [,...] | NONE | ALL }] [MAXINTERLEAVEDELAY=0..255] [MINIMPULSENOISEPROTECTION [UPSTREAMMININP={ 0 | 0.5 | 1 | 2 | 4 | 8 | 16 }] [DOWNSTREAMMININP={ 0 | 0.5 | 1 | 2 | 4 | 8 | 16 }]] [DEPLOYMENT={ CABINET | CENTRALOFFICE }] [PSDMASK UPSTREAMPSDMASK={ MASK1 | MASK2 } DOWNSTREAMPSDMASK={ MASK1 | MASK2 }] [DATABOOST={ ON | OFF }] [LINEQUALITYMONITOR={ LOW | MEDIUM | HIGH }] [VPI=0..4095] [VCI=32..65535] [ADMINSTATE={ UP | DOWN }]
326	Manager	SET PROFILE=name XEPORT [AUTONEGOTIATION={ ON | OFF }] [FLOWCONTROL={ AUTONEGOTIATE | ON | OFF }] [ADMINSTATE={ UP | DOWN }]
327	Manager	SET PROMPT=string
328	Manager	SET PSPAN={ pspanname-list | ALL } SATOP [UDPPORT=49152..65535] [PEERIPADDRESS=ipaddress] [PEERUDPPORT=49152..65535] [NUMBYTES=16..1023] [JITTERBUFFER=value] [TIMINGREFERENCE={ SELF | CONNECTION | CARD }] [RTP={ ON | OFF }] [VPRIORITY=0..7] [IPDSCP=0..63]
329	Manager	SET QOS [VLAN4QUEUEMAP=value-map] [VLAN8QUEUEMAP=value-map]
330	Manager	SET QOSPOLICY={ policyname-list | ALL } [DESCRIPTION=text] [MAXUPSTREAMRATE={ bits-per-second | MAX }] [MAXDOWNSTREAMRATE={ bits-per-second | MAX }] [MINUPSTREAMRATE={ bits-per-second | MIN }] [MINDOWNSTREAMRATE={ bits-per-second | MIN }] [UPBURSTSIZE={ 1..256 | MAX }] [DOWNBURSTSIZE={ 1..256 | MAX }] [UPDELAYSENSITIVITY={ SENSITIVE | TOLERANT }] [DOWNDELAYSENSITIVITY={ SENSITIVE | TOLERANT }]

No.	Level	Syntax
331	Sec_Off	SET RADIUS SERVER={ ipaddress-list | hostname-list | ALL } [SECRET=secret] [AUTHPORT=1..65535] [ACCTPORT=1..65535] [RETRIES=0..10] [TIMEOUT=1..60] [AUTHENTICATION={ ON | OFF }] [ACCOUNTING={ ON | OFF }]
332	Manager	SET RTP INTERFACE={ type:id-range | id-range | ifname-list | ALL } [IPDSCP=0..63] [VPRIORITY=0..7]
333	Manager	SET STP { INSTANCE={ stpname | mstid | MAIN | ALL } { DEFAULT | PRIORITY=0..65535 | INTERFACE={ type:id-range | id-range | ifname-list | ALL } { DEFAULT | [PATHCOST=path-cost] [PORTPRIORITY=port-priority] [EDGEPORT={ TRUE | FALSE }] [POINT2POINT={ TRUE | FALSE | AUTO }] [BPDUCOP={ ON | OFF }] } } | DEFAULT | [PRIORITY=0..65535] [FORWARDDELAY=4..30] [HELLOTIME=1..10] [MAXAGE=6..40] [TXMAX=1..10] [MAXHOPS=6..40] [MSTREGION=regionname] [REVISIONLEVEL=0..65535] [CISCOCONFIGURATIONDIGEST=hexstring] [CISCOLEARNEDINTERFACE={ type:id | id | ANY }] | PROTOCOL={ STP_ORIGINAL | RSTP | STP_COMPATIBLE_RSTP | MSTP | CISCO_COMPATIBLE_MSTP } [FORCE] | INTERFACE={ type:id-range | id-range | ifname-list | ALL } { DEFAULT | [PATHCOST=path-cost] [PORTPRIORITY=port-priority] [EDGEPORT={ TRUE | FALSE }] [POINT2POINT={ TRUE | FALSE | AUTO }] [BPDUCOP={ ON | OFF }] } }
334	Manager	SET SYSTEM POWERINPUT={ -48VDC | -60VDC }
335	Sec_Off	SET SYSTEM USERCONFIG [LOGINFAIL=1..10] [LOCKOUTPD=0..30000] [MANPWDFAIL=1..5] [SECUREDELAY={ OFF | 0 | 1..90 }] [MINPWDLEN=1..23] [PERSISTTIMER=1..1440] [PWDAGEING={ OFF | 0 | 1..365 }] [FORCEPWDCHANGE={ YES | NO }]
336	Manager	SET TELNET [TERMTYPE=termstring] [INSERTNULL={ ON | OFF }]
337	Manager	SET TRACE [BUFFERSIZE=events [FORCE]]
338	Manager	SET TRAFFICDESCRIPTOR=tdname-list [RATE=bits-per-second] [BURSTSIZE={ 4KB | 8KB | 16KB | 32KB | 64KB | 128KB | 256KB | 512KB | 1MB | 2MB | 4MB | 8MB | 16MB | 32MB | 64MB }]
339	Sec_Off	SET USER=login-name [PASSWORD=password [FORMAT={ CLEARTEXT | MD5 }]] [DESCRIPTION=description] [PRIVILEGE={ USER | MANAGER | SECURITYOFFICER }] [LOGIN={ TRUE | FALSE | ON | OFF | YES | NO }] [TELNET={ YES | NO }] [PWDAGEING={ OFF | 0 | 1..365 }] [DEACTIVATE={ OFF | yyyy-mm-dd }]
340	Sec_Off	SET USER=login-name [PASSWORD=password [FORMAT={ CLEARTEXT | MD5 }]] [DESCRIPTION=description] [PRIVILEGE={ USER | MANAGER | SECURITYOFFICER }] [LOGIN={ TRUE | FALSE | ON | OFF | YES | NO }] [TELNET={ YES | NO }] [SSH={ YES | NO }] [PUBLICKEY=key-name] [PWDAGEING={ OFF | 0 | 1..365 }] [DEACTIVATE={ OFF | yyyy-mm-dd }]
341	Manager	SET VC=vcid INTERFACE={ type:id-range | id-range | ifname-list } [VPI=0..255] [VCI=32..65535] [TXPEAKCELLRATE={ 150..65535 | MAX }]
342	Manager	SET VLAN={ vlanname | vid } INTERFACE={ type:id-range | id-range | ifname-list | ALL } [FRAME={ UNTAGGED | TAGGED }] [TRANSLATE={ 1..4094 | NONE }] [FORWARDING={ PRIMARYUPSTREAM | SECONDARYUPSTREAM | DOWNSTREAM | STP | UCP }]
343	Manager	SET ACCESSLIST=accesslistname RULE=rulenumber [{ PERMIT | DENY }] [IPSOURCE={ ipaddress | ANY } [SOURCEMASK=mask]] [IPDEST={ ipaddress |ANY } [DESTMASK=mask]] [MACSOURCE={ macaddress | ANY }] [MACDEST={macaddress | ANY }] [APPLICATION={ DHCPSERVER | DHCPCLIENT | NETBIOS |FUM | TELNET | SSH | SNMP | FTP | TFTP }] [TCPPORTDEST={ tcp-port-list |ANY }] [TCPPORTSOURCE={ tcp-port | ANY }] [UDPPORTDEST={ udp-port-list| ANY }] [UDPPORTSOURCE={ udp-port | ANY }] [PROTOCOL={ IPV4 | IPV6 |protocol-type | ANY }] [IPPROTOCOL={ TCP | UDP | ICMP | IGMP |ipprotocol-type | ANY }]
344	Manager	SET BOOTSERVER=ipaddress [PATH=pathname|NONE]
345	Manager	SET CARD={ slot-list | ACTCFC | INACTCFC } { PREFLOAD={ filename | NONE } | ALTLOAD={ filename | NONE } | TEMPLOAD={ filename | NONE } | CES8 [PORTTYPE={ DS1 | E1 }] [TIMINGREFERENCE={ type:id | ifname | INTERNAL }] }
346	Manager	SET CARD={slot-list|ACTCFC|INACTCFC} {PREFLOAD={filename|NONE}|ALTLOAD={filename|NONE}| TEMPLOAD={filename|NONE}}
347	Manager	SET CARD=slot-list PROFILE=name

No.	Level	Syntax
348	Manager	SET CLASSIFIER=classifiername-list [VID={ 1..4095 | ANY }] [VPRIORITY={ 0..7 | ANY }] [INNERVID={ 1..4095 | ANY }] [INNERVPRIORITY={ 0..7 | ANY }] [ETHFORMAT={ 802.3 | 802.3TAGGED | 802.3UNTAGGED | ETHII | ETHIITAGGED | ETHIIUNTAGGED | ANY }] [LSAP={ NETBIOS | lsap-value | ANY }] [IPDEST={ ipaddress-mask | MULTICAST | ANY }] [IPSOURCE={ ipaddress-mask | ANY }] [IPDSCP={ 0..63 | ANY }] [IPPROTOCOL={ TCP | UDP | ICMP | IGMP | ipprotocol-number | ANY }] [IPTOS={ 0..7 | ANY }] [MACDEST={ macaddress | MULTICAST | ANY }] [MACSOURCE={ macaddress | ANY }] [PROTOCOL={ IPV4 | IPV6 | protocol-type | ANY }] [TCPPORTDEST={ tcp-port-list | ANY }] [TCPPORTSOURCE={ tcp-port | ANY }] [TCPFLAGS={ { URG | ACK | RST | SYN | FIN | PSH } [,...] | ANY }] [UDPPORTDEST={ udp-port-list | ANY }] [UDPPORTSOURCE={ udp-port | ANY }]
349	Manager	SET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } COUNTER { ON | OFF }
350	Manager	SET INTERFACE={ type:id-range | id-range | ifname-list | ALL } RMONALERT { DROPEVENTS | OCTETS | PACKETS | BROADCAST | MULTICAST | UNDERSIZE | OVERSIZE | CRCALIGN | FRAGMENTS | JABBERS | COLLISIONS | PKTS64OCTETS | PKTS65TO127OCTETS | PKTS128TO255OCTETS | PKTS256TO511OCTETS | KTS512TO1023OCTETS | PKTS1024TO1518OCTETS } [{ ABSOLUTE | CHANGE }] [INTERVAL=2..3600] [RISINGTHRESHOLD=threshold] [FALLINGTHRESHOLD=threshold]
351	Manager	SET LAG=lagname [MODE={ON|OFF|PASSIVE|ACTIVE}] [SELECT={MACSRC|MACDEST|MACBOTH|IPSRC|IPDEST|IPBOTH|PORTSRC|PORTDEST}] [ADMINKEY=1..1024]
352	User	SET LOG FILTER=filterid [CATEGORY=category] [SEVERITY=[op]{CRITICAL|MAJOR|MINOR|NONE}]
353	User	SET LOG OUTPUT=outputid [{CLI [FORMAT={FULL|MSGONLY|SUMMARY}]| CONSOLE [FORMAT={FULL|MSGONLY|SUMMARY}]| SYSLOG SERVER={ipaddress|hostname}}]
354	User	SET PASSWORD
355	Manager	SET PORT=port-list PROFILE=name
356	Manager	SET PROFILE=name card_type [PREFLOAD=filename] [ADMINSTATE={UP|DOWN}]
357	Manager	SET PROFILE=name SHDSL16 [PREFLOAD=filename] [ADMINSTATE={ UP | DOWN }] [WETTINGCURRENT={ ON | OFF }] [ANNEXTYPE={ A | B }]
358	Manager	SET PROFILE=name SHDSL24 [PREFLOAD=filename] [ADMINSTATE={ UP | DOWN }] [WETTINGCURRENT={ ON | OFF }] [ANNEXTYPE={ A | B }]
359	Sec_Off	SET RADIUS AUTHMODE={ LOGIN | COMMAND }
360	Sec_Off	SET SNMP COMMUNITY=name [ACCESS={READ|WRITE}] [OPEN={ON|OFF|YES|NO|TRUE|FALSE}]
361	Manager	SET SNTP UTCOFFSET={+|-}hh:mm
362	Manager	SET STP INTERFACE={ type:id-range | id-range | ifname-list | ALL } {DEFAULT | [PATHCOST=path-cost] [PORTPRIORITY=port-priority] [EDGEPORT={ TRUE | FALSE }] [POINT2POINT={ TRUE | FALSE | AUTO }] }
363	Manager	SET SWITCH AGEINGTIMER=10..1000000
364	Manager	SET SYSTEM [PROVMODE={MANUAL|AUTO}]
365	Manager	SET SYSTEM [TIME=hh:mm:ss] [DATE=yyyy-mm-dd]
366	Manager	SET SYSTEM { CONTACT=contact | LOCATION=location | NAME=name | HOSTNAME=name | GATEWAY=ipaddress | DOMAINNAME=name | DNS=ipaddress-list }
367	Manager	SET SYSTEM LANGUAGE={EN}
368	Sec_Off	SET SYSTEM USERCONFIG { MANAGERPASSWORD={ password | NONE } | SECURITYOFFICERPASSWORD={ password | NONE } } [FORMAT={ CLEARTEXT | MD5 }]
369	Sec_Off	SET TACPLUS AUTHMODE={ LOGIN | COMMAND }

No.	*Level*	*Syntax*
370	Sec_Off	SET TACPLUS SERVER={ ipaddress-list | hostname-list | ALL } [KEY=key] [PORT=1..65535] [RETRIES=0..10] [TIMEOUT=1..60]
371	Manager	SET VLAN={vlanname|vid} FORWARDINGMODE={STD|UPSTREAMONLY}
372	Manager	SETDEFAULTS ALARMS THRESHOLD
373	Manager	SETDEFAULTS ALIAS
374	Manager	SETDEFAULTS CLASSIFIER=classifiername [VID] [VPRIORITY] [INNERVID] [INNERVPRIORITY] [ETHFORMAT] [LSAP] [IPDEST] [IPSOURCE] [IPDSCP] [IPPROTOCOL] [IPTOS] [MACDEST] [MACSOURCE] [PROTOCOL] [TCPPORTDEST] [TCPPORTSOURCE] [TCPFLAGS] [UDPPORTDEST] [UDPPORTSOURCE]
375	Manager	SETDEFAULTS EPSR={ epsrdomain-list | ALL } [HELLOTIME] [FAILOVERTIME] [RINGFLAPTIME]
376	Manager	SETDEFAULTS INTERFACE={ type:id-range | id-range | ifname-list | ALL } ALARM [SEVERITY]
377	Manager	SETDEFAULTS LLDP [TXINTERVAL] [TXHOLD] [TXDELAY] [REINITDELAY] [NOTIFYINTERVAL]
378	Manager	SETDEFAULTS LLDP INTERFACE={ type:id-range | id-range | ifname-list | ALL } [MODE] [NOTIFY]
379	Sec_Off	SETDEFAULTS LOGINBANNER [{ USER | MANAGER | SECURITYOFFICER | ALL }]
380	Manager	SETDEFAULTS MGCP INTERFACE={ type:id-range | id-range | ifname-list | ALL } [CALLAGENT] [CALLAGENTPROFILE] [DISCONNECTTHRESHOLD] [SUSPICIONTHRESHOLD] [INITIALRETRANSMITDELAY] [MAXRETRANSMITDELAY] [IPDSCP] [UDPPORT] [VPRIORITY]
381	Manager	SETDEFAULTS PROMPT
382	Manager	SETDEFAULTS RTP INTERFACE={ type:id-range | id-range | ifname-list | ALL } [IPDSCP] [VPRIORITY]
383	Manager	SETDEFAULTS TRACE [FORCE]
384	User	SHOW LOG [CATEGORY=category] [DATE=[op] yyyy-mm-dd [-yyyy-mm-dd]] [FORMAT={ FULL | MSGONLY | SUMMARY }] [REVERSE] [SEQUENCE=0..9999 [-0..9999]] [SEVERITY=[op] { CRITICAL | MAJOR | MINOR | NONE }] [TAIL [=count]] [TIME=[op] hh:mm:ss [-hh:mm:ss]]
385	User	SHOW { CONFIG STATUS }
386	User	SHOW { CONFIG }
387	User	SHOW ALARMS [{ CARD={ slot-list | ALL } | INTERFACE={ type:id-range | id-range | ifname-list | ALL } | SEVERITY={ CRITICAL | MAJOR | MINOR | INFO | ALL } | ALL }] [FULL]
388	User	SHOW ALARMS [PORT [={ port-list | ALL }]] [FULL]
389	User	SHOW ALARMS THRESHOLD
390	User	SHOW ALIAS [={ aliasname-list | ALL }]
391	User	SHOW CARD [={ slot-list | ACTCFC | INACTCFC | ALL }] [{ CPUSTATS [TASKS] | INVENTORY | MEMORY { HEAP | MESSAGEBUFFERS | QUICKHEAP } | PORTS | SOFTWARE }]
392	User	SHOW CARD={ slot-list | ALL } PORTS
393	User	SHOW CLASSIFIER COUNTER [{ INTERFACE={ type:id-range | id-range | ifname-list | ALL } }]
394	User	SHOW CLASSIFIER={ classifiername-list | ALL } [{ INTERFACE={ type:id-range | id-range | ifname-list | ALL } }] [{ SUMMARY | FULL }]

No.	Level	Syntax
395	Manager	SHOW CONNECTIONS [INTERFACE={ type:id-range | ifname-list | ALL }] [FULL]
396	User	SHOW CONTACTALARM [={ 0..2 | ALL }] [STATE={ OPEN | CLOSED | ALL }] [SEVERITY={ CRITICAL | MAJOR | MINOR | INFO | ALL }]
397	User	SHOW DATABASE
398	User	SHOW DHCPRELAY [={ dhcpname-list | MAIN | ALL }] [INTERFACE={ type:id-range | id-range | ifname-list | ALL }] [FULL]
399	User	SHOW DHCPRELAY COUNTER [INTERFACE={ type:id-range | id-range | ifname-list | ALL }] [FULL]
400	User	SHOW DIAGNOSTICS [{ INTERFACE={ type:id-range | id-range | ifname-list | ALL } | CARD={ slot-list | ALL } | ALL }]
401	User	SHOW EGRESSLIMITER [={ limitername-list | ALL }] [INTERFACE={ type:id-range | id-range | ifname-list | ALL }]
402	Manager	SHOW EPSR [={ epsrdomain-list | ALL }] [FULL]
403	User	SHOW IGMPSNOOPING [{ STATUS | MCASTGROUPS [FULL] | COUNTER [{ STANDARD | MESSAGERESPONSE | INTERFACE={ type:id-range | id-range | ifname-list | ALL } | CARD={ slot-list | ALL } }] | INTERFACE={ type:id-range | id-range | ifname-list | ALL } [FULL] | CARD={ slot-list | ALL } [FULL] }]
404	User	SHOW INTERFACE [={ type: | type:id-range | id-range | ifname-list | ALL }] [CARD=slot-list] [STATE={ UP | DOWN | ALL }] [DIRECTION={ NETWORK | CUSTOMER | INTERNAL }] [FULL]
405	User	SHOW INTERFACE [={ type:id-range | id-range | ifname-list | ALL }] ALARM SEVERITY [={ NONE | INFO | MINOR | MAJOR | CRITICAL | DEFAULT | NONDEFAULT | ALL }]
406	User	SHOW INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } COUNTER [{ STATUS | FULL }]
407	User	SHOW INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } FAULTCOUNT
408	User	SHOW INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } QUEUECOUNT [STATUS]
409	User	SHOW INTERFACE={ type:id-range | id-range | ifname-list | ALL } COUNTER HISTORY [STATUS] [INTERVAL={ interval-list | ALL }] [BUCKET={ bucket-list | ALL }] [FULL]
410	User	SHOW IP [INTERFACE [={ MGMT | type:id-range | ifname-list | ALL }] [FULL]]
411	User	SHOW IP ARP [={ ipaddress-list | ALL }] [INTERFACE={ MGMT | type:id-range | ifname-list | ALL }] [FULL]
412	User	SHOW IP CONNECTIONS [={ TCP | UDP }]
413	Manager	SHOW LLDP [INTERFACE [={ type:id-range | id-range | ifname-list | ALL }] [FULL]]
414	User	SHOW LLDP COUNTER [INTERFACE={ type:id-range | id-range | ifname-list | ALL }] [FULL]
415	User	SHOW LOGINBANNER
416	User	SHOW MEDIA [={ unit-list | ALL }] [FULL]
417	User	SHOW MGCP COUNTER [INTERFACE={ type:id-range | id-range | ifname-list | ALL }] [FULL]
418	User	SHOW MLPPP [={ mlpppname-list | ALL }] [INTERFACE={ type:id-range | id-range | ifname-list | ALL }] [FULL]
419	User	SHOW ONU [={ onuname-list | ALL }] [ONUID={ 0..15 | ALL }] [INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL }] [MACADDRESS={ macaddress | ALL }] [FULL]
420	User	SHOW PPP [INTERFACE={ type:id-range | id-range | ifname-list | ALL }] [FULL]

No.	***Level***	***Syntax***
421	User	SHOW PROFILE [={ name-list | NAMES | ALL }] [{ cardtype | porttype }] [FULL]
422	User	SHOW PROFILE [={ name-list | NAMES | ALL }] [{ CES8 | DS1PORT | E1PORT }] [FULL]
423	User	SHOW PROFILE [={ name-list | NAMES | ALL }] [FULL]
424	Manager	SHOW PROFILE [={ name-list | NAMES | ALL }] { NTE8 | DS1PORT | E1PORT } [FULL]
425	User	SHOW PROFILE [={ name-list | NAMES | ALL }] { XE1 | XEPORT } [FULL]
426	User	SHOW PROTECTIONGROUP [={ groupname-list | ALL }]
427	User	SHOW PSPAN [={ pspanname-list | ALL }] [{ INTERFACE={ type:id-range | ifname-list } | CARD=slot-list }] [{ JITTERBUFFER | FULL }]
428	User	SHOW QOSPOLICY [={ policyname-list | ALL }] [INTERFACE={ type:id-range | id-range | ifname-list | ALL }] [{ BRUUM | IPMC | BIDIRECTIONAL [VLAN={ vlanname-list | vid-range | ALL }] | ALL }] [FULL]
429	User	SHOW RTP COUNTER [INTERFACE={ type:id-range | id-range | ifname-list | ALL }] [FULL]
430	Manager	SHOW RTP INTERFACE={ type:id-range | id-range | ifname-list | ALL } [FULL]
431	User	SHOW STP [{ [INSTANCE={ stpname | mstid | MAIN | ALL }] [INTERFACE={ type:id-range | id-range | ifname-list | ALL }] [FULL] | COUNTER }]
432	User	SHOW SWITCH INTERNALMAC [{ INTERFACE={ type:id-range | id-range | ifname-list | ALL } | CARD={ slot-list | ALL } }] [ADDRESS=macaddress]
433	User	SHOW TECHSUPPORT FILE=filename [FORCE]
434	User	SHOW TELNET [{ SERVER | SESSIONS }]
435	User	SHOW TRACE [{ STATUS | BUFFER [DATE=[op] yyyy-mm-dd [-yyyy-mm-dd]] [FORMAT={ FULL | SUMMARY }] [REVERSE] [SEQUENCE=seqnum [-seqnum]] [TAIL [=count]] [TIME=[op] hh:mm:ss [-hh:mm:ss]] }]
436	User	SHOW TRACE EPSR [={ epsrdomain-list | ALL }] [MESSAGETYPE={ HEALTH | RINGUPFLUSH | RINGDOWNFLUSH | LINKDOWN | ALL }] [INTERFACE={ type:id-range | id-range | ifname-list | ALL }]
437	User	SHOW TRACE IGMPSNOOPING [MESSAGETYPE={ REPORTV1 | REPORTV2 | LEAVE | GENERALQUERY | LASTMEMBERQUERY | ALL }] [INTERFACE={ type:id-range | id-range | ifname-list | ALL }] [MACADDRESS={ macaddress | ALL }] [GROUPADDRESS={ ipaddress | ALL }]
438	User	SHOW TRACE PPP [EVENT={ PORT | LCP | BCP | ECHO | FRAME | TIMER | ERRPROTO | MAIN | ALL }] [INTERFACE={ type:id-range | id-range | ifname-list | ALL }]
439	User	SHOW TRACE VOICECALL [EVENT={ OPENLOOP | CLOSELOOP | MGCPOFFHOOK | MGCPONHOOK | MODEMDETECT | ALL }] [INTERFACE={ type:id-range | id-range | ifname-list | ALL }]
440	Manager	SHOW TRANSFER [={ transferid-list | ALL }]
441	Manager	SHOW VC [={ vcid-range | ALL }] [INTERFACE={ type:id-range | id-range | ifname-list | ALL }]
442	User	SHOW ACCESSLIST={ accesslistname-list | ALL } [INTERFACE={ type:id-range |id-range | ifname-list | ALL }]
443	User	SHOW ARPFILTER [INTERFACE={type:id-range|id-range|ifname-list|ALL}]
444	User	SHOW BOOTSERVER
445	User	SHOW CLASSIFIER COUNTER [{PORT={port-list|ALL}}]

No.	Level	Syntax
446	User	SHOW CLASSIFIER={classifiername-list|ALL} [{PORT={port-list|ALL}}] [{SUMMARY|FULL}]
447	User	SHOW FANMODULE
448	User	SHOW FEATURE [={ userlabel-list | ALL }]
449	Sec_Off	SHOW FEATURE [={ userlabel-list | ALL }] [KEYS]
450	User	SHOW FILES [FULL]
451	User	SHOW FILES MEDIA=unit [FULL]
452	User	SHOW FLASH [INACTCFC]
453	User	SHOW HVLAN[={hvlanname|vid|ALL}] [FULL]
454	User	SHOW IP COUNTER={TCP|UDP|ICMP}
455	User	SHOW IP ROUTE[={ipaddress-list|ALL}]
456	User	SHOW LAG={ lagname-list | ALL } [{ INFO | STATE | LACPSTATS | MACSTATS }]
457	User	SHOW LOG FILTER
458	User	SHOW LOG OUTPUT
459	User	SHOW PORT={port-list|ALL}
460	User	SHOW PROFILE NAMES [{cardtype|porttype}]
461	User	SHOW PROFILE=name { CES8 | DS1PORT | E1PORT }
462	User	SHOW QOS
463	User	SHOW RADIUS
464	User	SHOW SCRIPT=filename
465	User	SHOW SESSIONS
466	Sec_Off	SHOW SNMP
467	Sec_Off	SHOW SNMP COMMUNITY [={ name-list | ALL }]
468	User	SHOW SNTP
469	User	SHOW STP COUNTER
470	User	SHOW STP INTERFACE={ type:id-range | id-range | ifname-list | ALL }
471	User	SHOW SWITCH
472	User	SHOW SWITCH COUNTER
473	User	SHOW SWITCH FDB [INTERFACE={ type:id-range | id-range | ifname-list | ALL}] [ADDRESS=macaddress] [HVLAN={ hvlanname | vid }]

No.	Level	Syntax
474	User	SHOW SWITCH FDB [INTERFACE={ type:id-range | id-range | ifname-list | ALL}] [ADDRESS=macaddress] [VLAN={ vlanname | vid }]
475	User	SHOW SYSTEM
476	User	SHOW SYSTEM COOLING
477	User	SHOW SYSTEM PROVMODE
478	User	SHOW SYSTEM TIME
479	Sec_Off	SHOW SYSTEM USERCONFIG
480	User	SHOW TACPLUS
481	User	SHOW TRAFFICDESCRIPTOR[={tdname-list|ALL}]
482	User	SHOW USER[=login-name] [FULL]
483	User	SHOW VLAN [={ vlanname | vid | ALL }] [FORWARDINGMODE={ STD | UPSTREAMONLY | ALL }] [FULL]
484	User	SHOW VOICECALL
485	User	STOP TEST LCPECHOREQUEST [INTERFACE={ type:id-range | id-range | ifname-list | ALL }]
486	Manager	STOP TRANSFER={ transferid-list | ALL }
487	Sec_Off	STOP CONFIG
488	User	STOP PING
489	User	STOP TRACEROUTE
490	Manager	SWAP ACTIVITY [FORCE]
491	User	TELNET={ ipaddress | hostname }
492	User	TEST LCPECHOREQUEST INTERFACE={ type:id-range | id-range | ifname-list } [DELAY=1..900] [NUMBER={ 1..65535 | CONTINUOUS }] [TIMEOUT=1..900]
493	User	TRACEROUTE={ ipaddress | hostname } [FROM { INTERFACE={ type:id | id | ifname } | IPADDRESS=ipaddress }] [MINTTL=number] [MAXTTL=number] [TIMEOUT=seconds] [TOS=0..255] [NORESOLVE]

4. Command Descriptions

4.1 Overview

In the previous Section, the commands are listed by syntax only, so a command syntax could be looked up quickly. The row numbers are listed as well, and these match up with the row numbers used in this Section.

4.2 Command Listing

The following table lists the commands as follows:

- **Num**. - This number is referenced from the previous Section.
- **Syntax**
- **Command Description** - This is a detailed description of the command functions, and includes what specific parameters provide.

No.	Syntax	Description
1	ACTIVATE MEDIA=unit FORCE	The ACTIVATE MEDIA command brings the media card to an operational state of UP, with the status of Online indicating that it is available for service. During the activation sequence, the following steps are performed: - The device information is read - Out of service diagnostics are run - The file system on the media card is activated
2	ADD CLASSIFIER=classifiername INTERFACE={ type:id-range | id-range | ifname-list | ALL } PRECEDENCE=1..255	The ADD CLASSIFIER INTERFACE command serves the same purpose, but applies to INTERFACEs rather than PORTs. See the ADD CLASSIFIER=classifiername PORT={port-list|ALL} PRECEDENCE=1..255 command.
3	ADD DHCPRELAY={ dhcpname | MAIN } VLAN={ vlanname-list | vid-range | ALL }	Adds a VLAN (or set of VLANs) to the DHCPRELAY Instance(s)
4	ADD DHCPRELAY={ dhcpname-list | MAIN | ALL } SERVER=ipaddress-list	The ADD DHCPRELAY SERVER command is used to configure up to 10 DHCP server IP addresses with the Relay agent. The user can specify a single IP address or the comma separated list of IP addresses.
5	ADD EGRESSLIMITER=limitername INTERFACE={ type:id-range | id-range | ifname-list | ALL }	The ADD EGRESSLIMITER command associates an EGRESSLIMITER with one or more INTERFACEs. This limits the traffic that the system transmits through this INTERFACE to the values specified by the EGRESSLIMITER. A particular INTERFACE may only be associated with one EGRESSLIMITER, but a particular EGRESSLIMITER may be associated with any number of ports. EGRESSLIMITERs are not supported on LAG interfaces.
6	ADD EPSR=epsrdomain INTERFACE={ type:id-range | id-range | ifname-list } [TYPE={ PRIMARY | SECONDARY }]	The ADD EPSR INTERFACE command adds an Interface to the already existing EPSR domain. Only one interface can be specified at a time when the EPSR domain is of 'Master' node type. If it's a 'Transit' node type then user can specify two interfaces at a time. More than two interfaces are not allowed in any case. The optional parameter TYPE is used to designate the interface as PRIMARY or SECONDARY and its valid only in case of a 'Master' node. PRIMARY option is considered to be default if the user does not specify any TYPE. Two EPSR domains are considered to be in the same physical RING network if they share the same interfaces.
7	ADD EPSR=epsrdomain VLAN={ vlanname | vid } [TYPE={ CONTROL | DATA }]	The ADD EPSR VLAN command adds a VLAN to the already existing EPSR domain. The user can add a VLAN as a CONTROL or DATA type. A CONTROL vlan must be of UFO type. A CONTROL vlan once added to any EPSR domain cannot be added to any other domain either as CONTROL or DATA type. The interfaces associated with the EPSR domains shoud be tagged members of the CONTROL or DATA vlan being added to that domain. A DATA vlan cannot be associated with two EPSR domains that are part of the same physical RING network(EPSR domains having the same interfaces provisioned).
8	ADD HVLAN={ hvlanname | vid } INTERFACE={ type:id-range | id-range | ifname-list | ALL } [FRAME={ UNTAGGED | TAGGED }]	The ADD HVLAN command adds interfaces to the specified layer-2 virtual network. When adding interfaces to an HVLAN, some restrictions must be considered. - If an interface is part of a link aggregation group (LAG), all of the interfaces in the LAG must in the same HVLAN. Although a LAG interface can be added to a HVLAN by using 'interface' parameter. - If multiple interfaces are included in a request and one or many of the HVLAN-to-interface assignments fail, the entire operation fails. - An interface can only be associated with a single spanning tree after it is associated with a VLAN As an example, the following command adds interface 0 on card 4 to the interface-based VLAN called "Marketing" ADD HVLAN=Marketing INTERFACE=ETH:4.0 To add interfaces 8 through 10 on card 2 to the "Training" HVLAN as a tagged interface, use the following command: ADD HVLAN=Training INTERFACE=2.8-2.10 FRAME=TAGGED.

No.	Syntax	Description
9	ADD IGMPSNOOPING FLOODING { ALLSTANDARD | DVMRP | OSPFALL | OSPFDESIGNATED | RIP2 | IGRP | DHCPRELAY | PIM | RSVP | CBT | VRRP | DXCLUSTER | CISCONHAP | HSRP | MDNS | CUSTOM=groupname GROUPADDRESS=ipaddress }	The ADD IGMPSNOOPING FLOODING command is used to provision the reserved multicast IP addresses in the system, so that the provisioned addresses can be forwarded instead of being dropped.
10	ADD IGMPSNOOPING INTERFACE={ type:id-range | id-range | ifname-list | ALL } MACADDRESS={ macaddress-list | partial-macaddress-list }	The ADD IGMPSNOOPING command is used to configure the set-top box(STB) MAC address connected to a port on the switch. Up to five (5) STB MAC addresses can be configured for a given port. The purpose of this command is prevent STB mobility and prevent theft of the broadcast video service.
11	ADD INTERFACE={ type:id-range | id-range | ifname-list | ALL } RMONALERT { DROPEVENTS | OCTETS | PACKETS | BROADCAST | MULTICAST | UNDERSIZE | OVERSIZE | CRCALIGN | FRAGMENTS | JABBERS | COLLISIONS | PKTS64OCTETS | PKTS65TO127OCTETS | PKTS128TO255OCTETS | PKTS256TO511OCTETS | PKTS512TO1023OCTETS | PKTS1024TO1518OCTETS } { ABSOLUTE | CHANGE } { INTERVAL=2..3600 RISINGTHRESHOLD=threshold FALLINGTHRESHOLD=threshold }	The ADD INTERFACE RMONALERT command allows a user to specify threshold alarming settings for an Ethernet statistic on a specified interface. The supported Remote Monitoring (RMON) statistics for Ethernet interfaces are based on the RMON MIB (RFC2819). Samples are taken on an interval basis and compared to the provided thresholds. A management log and an SNMP trap are generated when either the rising or falling threshold is crossed.
12	ADD IP INTERFACE={ MGMT | type:id } IPADDRESS=ipaddress SUBNETMASK=mask [CARD={ slot | ACTCFC }] [IFNAME=ifname] [GATEWAY=ipaddress] [DOMAINNAME=name] [DNS=ipaddress-list]	The ADD IP INTERFACE command associates IP parameters with an existing interface. By default the interface is disabled. (To enable the interface see ENABLE IP INTERFACE). If the interface and telnet server are enabled (See ENABLE TELNET SERVER), users can log in to the system via the specified IP address.
13	ADD LAG=lagname INTERFACE={ type:id-range | id-range | ifname-list }	The ADD LAG command adds interfaces to a Link Aggregation Group (LAG). The LAG must already exist before interfaces are assigned to it (see CREATE LAG).Interfaces are identified using type:id-range|id-range|ifname-list notation, and can be added individually or as a comma-separated id-ranges or as a forward-slash separated type:id-ranges. All interfaces in a LAG must operate at the same speed and be in full duplex mode. An interface with STP enabled cannot be added to a LAG. All the interfaces in a LAG must belong to the same untagged VLANs. Interfaces in a LAG can belong to different tagged VLANs. Interfaces must be removed from a LAG prior to changing their untagged VLAN configuration or status. Interfaces in a LAG can change their tagged VLAN configuration independent of other interfaces in LAG. A mirror interface cannot belong to a LAG.
14	ADD LLDP INTERFACE={ type:id-range | id-range | ifname-list | ALL } OPTIONS [PORTDESC] [SYSNAME] [SYSDESC] [SYSCAP] [PORTVLAN] [VLANNAME] [PROTOVLAN] [PROTOCOL] [MACPHYCONFIGSTATUS] [POWERVIAMDI] [LINKAGGREGATION] [MAXFRAMESIZE] [EPSR] [UCP] [ALL]	Adds one or more OPTIONS to the Interface(s) for LLDP. Note that this command does not enable LDP (that is the SET LLDP INTERFACE MODE command), but adds values for these optional parameters.
15	ADD MLPPP=mlpppname INTERFACE={ type:id-range | id-range | ifname-list } [FORCE]	Add more PPP/DS1/E1 interfaces to an existing MLPPP group. If a DS1/E1 interface is specified and a PPP interface does not already exist on it, the PPP interface is implicitly created with default parameters, which are displayed. All members of the MLPPP group must be on the same card.
16	ADD PPP INTERFACE={ type:id-range | id-range | ifname-list } [RESTARTINTERVAL=seconds] [MAXTERMINATE={ value | CONTINUOUS }] [MAXCONFIGURE=value] [MAXFAILURE={ value | CONTINUOUS }] [ECHOREQUEST={ seconds | OFF }]	Creates a PPP interface instance for each of the specified underlying DS1/E1 interfaces, with the protocol parameter values specified. Each PPP interface will be named ppp:x where x is the ID of the underlying DS1/E1/DS0-bundle interface. Also creates an eth: interface with the same name. The values of MAXTERMINATE and MAXFAILURE will be limited to 1..1000, like MAXCONFIGURE. A larger value is CONTINUOUS.
17	ADD PROTECTIONGROUP=groupname INTERFACE={ type:id-range | id-range | ifname-list }	Adds an interface to a protection group. As long as one interface in a protection group is up the others are STANDBY and all alarms are suppressed.

No.	Syntax	Description
18	ADD QOSPOLICY=policyname INTERFACE={ type:id-range | id-range | ifname-list } { BRUUM | IPMC | BIDIRECTIONAL VLAN={ vlanname-list | vid-range | ALL } }	Requests to add a QOSPOLICY to an interface." - BRUUM and IPMC options are only available on the EPON interfaces - BIDIRECTIONAL option is only available on an ONU interface (or the ONU’s ETH) - Adding the “NONE” QOSPOLICY is effectively the same as DELETE QOSPOLICY. - VID or VID’s name should be validated before accepting the command.
19	ADD RADIUS SERVER={ ipaddress-list | hostname-list } SECRET=secret [AUTHPORT=1..65535] [ACCTPORT=1..65535] [RETRIES=0..10] [TIMEOUT=1..60] [AUTHENTICATION={ ON | OFF }] [ACCOUNTING={ ON | OFF }]	The ADD RADIUS SERVER command allows the user to set up a RADIUS server to be used for user authentication purposes. One or more IP addresses or hostnames plus a shared secret are required parameters. Users may optionally adjust the UDP port number to which the RADIUS requests should be directed (port 1812 by default), the number of times a request should be retried (3 by default) and the timeout in seconds for each request (5 seconds by default).
20	ADD STP INSTANCE={ stpname | mstid } VLAN={ vlanname | vid-range }	For MSTP. By default, all VLANs (and therefore all ports), belong to the Common STP Instance, the CIST. Once created, VLANs can be associated with the MSTI using this command: (VLANs can also be dis-associated with the MSTI as well.) The user can continue to associate VLANs with MSTIs until there are no VLANs associated with the CIST.
21	ADD TACPLUS SERVER={ ipaddress-list | hostname-list } KEY=key [PORT=1..65535] [RETRIES=0..10] [TIMEOUT=1..60] [AUTHENTICATION={ ON | OFF }] [AUTHORIZATION={ ON | OFF }] [ACCOUNTING={ ON | OFF }]	The ADD TACPLUS SERVER command allows the user to set up a TACACS+ server to be used for user authentication purposes. One or more IP addresses or hostnames plus a shared key are required parameters. Users may optionally adjust the TCP port number to which the TACACS+ requests should be directed (port 49 by default), the number of times a request should be retried (3 by default) and the timeout in seconds for each request (5 seconds by default).
22	ADD TRACE EPSR [={ epsrdomain-list | ALL }] MESSAGETYPE={ HEALTH | RINGUPFLUSH | RINGDOWNFLUSH | LINKDOWN | ALL } [INTERFACE={ type:id-range | id-range | ifname-list | ALL }]	Add an EPSR trace to an interface. Detailed call events pertaining to a port of set of ports can be obtained by defining and enabling trace log criteria.
23	ADD TRACE IGMPSNOOPING MESSAGETYPE={ REPORTV1 | REPORTV2 | LEAVE | GENERALQUERY | LASTMEMBERQUERY | ALL } [INTERFACE={ type:id-range | id-range | ifname-list | ALL }] [MACADDRESS={ macaddress | ALL }] [GROUPADDRESS={ ipaddress | ALL }]	This adds trace criteria. The parameters, when specified together in a single command, are taken to be AND'ed together. Multiple invocations of this command are OR'ed. If parameters are not specified, ALL is assumed.
24	ADD TRACE PPP [EVENT={ PORT | LCP | BCP | ECHO | FRAME | TIMER | ERRPROTO | MAIN | ALL }] [INTERFACE={ type:id-range | id-range | ifname-list | ALL }]	Starts sending logs to the Event log for specified LCP event(s) on the specified interface(s).
25	ADD TRACE VOICECALL [EVENT={ OPENLOOP | CLOSELOOP | MGCPOFFHOOK | MGCPONHOOK | MODEMDETECT | ALL }] [INTERFACE={ type:id-range | id-range | ifname-list | ALL }]	Add a voice call trace to an interface. Detailed call events pertaining to a port of set of ports can be obtained by defining and enabling trace log criteria. Currently voice call traces are restricted to POTS interfaces.
26	ADD USER=login-name PASSWORD=password [FORMAT={ CLEARTEXT | MD5 }] [DESCRIPTION=description] [PRIVILEGE={ USER | MANAGER | SECURITYOFFICER }] [LOGIN={ TRUE | FALSE | ON | OFF | YES | NO }] [TELNET={ YES | NO }] [PWDAGEING={ OFF | 0 | 1..365 }] [DEACTIVATE={ OFF | yyyy-mm-dd }]	Used to add new user accounts to the system. At a minimum, a user login name and password must be specified. The password can be clear text (non-encrypted) or in the form of a 32-character MD5 encrypted string. Unless the FORMAT option is specified, the password value is assumed to be clear text.
27	ADD USER=login-name PASSWORD=password [FORMAT={ CLEARTEXT | MD5 }] [DESCRIPTION=description] [PRIVILEGE={ USER | MANAGER | SECURITYOFFICER }] [LOGIN={ TRUE | FALSE | ON | OFF | YES | NO }] [TELNET={ YES | NO }] [SSH={ YES | NO } [PUBLICKEY=key-name]] [PWDAGEING={ OFF | 0 | 1..365 }] [DEACTIVATE={ OFF | yyyy-mm-dd }]	Used to add new user accounts to the system. At a minimum, a user login name and password must be specified. The password can be clear text (non-encrypted) or in the form of a 32-character MD5 encrypted string. Unless the FORMAT option is specified, the password value is assumed to be clear text.

No.	Syntax	Description
28	ADD VC=vcid INTERFACE={ type:id-range | id-range | ifname-list } VPI=0..255 VCI=32..65535 [TXPEAKCELLRATE={ 150..65535 | MAX }]	This command is used to create one or more VC(s) on one or more existing ATM interface(s). The default-VC is with VC-ID 0 and is created by system and so can not be added.
29	ADD VLAN={ vlanname | vid } INTERFACE={ type:id-range | id-range | ifname-list | ALL } [FRAME={ UNTAGGED | TAGGED }] [TRANSLATE={ 1..4094 }] [FORWARDING={ PRIMARYUPSTREAM | SECONDARYUPSTREAM | DOWNSTREAM | STP | UCP }]	The ADD VLAN command adds interfaces to the specified layer-2 virtual network. When adding interfaces to a VLAN, some restrictions must be considered. - If an interface is part of a link aggregation group (LAG), all of the interfaces in the LAG must in the same VLAN. Although a LAG interface can be added to a VLAN by using 'interface' parameter. - If multiple interfaces are included in a request and one or many of the VLAN-to-interface assignments fail, the entire operation fails. - An interface can only be associated with a single spanning tree after it is associated with a VLAN As an example, the following command adds interfaces 0 on card 4 to the interface-based VLAN called "Marketing" ADD VLAN=Marketing INTERFACE=ETH:4.0 To add interfaces 8 through 10 on card 2 to the 'Training'; V
30	ADD VLANTUNNELMAP VLAN={ vlanname-list | vid-range } HVLAN={ hvlanname | vid } [INTERFACE={ type:id-range | id-range | ifname-list }]	This command makes the association of the VLAN to a VLAN-based HVLAN tunnel. The tunnel is defined by the HVLAN and its interface membership.
31	ADD ACCESSLIST=accesslistname INTERFACE={ type:id-range | id-range | ifname-list }	See the ADD ACCESSLIST RULE command.
32	ADD ACCESSLIST=accesslistname RULE { PERMIT | DENY } [IPSOURCE={ ipaddress| ANY } [SOURCEMASK=mask]] [IPDEST={ ipaddress | ANY } [DESTMASK=mask]] [MACSOURCE={ macaddress | ANY }] [MACDEST={ macaddress | ANY }] [APPLICATION={ DHCPSERVER | DHCPCLIENT | NETBIOS | FUM | TELNET | SSH | SNMP| FTP | TFTP }] [TCPPORTDEST={ tcp-port-list | ANY }] [TCPPORTSOURCE={tcp-port | ANY }] [UDPPORTDEST={ udp-port-list | ANY }] [UDPPORTSOURCE={ udp-port | ANY }] [PROTOCOL={ IPV4 | IPV6 | protocol-type | ANY }] [IPPROTOCOL={ TCP | UDP | ICMP | IGMP | ipprotocol-type | ANY }] [BEFORE=rulenumber]	The ADD ACCESSLIST command does one of two things. It either adds a RULE to an ACCESSLIST or adds an ACCESSLIST to one or more INTERFACEs. An ACCESSLIST RULE has: - A match rule, which is a set of fieldname/fieldvalue pairs that discriminate among packets. A packet matches this rule only if all of the specified fields have the values specified. A match rule with no fieldname/fieldvalue pairs specified would match all packets. - The action that is to be performed if the incoming packet matches the RULE's match rule. The valid actions are PERMIT and DENY. The option BEFORE can be used to place the new RULE before an existing rule in the ACCESSLIST. By default the new RULE will be places at the end of the list (just before the default DENY). A RULE that is BEFORE another RULE in the list has higher precedence. Only one ACCESSLIST can exist on a given INTERFACE. Also, INTERFACEs can support only a limited number of RULEs (and CLASSIFIERs) and some INTERFACEs will not support all RULEs. Please refer to the User Guide for your product platform to find details on any restrictions.
33	ADD ACTION CLASSIFIER=classifiername-list { DROP | FORWARD | COUNT |SETVPRIORITY=0..7 | SETIPTOS=0..7 | SETIPDSCP=0..63 | MOVEPRIOTOTOS | MOVETOSTOPRIO }	The ADD ACTION CLASSIFIER command adds an ACTION to one or more CLASSIFIERs. As a result, when the CLASSIFIER is added to a port, the specified ACTION is performed on an incoming packet if the packet conforms to the CLASSIFIER's match rules, unless the ACTION conflicts with an ACTION on a matching CLASSIFIER with higher precedence. This command cannot add an ACTION that conflicts with an ACTION already on the CLASSIFIER. Note that some product platforms do not support all ACTIONs, or support them only in the presence of specific match fields. Please refer to the User Guide for your product platform to find details on any restrictions.

No.	*Syntax*	*Description*
34	ADD CLASSIFIER=classifiername PORT={port-list|ALL} PRECEDENCE=1..255	The ADD CLASSIFIER PORT command adds a CLASSIFIER to one or more PORTs. As a result, the CLASSIFIER is applied to every packet received on the PORT. This command attempts to add every specified combination of CLASSIFIER and PORT, and returns an error message for any combinations that cannot be added (e.g. due to conflicting PRECEDENCE, duplicate CLASSIFIERs, PORTs that do not exist). Because classifiers are a limited resource, there are constraints on the number of classifiers, and combinations of classifiers, that can be supported on a given physical interface. If these limits are exceeded, then an alarm is raised on the port and operational classifier behavior may differ from the classifier configuration. The "SHOW CLASSIFIER PORT" command shows details about errors loading the classifier configuration to a given port. Please refer to the User Guide for your product platform to find details on limits and restrictions.
35	ADD INTERFACE={ type:id-range | id-range | ifname-list | ALL } COUNTER HISTORY INTERVAL=interval-list [BUCKETS=1..2700]	The ADD INTERFACE COUNTER HISTORY command allows the user to create entries that specify data collection information for Remote Monitoring (RMON). A period of time to elapse (specified in seconds) between data collections called an INTERVAL is specified in the command as is the number of collections, called BUCKETS, to be retained before over writing the oldest BUCKET with newly collected data.
36	ADD LOG FILTER={filterid-list|ALL} OUTPUT=outputid	The ADD LOG FILTER command is used to associate existing management log filters with an existing management log output destination. After successful execution of this command, the specified management log output destination, if enabled, receives management logs that match the filter criteria contained in the management log filters (See ENABLE LOG OUTPUT).
37	ADD SNMP COMMUNITY=name [TRAPHOST=ipaddress-list] [V2CTRAPHOST=ipaddress-list] [MANAGER=ipaddress-list]	The ADD SNMP COMMUNITY command adds SNMPv1 and/or SNMPv2c trap host(s) and/or management station(s) to the specified SNMP community.
38	ADD SNTP SERVER={ipaddress|hostname}	The ADD SNTP SERVER command is used to identify an SNTP server used by the SNTP client in the device. The device only supports the specification of a single SNTP server. If an SNTP server is already specified, the command is rejected. To change the server, the existing server must be deleted using the DELETE SNTP SERVER command.
39	ADD TRAFFICDESCRIPTOR=tdname CLASSIFIER=classifiername-list {NCDROP | NCFORWARD} [NCCOUNT={ON|OFF}]	The ADD TRAFFICDESCRIPTOR command associates a TRAFFICDESCRIPTOR to one or more CLASSIFIER(s). As a result, the TRAFFICDESCRIPTOR is applied to all port/interfaces to which the CLASSIFIER(s) are associated. A particular TRAFFICDESCRIPTOR may be associated to any number of CLASSIFIERS, but a particular CLASSIFIER may have at most one TRAFFICDESCRIPTOR. Adding a TRAFFICDESCRIPTOR to a CLASSIFIER limits the ingress traffic flow, for packets matching the CLASSIFIER's match rules, to the RATE and BURSTSIZE indicated by the TRAFFICDESCRIPTOR. When an association is added between the TRAFFICDESCRIPTOR and the CLASSIFIER, some number of actions are added as well: - an NCDROP or NCFORWARD action, indicating whether to drop or forward non-conforming packets. - an indication of whether to increment the port's "Policed Count" on each non-conforming packet (NCCOUNT=ON). Defaults to not incrementing the counter (NCCOUNT=OFF). See the command "CREATE TRAFFICDESCRIPTOR" for help on creating new TRAFFICDESCRIPTORs. Not all RATEs and BURSTSIZEs are supported on all ports/interfaces. Also, TRAFFICDESCRIPTORs are not supported on LAG interfaces. Please refer to the User Guide for your product platform to find details on limits and restrictions.
40	AUDIT FILES	The AUDIT FILEs command audits all load files (files with extension .tar) and raises or clears file corruption alarms accordingly.

No.	*Syntax*	*Description*
41	BACKUP CONFIG FILE={ destinationfile | unit:destinationfile }	The BACKUP CONFIG command allows the user to create a configuration file which reflects current configuration of the system. This configuration file can be used to recreate the configuration on the same or similar system, using the RESTORE CONFIG command.
42	BACKUP DATABASE FILE={ destinationfile | unit:destinationfile | serverpath/destinationfile } [{ TFTP SERVER={ ipaddress | hostname } | ZMODEM | FTP SERVER={ ipaddress | hostname } USER=userid PASSWORD=password }]	The BACKUP DATABASE command backs up the contents of the system configuration database to a file on an external network server. The newly created file is not user readable or writable. While transfer of data is in progress, any configuration change caused by any CLI command aborts the transfer and the backup operation is cancelled.
43	CLEAR ALARMS CARD={ slot-list | ALL } MCASTGROUPLIMIT	The CLEAR ALARMS command clears the specified alarm condition on the given card. Currently only the MCASTGROUPLIMIT alarm can be cleared with this command.
44	CLEAR ALARMS PROTECTIONGROUP={ groupname-list | ALL }	Clears alarms on a protection group after the user has corrected the fault that caused the failover.
45	CLEAR DHCPRELAY INTERFACE={ type:id-range | id-range | ifname-list | ALL } { [IPADDRESS={ ipaddress-list | ALL }] | [MACADDRESS={ macaddress | ALL }] }	This command CLEAR DHCPRELAY allows the manual deletion of IP filters applied to the subscriber interfaces. Note that there is no means of manually adding an IP filter to an interface (this is performed automatically by DHCP Relay Agent, when filter is set to "on").
46	CLEAR DIAGNOSTICS [FORCE]	The CLEAR DIAGNOSTICS command is used to clear diagnostics results for all POTS lines.
47	CLEAR IP ARP [={ ipaddress-list | ALL }] [INTERFACE={ type:id-range | ifname-list | MGMT | ALL }] [FORCE]	This command is used to delete ARP entries for the user specified IP addresses or completely delete all entries in the ARP table if no IP addresses are specified. It is important to note that an ARP broadcast may rediscover and repopulate the ARP table with the recently deleted ARP entry.
48	CLEAR TRACE [FORCE]	The CLEAR TRACE command is used to remove all stored Trace logs from the system.
49	CLEAR SWITCH FDB [INTERFACE={type:id-range|id-range|ifname-list| ALL}] [ADDRESS=macaddress] [HVLAN={hvlanname|vid}]	The CLEAR SWITCH FDB clears the contents of the Forwarding Database. Parameters supported in the CLEAR SWITCH FDB command are: -- VLAN or HVLAN: The VID Identifier for the VLAN or HVLAN. -- MAC Address: The MAC address as learned from the source address field of a frame, or entered as part of a static filter entry. Example: 00:0C:25:00:13:8C -- Interface: The interface from which the MAC address was learned. To clear the contents of the Forwarding Database, use the CLEAR SWITCH FDB command.
50	CLEAR SWITCH FDB [INTERFACE={type:id-range|id-range|ifname-list| ALL}] [ADDRESS=macaddress] [VLAN={vlanname|vid}]	The CLEAR SWITCH FDB clears the contents of the Forwarding Database. Parameters supported in the CLEAR SWITCH FDB command are: -- VLAN or HVLAN: The VID Identifier for the VLAN or HVLAN. -- MAC Address: The MAC address as learned from the source address field of a frame, or entered as part of a static filter entry. Example: 00:0C:25:00:13:8C -- Interface: The interface from which the MAC address was learned. To clear the contents of the Forwarding Database, use the CLEAR SWITCH FDB command.
51	CONNECT INTERFACE={ type:id | ifname } TO={ type:id | ifname }	Associates two interfaces
52	COPY FILE={ sourcefile | unit:sourcefile } TO={ destinationfile | unit:destinationfile }	The COPY FILE command copies the specified source file to the specified destination file. The command is rejected if there is insufficient space on the CFC flash file system for the new file. For a 7700 with redundant CFCs, the operation is performed on both CFCs when they are both ONLINE. If either the source file or destination is a media card, the file name should be directly preceded by the unit name. For example, COPY FILE CFLASH9:myfile to myFile would copy the file myFile from the media card associated with CFC 9 to local flash.

No.	***Syntax***	***Description***
53	CREATE ALIAS=aliasname STRING=substitution	The CREATE ALIAS command allows the user to define shortcuts to command strings to simplify the use of the CLI. This list of alias commands is available for all users in the system. Validation is done on the alias name and its definition to ensure that the alias name has not already been created and that the definition does not reference itself. An alias name may not match all or part of existing CLI command root keywords. For example, since SHOW is an existing root keyword, there cannot be an alias name of "s", "sh", "sho", or "show". An alias string may consist of one or more valid CLI commands or other previously defined alias commands, separated by semicolons. The string may contain arguments, identified with a '$' and number, such as "$1 $2" etc. These arguments indicate placeholders where tokens will be substituted once the alias command is executed. The The integer value indicates the placement of the token in the command line. Examples of valid alias commands are: - CREATE ALIAS=su STRING="show user $1;show sys userconfig" - CREATE ALIAS=setu STRING="set user=$1 description=$1" - CREATE ALIAS=setuser STRING="set user=$1 password=$2 desc=$3" - CREATE ALIAS=showsys STRING="su $1;show sys time" Examples of valid executions of above aliases: officer> su officer officer> setu officer officer> setuser officer newpassword "Officer user description" officer> showsys officer
54	CREATE CARD=slot CES8 [{ [PREFLOAD=filename] [ADMINSTATE={ UP | DOWN }] [PORTTYPE={ DS1 | E1 }] | PROFILE=name }]	Creates the software provisioning for a CES8. Refer to the generic CREATE CARD for details.
55	CREATE CARD=slot NTE8 [{ [PREFLOAD=filename] [ADMINSTATE={ UP | DOWN }] [PORTTYPE={ DS1 | E1 }] | PROFILE=name }]	Creates the software provisioning for a NTE8. Refer to the generic CREATE CARD for an overview. For the NTE8, has the specific NTE8 attributes.
56	CREATE CARD=slot SHDSL16 [{ [PREFLOAD=filename] [WETTINGCURRENT={ ON | OFF }] [ANNEXTYPE={ A | B }] [WIREMODE={ NORMAL | BONDED }] [ADMINSTATE={ UP | DOWN }] | PROFILE=name }]	Creates the software provisioning for a SHDSL16. Refer to the generic CREATE CARD for an overview. For the SHDSL16, has the specific SHDSL16 attributes. Note that in 6.0 WETTINGCURRENT is not used.
57	CREATE CARD=slot SHDSL24 [{ [PREFLOAD=filename] [WETTINGCURRENT={ ON | OFF }] [ANNEXTYPE={ A | B }] [WIREMODE={ NORMAL | BONDED }] [ADMINSTATE={ UP | DOWN }] | PROFILE=name }]	Creates the software provisioning for a SHDSL24. Refer to the generic CREATE CARD for an overview. For the SHDSL24, has the specific SHDSL24 attributes. Note that in 7.0 WETTINGCURRENT is not used.
58	CREATE CONTACTALARM={ 0..2 } STATE={ OPEN | CLOSED } SEVERITY={ CRITICAL | MAJOR | MINOR | INFO } [MESSAGE=text]	The CREATE CONTACTALARM command provisions alarm attributes for dry contact input terminals. The input terminals can be connected to external equipment so that alarms can be generated by external stimulus, such as open door, motion detector, ambient temperature, etc. The trigger is defined by its contact number and its physical state (open or closed). Note that different triggers can be associated with different states for the same contact. For example, an alarm can be defined when a contact is open and a different alarm can be defined when the same contact is closed, if desired. Creation of an alarm trigger will generate an alarm immediately if the contact is already in the defined state.
59	CREATE DHCPRELAY=dhcpname [AGENT REMOTEID={ remote-id | DEFAULT }] [MODE={ RELAY | SNOOPING }] [SERVER={ ipaddress-list | NONE }] [VLAN={ vlanname-list | vid-range | ALL }]	Creates a DHCP Relay. Can associate with a VLAN ID
60	CREATE EGRESSLIMITER=limitername RATE=bits-per-second BURSTSIZE={ 4KB | 8KB | 16KB | 32KB | 64KB | 128KB | 256KB | 512KB | 1MB | 2MB | 4MB | 8MB | 16MB | 32MB | 64MB }	The CREATE EGRESSLIMITER command creates a new EGRESSLIMITER. EGRESSLIMITERs are used to limit the RATE and BURSTSIZE of traffic transmitted over a particular port or interface.

No.	Syntax	Description
61	CREATE EPSR=epsrdomain { TRANSIT | MASTER [HELLOTIME=value] [FAILOVERTIME=value] [RINGFLAPTIME=value] }	The CREATE EPSR command is used to create an EPSR domain. The domain being created can be of 'Transit' or 'Master' type. If its a 'Master' type domain then the user can also optionally set the HELLOTIME, FAILOVERTIME and RINGFLAPTIME. If the user does not specify these parameters, the default values are used during the EPSR domain creation.
62	CREATE HVLAN=hvlanname VID=2..4094 [TYPE={ PORTTUNNEL | VLANTUNNEL }]	Creates a Hierarchical Virtual LAN (HVLAN) entry with a unique name and identifier (VID). When an HVLAN entry is created, it is assigned to the default STP. To change the VID of an existing HVLAN, the HVLAN must be removed with the DESTROY HVLAN command and created again. A maximum of 4094 HVLANS/VLANS can be created with any VID in the range 2 to 4094. In release 7.0, the user can choose the port-based HVLAN (PORTTUNNEL) or VLAN-based HVLAN (VLANTUNNEL).
63	CREATE LOG OUTPUT=outputid [{ CLI [FORMAT={ FULL | MSGONLY | SUMMARY }] | CONSOLE [FORMAT={ FULL | MSGONLY | SUMMARY }] | SYSLOG SERVER={ ipaddress | hostname } | FILE=unit:filename [FORMAT={ FULL | MSGONLY | SUMMARY }] }]	The CREATE LOG OUTPUT command creates management log output destinations. Management log output destinations are used to direct a filtered management log stream to a specific destination. Currently, supported destinations include a CLI session, the system console and a Syslog server. Note that CLI session output destinations are not persisted. If a user sets up a management log output destination and then subsequently logs out, that management log output destination is removed from the system. In addition, created log output destinations are disabled upon creation. Execute the ENABLE LOG OUTPUT command to enable the management log output destination for output.
64	CREATE MLPPP=mlpppname ID=8..15 INTERFACE={ type:id-range | id-range | ifname-list } [SEGMENTSIZE={ 64..1526 }] [SEQUENCENUMBERBITS={ 12 | 24 }] [FORCE]	Creates a single MLPPP instance and associatse it with the specified set of underlying interfaces. The interfaces may be PPP interfaces, DS1/E1 interfaces, or a mix. If a DS1/E1 interface is specified and a PPP interface does not already exist on it, the PPP interface is implicitly created with default parameters, which are displayed.
65	CREATE ONU=onuname ONUID=0..15 INTERFACE={ type:id | id | ifname } MACADDRESS=macaddress	Creates an ONU interface and its associated ETH interface. - Adds the ETH interface to the default VLAN, untagged. - ONU interfaces share the same namespace as other interface names.
66	CREATE PROFILE=name ADSLPORT [MODE={ GLITE | GDMT | T1.413 | ADSL2 | ADSL2+ | AUTO | AUTO2+ | ADSL2M | ADSL2+M }] [BITMAPMODE={ FBM | DBM }] [LINETYPE={ FAST | INTERLEAVE }] [INTERLEAVEDELAY=1..64] [ECHOCANCELLATION={ ON | OFF }] [DATABOOST={ ON | OFF }] [MAXUPSTREAMRATE=32..3072] [MINUPSTREAMRATE=32..3072] [MAXDOWNSTREAMRATE=32..26624] [MINDOWNSTREAMRATE=32..26624] [TARGETSNRMARGIN=0..15] [MAXSNRMARGIN={ OFF | 1..30 }] [LINEQUALITYMONITOR={ LOW | MEDIUM | HIGH }] [VPI=0..4095] [VCI=32..65535] [ADMINSTATE={ UP | DOWN }]	Creates a Profile for an ADSL port. Once defined, it can be associated with the appropriate ADSL port type
67	CREATE PROFILE=name cardtype [PREFLOAD=filename] [ADMINSTATE={ UP | DOWN }]	Creates a profile for the specfied card type. Atttributes required are usually the PREFLOAD and ADMINSTATE. For release 7.0, cardtypes with this syntax are ADSL16B, ADSL16C, ADSL16, ADSL24A, ADSL24B, ADSL24, ADSL8S, CES8, CFC24, CFC4, CFC6, FE10, FE2, FX10, GE1, GE2, GE3, and POTS24. In release 8.0 new cards are CFC56, EPON2, VDSL24A, VDSL24B, and XE1.

No.	*Syntax*	*Description*
68	CREATE PROFILE=name DS1PORT [ADMINSTATE={ UP CREATE PROFILE=name DS1PORT [ADMINSTATE={ UP | DOWN }] [TIMINGREFERENCE={ SELF | CONNECTION | CARD }] [LINEENCODING={ B8ZS | AMI }] [LINEBUILDOUT { LONGHAUL={ 0.0DB | -7.5DB | -15.0DB | -22.5DB } | SHORTHAUL={ 133FT | 266FT | 399FT | 533FT | 655FT } }] [FRAMING={ UNFRAMED | SF | ESF | STANDARD }] | DOWN }] [TIMINGREFERENCE={ SELF | CONNECTION | CARD }] [LINEBUILDOUT { LONGHAUL={ 0.0DB | -7.5DB | -15.0DB | -22.5DB } | SHORTHAUL={ 133FT | 266FT | 399FT | 533FT | 655FT } }] [LINEENCODING={ B8ZS | AMI }] [LOOPBACK={ NONE | INWARD | LINE }]	Creates a Profile for a DS1 Port. The profile can then be associated with a DS1 port.
69	CREATE PROFILE=name E1PORT [ADMINSTATE={ UP | DOWN }] [TIMINGREFERENCE={ SELF | CONNECTION | CARD }] [LINEENCODING={ HDB3 | AMI }] [FRAMING={ UNFRAMED | E1 | E1CRC | STANDARD }]	Creates a Profile for an E1 port. Once created, this profile can be associated with an E1 port.
70	CREATE PROFILE=name EPONPORT [ADMINSTATE={ UP | DOWN }] [IPMCVLAN={ vlanname | vid }] [IPADDRESS=ipaddress]	Creates the profile for the EPON port. The IPMC VLAN is the VLAN that is used for broadcast (video) traffic. The IP address identifies the EPON as the IGMP entity that the Multicast router will request reports from.
71	CREATE PROFILE=name FEPORT [ADMINSTATE={ UP | DOWN }] [AUTONEGOTIATION={ ON | OFF }] [SPEED={ AUTONEGOTIATE | 10 | 100 }] [DUPLEX={ AUTONEGOTIATE | FULL | HALF }] [FLOWCONTROL={ AUTONEGOTIATE | ON | OFF }]	Creates a Profile for an FE port. Once defined, it can be associated with FE port(s)
72	CREATE PROFILE=name FXPORT [FLOWCONTROL={ ON | OFF }] [ADMINSTATE={ UP | DOWN }]	Creates a Profile for an FX port. Once defined, it can be associated with FX port(s)
73	CREATE PROFILE=name GEPORT [AUTONEGOTIATION={ ON | OFF }] [SPEED={ AUTONEGOTIATE | 10 | 100 | 1000 }] [DUPLEX={ AUTONEGOTIATE | FULL | HALF }] [FLOWCONTROL={ AUTONEGOTIATE | ON | OFF }] [ADMINSTATE={ UP | DOWN }]	Creates a Profile for a GE port. Once defined, it can be associated with GE port(s)
74	CREATE PROFILE=name NTE8 [PREFLOAD=filename] [ADMINSTATE={ UP | DOWN }] [PORTTYPE={ DS1 | E1 }]	Creates a Profile for an NTE8 card. Once created, it can be associated with NTE8 card(s).
75	CREATE PROFILE=name POTSPORT [CAPABILITY={ PCMU | G726 | ALL }] [MINPACKETIZATION=10..30] [MAXPACKETIZATION=10..30] [BUFFERDELAY=0..150] [BUFFERMODE={ STATIC | DYNAMIC }] [TXPREECHOGAIN=-9.0..+3.0] [TXPOSTECHOGAIN=-9.0..+3.0] [RXPREECHOGAIN=-9.0..+3.0] [RXPOSTECHOGAIN=-9.0..+3.0] [ECHOCANCELLATION={ ON | OFF }] [VOICEACTIVITYDETECTION={ ON | OFF }] [COMFORTNOISEGENERATION={ ON | OFF }] [PACKETLOSSCONCEALMENT={ ON | OFF }] [ADMINSTATE={ UP | DOWN }]	Creates a Profile for a POTS port. Once defined, it can be associated with the appropriate ADSL port type
76	CREATE PROFILE=name SHDSL16 [PREFLOAD=filename] [ADMINSTATE={ UP | DOWN }] [WETTINGCURRENT={ ON | OFF }] [ANNEXTYPE={ A | B }] [WIREMODE={ NORMAL | BONDED }]	Creates a Profile for a SHDSL card. Once created, it can be associated with a SHDSL16 card.
77	CREATE PROFILE=name SHDSL24 [PREFLOAD=filename] [ADMINSTATE={ UP | DOWN }] [WETTINGCURRENT={ ON | OFF }] [ANNEXTYPE={ A | B }] [WIREMODE={ NORMAL | BONDED }]	Create the SHDSL card profile with the appropriate attribute values.

<table>
<tr><th>No.</th><th>Syntax</th><th>Description</th></tr>
<tr><td>78</td><td>CREATE PROFILE=name SHDSLPORT [MAXCONNECTRATE=72..2312] [MINCONNECTRATE=72..2312] [TARGETSNRMARGIN=0..10] [LINEQUALITYMONITOR={ LOW | MEDIUM | HIGH }] [VPI=0..4095] [VCI=32..65535] [ADMINSTATE={ UP | DOWN }]</td><td>Create the SHDSLPORT Profile with the appropriate attribute values</td></tr>
<tr><td>79</td><td>CREATE PROFILE=name VDSLPORT [MODE={ VDSL2 | GLITE | GDMT | T1.413 | ADSL2 | ADSL2+ | AUTO | AUTO2 | ADSL2M | ADSL2+M }] [LINETYPE={ FAST | INTERLEAVE }] [MAXUPSTREAMRATE=32..14848] [MINUPSTREAMRATE=32..14848] [MAXDOWNSTREAMRATE=32..51200] [MINDOWNSTREAMRATE=32..51200] [TARGETSNRMARGIN=snr-margin-dB] [MAXSNRMARGIN={ OFF | snr-margin-dB }] [MINSNRMARGIN={ OFF | snr-margin-dB }] [MAXRECEIVEPOWER={ OFF | value }] [BANDPLAN={ 997 | 998 }] [OPTUPSTREAMBAND={ ON | OFF }] [RFIBAND={ { 30M | 40M | 80M | 160M } [,...] | NONE | ALL }] [MAXINTERLEAVEDELAY=0..255] [MINIMPULSENOISEPROTECTION UPSTREAMMININP={ 0 | 0.5 | 1 | 2 | 4 | 8 | 16 } DOWNSTREAMMININP={ 0 | 0.5 | 1 | 2 | 4 | 8 | 16 }] [DEPLOYMENT={ CABINET | CENTRALOFFICE }] [PSDMASK UPSTREAMPSDMASK={ MASK1 | MASK2 } DOWNSTREAMPSDMASK={ MASK1 | MASK2 }] [DATABOOST={ ON | OFF }] [LINEQUALITYMONITOR={ LOW | MEDIUM | HIGH }] [VPI=0..4095] [VCI=32..65535] [ADMINSTATE={ UP | DOWN }]</td><td>For future release</td></tr>
<tr><td>80</td><td>CREATE PROFILE=name XEPORT [AUTONEGOTIATION={ ON | OFF }] [FLOWCONTROL={ AUTONEGOTIATE | ON | OFF }] [ADMINSTATE={ UP | DOWN }]</td><td>Creates a Profile for an XE port. Once defined, it can be associated with XE port(s)</td></tr>
<tr><td>81</td><td>CREATE PROTECTIONGROUP=groupname</td><td>Create a protection group and name it.</td></tr>
<tr><td>82</td><td>CREATE PSPAN=pspanname PSPANID=0..127 SATOP { INTERFACE={ VLAN:id | id | ifname } | IPADDRESS=ipaddress } { UDPPORT=49152..65535 } { PEERIPADDRESS=ipaddress } { PEERUDPPORT=49152..65535 } [NUMBYTES=16..1023] [JITTERBUFFER=value] [TIMINGREFERENCE={ SELF | CONNECTION | CARD }] [RTP={ ON | OFF }] [VPRIORITY=0..7] [IPDSCP=0..63]</td><td>Creates the PSAPN and implicitely the VLAN and its IP address. The PSPAN name should be descriptive. Use the connect command to connect the PSPAN and the T1 interface</td></tr>
<tr><td>83</td><td>CREATE QOSPOLICY=policyname [DESCRIPTION=text] [MAXUPSTREAMRATE={ bits-per-second | MAX }] [MAXDOWNSTREAMRATE={ bits-per-second | MAX }] [MINUPSTREAMRATE={ bits-per-second | MIN }] [MINDOWNSTREAMRATE={ bits-per-second | MIN }] [UPBURSTSIZE={ 1..256 | MAX }] [DOWNBURSTSIZE={ 1..256 | MAX }] [UPDELAYSENSITIVITY={ SENSITIVE | TOLERANT }] [DOWNDELAYSENSITIVITY={ SENSITIVE | TOLERANT }]</td><td>Requests to create a QOSPOLICY. The bits-per-second values can be entered with a “units” postfix (e.g. “512K” means 512Kbps, while “10M” means 10000Kbps). The bits-per-second values can be between 512K and 1000M (not 1G). The values of “MIN” and “MAX” will be appropriate to the interface. In this case “MIN” will be set to minimize bandwidth while ensuring OAMPDU flow, and “MAX” will be 1000Mbps. Default burst values are all 100K.</td></tr>
<tr><td>84</td><td>CREATE STP INSTANCE=stpname MSTID=1..4094 [PRIORITY=0..65535]</td><td>For MSTP, create an STP instance and give it a name as well as ID. VLANs can then be associated with this instance.</td></tr>
<tr><td>85</td><td>CREATE TRAFFICDESCRIPTOR=tdname RATE=bits-per-second BURSTSIZE={ 4KB | 8KB | 16KB | 32KB | 64KB | 128KB | 256KB | 512KB | 1MB | 2MB | 4MB | 8MB | 16MB | 32MB | 64MB }</td><td>The CREATE TRAFFICDESCRIPTOR command creates a new TRAFFICDESCRIPTOR. A TRAFFICDESCRIPTOR is used to define the maximum bandwidth and buffer memory (defined by RATE and BURSTSIZE) allowed for a particular traffic flow. Particular traffic flows can be metered and/or policed by associating a TRAFFICDESCRIPTOR with a classifier. The classifier identifies the packets that make up the traffic flow, and the TRAFFICDESCRIPTOR describes the maximum values allowed for that traffic flow. See the command "ADD TRAFFICDESCRIPTOR" for help on how to associate a TRAFFICDESCRIPTOR to a classifier.</td></tr>
</table>

No.	*Syntax*	*Description*
86	CREATE ACCESSLIST=accesslistname [RULE { PERMIT | DENY } [IPSOURCE={ipaddress | ANY } [SOURCEMASK=mask]] [IPDEST={ ipaddress | ANY } [DESTMASK=mask]] [MACSOURCE={ macaddress | ANY }] [MACDEST={ macaddress| ANY }] [APPLICATION={ DHCPSERVER | DHCPCLIENT | NETBIOS | FUM | TELNET| SSH | SNMP | FTP | TFTP }] [TCPPORTDEST={ tcp-port-list | ANY }] [TCPPORTSOURCE={ tcp-port | ANY }] [UDPPORTDEST={ udp-port-list | ANY }][UDPPORTSOURCE={ udp-port | ANY }] [PROTOCOL={ IPV4 | IPV6 | protocol-type | ANY }] [IPPROTOCOL={ TCP | UDP | ICMP | IGMP | ipprotocol-type |ANY }]] [INTERFACE={ type:id-range | id-range | ifname-list }]	The CREATE ACCESSLIST command creates an ACCESSLIST. ACCESSLISTs are used to filter traffic at ingress to an interface or set of interfaces. An ACCESSLIST contains a group of RULEs each of which supports performing an action to certain received packets. Actions are restricted to blocking or allowing traffic. The use of RULE and/or INTERFACE during the creation of ACCESSLISTs is optional. RULEs may be added to the ACCESSLIST and/or the ACCESSLIST added to INTERFACEs later using the ADD ACCESSLIST commands. An ACCESSLIST RULE has: - A match rule, which is a set of fieldname/fieldvalue pairs that discriminate among packets. A packet matches this rule only if all of the specified fields have the values specified. A match rule with no fieldname/fieldvalue pairs specified would match all packets. - The action that is to be performed if the incoming packet matches the RULE's match rule. The valid actions are PERMIT and DENY. The match rule and action are specified together by CREATE ACCESSLIST, ADD ACCESSLIST RULE, and SET ACCESSLIST RULE commands. The numbering of ACCESSLIST RULEs represents the relative precedence of that RULE to other RULEs in the list. RULE 1 is checked before rule 2 and so on. For example, if RULE 1 is a DENY that matches IPSOURCE 1.1.1.1 and RULE 2 is a PERMIT that matches all packets, then all packets are PERMITED except those from the address 1.1.1.1. RULE numbers can change as RULEs are inserted or removed. All ACCESSLISTs contain the default RULE to DENY all packets. This means that a default ACCESSLIST (i.e. one created by CREATE ACCESSLIST with no rules) would always drop all packets. The default DENY rule is always the last RULE in the list and cannot be deleted or modified. An ACCESSLIST may be associated with many INTERFACEs. ACCESSLISTs are associated to INTERFACEs during creation using the CREATE ACCESSLIST command or afterwards with the ADD ACCESSLIST command. ACCESSLIST RULEs are implemented using CLASSIFIERS. The CLASSIFIERS used to implement a specific rule can be seen using the FULL option on the SHOW CLASSIFIERS commands.
87	CREATE CARD=slot card_type [{[PREFLOAD=filename] [ADMINSTATE={UP|DOWN}]| PROFILE=name}]	The CREATE CARD command creates software provisioning for a card in a specific slot. A CARD is a field replaceable module that occupies a slot. The ports on the specified card are automatically provisioned when the card is provisioned. The CFC6 (Control Module) and FC7 (Fan Control Module in the x400 system) are automatically provisioned during system startup and are not affected by the CREATE CARD command. For release 6.0, the cards that can be created are CES8, CFC24, CFC6, FE10, FX10, GE1, GE3, POTS24, SHSDL16, ADSL16B, ADSL16C, ADSL16, ADSL24A, ADSL24B, ADSL24, ADSL8S. New for release 6.0 are the ADSL16C, ADSL24A, and ADSL24B cards. New for 7.0 are the SHDSL24 and NTE8. The SHDSL16/24 is modified for 4-wire bonding. New for 8.0 are the CFC56, XE1, VDSL24A, VDSLB, and EPON2 cards. At minimum, when creating a card, the user must specify the slot number and the card type. The other attributes are set based on the following: - if no other parameters are entered, the card and its ports are provisioned using default values - any individual card attributes that are entered are used, any card attributes not specifically entered are set to default, all port attributes are set to default - if the card auto provisioning profile is specified, then all card attributes are set to the values in the card auto provisioning profile and all port attributes are set to the values in the port auto provisioning profile

<table>
<tr><th>No.</th><th>Syntax</th><th>Description</th></tr>
<tr><td>88</td><td>CREATE CLASSIFIER=classifiername[VID={1..4095|ANY}] [VPRIORITY={0..7|ANY}] [INNERVID={1..4095|ANY}] [INNERVPRIORITY={0..7|ANY}] [ETHFORMAT={802.3|802.3TAGGED|802.3UNTAGGED |ETHII|ETHIITAGGED|ETHIIUNTAGGED |ANY}] [LSAP={NETBIOS|lsap-value|ANY}] [IPDEST={ipaddress-mask|MULTICAST|ANY}] [IPSOURCE={ipaddress-mask|ANY}] [IPDSCP={0..63|ANY}] [IPPROTOCOL={TCP|UDP|ICMP|IGMP| ipprotocol-number|ANY}] [IPTOS={0..7|ANY}] [MACDEST={macaddress|MULTICAST|ANY}] [MACSOURCE={macaddress|ANY}] [PROTOCOL={IPV4|IPV6|protocol-type|ANY}] [TCPPORTDEST={tcp-port-list|ANY}] [TCPPORTSOURCE={tcp-port|ANY}][TCPFLAGS={{URG|ACK|RST|SYN|FIN|PSH}[,...] |ANY}] [UDPPORTDEST={udp-port-list|ANY}] [UDPPORTSOURCE={udp-port|ANY}]</td><td>The CREATE CLASSIFIER command creates a CLASSIFIER. A CLASSIFIER supports performing certain actions to certain received packets. A CLASSIFIER has: - A match rule, which is a set of fieldname/fieldvalue pairs that discriminate among packets. A packet matches this rule only if all of the specified fields have the values specified. The match rule is specified by CREATE CLASSIFIER and SET CLASSIFIER commands. - Zero or more match actions, which are performed if the incoming packet matches the CLASSIFIER's match rule. A CLASSIFIER's actions are managed via ADD ACTION and DELETE ACTION commands. - Zero or one traffic descriptors, which specify a profile (traffic rate and burst size) for packets that match the CLASSIFIER's match rule. A CLASSIFIER's association to a traffic descriptor is managed via the ADD TRAFFICDESCRIPTOR and DELETE TRAFFICDESCRIPTOR commands. A default CLASSIFIER (i.e. one created by CREATE CLASSIFIER with no match fields) always matches all packets. If a CLASSIFIER has no match actions, then the default action is to FORWARD. A CLASSIFIER may be associated with many ports. CLASSIFIERs are associated to ports using the ADD CLASSIFIER command.</td></tr>
<tr><td>89</td><td>CREATE LAG=lagname [INTERFACE={ type:id-range | id-range | ifname-list }][MODE={ ON | OFF | PASSIVE | ACTIVE }] [SELECT={ MACSRC | MACDEST |MACBOTH | IPSRC | IPDEST | IPBOTH | PORTSRC | PORTDEST }] [ADMINKEY=1..1024]</td><td>The CREATE LAG command creates a Link Aggregation Group(LAG). When a LAG is created, the user must specify a unique identifier or allow the system to assign an identifier. The LAG ID is used for SET, DESTROY, SHOW, ADD, and DELETE commands for the LAG. Optionally, ports belonging to the LAG can be specified at LAG creation time, as well as the MODE, SELECT criteria, and ADMINKEY. Interfaces can also be added to the LAG at a later time via ADD LAG command. If the optional parameters for the command are not supplied, the following defaults are used: - MODE=OFF - SELECT=MACBOTH - ADMINKEY=automatically assigned The MODE, SELECT, and ADMINKEY parameters can all be set at a later time, using the SET LAG command.</td></tr>
<tr><td>90</td><td>CREATE LOG FILTER=filterid [CATEGORY=category] [SEVERITY=[op]{CRITICAL|MAJOR|MINOR|NONE}]</td><td>The CREATE LOG FILTER command creates a management log filter. Management log filters are used to set filter criteria for management logs. If a management log passes the criteria in a given log filter, the management log is routed to all of the management log output destinations that are associated with that filter via the ADD LOG FILTER command. By default, without a category or severity value specified, a management log filter matches all logs.</td></tr>
<tr><td>91</td><td>CREATE LOG OUTPUT=outputid [{CLI [FORMAT={FULL|MSGONLY|SUMMARY}]| CONSOLE [FORMAT={FULL|MSGONLY|SUMMARY}]| SYSLOG SERVER={ipaddress|hostname}}]</td><td>Deleted</td></tr>
<tr><td>92</td><td>CREATE SNMP COMMUNITY=name [ACCESS={READ|WRITE}] [V2CTRAPHOST=ipaddress-list] [TRAPHOST=ipaddress-list] [MANAGER=ipaddress-list]</td><td>The CREATE SNMP COMMUNITY command creates an SNMP community. Optionally, the command sets the access mode for the community and defines a trap host and manager. Trap hosts and managers are also added through the ADD SNMP COMMUNITY command. The community is disabled by default and needs to be explicitly enabled before attempting to access the device. (See ENABLE SNMP COMMINITY).</td></tr>
<tr><td>93</td><td>CREATE VLAN=vlanname VID=2..4094 [FORWARDINGMODE={STD|UPSTREAMONLY}]</td><td>The CREATE VLAN command creates a Virtual LAN (VLAN) entry with a unique name and identifier (VID). When a VLAN entry is created, it is assigned to the default STP. To change the VID of an existing VLAN, the VLAN must be removed with the DESTROY VLAN command and created again. A maximum of 4094 HVLANS/VLANS can be created with any VID in the range 2 to 4094. The user can configure up to 24 VLANs that use UFO, and these can be anywhere in the 1-4094 range. Refer to the Telesyn User Guide for details for each product.</td></tr>
</table>

No.	Syntax	Description
94	DEACTIVATE MEDIA=unit [FORCE]	The DEACTIVATE MEDIA command brings the media card to an operational state of DOWN, with the status of Offline indicating that is not available for service. During the deactivation sequence, the following steps are performed: - Applications that could be using the media card are polled for approval. If there is an operation in progress, the request to deactivate the device may be denied. - The file system on the media card is deactivated.
95	DEACTIVATE SESSION={session-list|ALL} [{CANCEL|[MESSAGE=message-text][DELAY=1..600]}]	The DEACTIVATE SESSION command provides a means to force a user off the system. There are two primary modes of operation for the command. By running the command with just a session id, the associated user is forced off immediately. If there is a need to offer users an opportunity to complete their work before logging off, the DELAY and MESSAGE options can be used. If delayed deactivation is used, the deactivation can be aborted through the use of the CANCEL option. Session Id values can be found by running the SHOW SESSIONS command. The session Id corresponds to either the console number (0) or one of the 10 telnet sessions. The SHOW SESSION command will indicate which sessions have been initiated for a delayed deactivation. A number in the 'Deact' column indicates the number of seconds left before that session is forced off.
96	DELETE CLASSIFIER=classifiername-list INTERFACE={ type:id-range | id-range | ifname-list | ALL }	The DELETE CLASSIFIER INTERFACE command serves the same purpose as the DELETE CLASSIFIER=classifiername-list PORT={port-list|ALL} command, but applies to INTERFACEs rather than PORTs. See DELETE CLASSIFIER=classifiername-list PORT={port-list|ALL}.
97	DELETE DHCPRELAY={ dhcpname-list | MAIN | ALL } SERVER={ ipaddress-list | ALL } [FORCE]	The DELETE DHCPRELAY SERVER command is used to delete the DHCP server IP addresses configured with the Relay agent instance(s). The user can specify a single IP address or the comma seperated list of IP addresses.
98	DELETE DHCPRELAY={ dhcpname-list | MAIN | ALL } VLAN={ vlanname-list | vid-range | ALL }	Disassociates a DHCP Relay instance (or set of instances) with a VLAN (or set of VLANs)
99	DELETE EGRESSLIMITER=limitername INTERFACE={ type:id-range | id-range | ifname-list | ALL }	The DELETE EGRESSLIMITER command removes the association of an EGRESSLIMITER with one or more INTERFACEs. This removes this limit on the traffic that the system transmits through this INTERFACE.
100	DELETE EPSR={ epsrdomain-list | ALL } INTERFACE={ type:id-range | id-range | ifname-list | ALL }	The DELETE EPSR INTERFACE command deletes an Interface from the already existing EPSR domain. This operation is only allowed when the EPSR domain is disabled.
101	DELETE EPSR={ epsrdomain-list | ALL } VLAN={ vlanname | vid | ALL }	The DELETE EPSR VLAN command deletes a VLAN from the already exisiting EPSR domain. This operation is only allowed when the EPSR domain is disabled.
102	DELETE FILES={ filename-pattern | unit:filename-pattern } [FORCE]	The DELETE FILE command deletes the specified file from the CFC flash file system. The file must already exist on the CFC flash file system. The command is disallowed if the specified file is already designated as a preferred load file for a provisioned card. The command is allowed for files that are designated as alternate or temporary load files for a provisioned card. For a 7700 with redundant CFCs, the operation is performed on both CFCs when they are both ONLINE. The DELETE FILE command can also be used to delete the specified file from a media card. In this case, file name must be preceded by the unit name, for example CFLASH9:myFile.

No.	*Syntax*	*Description*
103	DELETE HVLAN={ hvlanname | vid } INTERFACE={ type:id-range | id-range | ifname-list | ALL }	The DELETE HVLAN command removes the interface association from the specified Hierarchical VLAN (HVLAN) Once an untagged interface is disassociated with all user-defined HVLANs, it is automatically added to the default VLAN (VID=1). A user cannot remove the association between the default VLAN and an untagged interface if the interface has no other HVLAN/VLAN associations. If a group of interfaces is included in the command and the association of any one of them cannot be removed, the entire operation fails and no interfaces are removed from the HVLAN.
104	DELETE IGMPSNOOPING FLOODING { ALL | ALLSTANDARD | DVMRP | OSPFALL | OSPFDESIGNATED | RIP2 | IGRP | DHCPRELAY | PIM | RSVP | CBT | VRRP | DXCLUSTER | CISCONHAP | HSRP | MDNS | CUSTOM=groupname }	The DELETE IGMPSNOOPING FLOODING command is used to delete the reserved multicast IP addresses from the system, so that the requested addresses can be dropped instead of being forwarded.
105	DELETE IGMPSNOOPING INTERFACE={ type:id-range | id-range | ifname-list | ALL } MACADDRESS={ macaddress-list | partial-macaddress-list | ALL }	The DELETE IGMPSNOOPING command is used to delete either some or all of the set-top box(STB) MAC addresses that have been configured for a given port.
106	DELETE INTERFACE={ type:id-range | id-range | ifname-list | ALL } COUNTER HISTORY [INTERVAL={ interval-list | ALL }]	The DELETE INTERFACE COUNTER HISTORY command allows the user to delete entries that specify data collection information for Remote Monitoring (RMON). A period of time to elapse (specified in seconds) between data collections called an INTERVAL is spcified in the command to uniquely identify the entries to be deleted. NOTE: collected buckets of historical data are deleted along with the data collection entry responsible for them.
107	DELETE IP INTERFACE={ MGMT | type:id-range | ifname-list | ALL } [FORCE]	The DELETE IP INTERFACE command removes the association of IP parameters with an existing interface.
108	DELETE LLDP INTERFACE={ type:id-range | id-range | ifname-list | ALL } OPTIONS [PORTDESC] [SYSNAME] [SYSDESC] [SYSCAP] [PORTVLAN] [VLANNAME] [PROTOVLAN] [PROTOCOL] [MACPHYCONFIGSTATUS] [POWERVIAMDI] [LINKAGGREGATION] [MAXFRAMESIZE] [EPSR] [UCP] [ALL]	Deletes one or more OPTIONS to the Interface(s) for LLDP. Note that this command does not disable LDP (that is the SET LLDP INTERFACE MODE command), but adds values for these optional parameters.
109	DELETE MLPPP={ mlpppname-list | ALL } INTERFACE={ type:id-range | id-range | ifname-list | ALL } [FORCE]	Deletes the PPP/DS1/E1 interfaces from an MLPPP group. The PPP interfaces remain on the DS1/E1 interfaces after this disassociation, and new eth: interfaces corresponding to the PPP interfaces are created. The original eth: interface for the MLPP also remains.
110	DELETE PPP INTERFACE={ type:id-range | id-range | ifname-list } [FORCE]	Deletes the PPP interface instances from the specified list of underlying DS1/E1 interfaces. The user is prompted for confirmation, because this also removes the ETH interface and all associated provisioning. (The FORCE option skips the confirmation.)
111	DELETE PROTECTIONGROUP=groupname INTERFACE={ type:id-range | id-range | ifname-list | ALL }	Delete an interface from a protection group.
112	DELETE QOSPOLICY={ policyname-list | ALL } INTERFACE={ type:id-range | id-range | ifname-list | ALL } { BRUUM | IPMC | BIDIRECTIONAL VLAN={ vlanname-list | vid-range | ALL } | ALL }	Requests to delete QOSPOLICY from an interface." - This sets the QOSPOLICY to “NONE”.
113	DELETE STP INSTANCE={ stpname | mstid | ALL } VLAN={ vlanname | vid-range | ALL }	Disassociates a VLAN (range) with an STP instance. Once all VLANs are disassociated, the instance can be destroyed.
114	DELETE TRACE EPSR [={ epsrdomain-list | ALL }] [MESSAGETYPE={ HEALTH | RINGUPFLUSH | RINGDOWNFLUSH | LINKDOWN | ALL }] [INTERFACE={ type:id-range | id-range | ifname-list | ALL }]	Delete the events which match the given filters. Not specifying MESSAGETYPE or INTERFACE will treat that parameter as a wildcard.

No.	*Syntax*	*Description*
115	DELETE TRACE IGMPSNOOPING [MESSAGETYPE={ REPORTV1 | REPORTV2 | LEAVE | GENERALQUERY | LASTMEMBERQUERY | ALL }] [INTERFACE={ type:id-range | id-range | ifname-list | ALL }] [MACADDRESS={ macaddress | ALL }] [GROUPADDRESS={ ipaddress | ALL }]	Delete the events which match the given filters. Not specifying MESSAGETYPE or INTERFACE or MACADDRESS or GROUPADDRESS will treat that parameter as a wildcard.
116	DELETE TRACE PPP [EVENT={ PORT | LCP | BCP | ECHO | FRAME | TIMER | ERRPROTO | MAIN | ALL }] [INTERFACE={ type:id-range | id-range | ifname-list | ALL }]	Stop sending logs to the Event log for specified LCP event(s) on the specified interface(s).
117	DELETE TRACE VOICECALL [EVENT={ OPENLOOP | CLOSELOOP | MGCPOFFHOOK | MGCPONHOOK | MODEMDETECT | ALL }] [INTERFACE={ type:id-range | id-range | ifname-list | ALL }]	Delete the events which match the given filters. Not specifying EVENT or INTERFACE will treat that parameter as a wildcard.
118	DELETE TRAFFICDESCRIPTOR={ tdname-list | ALL } CLASSIFIER={ classifiername-list | ALL }	The DELETE TRAFFICDESCRIPTOR command removes the association of a TRAFFICDESCRIPTOR with one or more CLASSIFIERs. This removes this limit on the traffic that the system allows to be received through this INTERFACE for the traffic flow identified by the CLASSIFIER.
119	DELETE VC={ vcid-range | ALL } INTERFACE={ type:id-range | id-range | ifname-list | ALL } [FORCE]	This command is used to delete one or more VC(s) from a ATM-interface or a list of ATM interfaces. User can not delete the default-VC with VC-ID 0 since it is created by the system.
120	DELETE VLANTUNNELMAP VLAN={ vlanname-list | vid-range | ALL } HVLAN={ hvlanname | vid } [INTERFACE={ type:id-range | id-range | ifname-list | ALL }]	This command disassociates a VLAN from a VLAN-based HVLAN tunnel.
121	DELETE ACCESSLIST={ accesslistname-list | ALL } INTERFACE={ type:id-range |id-range | ifname-list }	The DELETE ACCESSLIST command does one of two things. It either deletes a RULE from an ACCESSLIST or removes one or more ACCESSLISTs from one or more INTERFACEs.
122	DELETE ACCESSLIST=accesslistname RULE=rulenumber	The DELETE ACCESSLIST command does one of two things. It either deletes a RULE from an ACCESSLIST or removes one or more ACCESSLISTs from one or more INTERFACEs.
123	DELETE ACTION CLASSIFIER=classifiername-list {DROP|FORWARD|COUNT|SETVPRIORITY|SETIPTOS|SETIPDSCP| MOVEPRIOTOTOS|MOVETOSTOPRIO|ALL}	The DELETE ACTION CLASSIFIER command deletes one ACTION or ALL ACTIONs from one or more CLASSIFIERs. This is the opposite of ADD ACTION CLASSIFIER.
124	DELETE CLASSIFIER=classifiername-list PORT={port-list|ALL}	The DELETE CLASSIFIER PORT command deletes one or more CLASSIFIERs from one or more PORTs. This command causes the specified CLASSIFIER(s), and their actions, to no longer affect traffic on the specified PORT(s). This command deletes every combination of specified CLASSIFIER(s) and PORT(s) that actually exists. The DELETE CLASSIFIER INTERFACE command serves the same purpose, but applies to INTERFACEs rather than PORTs.
125	DELETE INTERFACE={ type:id-range | id-range | ifname-list | ALL } RMONALERT { DROPEVENTS | OCTETS | PACKETS | BROADCAST | MULTICAST | UNDERSIZE | OVERSIZE | CRCALIGN | FRAGMENTS | JABBERS COLLISIONS | PKTS64OCTETS | PKTS65TO127OCTETS | PKTS128TO255OCTETS | PKTS256TO511OCTETS | PKTS512TO1023OCTETS | PKTS1024TO1518OCTETS | ALL }	The DELETE INTERFACE RMONALERT command allows a user to delete threshold alarming settings for an Ethernet statistic on a specified interface. The supported Remote Monitoring (RMON) statistics for Ethernet interfaces are based on the RMON MIB (RFC2819).
126	DELETE LAG=lagname INTERFACE={ type:id-range | id-range | ifname-list | ALL}	The DELETE LAG command is used to remove ports from a Link Aggregation Group(LAG).

No.	*Syntax*	*Description*
127	DELETE LOG FILTER={filterid-list|ALL} OUTPUT=outputid	The DELETE LOG FILTER command is used to remove the association between management log filters and a management log output destination. Upon successful execution of this command, the specified management log filters are removed from the management log output destination. The management log output destination will no longer receive logs that match the filter criteria in the log filters that were removed.
128	DELETE NONPREFLOADS	The DELETE NONPREFLOADS command deletes all files on the CFC flash file system that are not designated as a preferred load for a provisioned card. This command is useful during load upgrade, to remove all non-essential files so that space for new load files is available. For a 7700 with redundant CFCs, the operation is performed on both CFCs when they are both ONLINE.
129	DELETE RADIUS SERVER={ ipaddress-list | hostname-list | ALL }	The DELETE RADIUS SERVER command is used to remove RADIUS servers from the system. Once removed, user authentication requests are no longer sent to those servers
130	DELETE SNMP COMMUNITY=name [TRAPHOST=ipaddress-list] [V2CTRAPHOST=ipaddress-list] [MANAGER=ipaddress-list]	The DELETE SNMP COMMUNITY command removes an SNMPv1 and/or SNMPv2c trap host(s) and/or management station(s) from the specified SNMP community.
131	DELETE SNTP SERVER	The DELETE SNTP SERVER command removes the SNTP server settings for the device. The SNTP server may be removed regardless of the state of the SNTP client on the device (see ENABLE SNTP or DISABLE SNTP)
132	DELETE TACPLUS SERVER={ ipaddress-list | hostname-list | ALL }	The DELETE TACPLUS SERVER command is used to remove TACACS+ servers from the system. Once removed, user authentication requests are no longer sent to those servers.
133	DELETE USER=login-name	The DELETE USER command is used to removed user accounts from the system. Once removed, the associated user cannot log into the system again until his/her account is recreated via the ADD USER command. The DELETE USER command does not, however, log the associated user off the system. If the affected user is currently logged in, he/she is informed that his/her account was removed, but no other action is taken. If there is a desire to force the user off the system as part of deleting the account, the DEACTIVATE SESSION command must also be used.
134	DELETE VLAN={ vlanname | vid } INTERFACE={ type:id-range | id-range |ifname-list | ALL }	The DELETE VLAN command removes the port/interface association from the specified Virtual LAN (VLAN) Once an untagged port is disassociated with all user-defined VLANs, it is automatically added to the default VLAN (VID=1). A user cannot remove the association between the default VLAN and an untagged port if the port has no other HVLAN/VLAN associations. If a group of ports/interfaces is included in the command and the association of any one of them cannot be removed, the entire operation fails and no ports are removed from the VLAN.
135	DESTROY PROFILE=name cardtype	Destroys a profile for the specfied card type. No other atttributes are required. For release 7.0, cardtypes with this syntax are ADSL16B, ADSL16C, ADSL16, ADSL24A, ADSL24B, ADSL24, ADSL8S, CES8, CFC24, CFC4, CFC6, FE10, FE2, FX10, GE1, GE2, GE3, POTS24, SHDSL, and NTE8. New cards for 8.0 are the GE8, CFC56, EPON2, VDSL24A, VDSL24B, and XE1.
136	DESTROY ALIAS={ aliasname-list | ALL }	The DESTROY ALIAS command will remove all alias commands as identified in the list provided.

No.	*Syntax*	*Description*
137	DESTROY CONTACTALARM={ 0..2 } STATE={ OPEN | CLOSED }	The DESTROY CONTACTALARM command removes provisioning for a dry contact input terminal alarm that has been previously defined using the CREATE CONTACTALARM command. The trigger is defined by its contact number and its physical state (open or closed). Destruction of an alarm trigger will immediately clear any raised alarm associated with it.
138	DESTROY DHCPRELAY={ dhcpname-list | ALL } [FORCE]	Destroys a DHCP Relay
139	DESTROY DHCPRELAY={ dhcpname-list | ALL } [FORCE]	Destroys the DHCP Relay instance (or set of instances). FORCE will override a warning that the instance still has associations
140	DESTROY EPSR={ epsrdomain-list | ALL }	The DESTROY EPSR command is used to destroy the already existing EPSR domains. The EPSR domain must be disabled before it can be destroyed.
141	DESTROY MLPPP={ mlpppname-list | ALL } [FORCE]	Destroys the MLPPP group, disassociating it from any PPP instances. The PPP interfaces remain on the DS1/E1 interfaces after this destruction, and new eth: interfaces corresponding to the PPP interfaces are created. The user is prompted for confirmation, because this also removes the MLPPP's ETH interface and all associated provisioning.
142	DESTROY ONU={ onuname-list | ALL } [INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL }] [FORCE]	Requests to destroy ONU interface(s)." Destroys one or more ONU interfaces and its associated ETH interface. FORCE does not prompt the user, and does not require that the ONU interface be disabled
143	DESTROY PROFILE=name port_type	Destroys a profile for the specfied port type. No other atttributes are required. For release 6.0, port types with this syntax are ADSLPORT, DS1PORT, E1PORT, FEPORT, FXPORT, GEPORT, POTSPORT, and SHDSLPORT. For release 8.0, port types are CFC56, EPONPORT, and XE1.
144	DESTROY PROTECTIONGROUP={ groupname-list | ALL } [FORCE]	Destroy any or all protection groups.
145	DESTROY PSPAN [={ pspanname-list | ALL }] [INTERFACE={ type:id-range | ifname-list | ALL }] [FORCE]	Destroys the specificied PSPAN. The DESTROY PSPAN with no parameters is rejected. The FORCE option destroys the PSPAN even if it is connected to a T1 interface.
146	DESTROY QOSPOLICY={ policyname-list | ALL } [FORCE]	Requests to destroy a QOSPOLICY. - Can't destroy the QOSPOLICY of "NONE". - By default, this command will be rejected if the QOSPOLICY is in use.
147	DESTROY STP INSTANCE={ stpname | mstid | ALL }	Once all relevant VLANs are disassociated with the STP instance, the Instance itself can be destroyed. (You cannot destroy to default STP instance, or CIST.)
148	DESTROY TRAFFICDESCRIPTOR={ tdname-list | ALL }	The DESTROY TRAFFICDESCRIPTOR command attempts to remove every specified TRAFFICDESCRIPTOR from the system, and returns an error message for any that cannot be destroyed. This command is allowed only if the TRAFFICDESCRIPTOR is not associated with any classifiers. Use "DELETE TRAFFICDESCRIPTOR" to delete TRAFFICDESCRIPTOR associations to classifiers.
149	DESTROY ACCESSLIST={ accesslistname-list | ALL } [FORCE]	The DESTROY ACCESSLIST command attempts to remove every specified ACCESSLIST from the system, and returns an error message for any that cannot be destroyed. By default this command is allowed only if no interfaces are currently associated with the ACCESSLIST(s). Using the FORCE option will override this behavior and remove ACCESSLIST(s) from the interfaces before destroying them. Otherwise, use DELETE ACCESSLIST to delete the interface associations.

No.	Syntax	Description
150	DESTROY CARD=slot-list [FORCE]	The DESTROY CARD command removes software provisioning for the specified card or list of cards. The command fails if the administrative state for each card has not already been set to DOWN (See DISABLE CARD). A warning is provided for this command and confirmation is required. The FORCE parameter suppresses the warning and bypasses the confirmation.
151	DESTROY CLASSIFIER={classifiername-list|ALL}	The DESTROY CLASSIFIER command attempts to remove every specified CLASSIFIER from the system, and returns an error message for any that cannot be destroyed. This command is allowed only if no ports are currently associated with the CLASSIFIER(s). Use "DELETE CLASSIFIER=classifiername-list PORT=ALL" to delete all port associations for the classifiers in one command.
152	DESTROY EGRESSLIMITER={limitername-list|ALL}	The DESTROY EGRESSLIMITER command attempts to remove every specified EGRESSLIMITER from the system, and returns an error message for any that cannot be destroyed. This command is allowed only if no ports or interfaces are currently associated with the EGRESSLIMITER(s). Use "DELETE EGRESSLIMITER" to delete EGRESSLIMITER associations to ports/interfaces.
153	DESTROY HVLAN={hvlanname|vid|ALL}	The DESTROY HVLAN command destroys the specified Hierarchical VLAN (HVLAN) or all HVLANs in the switch. If 'ALL' is specified then all HVLANs are destroyed. An HVLAN cannot be destroyed if interfaces still belong to it.
154	DESTROY LAG=lagname	The DESTROY LAG command destroys a Link Aggregation Group(LAG). The LAG mode must be set to OFF prior to destroying the LAG. This can be accomplished with the SET LAG command. It is necessary to delete all interfaces from the LAG prior to destroying it.
155	DESTROY LOG FILTER={filterid-list|ALL}	The DESTROY LOG FILTER command removes management log filters from the system. Upon successful completion of this command, the specified management log filter is completely removed from the system. The log filter is also removed from all log output destinations that have had the filter added with the ADD LOG FILTER command.
156	DESTROY LOG OUTPUT={outputid-list|ALL}	The DESTROY LOG OUTPUT command removes existing management log output destinations from the system. CLI output destinations are automatically destroyed when the user logs out of his/her session. Upon successful completion of this command, the specified management log destination is completely removed from the system.
157	DESTROY SNMP COMMUNITY=name	The DESTROY SNMP COMMINUTY command destroys an existing SNMP community from the system and all of the trap hosts and managers that are associated with it. The COMMUNITY parameter specifies the SNMP community. The community must exist in order to destroy it.
158	DESTROY VLAN={vlanname|vid|ALL}	The DESTROY VLAN command destroys the specified Virtual LAN (VLAN) or all VLANs in the switch. The default VLAN (VID=1), cannot be destroyed. If ALL is specified then all VLANs except the default VLAN are destroyed. A VLAN cannot be destroyed if interfaces still belong to it.
159	DIAGNOSE INTERFACE={ type:id-range | id-range | ifname-list }	Run diagnostics on the given interface and report success or failure. Detailed results can be retrieved through SHOW DIAGNOSTICS.

No.	*Syntax*	*Description*
160	DIAGNOSE CARD={slot-list|ALL} {INSERVICE|OUTOFSERVICE}	The DIAGNOSE CARD command runs a series of diagnostic tests on the specified card or list of cards. Currently, out-of-service diagnostics are the only diagnostics supported. For ADSL16, ADSL8S, GE1, GE3, and the inactive CFC cards, the card must be in the administratively DOWN for the diagnostics to run (See DISABLE CARD). For the active CFC card, the diagnostics are not run immediately, but are instead scheduled to run during the next restart of the active CFC. The restart is requested using the RESTART CARD command. The ALL parameter is not currently supported.
161	DIAGNOSE MEDIA=unit	The DIAGNOSE command runs Out Of Service diagnostics on the media card. These diagnostics require the media card to be deactivated before being permitted to run. The diagnostics get run automatically when the media card is activated.
162	DISABLE DHCPRELAY={ dhcpname-list | MAIN | ALL } INTERFACE={ type:id-range | id-range | ifname-list | ALL	The command DISABLE DHCPRELAY disables the specified DHCP relay function on the specified interfaces.
163	DISABLE EPSR={ epsrdomain-list | ALL }	The DISABLE EPSR command is used to disable the EPSR domain.
164	DISABLE IGMPSNOOPING [INTERFACE={ type:id-range | id-range | ifname-list | ALL }]	The DISABLE IGMPSNOOPING command is used to disable the snooping feature and not intercept and monitor the IGMP protocol messages. This command is used to disable the IGMP system-wide and also on port or interface basis.
165	DISABLE INTERFACE={ type:id-range | id-range | ifname-list } [FORCE]	Disables an interface for the system. This command should be used with caution.
166	DISABLE IP INTERFACE={ MGMT | type:id | ifname }	The DISABLE IP INTERFACE command disables an existing interface. If the telnet service is enabled prior to executing this command (See ENABLE TELNET SERVER), users can no longer log in to the system via the IP address associated with the disabled interface.
167	DISABLE PSPAN [={ pspanname-list | ALL }] [{ INTERFACE={ type:id-range | ifname-list | ALL } | CARD={ slot-list | ALL } }]	Disables the PSPAN so it cannot carry traffic (although it is still connected). If only an INTERFACE or PSPAN is specified, ALL is assumed.
168	DISABLE STP [{ [INSTANCE={ stpname | mstid | MAIN | ALL } INTERFACE={ type:id-range | id-range | ifname-list | ALL } [TOPOLOGYCHANGE]] | [INTERFACE={ type:id-range | id-range | ifname-list | ALL } [TOPOLOGYCHANGE]] }]	The DISABLE STP command is used to disable Spanning Tree Protocol operations for the system. When this command is issued, all ports in the system are set to the STP FORWARDING state so that they are traffic capable. The STP port state displayed for all ports is STP DISABLED to indicate that STP operations are disabled.
169	DISABLE TRACE	The DISABLE TRACE command turns off Trace logging. No more traces will go into the buffer or to the CLI.
170	DISABLE ARPFILTER INTERFACE={type:id-range|id-range|ifname-list|ALL}	The DISABLE ARPFILTER command is used to disable the behavior of ENABLE ARPFILTER for the specified interface or interfaces.
171	DISABLE CARD={slot-list|INACTCFC} [FORCE]	The DISABLE CARD command takes a card out-of-service and sets the card&apos;s administrative state to DOWN. A list or range of slots is accepted. It is recommended that the user disable the card before physically removing it from the slot. Once the card is disabled, the PULL LED on the card is illuminated. For the FC7 card in the 7400 shelf, the DISABLE CARD command changes the administrative state to DOWN and illuminates the PULL LED. Even though the card is classified as disabled, the in-service(INSRVC) LED remains lit and the fans continue to function. Despite the fact that the fans continue to function, both the fans and the FC7 card are ready to pull. The DISABLE CARD command is disallowed for the slot containing the active CFC card. A confirmation is provided before the card is taken out-of-service. The confirmation is suppressed if the FORCE parameter is provided.

No.	Syntax	Description
172	DISABLE CONFIRMATION	The DISABLE CONFIRMATION command is used to suppress user confirmation prompts for potentially dangerous commands. This command is intended for expert users who understand the impact of the various operations on the device. For example, if a user wishes to reboot an active CFC, the following would appear with confirmation prompts enabled: officer SEC> restart card actcfc cold Do you really want to restart card actcfc (Y/N)? With confirmation disabled, the operation is performed without prompt or delay. When this command is used, the settings only affect the current user session. No other user sessions are altered or changed by. When a user logs out, the confirmation settings are automatically restored to enable confirmation prompts.
173	DISABLE FANMODULE	The DISABLE FANMODULE command changes the ADMINSTATE of the system fan module to DOWN. The operational state remains UP and the fan module continues to operate. On the 7700 shelf only, the PULL LED on the fan module is illuminated, and the INSRVC green LED remains illuminated. Use of this command is recommended before physically removing the module.
174	DISABLE FEATURE={ userlabel-list | ALL } [FORCE]	Future
175	DISABLE LOG OUTPUT={outputid-list|ALL}	The DISABLE LOG OUTPUT command disables management log streaming for existing management log output destinations.
176	DISABLE MORE	When large amounts of data are output, the data is displayed a screen full at a time, waiting for user input to display the next page. This paging can be disabled via the DISABLE MORE command. BY doing so, the data will be displayed to the screen in its entirety. The disabling of the MORE prompt via this command will only affect the current CLI session. The MORE prompt can be re-enabled via the ENABLE MORE command.
177	DISABLE PORT=port-list [FORCE]	The DISABLE PORT command takes a port out-of-service and changes the administrative state to DOWN. A list or range of ports is accepted. Once disabled, the port is given a status of OFFLINE. A warning is provided for this command and confirmation is required. The FORCE parameter suppresses the warning and bypasses the confirmation.
178	DISABLE RADIUS SERVER={ ipaddress-list | hostname-list | ALL }	The DISABLE RADIUS SERVER command disables one or more RADIUS servers for use in user authentication requests. Once disabled, the RADIUS server(s) are not used for user authentication requests
179	DISABLE SNMP	The DISABLE SNMP command disables the device's SNMP agent. SNMP packets sent to the device are treated as unknown protocol packets by the underlying transport layer(UDP). In addition, the device ceases SNMP trap generation.
180	DISABLE SNMP AUTHENTICATE_TRAP	The DISABLE SNMP AUTHENTICATE_TRAP command disables the generation of authentication failure traps by the SNMP agent. The following authentication failure traps are suppressed: - Invalid community used to access the device. - Invalid use of community (Attempting a SET with a READ-ONLY community. - Invalid access from a MANAGER which is not a "trusted" host OR not associated with the community associated with the SNMP operation. An authentication failure trap is not generated if the community is set with OPEN=true.(See CREATE SNMP COMMUNITY or SET SNMP COMMUNITY).

No.	*Syntax*	*Description*
181	DISABLE SNMP COMMUNITY=name [TRAP]	The DISABLE SNMP COMMUNITY command disables an SNMP community OR the traps it generates. This command does not, however, allow the user to disable the community and trap generation at the same time. In order to disable both the community and trap, the user must run the command twice; once with the TRAP parameter and another time without. The following describes the behavior of the command: - DISABLE SNMP COMMUNITY=comm_name disables the community for any access to the system by any MANAGER. Traps will continue to be transmitted with this community unless it is explicitly disabled. - DISABLE SNMP COMMUNITY=comm_name TRAP disables traps generated by the community. As a result, traps are no longer transmitted with the specified community to any SNMPv1/SNMPv2c TRAPHOSTs associated with the community. A MANAGER can still use this community to access the device unless the community is disabled.
182	DISABLE SNTP	The DISABLE SNTP command disables SNTP client. Once disabled, the clock within the device is no longer synchronized with any external time source. If the SNTP client is unable to communicate with the SNTP server, the disable operation places the client in a state where it can attempt to communicate with the server when ENABLE SNTP is executed.
183	DISABLE STP INTERFACE={ type:id-range | id-range | ifname-list | ALL } [TOPOLOGYCHANGE]	The DISABLE STP PORT command is used to specify a port or ports that are excluded from STP operations. Ports identified by this command have their STP state set to forwarding without going through the STP state transitions. These ports are also not be considered as part of the active topology as defined for the STP algorithm. When the port state is displayed for one of these ports, the port shows STP DISABLED, even though the actual port state is set to forwarding so it can pass traffic. This command is also used to exclude a port from STP topology change detection and notification. With the optional TOPOLOGYCHANGE change parameter specified, the port is not included in the topology change detection though all other STP operations continue to function.
184	DISABLE SWITCH AGEINGTIMER	The DISABLE SWITCH AGEINGTIMER disables the ageing timer from ageing out dynamically learned entries in the Forwarding Database. The default setting for the ageing timer is enabled. To disable the ageing out of learned MAC addresses, use the command: DISABLE SWITCH AGEINGTIMER.If the ageing timer ages out all dynamically learned filter entries, and switch learning is disabled, only statically entered MAC source addresses will be used to decide which packets to forward or discard. If the switch finds no matching entries in the Forwarding Database during the Forwarding Process, then all switch interfaces in the VLAN/HVLAN will be flooded with the packet, except the interface on which the packet was received.
185	DISABLE SWITCH LEARNING	The DISABLE SWITCH LEARNING disables the dynamic learning and updating of the Forwarding Database. The default setting for the learning function is enabled. To disable the switch learning function, use the command: DISABLE SWITCH LEARNING. If switch learning is disabled and the ageing timer has aged out all dynamically learned filter entries, only statically entered MAC source addresses will be used to decide which packets to forward or discard. If the switch finds no matching entries in the Forwarding Database during the Forwarding Process, then all switch interfaces in the VLAN/HVLAN will be flooded with the packet, except the interface on which the packet was received.
186	DISABLE TACPLUS SERVER={ ipaddress-list | hostname-list | ALL }	The DISABLE TACPLUS SERVER command disables one or more TACACS+ servers for use in user authentication requests. Once disabled, the TACACS+ server(s) are not used for user authentication requests.

No.	Syntax	Description
187	DISABLE TELNET SERVER	The DISABLE TELNET SERVER command blocks access to the device via telnet. For security reasons, there may be a need to disable the telnet server. Once deactivated, the only other means of access are through SNMP (if enabled) and the Console. After deactivation and all users log off, the Console provides the only interface through which the telnet server can be re-enabled. Users are not automatically forced out of the system when telnet server is disabled. If there is a desire to force users off the system as part of disabling telnet, the DEACTIVATE SESSIONS command must also be used.
188	DISABLE USER=login-name	The DISABLE USER command is used to disable user accounts from accessing the system. Once disabled, the associated user cannot log into the system again until his/her access is re-enabled via the ENABLE USER command. The DISABLE USER command does not, however, log the associated user off the system. If the affected user is currently logged in, he/she is informed that his/her account was removed, but no other action is taken. If there is a desire to force the user off the system as part of deleting the account, the DEACTIVATE SESSION command must also be used.
189	DISCONNECT INTERFACE={ type:id-range | ifname-list | ALL }	Dis-associates the two interfaces
190	ENABLE DHCPRELAY={ dhcpname-list | MAIN | ALL } INTERFACE={ type:id-range | id-range | ifname-list | ALL }	The command ENABLE DHCPRELAY enables the DHCP relay function on the specified interfaces.
191	ENABLE EPSR={ epsrdomain-list | ALL }	The ENABLE EPSR command is used to enable the EPSR domain. Before any EPSR domain can be enabled, the Control Vlan, Primary and Secondary interfaces should have been provisioned on that EPSR domain.
192	ENABLE IGMPSNOOPING [INTERFACE={ type:id-range | id-range | ifname-list | ALL }]	The ENABLE IGMPSNOOPING command is used to enable the snooping for the intercept and monitoring of the IGMP protocol messages that setup the layer 2 multicast group information in the forwarding database. This command is used to disable the IGMP system-wide and also on port or interface basis. This command is also used to set the option to flood the unknown multicast packets.
193	ENABLE INTERFACE={ type:id-range | id-range | ifname-list }	Enables an interface
194	ENABLE IP INTERFACE={ MGMT | type:id | ifname }	The ENABLE IP INTERFACE command enables an existing interface. Only one IP Interface can be enabled at a given time. If necessary, the ENABLE IP INTERFACE command will automatically disable the other IP Interface. If the telnet service is enabled (See ENABLE TELNET SERVER), users can log in to the system the IP address associated with the enabled interface.
195	ENABLE PSPAN [={ pspanname-list | ALL }] [{ INTERFACE={ type:id-range | ifname-list | ALL } | CARD={ slot-list | ALL } }]	Enables the PSPAN so it can carry traffic (it must be connected). If only an INTERFACE or PSPAN is specified, ALL is assumed.
196	ENABLE STP [{ [INSTANCE={ stpname | mstid | MAIN | ALL } INTERFACE={ type:id-range | id-range | ifname-list | ALL } [{ TOPOLOGYCHANGE | RSTPCHECK }]] | [INTERFACE={ type:id-range | id-range | ifname-list | ALL } [{ TOPOLOGYCHANGE | RSTPCHECK }]] }]	The ENABLE STP command is used to enable Spanning Tree Protocol operations for the system. When this command is issued, all interfaces in the system that have not been identified by the user to be excluded from STP operations are processed by the Spanning Tree Protocol algorithm (see DISABLE STP INTERFACE and ENABLE STP INTERFACE for information on interface exclusion from STP operations). This algorithm will determine which interfaces in the system should transition into the forwarding state and which ones are held in the blocking state as alternate interfaces.

No.	*Syntax*	*Description*
197	ENABLE TRACE [OUTPUT={ CLI } [FORMAT={ FULL | SUMMARY }]]	The ENABLE TRACE command turns on Trace logging. This allows Trace logs to go into the log buffer. These logs can then be viewed with the SHOW TRACE BUFFER command. An OUTPUT option can also be specified. This controls how the Trace logs are displayed as they are generated. This does NOT stop the logs from going into the buffer.
198	ENABLE ARPFILTER INTERFACE={type:id-range|id-range|ifname-list|ALL}	The ENABLE ARPFILTER command is used to enable the specified interface or interfaces to intercept all ARP requests. The intercepted ARP requests are inspected to determine if the Layer 3 source address matches the IP source address of any IP filters installed on the same interface and if a match is found then the ARP packet is either forwarded or discarded depending on the action of the IP filter. The IP filter may have been installed explicitly by use of the CREATE CLASSIFIER and ADD CLASSIFIER commands or learned through the use of the FILTER option of the SET DHCPRELAY INTERFACE command. Refer to the help of these respective commands to learn how to setup IP filters or to display the current set of IP filters for a given interface or interfaces.
199	ENABLE CARD={slot-list|INACTCFC} [NODIAGS] [VERBOSE]	The ENABLE CARD command changes the administrative state of the specified card to UP, making it available for service. A list or range of slots is accepted. During the enable sequence, several steps are performed to initialize the card and return it to service, including: - The PULL LED is turned OFF - card reset - hardware/software version compatibility checking - reloading of the card if applicable and necessary - booting the software load if applicable - running out of service diagnostics if applicable - sending card configuration data - initiating defect monitoring on the card - The INSRV LED is illuminated to indicate that the card is providing service If any of the ports on the card are in the enabled state (administrative state set to UP), they are also initialized. Initialization steps for ports include: - configuration of enabled ports on the card - initiation of defect monitoring on the port The ENABLE CARD command is disallowed for the slot containing the active CFC card.
200	ENABLE CONFIRMATION	The ENABLE CONFIRMATION command is used to re-enable confirmation prompts after they were disabled by the DISABLE CONFIRMATION command. By default, confirmations are enabled. Confirmation prompts should only be disabled by experienced users since the prompts are intended to prevent accidental loss of service. For example, if a user wishes to reboot an active CFC, the following would appear: officer SEC> restart card actcfc cold Do you really want to restart card actcfc (Y/N)? With confirmation disabled, the operation is performed without delay. When this command is used, the settings only affect the current user session. No other user sessions are altered or changed. When a user logs out, the confirmation settings are automatically restored to enable confirmation prompts.
201	ENABLE FANMODULE	The ENABLE FANMODULE command changes the ADMINSTATE of the system fan module to UP. The operational state remains UP and the fan module continues to operate. On the 7700 shelf only, the PULL LED on the card is extinguished, and the INSRVC green LED remains illuminated.
202	ENABLE FEATURE=userlabel KEY=hexkey	Future
203	ENABLE LOG OUTPUT={outputid-list|ALL}	The ENABLE LOG OUTPUT command enables management log streaming for existing management log output destinations.

No.	Syntax	Description
204	ENABLE MORE	When large amounts of data are output, the data is displayed a screen full at a time, waiting for user input to display the next page. This paging can be disabled via the DISABLE MORE command. BY doing so, the data will be displayed to the screen in its entirety. The MORE prompt can be re-enabled via the ENABLE MORE command.
205	ENABLE PORT=port-list	The ENABLE PORT command places the port in the UP administrative state and attempts to make the port in-service. A list or range of ports are accepted. During the enable sequence, the port's configuration data is sent from the CFC and port defect monitoring is activated. If the operational state remains set to DOWN after the port is enabled, the status value is changed to one of the following values: - DEPENDENCY : the operational state of the card is not UP - FAILED : a problem occurred when configuring the port or a defect was reported
206	ENABLE RADIUS SERVER={ ipaddress-list | hostname-list | ALL }	The ENABLE RADIUS SERVER command is used to enable one or more RADIUS servers for use in user authentication requests. Once enabled, the RADIUS server(s) are used for future user authentication requests
207	ENABLE SNMP	The ENABLE SNMP command enables the device's SNMP agent. Once enabled, the SNMP agent can receive and process SNMP packets and generate traps. By default, the SNMP agent is disabled.
208	ENABLE SNMP AUTHENTICATE_TRAP	The ENABLE SNMP AUTHENTICATE_TRAP command enables the generation of authentication failure traps by the SNMP agent whenever an SNMP authentication failure occurs. By default, authentication failure traps are disabled. When enabled, the following conditions cause the generation of authentication failure traps: - Invalid community used to access the device. - Invalid use of community (Attempting a SET with a READ-ONLY community. - Invalid access from a MANAGER which is not a "trusted" host OR not associated with the community associated with the SNMP operation. An authentication failure trap is not generated if the community is set with OPEN=true.(See CREATE SNMP COMMUNITY or SET SNMP COMMUNITY).
209	ENABLE SNMP COMMUNITY=name [TRAP]	The ENABLE SNMP COMMUNITY command enables a SNMP community for access OR enables the generation of trap messages for the community. This command does not, however, allow the user to enable the community and trap generation at the same time. In order to enable both the community and trap, the user must run the command twice; once with the TRAP parameter and another time without. The following describes the behavior of the command: - ENABLE SNMP COMMUNITY=comm_name command allows access to the device through the specified community. If the community was created with READ-ONLY access, the user can perform read operations on any accessible and supported SNMP MIB variable. A community has READ-ONLY access by default. If the community was created with READ-WRITE access, the user is allowed to perform SNMP SETs as well GETs. - ENABLE SNMP COMMUNITY=public TRAP command enables trap generation for the community. The device only generates traps if one or more communities are enabled for trap generation. Since community and trusted host checks are the only security mechanisms available in SNMPv1/SNMPv2c, a READ-WRITE community must NOT be trap enabled. Since the community acts as a crude password and the community name is included in the trap, the trap would reveal how to access the device for configuration changes. Typically only one community is trap-enabled on a device unless a user intends to use the trap community as a trap filter on the Network Management Station.

No.	Syntax	Description
210	ENABLE SNTP	The ENABLE SNMP command enables the device's SNMP agent. Once enabled, the SNMP agent can receive and process SNMP packets and generate traps. By default, the SNMP agent is disabled.
211	ENABLE STP INTERFACE={ type:id-range | id-range | ifname-list | ALL } [{TOPOLOGYCHANGE | RSTPCHECK }]	The ENABLE STP INTERFACE command allows the user to specify an interface or interfaces that should now be included as part of the Spanning Tree Protocol operations. This command is used to undo the exclusion of interfaces from STP that were specified by the user via the DISABLE STP INTERFACE command. This command is also used to add an interface to STP topology change detection and notification. With the optional TOPOLOGYCHANGE change parameter specified, the interface is added to the topology change detection and notification scheme that is triggered by interface state changes. This parameter is functional only in the ORINGINAL STP operational mode. This command is also used to make the interface undergo the migration check process. With the optional RSTPCHECK parameter specified, the interface can be forced to go for migration check. This parameter is functional only in the RSTP and STP_COMPATIBLE_RSTP operational mode.
212	ENABLE SWITCH AGEINGTIMER	The ENABLE SWITCH AGEINGTIMER enables the ageing timer to age out dynamically learned entries in the Forwarding Database. The default setting for the ageing timer is enabled. To enable the ageing out of learned MAC addresses, use the command: ENABLE SWITCH AGEINGTIMER.If the ageing timer ages out all dynamically learned filter entries, and switch learning is disabled, only statically entered MAC source addresses will be used to decide which packets to forward or discard. If the switch finds no matching entries in the Forwarding Database during the Forwarding Process, then all switch interfaces in the VLAN/HVLAN will be flooded with the packet, except the interface on which the packet was received.
213	ENABLE SWITCH LEARNING	The ENABLE SWITCH LEARNING enables the dynamic learning and updating of the Forwarding Database. The default setting for the learning function is enabled. To enable the switch learning function, use the command: ENABLE SWITCH LEARNING. If switch learning is disabled and the ageing timer has aged out all dynamically learned filter entries, only statically entered MAC source addresses will be used to decide which packets to forward or discard. If the switch finds no matching entries in the Forwarding Database during the Forwarding Process, then all switch interfaces in the VLAN/HVLAN will be flooded with the packet, except the interface on which the packet was received.
214	ENABLE TACPLUS SERVER={ ipaddress-list | hostname-list | ALL }	The ENABLE TACPLUS SERVER command is used to enable one or more TACACS+ servers for use in user authentication requests. Once enabled, the TACACS+ server(s) are used for future user authentication requests.
215	ENABLE TELNET SERVER	The ENABLE TELNET SERVER command will allow remote users to telnet to the system. Telnet access is disabled by default.
216	ENABLE USER=login-name	The ENABLE USER command is used to enable user accounts for accessing the system. Once enabled, the associated user can log into the system again until his/her access is disabled via the DISABLE USER command.

No.	Syntax	Description
217	EXECUTE SCRIPT=filename	The EXECUTE SCRIPT command processes all of the commands specified in the specified filename. The script file contains one or many CLI commands. The first line in the file must contain a comment that identifies the file as a script. Other words can also exist on the line, but the word 'script' must appear some place in the line. Comments are identified as a hash(#) character on a line in the file. A CLI command in the script file must occupy a single line. A command cannot span more than one line. If a command requires user interaction like a confirmation, the user response text is included on the line after the command. The following is an example for disabling a port: DISABLE PORT=4.1 y The contents of a script file are played back as written. A syntax error in the file is detected as the script is run. If an error is encountered, the device is left in an unknown condition.
218	FORMAT MEDIA=unit	The FORMAT MEDIA command allows the user to format a new media card so that is able to be used. Care should be taken, as any files or data already on the media card will be lost. Unit should be expressed as CFLASHx - for example FORMAT MEDIA CFLASH9 will format the media card associated with the CFC in slot 9.
219	GET FILE={ sourcefilename | serverpath/sourcefilename } { TFTP SERVER={ ipaddress | hostname } | ZMODEM | FTP SERVER={ ipaddress | hostname } USER=userid PASSWORD=password } [TO=unit:]	The GET FILE command is used to transfer files onto either the CFC flash file system or, (if the optional TO parameter is used) a specified media card, from the specified SERVER, using the specified file transfer METHOD. The command fails if there is insufficient space on the CFC flash file system or media card, or if the filename is the same as a pre-existing preferred load file for a provisioned card. For a 7700 with redundant CFCs, the operation is performed on both CFCs when they are both ONLINE. The CARD parameter is currently not supported.
220	GET FILE=filename CARD=slot	The GET FILE command is used to transfer files onto either the CFC flash file system or, (if the optional TO parameter is used) a specified media card, from the specified SERVER, using the specified file transfer METHOD. The command fails if there is insufficient space on the CFC flash file system or media card, or if the filename is the same as a pre-existing preferred load file for a provisioned card. For a 7700 with redundant CFCs, the operation is performed on both CFCs when they are both ONLINE. The CARD parameter is currently not supported.
221	LOOPBACK INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } { NEAREND | FAREND } { INWARD | PAYLOAD | LINE | PACKET | NONE	Sets the loopback state of the interface. Loopbacks are removed by setting the value to NONE. Defaults to the near-end of the interface. Release 7.0 will only support near-end requests
222	PING={ ipaddress | hostname } [FROM { INTERFACE={ type:id | id | ifname } | IPADDRESS=ipaddress }] [DELAY=1..900] [LENGTH=1..8192] [NUMBER={ 1..65535 | CONTINUOUS }] [TIMEOUT=1..900]	The PING command is used to find other hosts in the same network. The PING command sends ICMP echo packets to the specified host and waits for a response. If a response is received, an indication of success is shown to the user. Once the command operation completes, the user is presented with a summary of the number of packets sent and received along with an indication of the percentage of packets lost. In the event that a user wishes to end a repetitive PING request, the STOP PING command terminates ping operation and presents information regarding the number of packets sent and received.
223	PURGE DATABASE [FORCE]	The PURGE DATABASE command purges all contents in the system configuration database and then automatically restarts the CFC. After the restart, the database is repopulated only with factory default configuration. All other configuration must be restored through individual CLI commands, or read from a script file using the EXECUTE SCRIPT command, or by restoring the database contents from a network server using the RESTORE DATABASE command. * This command impacts service if completed successfully * User warning confirmation is required unless overridden with the FORCE option.
224	PURGE LOG	The PURGE LOG command is used to remove all stored management logs from the system.

No.	Syntax	Description
225	PURGE MEDIA=unit	The PURGE MEDIA command deletes all files from the specificed media card.
226	PURGE STP	The PURGE STP command is not supported.
227	PURGE USER	The PURGE USER command deletes all users from the User Authentication Database. The OFFICER account remains but the password is set to the default password. Global configuration parameters and counters are not affected. To clear these counters use the RESET USER command.
228	PUT FILE={sourcefile|unit:sourcefile} {TFTP SERVER={ipaddress|hostname} | FTP SERVER={ipaddress|hostname} USER=userid PASSWORD=password | ZMODEM} [TO=serverpath]	The PUT FILE command transfers the specified file from the CFC flash file system or specified media card to the given destination. The destination is either an external server, or a card or set of cards in the shelf. The source file must already exist on the flash file system.
229	PUT FILE=filenamemCARD={ slot | slot-list }	The PUT FILE command transfers the specified file from the CFC flash file system or specified media card to the given destination. The destination is either an external server, or a card or set of cards in the shelf. The source file must already exist on the flash file system.
230	PUT LOG FILE={ destinationfile | unit:destinationfile |serverpath/destinationfile } [{ TFTP SERVER={ ipaddress | hostname } |ZMODEM | FTP SERVER={ ipaddress | hostname } USER=userid PASSWORD=password}] [TYPE={ MGMT | ERROR | TRACE | CRASH }] [CARD={ ACTCFC | INACTCFC }]	The PUT LOG command is used to transfer management, error, trace or crash logs off the device. Currently, TFTP is the only supported transfer method.
231	RENAME DHCPRELAY=dhcpname TO=dhcpname	Renames a DHCP Relay instance. All of the attributes of the old name are transferred to the new name. NEED INFO - is this true?
232	RENAME ONU=onuname TO=onuname	Requests to change the name of an ONU interface(s).
233	RENAME QOSPOLICY=policyname TO=policyname	Requests to change the name of a QOSPOLICY. The policy NONE cannot be renamed.
234	RENAME STP INSTANCE={ stpname | mstid } TO=stpname	Rename the STP instance (using the name or id to specify) to another name.
235	RENAME FILE={ sourcefile | unit:sourcefile } TO={ destinationfile | unit:destinationfile }	The RENAME FILE command renames the specified file on the CFC flash file system. The file must already exist on the CFC flash file system. The command is disallowed if the specified file is already designated as a preferred, alternate or temporary load file for a provisioned card. For a duplex system, the operation is performed on both CFCs when they are both ONLINE. The RENAME FILE command can also be used to rename the specified file on a specified media card by prepending the name of the media card to the respective filenames. Example: RENAME cflash9:myOldFilName TO cflash9:myNewFileName
236	RESET CARD={ slot-list | ACTCFC | INACTCFC | ALL } { CPUSTATS }	Reset the CPU usage statistics (CFC only) and memory usage statistics (CFC only)
237	RESET CLASSIFIER COUNTER INTERFACE={ type:id-range | id-range | ifname-list | ALL }	The RESET CLASSIFIER COUNTER command resets (sets to 0) all CLASSIFIER counters associated with the specified PORT(s) or INTERFACE(s). There are 3 pre-defined CLASSIFIER counters for each PORT or INTERFACE, as described in "SHOW CLASSIFIER INTERFACE COUNTER".
238	RESET IGMPSNOOPING COUNTER [{ STANDARD | MESSAGERESPONSE | INTERFACE={ type:id-range | id-range | ifname-list | ALL } | CARD={ slot-list | ALL } }]	The RESET IGMPSNOOPING command is used to reset IGMP counters/statistics.
239	RESET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } COUNTER [FORCE]	The RESET INTERFACE COUNTER command resets the current statistical counts to zero. The reset affects all statistics associated with the provided interface or interfaces.

No.	Syntax	Description
240	RESET LLDP COUNTER [INTERFACE={ type:id-range | id-range | ifname-list | ALL }]	Allows the user to clear the LLDP interface counters. data (local system LLDP counters) for each interface specified.
241	RESET MGCP COUNTER [INTERFACE={ type:id-range | id-range | ifname-list | ALL }]	The RESET MGCP COUNTER is used to reset the current MGCP statistics to zero. This is useful when attempting to diagnose an MGCP problem where old counts would interfere with the tests performed.
242	RESET STP [{ INSTANCE={ stpname | mstid | MAIN | ALL } | LEARNCISCODIGEST }]	The RESET STP command is used to reset the counters for the default STP instance and to force the spanning tree algorithm to restart. This causes this bridge to temporarily assume the role of "root bridge" and declare all its ports as "designated ports", as would happen when the bridge is powered cycled or rebooted.
243	RESET ACCESSLIST=accesslistname RULE=rulenumber [{ PERMIT | DENY }]	The RESET ACCESSLIST command clears all of the fieldname/fieldvalue pairs from the RULE, resulting in a classifier that always matches all packets. Unless specified, the action (PERMIT or DENY) on the RULE remains unchanged. This command does not remove association of the ACCESSLIST or INTERFACE(s). Use DELETE ACCESSLIST for those types of changes.
244	RESET CLASSIFIER COUNTER PORT={port-list|ALL}	The RESET CLASSIFIER COUNTER command resets (sets to 0) all CLASSIFIER counters assocated with the specified PORT(s) or INTERFACE(s). There are 3 pre-defined CLASSIFIER counters for each PORT or INTERFACE, as described in "SHOW CLASSIFIER INTERFACE COUNTER".
245	RESET CLASSIFIER=classifiername	The RESET CLASSIFIER command clears all of the match rules from the CLASSIFIER, resulting in a classifier that always matches all packets. This command does not remove association of the CLASSIFIER to ACTION(s) or PORT(s). Use DELETE ACTION CLASSIFIER or DELETE CLASSIFIER PORT for those types of changes.
246	RESET DHCPRELAY COUNTER INTERFACE={type:id-range|id-range|ifname-list|ALL}	This command resets the DHCP Relay packet counts on the specified interface. If 'all' interfaces are specified, the cumulative DHCP Relay counter as well as all individual interface DHCP Relay counters are reset.
247	RESET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } FAULTCOUNT [FORCE]	The RESET INTERFACE command is used to reset interface faults or ADSL egress counters to zero. The current fault count information is reset using the FAULTCOUNT parameter. The QUEUECOUNT parameter is used to reset all four priority queue's egress counters for ADSL interfaces.
248	RESET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } QUEUECOUNT [FORCE]	The RESET INTERFACE command is used to reset interface faults or ADSL egress counters to zero. The current fault count information is reset using the FAULTCOUNT parameter. The QUEUECOUNT parameter is used to reset all four priority queue's egress counters for ADSL interfaces.
249	RESET LAG COUNTER={LACPSTATS|MACSTATS|ALL}	The RESET LAG COUNTER command clears Link Aggregation Group(LAG) statistics. Link Aggregation Control Protocol(LACP) and Medium Access Control(MAC) statistics are cleared independently or simultaneously, as specified by user.
250	RESET SNTP	The RESET SNTP command resets statistics and forces a resynchronization with the SNTP server. This command is rejected if the client is not enabled (See ENABLE SNTP). If the server has not been added (See ADD SNTP SERVER), the client remains idle.
251	RESET SWITCH COUNTER [FORCE]	This command resets the CXE Queue Discard (QED) counters on the device to zero. For the list of QED counters supported type: HELP SHOW SWITCH COUNTER.

No.	*Syntax*	*Description*
252	RESET USER[=login-name] [COUNTER[={ALL|GLOBAL|USER}]]	The RESET USER command is used to reset User Authentication Database counters for one or all users, or to reset global counters for the User Authentication Facility. If a login name is specified with the USER parameter, the COUNTER parameter is optional (only USER may be specified) and the activity counters for the specified user are reset. The login name is not case sensitive. If a login name is not specified with the USER parameter then the COUNTER parameter is used to specify which counters should be reset. If USER is specified, the activity counters for all users are reset. If GLOBAL is specified, the global counters for the User Authentication Facility are reset. If ALL is specified, all counters are reset. The default value for COUNTER is USER.
253	RESTART CARD={ slot-list | INACTCFC | ACTCFC } [COLD] [FORCE]	The RESTART CARD command performs a restart of the software running on the specified card. For the active CFC card, the entire system is affected and all cards are restarted. For the active CFC card, a COLD restart - resets the CFC and all other cards in the shelf - reboots and reinitializes the software on the CFC - runs out of service diagnostics on the CFC if previously scheduled through use of the DIAGNOSE CARD command - reloads configuration data from the system database - manages recovery of the remaining cards in the shelf For the inactive CFC card, a COLD restart - changes the operational state to DOWN, if not already DOWN - performs a hardware reset on the card - reboots and reinitializes the software - runs out of service diagnostics - reloads configuration data - restores the operational state to UP if the administrative state is UP, including data initialization and initiation of defect monitoring For the ADSL16, ADSL8S and FE10 cards, a COLD restart - changes the operational state to DOWN, if not already DOWN - performs a hardware reset on the card - reboots and reinitializes the software - runs out of service diagnostics - reloads configuration data - restores the operational state to UP if the administrative state is UP, including data initialization, initiation of defect monitoring, and restoration of ports For the GE1 and GE3 cards, a COLD restart - changes the operational state to DOWN, if not already DOWN - performs a hardware reset on the card - runs out of service diagnostics - reloads configuration data - restores the operational state to UP if the administrative state is UP, including data initialization, initiation of defect monitoring, and restoration of ports
254	RESTART SYSTEM [FORCE]	This command restarts the system. If the command is executed on a duplex system
255	RESTORE CONFIG FILE={ sourcefile | unit:sourcefile } [OUTPUT={ CONSOLE | logfile | unit:logfile }]	The RESTORE CONFIG command allows the user to restore a previously generated configuration, which was created via the BACKUP CONFIG command. During the processing of RESTORE CONFIG, the current data is purged, the system is rebooted, and the configuration is then restored by executing the commands in the configuration file that is provided with the FILE parameter. The OUTPUT parameter indicates the destination of the responses to the commands executed. If the OUTPUT parameter is not provided, the responses to the commands are not recorded or displayed. To monitor the progress of the RESTORE CONFIG command, the user may run the SHOW CONFIG STATUS command.
256	RESTORE DATABASE FILE={sourcefile|unit:sourcefile|serverpath/sourcefile} [{TFTP SERVER={ipaddress|hostname}|ZMODEM| FTP SERVER={ipaddress|hostname} USER=userid PASSWORD=password}] [FORCE]	The RESTORE DATABASE command rewrites the configuration database with contents from a file transferred from an external network server. While the data is transferred from the server, it is buffered in RAM memory in the CFC and not written to the flash. If the transfer fails or is aborted, the existing database is retained. If the file transfer is successful, then the database in flash memory is automatically purged and rewritten with the new contents. Once the flash memory write completes, the CFC automatically restarts to apply the updates from the database. * This command impacts service if completed successfully * User warning confirmation is required unless overridden with the FORCE option.

No.	*Syntax*	*Description*
257	SEND MESSAGE=message-text SESSION={session-list|ALL}	The SEND MESSAGE command will allow the user to send a simple text message to any other active CLI session. The message will be displayed asynchronously on the command window of each session listed in the SESSION parameter. Session Id values can be found by running the SHOW SESSIONS command. The session Id corresponds to either the console number (0) or one of the 10 telnet sessions.
258	SET LOG OUTPUT=outputid [{ CLI [FORMAT={ FULL | MSGONLY | SUMMARY }] | CONSOLE [FORMAT={ FULL | MSGONLY | SUMMARY }] | SYSLOG SERVER={ ipaddress | hostname } | FILE=unit:filename [FORMAT={ FULL | MSGONLY | SUMMARY }] }]	The SET LOG OUTPUT command is used to change the management log output destination settings. By default, if no category, severity or format options are specified, the management log filter is set to match all logs.
259	SET ALARMS THRESHOLD [MINOR=value] [MAJOR=value] [CRITICAL=value]	The alarm thresholds control when the MINOR, MAJOR, and CRITICAL Port Outage Threshold alarms are raised. The entered values must be non-zero and satify the condition: MINOR < MAJOR < CRITICAL These signify the lowest number of ports for that alarm to be raised. When all UPLINK ports are out of service a CRITICAL alarm will be raised regardless of the threshold values.
260	SET CARD={ slot-list | ACTCFC | INACTCFC } [{ NTE8 [PORTTYPE={ DS1 | E1 }] [TIMINGREFERENCE={ type:id | ifname | INTERNAL }] }] [PREFLOAD={ filename | NONE }] [ALTLOAD={ filename | NONE }] [TEMPLOAD={ filename | NONE }]	Allows the user to modify card attributes, here the ones for the NTE8 are set.
261	SET CARD={ slot-list | ACTCFC | INACTCFC } [{ SHDSL24 [WETTINGCURRENT={ ON | OFF }] [ANNEXTYPE={ A | B }] [WIREMODE={ NORMAL | BONDED }] }] [PREFLOAD={ filename | NONE }] [ALTLOAD={ filename | NONE }] [TEMPLOAD={ filename | NONE }]	The SET CARD command modifies the provisioning attributes for the SHDSL16 card or list of cards. The administrative state is modified through the ENABLE CARD or DISABLE CARD commands, so the only provisioning attributes that are modifiable with the SET CARD command relate to software load file preferences. Therefore, this command is only used during software load changes to set software load preferences for cards. Note that the SHDSL24 card replaces the SHDSL16 card.
262	SET CARD={ slot-list | ACTCFC | INACTCFC } [SHDSL16 [WETTINGCURRENT={ ON | OFF }] [ANNEXTYPE={ A | B }] [WIREMODE={ NORMAL | BONDED }]] [PREFLOAD={ filename | NONE }] [ALTLOAD={ filename | NONE }] [TEMPLOAD={ filename | NONE }]	The SET CARD command modifies the provisioning attributes for the SHDSL16 card or list of cards. The administrative state is modified through the ENABLE CARD or DISABLE CARD commands, so the only provisioning attributes that are modifiable with the SET CARD command relate to software load file preferences. Therefore, this command is only used during software load changes to set software load preferences for cards. Note that the SHDSL24 card replaces the SHDSL16 card.
263	SET CONTACTALARM={ 0..2 } STATE={ OPEN | CLOSED } [SEVERITY={ CRITICAL | MAJOR | MINOR | INFO }] [MESSAGE=text]	The SET CONTACTALARM command modifies provisioning for a dry contact input terminal alarm that has been previously defined using the CREATE CONTACTALARM command. The trigger is defined by its contact number and its physical state (open or closed). The severity and message text are modifiable. Setting of an alarm trigger is immediately reflected for any raised alarm associated with it.

No.	*Syntax*	*Description*
264	SET DHCPRELAY AGENT [REMOTEID={ remote-id | DEFAULT }] [CIDFORMAT={ AUTOMATIC | IFDESC | BOTH }]	This command configures Relay Agent parameters for the entire switch. The REMOTEID is used by DHCP Servers to identify this Relay Agent. Setting this parameter is optional. The default remoteid is the MAC address of the switch the Relay Agent is running on. The user can specify the remote Id by entering a string containing 1..30 ASCII characters, or default the remote Id by entering DEFAULT. The Circuit ID format (CIDFORMAT) is used to specify whether the Circuit ID (cid) should be formed automatically by the DHCP feature, or if the user-defined interface description should be used. The cid is used to uniquely identify the subscriber port a DHCP packet is received on. DHCP Servers can use the cid for assigning IP addresses, and (in conjunction with the giaddr value) for lease reports/statistics. The cid is used by the Relay Agent to direct server responses (DHCPOFFER, DHCPACK, DHCPNACK) back to the proper circuit (interface). The default cid-format is AUTOMATIC. When AUTOMATIC is specified, the cid value will automatically be generated by the DHCP Relay Agent. The benefit of using this format, is that the cid is guaranteed to be unique for all ports on the switch (a requirement of option 82). The cid-format value of IFDESC will use the interface description, entered during OAMP interface provisioning as the cid. This is a user-defined string containing 1..31 ASCII characters. The cid-format value of BOTH will concatenate the auto-generated cid and the interface description (entered by the user during OAMP interface provisioning).
265	SET DHCPRELAY INTERFACE={ type:id-range | id-range | ifname-list | ALL } [FILTER={ ON | OFF }] [AGEING={ ON | OFF }]	This command will enable/disable the IP Filtering function on the specified interface. When enabled, a maximum of five (5) IP Filters will be applied to the interface, based on the number of learned MAC addresses that have been assigned IP addresses from DHCP Servers. IP Filtering is off by default, for interfaces with DHCP Relay Agent enabled. Additionally, setting filter to "on" has meaning only when DHCP Relay is enabled on the interface.
266	SET DHCPRELAY={ dhcpname-list | MAIN | ALL } [AGENT REMOTEID={ remote-id | DEFAULT }] [MODE={ RELAY | SNOOPING }] [FORCE]	Changes attributes of the specified DHCP Relay
267	SET EGRESSLIMITER=limitername [RATE=bits-per-second] [BURSTSIZE={ 4KB | 8KB | 16KB | 32KB | 64KB | 128KB | 256KB | 512KB | 1MB | 2MB | 4MB | 8MB | 16MB | 32MB | 64MB }]	The SET EGRESSLIMITER command modifies an existing EGRESSLIMITER. This changes the limit on all ports/interfaces with which the EGRESSLIMITER is associated. See CREATE EGRESSLIMITER for a description of the use of EGRESSLIMITERs.
268	SET EPSR={ epsrdomain-list | ALL } [HELLOTIME=value] [FAILOVERTIME=value] [RINGFLAPTIME=value]	The SET EPSR command is used to set the values of hello time, failover time and ringflap time for the EPSR domains. This command is valid only for Master type of EPSR domains. This operation is only allowed when the EPSR domain is disabled.
269	SET EPSR=epsrdomain INTERFACE={ type:id | id | ifname } [TYPE={ PRIMARY | SECONDARY }]	The SET EPSR INTERFACE command is used to change the interface designation in the EPSR domain. This operation is valid only for Master type of EPSR domains. This operation is only allowed when the EPSR domain is disabled.
270	SET HVLAN={ hvlanname | vid } INTERFACE={ type:id-range | id-range | ifname-list | ALL } [FRAME={ UNTAGGED | TAGGED }]	The SET HVLAN command toggles the status of interfaces in a Hierarchical VLAN (HVLAN) between tagged and untagged. If a group of interfaces is included in the command and the setting of any one of them cannot be performed, the entire operation fails and no interfaces are modified in the HVLAN.
271	SET IGMPSNOOPING { CARD={ slot-list | ALL } MCASTGROUPLIMIT=1..512 | INTERFACE={ type:id-range | id-range | ifname-list | ALL } SNOOPINGMODE={ INTERNAL | EXTERNAL | MCPASSTHROUGH } | [FLOODUNKNOWNS={ ON | OFF }] [ROUTERAGEINGTIMER=10..1200] [GENQUERYTIMER=5..120] [DUPREPORTTIMER=5..120] }	The SET IGMPSNOOPING command is used to set various configurable IGMP settings in the switch. These being setting the multicast stream count per slot, the flooding of unknown multicast packets, and various timers are options you can set.

<table>
<tr><th>No.</th><th>Syntax</th><th>Description</th></tr>
<tr><td>272</td><td>SET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } ADSL [MODE={ GLITE | GDMT | T1.413 | ADSL2 | ADSL2+ | AUTO | AUTO2+ | ADSL2M | ADSL2+M }] [BITMAPMODE={ FBM | DBM }] [LINETYPE={ FAST | INTERLEAVE }] [INTERLEAVEDELAY=1..64] [ECHOCANCELLATION={ ON | OFF }] [DATABOOST={ ON | OFF }] [MAXUPSTREAMRATE=32..3072] [MINUPSTREAMRATE=32..3072] [MAXDOWNSTREAMRATE=32..26624] [MINDOWNSTREAMRATE=32..26624] [TARGETSNRMARGIN=0..15] [MAXSNRMARGIN={ OFF | 1..30 }] [LINEQUALITYMONITOR={ LOW | MEDIUM | HIGH }] [VPI=0..4095] [VCI=32..65535] [DESCRIPTION=description]</td><td>Changes the attribute of the ADSL interface. This should be used with caution since Profiles should be used to define the ADSL interfaces</td></tr>
<tr><td>273</td><td>SET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } COUNTER { ON | OFF }</td><td>The SET INTERFACE COUNTER command enables or disables network monitoring on an interface or interfaces. The act of enabling monitoring does not affect the administrative state of the interface. This command only affects the state of network monitoring. Note: If SET INTERFACE COUNTER is used to enable network monitoring while the interface is disabled, no monitoring will occur until the interface is enabled with the ENABLE INTERFACE command.</td></tr>
<tr><td>274</td><td>SET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } DS1 [TIMINGREFERENCE={ SELF | CONNECTION | CARD }] [LINEENCODING={ B8ZS | AMI }] [LINEBUILDOUT { LONGHAUL={ 0.0DB | -7.5DB | -15.0DB | -22.5DB } | SHORTHAUL={ 133FT | 266FT | 399FT | 533FT | 655FT } }] [FRAMING={ UNFRAMED | SF | ESF | STANDARD }] [DIRECTION={ NETWORK | CUSTOMER }] [DESCRIPTION=description] [FORCE]</td><td>Changes attributes for the DS1 interface</td></tr>
<tr><td>275</td><td>SET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } E1 [TIMINGREFERENCE={ SELF | CONNECTION | CARD }] [LINEENCODING={ HDB3 | AMI }] [FRAMING={ UNFRAMED | E1 | E1CRC | STANDARD }] [DIRECTION={ NETWORK | CUSTOMER }] [DESCRIPTION=description] [FORCE]</td><td>Changes attributes for the E1 interface</td></tr>
<tr><td>276</td><td>SET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } EPON [IPMCVLAN={ vlanname | vid }] [IPADDRESS=ipaddress] [DESCRIPTION=description]</td><td>Changes the EPON interface attributes. (See CREATE PROFILE EPON for information.) This command includes adding a text description.</td></tr>
<tr><td>277</td><td>SET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } FE [AUTONEGOTIATION={ ON | OFF }] [SPEED={ AUTONEGOTIATE | 10 | 100 }] [DUPLEX={ AUTONEGOTIATE | FULL | HALF }] [FLOWCONTROL={ AUTONEGOTIATE | ON | OFF }] [DIRECTION={ NETWORK | CUSTOMER } [FORCE]] [DESCRIPTION=description]</td><td>Changes attributes for the FE interface</td></tr>
<tr><td>278</td><td>SET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } FX [FLOWCONTROL={ ON | OFF }] [DIRECTION={ NETWORK | CUSTOMER } [FORCE]] [DESCRIPTION=description]</td><td>Changes attributes for the FX interface</td></tr>
<tr><td>279</td><td>SET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } GE [AUTONEGOTIATION={ ON | OFF }] [SPEED={ AUTONEGOTIATE | 10 | 100 | 1000 }] [DUPLEX={ AUTONEGOTIATE | FULL | HALF }] [FLOWCONTROL={ AUTONEGOTIATE | ON | OFF }] [DIRECTION={ NETWORK | CUSTOMER }] [DESCRIPTION=description] [FORCE]</td><td>Changes attributes for the GE interface. Note that DUPLEX and SPEED are used only for the 9100.</td></tr>
</table>

No.	Syntax	Description
280	SET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } POTS [CAPABILITY={ PCMU | G726 | ALL }] [MINPACKETIZATION=10..30] [MAXPACKETIZATION=10..30] [BUFFERDELAY=0..150] [BUFFERMODE={ STATIC | DYNAMIC }] [TXPREECHOGAIN=-9.0..+3.0] [TXPOSTECHOGAIN=-9.0..+3.0] [RXPREECHOGAIN=-9.0..+3.0] [RXPOSTECHOGAIN=-9.0..+3.0] [ECHOCANCELLATION={ ON | OFF }] [VOICEACTIVITYDETECTION={ ON | OFF }] [COMFORTNOISEGENERATION={ ON | OFF }] [PACKETLOSSCONCEALMENT={ ON | OFF }] [DESCRIPTION=description]	Changes attributes for the POTs interface
281	SET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } PROFILE=name	Changes the interface(s) to a Profile
282	SET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } SHDSL [MAXCONNECTRATE=72..2312] [MINCONNECTRATE=72..2312] [TARGETSNRMARGIN=0..10] [LINEQUALITYMONITOR={ LOW | MEDIUM | HIGH }] [VPI=0..4095] [VCI=32..65535] [DESCRIPTION=description]	Changes attributes for the SHDSL interface
283	SET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } VDSL [MODE={ VDSL2 | GLITE | GDMT | T1.413 | ADSL2 | ADSL2+ | AUTO | AUTO2 | ADSL2M | ADSL2+M }] [LINETYPE={ FAST | INTERLEAVE }] [MAXUPSTREAMRATE=32..14848] [MINUPSTREAMRATE=32..14848] [MAXDOWNSTREAMRATE=32..51200] [MINDOWNSTREAMRATE=32..51200] [TARGETSNRMARGIN=snr-margin-dB] [MAXSNRMARGIN={ OFF | snr-margin-dB }] [MINSNRMARGIN={ OFF | snr-margin-dB }] [MAXRECEIVEPOWER={ OFF | value }] [BANDPLAN={ 997 | 998 }] [OPTUPSTREAMBAND={ ON | OFF }] [RFIBAND={ { 30M | 40M | 80M | 160M } [,...] | NONE | ALL }] [MAXINTERLEAVEDELAY=0..255] [MINIMPULSENOISEPROTECTION [UPSTREAMMININP={ 0 | 0.5 | 1 | 2 | 4 | 8 | 16 }] [DOWNSTREAMMININP={ 0 | 0.5 | 1 | 2 | 4 | 8 | 16 }]] [DEPLOYMENT={ CABINET | CENTRALOFFICE }] [PSDMASK UPSTREAMPSDMASK={ MASK1 | MASK2 } DOWNSTREAMPSDMASK={ MASK1 | MASK2 }] [DATABOOST={ ON | OFF }] [LINEQUALITYMONITOR={ LOW | MEDIUM | HIGH }] [VPI=0..4095] [VCI=32..65535] [DESCRIPTION=description]	For future release
284	SET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } XE [AUTONEGOTIATION={ ON | OFF }] [FLOWCONTROL={ AUTONEGOTIATE | ON | OFF }] [DESCRIPTION=description]	Changes attributes for the specified XE interface
285	SET INTERFACE={ type:id-range | id-range | ifname-list } DESCRIPTION=description	The SET INTERFACE command is used to modify attributes common to all interfaces. Currently, a user may only set the description for an interface. The description provides a label that is used to identify the purpose or function of an interface. A list of all interfaces is provided by running the SHOW INTERFACE command.

No.	*Syntax*	*Description*
286	SET INTERFACE={ type:id-range | id-range | ifname-list | ALL } [ACCEPTABLE={ ALL | VLAN | HVLAN }] [INFILTERING={ OFF | ON }] [TAGALL={ ON | OFF }] [TPID=tpidvalue] [LEARNLIMIT={ 1..64 | OFF }]	The SET INTERFACE modifies the value of parameters for switch interfaces. To accept only tagged frames on interface 3.0, use the command: SET INTERFACE=3.0 ACCEPTABLE=VLAN. The SHOW INTERFACE displays general information about the specified switch interfaces or all switch interfaces. Parameters displayed in the output of the SHOW INTERFACE command are: -- Port: The number of the switch interface. -- Description: A description of an interface. -- Acceptable Frame Types: The value of the Acceptable Frame Types parameter, one of: "Admit All Frames" or "Admit Only tagged Frames". -- Ingress Filtering: The state of Ingress Filtering: one of "ON" or "OFF". -- TAGALL: The state of TAGALL parameter: one of "ON" or "OFF". -- TPID: The value of TPID (Tag protocol identifier). -- VLAN Translation Info: It list all the VLANs to which are translated to and translate from. -- Untagged VLAN: The name and VLAN Identifier of the interface- based VLAN to which the interface belongs. -- Tagged VLAN(s): The name and VLAN Identifier of the tagged VLAN(s), if any, to which the interface belongs. -- Untagged HVLAN: The name and HVLAN Identifier of the port-based HVLAN to which the interface belongs. -- Tagged HVLAN(s): The name and HVLAN Identifier of the tagged HVLAN(s), if any, to which the interface belongs.
287	SET INTERFACE={ type:id-range | id-range | ifname-list | ALL } ALARM SEVERITY={ NONE | INFO | MINOR | MAJOR | CRITICAL } [FORCE]	Changes the alarm severity for the interfaces specified.
288	SET INTERFACE={ type:id-range | id-range | ifname-list | ALL } COUNTER HISTORY [INTERVAL={ interval-list | ALL }] [BUCKETS=1..2700]	The SET INTERFACE COUNTER HISTORY command allows the user to modify existing entries that specify data collection information for Remote Monitoring (RMON). The number of collections, called BUCKETS, to be retained before over writing the oldest BUCKET for an entry is changeable with this command. To change the INTERVAL, the entry must be deleted and then re-created with the new INTERVAL value.
289	SET INTERFACE={ type:id-range | id-range | ifname-list | ALL } PMONALERT { ATUC [LOFS=0..900] [LOSS=0..900] [LPRS=0..900] [ES=0..900] [SES=0..900] [UAS=0..900] [LOLS=0..900] [FAILEDFASTRETRAIN=threshold] | ATUR [LOFS=0..900] [LOSS=0..900] [LPRS=0..900] [ES=0..900] }	The SET INTERFACE PMONALERT command allows a user to modify the threshold settings for Performance Monitoring (PMON) statistics on a given interface or interfaces. The supported PMON statistics for ADSL interfaces are based on the ADSL-LINE MIB (RFC2662) and ADSL-LINE-EXT MIB (RFC3440).
290	SET INTERFACE={ type:id-range | id-range | ifname-list | ALL } PMONALERT { DS1 | E1 } { NEAREND } { LINE | PATH [FCP=0..32767] [ESAP=0..900] [CSS=0..900] [BES=0..900] [SEFS=0..900] [AISSP=0..900] } [ES=0..900] [SES=0..900] [UAS=0..900] [CV=0..32767]	The SET INTERFACE PMONALERT command allows a user to modify the threshold settings for Performance Monitoring (PMON) statistics on the DS1 or E1 interface
291	SET INTERFACE={ type:id-range | id-range | ifname-list | ALL } PMONALERT ADSL { ATUC [LOFS=0..900] [LOSS=0..900] [LPRS=0..900] [ES=0..900] [SES=0..900] [UAS=0..900] [LOLS=0..900] [FAILEDFASTRETRAIN=threshold] | ATUR [LOFS=0..900] [LOSS=0..900] [LPRS=0..900] [ES=0..900] }	The SET INTERFACE PMONALERT command allows a user to modify the threshold settings for Performance Monitoring (PMON) statistics on a given interface or interfaces. The supported PMON statistics for ADSL interfaces are based on the ADSL-LINE MIB (RFC2662) and ADSL-LINE-EXT MIB (RFC3440).
292	SET INTERFACE={ type:id-range | id-range | ifname-list | ALL } PMONALERT PPP [SENTECHOREQUESTS=0..900] [FAILEDECHOREQUESTS=0..900]	The SET INTERFACE PMONALERT command allows a user to modify the threshold settings for Performance Monitoring (PMON) statistics on the PPP interface
293	SET INTERFACE={ type:id-range | id-range | ifname-list | ALL } PMONALERT PSPAN { SATOP } [ES=0..900] [LOPSS=0..900] [LATEPACKETS=0..230400000] [EARLYPACKETS=0..230400000] [LOSTPACKETS=0..230400000]	The SET INTERFACE PMONALERT command allows a user to modify the threshold settings for Performance Monitoring (PMON) statistics on a PSPAN interface
294	SET INTERFACE={ type:id-range | id-range | ifname-list | ALL } PMONALERT PSPAN { SATOP } [ES=0..900] [LOPSS=0..900] [LATEPACKETS=0..230400000] [EARLYPACKETS=0..230400000] [LOSTPACKETS=0..230400000]	The SET INTERFACE PMONALERT command allows a user to modify the threshold settings for Performance Monitoring (PMON) statistics on the PSAPN interface

No.	Syntax	Description
295	SET INTERFACE={ type:id-range | id-range | ifname-list | ALL } PMONALERT SHDSL [LOSWS=0..900] [CRCANOMALIES=0..900] [ES=0..900] [SES=0..900] [UAS=0..900]	The SET INTERFACE PMONALERT command allows a user to modify the threshold settings for Performance Monitoring (PMON) statistics on the SHDSL interface
296	SET INTERFACE={ type:id-range | id-range | ifname-list | ALL } PMONALERT VDSL { VTUC [LOFS=0..900] [LOSS=0..900] [LPRS=0..900] [ES=0..900] [SES=0..900] [UAS=0..900] [LOLS=0..900] [FAILEDFASTRETRAIN=threshold] | VTUR [LOFS=0..900] [LOSS=0..900] [LPRS=0..900] [ES=0..900] }	For future release
297	SET IP INTERFACE={ MGMT | type:id-range | ifname-list | ALL } [IPADDRESS=ipaddress] [SUBNETMASK=mask] [IFNAME=ifname] [GATEWAY=ipaddress] [DOMAINNAME=name] [DNS=ipaddress-list]	The SET IP INTERFACE command modifies the IP configuration attributes on an existing interface. If this command is executed while the interface is in use, users of the interface must reconnect after the settings are applied by the system.
298	SET LLDP [TXINTERVAL=5..32768] [TXHOLD=2..10] [TXDELAY=1..8192] [REINITDELAY=1..10] [NOTIFYINTERVAL=5..3600]	Sets the global LLDP values
299	SET LLDP INTERFACE={ type:id-range | id-range | ifname-list | ALL } [MODE={ TX | RX | BOTH | OFF }] [NOTIFY={ ON | OFF }]	Used to enable or disable LLDP for the interface(s). To enable, set the MODE command to TX, RX, or BOTH. (If the MODE command is not entered, the default is BOTH). To disable, set the MODE to OFF. NOTIFY controls whether traps are sent to an NMS if there is a change in the link set
300	SET LOGINBANNER { FILE=filename | STRING=string } [{ USER | MANAGER | SECURITYOFFICER | ALL }]	The SET LOGINBANNER command allows the user to set the loginbanner to be displayed when a user logins into the system. If a FILE parameter is provided, the contents of the file is retrieved and stored locally. The contents of the file is also retrieved upon system reboot. If the file is deleted or replaced, the local storage of the loginbanner is not updated unless the command is re-run or the system is rebooted. If the STRING parameter is provided, the contents of the string is stored locally and persisted for use after system reboots. The maximum length of the STRING value is 255 characters. The USER, MANAGER, SECURITYOFFICER and ALL parameters define which user level(s) the loginbanner is applied to.
301	SET MGCP INTERFACE={ type:id-range | id-range | ifname-list | ALL } [CALLAGENT={ domain | domain:udp-port | localname@domain | localname@domain:udp-port }] [CALLAGENTPROFILE={ GENERIC | GENBAND | METASWITCH | ASTERISK }] [DISCONNECTTHRESHOLD=number] [SUSPICIONTHRESHOLD=number] [INITIALRETRANSMITDELAY=100..4000] [MAXRETRANSMITDELAY=100..4000] [IPDSCP=0..63] [UDPPORT=udp-port] [VPRIORITY=0..7]	The SET MGCP INTERFACE command sets MGCP parameters associated with an existing interface.
302	SET MLPPP={ mlpppname-list | ALL } [SEGMENTSIZE={ 64..1526 }] [SEQUENCENUMBERBITS={ 12 | 24 }] [FORCE]	Set configuration parameters for an MLPPP group. Note the ID cannot be changed. Interface associations should be changed using the ADD and DELETE commands.
303	SET ONU=onuname MACADDRESS=macaddress	Requests to modify an ONU interface(s). The ONNU name is used in an effort to reflect that this should only be used on one ONU at a time to avoid duplicate MACs.
304	SET PORT={ port-list | ALL } ADSL [attributes]	The SET PORT command is deleted in 7.0. Use the SET INTERFACE command instead.
305	SET PORT={ port-list | ALL } DS1 [DS1 attributes]	The SET PORT command is deleted in 7.0. Use the SET INTERFACE command instead.
306	SET PORT={ port-list | ALL } E1 [E1 attributes]	The SET PORT command is deleted in 7.0. Use the SET INTERFACE command instead.
307	SET PORT={ port-list | ALL } FE [FE attributes]	The SET PORT command is deleted in 7.0. Use the SET INTERFACE command instead.
308	SET PORT={ port-list | ALL } FX [FX attributes]	The SET PORT command is deleted in 7.0. Use the SET INTERFACE command instead.

No.	*Syntax*	*Description*
309	SET PORT={ port-list | ALL } GE [GE attributes]	The SET PORT command is deleted in 7.0. Use the SET INTERFACE command instead.
310	SET PORT={ port-list | ALL } POTS [POTS attributes]	The SET PORT command is deleted in 7.0. Use the SET INTERFACE command instead.
311	SET PORT={ port-list | ALL } SHDSL [SHDSL Attributes]	The SET PORT command is deleted in 7.0. Use the SET INTERFACE command instead.
312	SET PORT={ port-list | ALL } XE [WITH LAG=lagname] [AUTONEGOTIATION={ ON | OFF }] [FLOWCONTROL={ AUTONEGOTIATE | ON | OFF }] [DESCRIPTION=description]	Associates and XE port with a LAG and sets its attributes
313	SET PPP INTERFACE={ type:id-range | id-range | ifname-list } [RESTARTINTERVAL=seconds] [MAXTERMINATE={ value | CONTINUOUS }] [MAXCONFIGURE=value] [MAXFAILURE={ value | CONTINUOUS }] [ECHOREQUEST={ seconds | OFF }]	Modifies PPP configuration parameters for the specified interfaces. The interfaces can be entered as ppp:x, ds1:x, e1:x... all will be accepted
314	SET PROFILE=name ADSLPORT [MODE={ GLITE | GDMT | T1.413 | ADSL2 | ADSL2+ | AUTO | AUTO2+ | ADSL2M | ADSL2+M }] [BITMAPMODE={ FBM | DBM }] [LINETYPE={ FAST | INTERLEAVE }] [INTERLEAVEDELAY=1..64] [ECHOCANCELLATION={ ON | OFF }] [DATABOOST={ ON | OFF }] [MAXUPSTREAMRATE=32..3072] [MINUPSTREAMRATE=32..3072] [MAXDOWNSTREAMRATE=32..26624] [MINDOWNSTREAMRATE=32..26624] [TARGETSNRMARGIN=0..15] [MAXSNRMARGIN={ OFF | 1..30 }] [LINEQUALITYMONITOR={ LOW | MEDIUM | HIGH }] [VPI=0..4095] [VCI=32..65535] [ADMINSTATE={ UP | DOWN }] [MODE={ GLITE | GDMT | T1.413 | ADSL2 | ADSL2+ | AUTO | AUTO2+ }] [BITMAPMODE={ FBM | DBM }] [LINETYPE={ FAST | INTERLEAVE }] [INTERLEAVEDELAY=1..64] [ECHOCANCELLATION={ ON | OFF }] [MAXUPSTREAMRATE=32..1024] [MINUPSTREAMRATE=32..1024] [MAXDOWNSTREAMRATE=32..26624] [MINDOWNSTREAMRATE=32..26624] [TARGETSNRMARGIN=0..15] [LINEQUALITYMONITOR={ LOW | MEDIUM | HIGH }] [VPI=0..255] [VCI=32..65535] [ADMINSTATE={ UP | DOWN }]	The SET PROFILE command modifies provisioning attributes for the profile specified by name and component type. A profile for a component is similar to a template, since it contains a set of pre-defined provisioning attributes. For this release, only the profile name AutoProv is supported, which signifies the auto provisioning profile. The auto provisioning profile is used by the system when cards and ports are discovered during card insertion or system startup. The auto provisioning profile can also be manually applied to an already provisioned card or port using the SET CARD or SET PORT commands. Upon initial system startup (before any user modification is done) the profiles are populated with factory default attributes. Any subsequent user modification of the profile attributes using this command is stored in the system database and is retained over subsequent restarts.
315	SET PROFILE=name CES8 [PREFLOAD=filename] [ADMINSTATE={ UP | DOWN }] [PORTTYPE={ DS1 | E1 }]	Changes attributes for the PROFILE
316	SET PROFILE=name DS1PORT [ADMSET PROFILE=name DS1PORT [ADMINSTATE={ UP | DOWN }] [TIMINGREFERENCE={ SELF | CONNECTION | CARD }] [LINEENCODING={ B8ZS | AMI }] [LINEBUILDOUT { LONGHAUL={ 0.0DB | -7.5DB | -15.0DB | -22.5DB } | SHORTHAUL={ 133FT | 266FT | 399FT | 533FT | 655FT } }] [FRAMING={ UNFRAMED | SF | ESF | STANDARD }]INSTATE={ UP | DOWN }] [TIMINGREFERENCE={ SELF | CONNECTION | CARD }] [LINEBUILDOUT { LONGHAUL={ 0.0DB | -7.5DB | -15.0DB | -22.5DB } | SHORTHAUL={ 133FT | 266FT | 399FT | 533FT | 655FT } }] [LINEENCODING={ B8ZS | AMI }] [LOOPBACK={ NONE | INWARD | LINE }]	Sets the attributes for the DS1PORT Profile
317	SET PROFILE=name E1PORT [ADMINSTATE={ UP | DOWN }] [TIMINGREFERENCE={ SELF | CONNECTION | CARD }] [LINEENCODING={ HDB3 | AMI }] [FRAMING={ UNFRAMED | E1 | E1CRC | STANDARD }]	Sets the attibutes for the E1PORT profile
318	SET PROFILE=name EPONPORT [ADMINSTATE={ UP | DOWN }] [IPMCVLAN={ vlanname | vid }] [IPADDRESS=ipaddress]	Changes the EPON profile interface attributes. (See CREATE PROFILE EPON for information.)

No.	Syntax	Description
319	SET PROFILE=name FEPORT [ADMINSTATE={ UP | DOWN }] [AUTONEGOTIATION={ ON | OFF }] [SPEED={ AUTONEGOTIATE | 10 | 100 }] [DUPLEX={ AUTONEGOTIATE | FULL | HALF }] [FLOWCONTROL={ AUTONEGOTIATE | ON | OFF }]	The SET PROFILE command modifies provisioning attributes for the profile specified by name and component type. For a description, refer to the SET PROFILE command for the ADSL port.
320	SET PROFILE=name FXPORT [FLOWCONTROL={ ON | OFF }] [ADMINSTATE={ UP | DOWN }]	See SET PROFILE=name ADSL16 [PREFLOAD=filename] [ADMINSTATE={UP|DOWN}]
321	SET PROFILE=name GEPORT [AUTONEGOTIATION={ ON | OFF }] [SPEED={ AUTONEGOTIATE | 10 | 100 | 1000 }] [DUPLEX={ AUTONEGOTIATE | FULL | HALF }] [FLOWCONTROL={ AUTONEGOTIATE | ON | OFF }] [ADMINSTATE={ UP | DOWN }]	The SET PROFILE command modifies the provisioning attributes for the specified port or list of ports. For a description, refer to the command SET PORT for ADSL.
322	SET PROFILE=name NTE8 [PREFLOAD=filename] [ADMINSTATE={ UP | DOWN }] [PORTTYPE={ DS1 | E1 }]	Sets the attribute for the NTE8 card profile. Note that PORTTYPE determines if the card will function for DS1 or E1 paths.
323	SET PROFILE=name POTSPORT [CAPABILITY={ PCMU | G726 | ALL }] [MINPACKETIZATION=10..30] [MAXPACKETIZATION=10..30] [BUFFERDELAY=0..150] [BUFFERMODE={ STATIC | DYNAMIC }] [TXPREECHOGAIN=-9.0..+3.0] [TXPOSTECHOGAIN=-9.0..+3.0] [RXPREECHOGAIN=-9.0..+3.0] [RXPOSTECHOGAIN=-9.0..+3.0] [ECHOCANCELLATION={ ON | OFF }] [VOICEACTIVITYDETECTION={ ON | OFF }] [COMFORTNOISEGENERATION={ ON | OFF }] [PACKETLOSSCONCEALMENT={ ON | OFF }] [ADMINSTATE={ UP | DOWN }]	The SET PROFILE command modifies provisioning attributes for the profile specified by name and component type. A profile for a component is similar to a template, since it contains a set of pre-defined provisioning attributes. For this release, only the profile name AutoProv is supported, which signifies the auto provisioning profile. Auto provisioning profiles are available for the GE1 card, GE3 card, GE port, ADSL16 card, ADSL8S card, ADSL port, FE10 card and FE port. The auto provisioning profile is used by the system when cards and ports are discovered during card insertion or system startup. The auto provisioning profile can also be manually applied to an already provisioned card or port using the SET CARD or SET PORT commands. Upon initial system startup (before any user modification is done) the profiles are populated with factory default attributes. Any subsequent user modification of the profile attributes using this command is stored in the system database and is retained over subsequent restarts.
324	SET PROFILE=name SHDSLPORT [MAXCONNECTRATE=72..2312] [MINCONNECTRATE=72..2312] [TARGETSNRMARGIN=0..10] [LINEQUALITYMONITOR={ LOW | MEDIUM | HIGH }] [VPI=0..4095] [VCI=32..65535] [ADMINSTATE={ UP | DOWN }]	The SET PROFILE command modifies provisioning attributes for the profile specified by name and component type. A profile for a component is similar to a template, since it contains a set of pre-defined provisioning attributes. For this release, only the profile name AutoProv is supported, which signifies the auto provisioning profile. Auto provisioning profiles are available for the GE1 card, GE3 card, GE port, ADSL16 card, ADSL8S card, ADSL port, FE10 card and FE port. The auto provisioning profile is used by the system when cards and ports are discovered during card insertion or system startup. The auto provisioning profile can also be manually applied to an already provisioned card or port using the SET CARD or SET PORT commands. Upon initial system startup (before any user modification is done) the profiles are populated with factory default attributes. Any subsequent user modification of the profile attributes using this command is stored in the system database and is retained over subsequent restarts.

No.	Syntax	Description
325	SET PROFILE=name VDSLPORT [MODE={ VDSL2 | GLITE | GDMT | T1.413 | ADSL2 | ADSL2+ | AUTO | AUTO2 | ADSL2M | ADSL2+M }] [LINETYPE={ FAST | INTERLEAVE }] [MAXUPSTREAMRATE=32..14848] [MINUPSTREAMRATE=32..14848] [MAXDOWNSTREAMRATE=32..51200] [MINDOWNSTREAMRATE=32..51200] [TARGETSNRMARGIN=snr-margin-dB] [MAXSNRMARGIN={ OFF | snr-margin-dB }] [MINSNRMARGIN={ OFF | snr-margin-dB }] [MAXRECEIVEPOWER={ OFF | value }] [BANDPLAN={ 997 | 998 }] [OPTUPSTREAMBAND={ ON | OFF }] [RFIBAND={ { 30M | 40M | 80M | 160M } [,...] | NONE | ALL }] [MAXINTERLEAVEDELAY=0..255] [MINIMPULSENOISEPROTECTION [UPSTREAMMININP={ 0 | 0.5 | 1 | 2 | 4 | 8 | 16 }] [DOWNSTREAMMININP={ 0 | 0.5 | 1 | 2 | 4 | 8 | 16 }]] [DEPLOYMENT={ CABINET | CENTRALOFFICE }] [PSDMASK UPSTREAMPSDMASK={ MASK1 | MASK2 } DOWNSTREAMPSDMASK={ MASK1 | MASK2 }] [DATABOOST={ ON | OFF }] [LINEQUALITYMONITOR={ LOW | MEDIUM | HIGH }] [VPI=0..4095] [VCI=32..65535] [ADMINSTATE={ UP | DOWN }]	For future release
326	SET PROFILE=name XEPORT [AUTONEGOTIATION={ ON | OFF }] [FLOWCONTROL={ AUTONEGOTIATE | ON | OFF }] [ADMINSTATE={ UP | DOWN }]	Changes attributes of the specified XEPORT
327	SET PROMPT=string	The SET PROMPT command is used to define a new, default CLI command prompt for user login sessions. The prompt string can contain alphanumeric text and special tokens. The special tokens identify dynamic information in the prompt. The following are special tokens supported for the prompt: %d - The current date in YYYY/MM/DD format %i - The management IP address of the device %n - The hostname of the device as defined by the SET SYSTEM HOSTNAME command %s - The current security level of the user %t - The current time in HH:MM:SS format in 24-hour format %u - The name of the user logged in to a given session When entering a new prompt, the 'string' must be enclosed in quotes(") if any space characters are used. For example, the following prompt uses the prompt string "%u %s": officer SEC>> To create a prompt that contains the current time and hostname, the following command is used: officer SEC>> SET PROMPT="%t %n" Info (010017): Operation Successful 10:23:11 cerberus>> Prompts are limited to 70 characters. When a token is included in the prompt definition, a worst-case calculation is used for each token to ensure that the prompt will fit in the space provided. As a result, it is possible to create a prompt definition with tokens that appears to be short, but is still rejected because the possible expansion for the prompt is too long.
328	SET PSPAN={ pspanname-list | ALL } SATOP [UDPPORT=49152..65535] [PEERIPADDRESS=ipaddress] [PEERUDPPORT=49152..65535] [NUMBYTES=16..1023] [JITTERBUFFER=value] [TIMINGREFERENCE={ SELF | CONNECTION | CARD }] [RTP={ ON | OFF }] [VPRIORITY=0..7] [IPDSCP=0..63]	Changes the PSPAN's attributes

No.	*Syntax*	*Description*
329	SET QOS [VLAN4QUEUEMAP=value-map] [VLAN8QUEUEMAP=value-map]	The SET QOS VLAN4QUEUEMAP,VLAN8QUEUEMAP command(s) sets the mapping of VLAN priority bits to egress queues. This allows the user to configure the prioritization of traffic through the system. The VLAN8QUEUEMAP is applied to interfaces capable of 8 egress queues, while the VLAN4QUEUEMAP is applied to interfaes capable of 4 egress queues. The user priority field in an incoming frame (with value 0 to 7) determines the packet's egress queue. Egress queues are numbered from 0 (lowest priority) to N (highest priority), where the value of N depends on the hardware/software capabilities of the system. All frames in queue N are sent before any frames in queue N-1, and so on until queue 0 which is only serviced when no other queues contain any packets. The format for entering VLAN4QUEUEMAP and VLAN8QUEUEMAP is a comma-delimited list of 8 egress queue number values. An example of a comma-delimited list of 8 egress queues: SET QOS VLAN4QUEUEMAP=0,0,1,1,2,2,3,3 VLAN8QUEUEMAP=0,1,2,3,4,5,6,7 To display the mapping of VLAN priority field values to egress queues, use the command: "SHOW QOS".
330	SET QOSPOLICY={ policyname-list | ALL } [DESCRIPTION=text] [MAXUPSTREAMRATE={ bits-per-second | MAX }] [MAXDOWNSTREAMRATE={ bits-per-second | MAX }] [MINUPSTREAMRATE={ bits-per-second | MIN }] [MINDOWNSTREAMRATE={ bits-per-second | MIN }] [UPBURSTSIZE={ 1..256 | MAX }] [DOWNBURSTSIZE={ 1..256 | MAX }] [UPDELAYSENSITIVITY={ SENSITIVE | TOLERANT }] [DOWNDELAYSENSITIVITY={ SENSITIVE | TOLERANT }]	Requests to modify a QOSPOLICY. For parameters, see CREATE QOSPOLICY
331	SET RADIUS SERVER={ ipaddress-list | hostname-list | ALL } [SECRET=secret] [AUTHPORT=1..65535] [ACCTPORT=1..65535] [RETRIES=0..10] [TIMEOUT=1..60] [AUTHENTICATION={ ON | OFF }] [ACCOUNTING={ ON | OFF }]	The SET RADIUS SERVER command allows the user to change the settings of one or more existing configured RADIUS servers. Users can change the servers' shared secret, port number, retries and timeout values.
332	SET RTP INTERFACE={ type:id-range | id-range | ifname-list | ALL } [IPDSCP=0..63] [VPRIORITY=0..7]	The SET RTP INTERFACE command sets RTP parameters associated with an existing interface.
333	SET STP { INSTANCE={ stpname | mstid | MAIN | ALL } { DEFAULT | PRIORITY=0..65535 | INTERFACE={ type:id-range | id-range | ifname-list | ALL } { DEFAULT | [PATHCOST=path-cost] [PORTPRIORITY=port-priority] [EDGEPORT={ TRUE | FALSE }] [POINT2POINT={ TRUE | FALSE | AUTO }] [BPDUCOP={ ON | OFF }] } } | DEFAULT | [PRIORITY=0..65535] [FORWARDDELAY=4..30] [HELLOTIME=1..10] [MAXAGE=6..40] [TXMAX=1..10] [MAXHOPS=6..40] [MSTREGION=regionname] [REVISIONLEVEL=0..65535] [CISCOCONFIGURATIONDIGEST=hexstring] [CISCOLEARNEDINTERFACE={ type:id | id | ANY }] | PROTOCOL={ STP_ORIGINAL | RSTP | STP_COMPATIBLE_RSTP | MSTP | CISCO_COMPATIBLE_MSTP } [FORCE] | INTERFACE={ type:id-range | id-range | ifname-list | ALL } { DEFAULT | [PATHCOST=path-cost] [PORTPRIORITY=port-priority] [EDGEPORT={ TRUE | FALSE }] [POINT2POINT={ TRUE | FALSE | AUTO }] [BPDUCOP={ ON | OFF }] } }	The SET STP command allows a user to modify select Spanning Tree Protocol(STP) parameters. STP uses three configurable parameters for the time intervals that control the flow of STP information on which the dynamic STP topology depends: the HELLOTIME, FORWARDDELAY and MAXAGE parameters. All switches in the same spanning tree topology must use the same values for these parameters, but can themselves be configured with different, and potentially incompatible time intervals. The parameter values actually used by each switch are those sent by the root bridge, and forwarded to all other switches by the designated bridges. The FORWARDDELAY, MAXAGE and HELLOTIME parameters should be set according to the following formulae, as specified in IEEE Standard 802.1D: 2 x (FORWARDDELAY - 1.0 seconds) >= MAXAGE MAXAGE >= 2 x (HELLOTIME + 1.0 seconds) New for 7.2 is the BPDU Cop feature, which, when enabled, disables an interface that receives a BPDU
334	SET SYSTEM POWERINPUT={ -48VDC | -60VDC }	Sets the power input for the system. The default is for POWERINPUT is -48VDC.
335	SET SYSTEM USERCONFIG [LOGINFAIL=1..10] [LOCKOUTPD=0..30000] [MANPWDFAIL=1..5] [SECUREDELAY={ OFF | 0 | 1..90 }] [MINPWDLEN=1..23] [PERSISTTIMER=1..1440] [PWDAGEING={ OFF | 0 | 1..365 }] [FORCEPWDCHANGE={ YES | NO }]	The SET SYSTEM USERCONFIG command is used to modify global security parameters for user authentication. Changes to the minimum password length will affect only new users or future updates to existing user passwords.

No.	Syntax	Description
336	SET TELNET [TERMTYPE=termstring] [INSERTNULL={ ON | OFF }]	Allows the user to set the system-wide settings of the telnet client configuration, including the TERMTYPE and INSERTNULL data. The TERMTYPE string is the string that will be sent to a remote telnet server during the negotiation of the telnet connection. The default value is "XTERM". The terminal identification is usually used by the remote system to set the terminal attributes for the Telnet session. The INSERTNULL parameter, when set to ON, specifies that a NULL character should be inserted after each CR sent to the remote system. The default is OFF.
337	SET TRACE [BUFFERSIZE=events [FORCE]]	The SET TRACE command is used to control the settings of the Trace system.
338	SET TRAFFICDESCRIPTOR=tdname-list [RATE=bits-per-second] [BURSTSIZE={ 4KB | 8KB | 16KB | 32KB | 64KB | 128KB | 256KB | 512KB | 1MB | 2MB | 4MB | 8MB | 16MB | 32MB | 64MB }]	The SET TRAFFICDESCRIPTOR command modifies one or more TRAFFICDESCRIPTORs. This applies new values for RATE and BURSTSIZE for all CLASSIFIERS to which the TRAFFICDESCRIPTOR(s) are associated.
339	SET USER=login-name [PASSWORD=password [FORMAT={ CLEARTEXT | MD5 }]] [DESCRIPTION=description] [PRIVILEGE={ USER | MANAGER | SECURITYOFFICER }] [LOGIN={ TRUE | FALSE | ON | OFF | YES | NO }] [TELNET={ YES | NO }] [PWDAGEING={ OFF | 0 | 1..365 }] [DEACTIVATE={ OFF | yyyy-mm-dd }]	The SET USER command is used to modify an existing user account in the system. At a minimum, a user login name must be specified. The password can be clear text (non-encrypted) or in the form of a 32-character MD5 encrypted string. Unless the FORMAT option is specified, the password value is assumed to be clear text.
340	SET USER=login-name [PASSWORD=password [FORMAT={ CLEARTEXT | MD5 }]] [DESCRIPTION=description] [PRIVILEGE={ USER | MANAGER | SECURITYOFFICER }] [LOGIN={ TRUE | FALSE | ON | OFF | YES | NO }] [TELNET={ YES | NO }] [SSH={ YES | NO }] [PUBLICKEY=key-name] [PWDAGEING={ OFF | 0 | 1..365 }] [DEACTIVATE={ OFF | yyyy-mm-dd }]	The SET USER command is used to modify an existing user account in the system. At a minimum, a user login name must be specified. The password can be clear text (non-encrypted) or in the form of a 32-character MD5 encrypted string. Unless the FORMAT option is specified, the password value is assumed to be clear text.
341	SET VC=vcid INTERFACE={ type:id-range | id-range | ifname-list } [VPI=0..255] [VCI=32..65535] [TXPEAKCELLRATE={ 150..65535 | MAX }]	This command is used to change the VC configuration parameters like VPI, VCI or traffic parameters like txpeakcellrate.
342	SET VLAN={ vlanname | vid } INTERFACE={ type:id-range | id-range | ifname-list | ALL } [FRAME={ UNTAGGED | TAGGED }] [TRANSLATE={ 1..4094 | NONE }] [FORWARDING={ PRIMARYUPSTREAM | SECONDARYUPSTREAM | DOWNSTREAM | STP | UCP }]	The SET VLAN command toggles the status of interfaces in a Virtual LAN (VLAN) between tagged and untagged. If a group of interfaces is included in the command and the setting of any one of them cannot be performed, the entire operation fails and no interfaces are modified in the VLAN.
343	SET ACCESSLIST=accesslistname RULE=rulenumber [{ PERMIT | DENY }] [IPSOURCE={ ipaddress | ANY } [SOURCEMASK=mask]] [IPDEST={ ipaddress |ANY } [DESTMASK=mask]] [MACSOURCE={ macaddress | ANY }] [MACDEST={macaddress | ANY }] [APPLICATION={ DHCPSERVER | DHCPCLIENT | NETBIOS |FUM | TELNET | SSH | SNMP | FTP | TFTP }] [TCPPORTDEST={ tcp-port-list |ANY }] [TCPPORTSOURCE={ tcp-port | ANY }] [UDPPORTDEST={ udp-port-list| ANY }] [UDPPORTSOURCE={ udp-port | ANY }] [PROTOCOL={ IPV4 | IPV6 |protocol-type | ANY }] [IPPROTOCOL={ TCP | UDP | ICMP | IGMP |ipprotocol-type | ANY }]	The SET ACCESSLIST command changes the action and/or match rule information for a given RULE. The SET command only alters the match rules specified. All others are left the same. For example, if rule 1 was: PERMIT IPS=1.1.1.1 TCPPORTDEST=23 then the command entered was: SET ACCESSLIST myACL PERMIT IPS=2.2.2.2 TCPPORTDEST would NOT be removed. To remove all match rules use the RESET ACCESSLIST command.
344	SET BOOTSERVER=ipaddress [PATH=pathname|NONE]	The SET BOOTSERVER command sets static IP address of the network boot server. The network boot server is the source for the preferred CFC software load file. The device downloads the preferred load from the boot server via TFTP when all boot attempts for the CFC fail from the CFC flash file system. The preferred software load is set using the command SET CARD=ACTCFC PREFLOAD=filename. In the event the CFC cannot use the preferred load from its own flash filesystem, the preferred load file is transferred from the boot server and written to the flash, replacing any existing preferred load file for the CFC.

No.	Syntax	Description
345	SET CARD={ slot-list | ACTCFC | INACTCFC } { PREFLOAD={ filename | NONE } | ALTLOAD={ filename | NONE } | TEMPLOAD={ filename | NONE } | CES8 [PORTTYPE={ DS1 | E1 }] [TIMINGREFERENCE={ type:id | ifname | INTERNAL }] }	For CES8, adds PORTTYPE and TIMINGREFERENCE
346	SET CARD={slot-list|ACTCFC|INACTCFC} {PREFLOAD={filename|NONE}|ALTLOAD={filename|NONE}| TEMPLOAD={filename|NONE}}	The SET CARD command modifies the provisioning attributes for the specified card or list of cards. The administrative state is modified through the ENABLE CARD or DISABLE CARD commands, so the only provisioning attributes that are modifiable with the SET CARD command relate to software load file preferences. Therefore, this command is only used during software load changes to set software load preferences for cards.
347	SET CARD=slot-list PROFILE=name	The SET CARD command modifies the provisioning attributes for the specified card or list of cards. The administrative state is modified through the ENABLE CARD or DISABLE CARD commands, so the only provisioning attributes that are modifiable with the SET CARD command relate to software load file preferences. Therefore, this command is only used during software load changes to set software load preferences for cards.
348	SET CLASSIFIER=classifiername-list [VID={ 1..4095 | ANY }] [VPRIORITY={ 0..7 | ANY }] [INNERVID={ 1..4095 | ANY }] [INNERVPRIORITY={ 0..7 | ANY }] [ETHFORMAT={ 802.3 | 802.3TAGGED | 802.3UNTAGGED | ETHII | ETHIITAGGED | ETHIIUNTAGGED | ANY }] [LSAP={ NETBIOS | lsap-value | ANY }] [IPDEST={ ipaddress-mask | MULTICAST | ANY }] [IPSOURCE={ ipaddress-mask | ANY }] [IPDSCP={ 0..63 | ANY }] [IPPROTOCOL={ TCP | UDP | ICMP | IGMP | ipprotocol-number | ANY }] [IPTOS={ 0..7 | ANY }] [MACDEST={ macaddress | MULTICAST | ANY }] [MACSOURCE={ macaddress | ANY }] [PROTOCOL={ IPV4 | IPV6 | protocol-type | ANY }] [TCPPORTDEST={ tcp-port-list | ANY }] [TCPPORTSOURCE={ tcp-port | ANY }] [TCPFLAGS={ { URG | ACK | RST | SYN | FIN | PSH } [,...] | ANY }] [UDPPORTDEST={ udp-port-list | ANY }] [UDPPORTSOURCE={ udp-port | ANY }]	The SET CLASSIFIER command sets the match rule for the specified CLASSIFIER(s). The match rule specified in this command replaces any existing match rule on the CLASSIFIER(s).
349	SET INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } COUNTER { ON | OFF }	The SET INTERFACE COUNTER command enables or disables network monitoring on an interface or interfaces. The act of enabling monitoring does not affect the administrative state of the interface. This command only affects the state of network monitoring. Note: If SET INTERFACE COUNTER is used to enable network monitoring while the interface is disabled, no monitoring will occur until the interface is enabled with the ENABLE INTERFACE command.
350	SET INTERFACE={ type:id-range | id-range | ifname-list | ALL } RMONALERT { DROPEVENTS | OCTETS | PACKETS | BROADCAST | MULTICAST | UNDERSIZE | OVERSIZE | CRCALIGN | FRAGMENTS | JABBERS | COLLISIONS | PKTS64OCTETS | PKTS65TO127OCTETS | PKTS128TO255OCTETS | PKTS256TO511OCTETS | KTS512TO1023OCTETS | PKTS1024TO1518OCTETS } [{ ABSOLUTE | CHANGE }] [INTERVAL=2..3600] [RISINGTHRESHOLD=threshold] [FALLINGTHRESHOLD=threshold]	The SET INTERFACE RMONALERT command allows a user to modify threshold alarming settings for an Ethernet statistic on a specified interface. The supported Remote Monitoring (RMON) statistics for Ethernet interfaces are based on the RMON MIB (RFC2819). Samples are taken on an interval basis and compared to the provided thresholds. A management log and an SNMP trap are generated when either the rising or falling threshold is crossed.
351	SET LAG=lagname [MODE={ON|OFF|PASSIVE|ACTIVE}] [SELECT={MACSRC|MACDEST|MACBOTH|IPSRC|IPDEST|IPBOTH|PORTSRC|PORTDEST}] [ADMINKEY=1..1024]	The SET LAG command modifies an existing Link Aggregation Group(LAG). This command can change the MODE, SELECT criteria, and ADMINKEY settings on the LAG. If a user desires to change the set of interfaces associated with the LAG, to change interface membership for a LAG, the ADD LAG INTERFACE and DELETE LAG INTERFACE commands must be used. It is also not possible to change the LAG ID for a LAG once it is created.
352	SET LOG FILTER=filterid [CATEGORY=category] [SEVERITY=[op]{CRITICAL|MAJOR|MINOR|NONE}]	The SET LOG FILTER command is used to change the filter criteria on an existing management log filter. By default, if no category, severity or format options are specified, the management log filter is set to match all logs.

No.	*Syntax*	*Description*
353	SET LOG OUTPUT=outputid [{CLI [FORMAT={FULL|MSGONLY|SUMMARY}]| CONSOLE [FORMAT={FULL|MSGONLY|SUMMARY}]| SYSLOG SERVER={ipaddress|hostname}}]	The SET LOG OUTPUT command is used to change the management log output destination settings. By default, if no category, severity or format options are specified, the management log filter is set to match all logs.
354	SET PASSWORD	Allows Users to change their password at anytime. The command prompts for the old password and asks to reconfirm the new password.
355	SET PORT=port-list PROFILE=name	The SET PORT command is deleted in 7.0. Use the SET INTERFACE command instead.
356	SET PROFILE=name card_type [PREFLOAD=filename] [ADMINSTATE={UP|DOWN}]	The SET PROFILE command modifies provisioning attributes for the profile specified by name and component type. A profile for a component is similar to a template, since it contains a set of pre-defined provisioning attributes. For release 7.0, user-created Profiles and the name AutoProv are supported, which signifies the auto provisioning profile. The auto provisioning profile is used by the system when cards and ports are discovered during card insertion or system startup. The auto provisioning profile can also be manually applied to an already provisioned card or port using the SET CARD or SET INTERFACE commands. Upon initial system startup (before any user modification is done) the profiles are populated with factory default attributes. Any subsequent user modification of the profile attributes using this command is stored in the system database and is retained over subsequent restarts. For release 7.0, card types are ADSL16B, ADSL16C, ADSL16, ADSL24A, ADSL24B, ADSL24, ADSL8S, CES8, CFC24, CFC4, CFC6, FE10, FE2, FX10, GE1, GE2, GE3, POTS24, SHDSL16, SHDSL24, NTE8, and GE8. In release 8.0, new cards are CFC56, EPON2, VDSL24A, VDSL24B, and XE1.
357	SET PROFILE=name SHDSL16 [PREFLOAD=filename] [ADMINSTATE={ UP | DOWN }] [WETTINGCURRENT={ ON | OFF }] [ANNEXTYPE={ A | B }]	The SET PROFILE command modifies provisioning attributes for the profile of the SHDSL16 card. A profile for a component is similar to a template, since it contains a set of pre-defined provisioning attributes. For this release, only the profile name AutoProv is supported, which signifies the auto provisioning profile. Auto provisioning profiles are available for the SHDSL16 card, SHDSL port. The auto provisioning profile is used by the system when cards and ports are discovered during card insertion or system startup. The auto provisioning profile can also be manually applied to an already provisioned card or port using the SET CARD or SET PORT commands. Upon initial system startup (before any user modification is done) the profiles are populated with factory default attributes. Any subsequent user modification of the profile attributes using this command is stored in the system database and is retained over subsequent restarts.
358	SET PROFILE=name SHDSL24 [PREFLOAD=filename] [ADMINSTATE={ UP | DOWN }] [WETTINGCURRENT={ ON | OFF }] [ANNEXTYPE={ A | B }]	The SET PROFILE command modifies provisioning attributes for the profile of the SHDSL24 card. Refer to the SET PROFILE command for the SHDSL16 card for details.
359	SET RADIUS AUTHMODE={ LOGIN | COMMAND }	The SET RADIUS AUTHMODE command is used to change the authentication mode for use with RADIUS servers. When the RADIUS authentication mode is set to LOGIN, the user will be logged in with the privilege level assigned by the RADIUS server. If the authentication mode is set to COMMAND, then the user is always logged in at USER privilege level and must run the ENABLE {MANAGER|SECURITYOFFICER} command to request increased privilege. For RADIUS, the privilege level is determined by examining the Service-Type attribute in the Access-Accept packet returned by the RADIUS server. A Service-Type of NAS-Prompt or Login is equivalent to USER level privilege. A Service-Type of Administrative equates to MANAGER or SECURITYOFFICER privilege.
360	SET SNMP COMMUNITY=name [ACCESS={READ|WRITE}] [OPEN={ON|OFF|YES|NO|TRUE|FALSE}]	The SET SNMP COMMUNITY command modifies the access mode and open access configuration for the specified SNMP community.

No.	Syntax	Description
361	SET SNTP UTCOFFSET={+|-}hh:mm	The SET SNTP UTCOFFSET command allows the user to specify the UTC offset for the device. The UTC offset indicates the number of hours and minutes difference between Universal Time/Greenwich Mean Time and local time for the device. Note: This change affects every command in the system that displays time. The UTC offset from Universal Time is specified as a value from -23:59 to +23:59. For example, the UTC offset for Eastern Standard Time for the US and Canada is -5:00.
362	SET STP INTERFACE={ type:id-range | id-range | ifname-list | ALL } {DEFAULT | [PATHCOST=path-cost] [PORTPRIORITY=port-priority] [EDGEPORT={ TRUE | FALSE }] [POINT2POINT={ TRUE | FALSE | AUTO }] }	The SET STP INTERFACE command allows a user to modify Spanning Tree Protocol settings for a specified interface or interfaces. Each interface associated with the spanning tree protocol has a port priority, with a default value of 128, used to determine which interface should be the root port for the STP if two interfaces are connected in a loop. A lower number indicates the higher priority. SET STP INTERFACE={type:id-range|id-range|ifname-list|ALL} PORTPRIORITY=port-priority NOTE: the range of the port-priority value for STP mode specified by ANSI/IEEE 802.1D, 1998 is 0-255, thus utilizing 8-bits. However, this only allows for a maximum number of 255 ports, since the 16-bit port ID is split between the priority component and the port number. As a result, two bits have been taken from the priority component to allow for additional interfaces. To provide for backward compatibility with older systems, the priority component is held in the upper 6-bit positions and is considered to be an 8-bit value that is shifted left 2 bit positions (i.e. multiplied by 4), with its two least significant bits assumed to be zero. Thus, providing a range of 0-252. NOTE: the range of port-priority value for RSTP mode specified by ANSI/IEEE 802.1D/D3, 2003 is 0-240 in steps of 16. The priority component is held in the upper 4-bit positions and is considered to be an 8 bit value that is shifted left by 4 bit positions (i.e. multiplied by 16), with its four least significant bits assumed to be zero.
363	SET SWITCH AGEINGTIMER=10..1000000	The SET SWITCH AGEINGTIMER sets the threshold value, in seconds, of the ageing timer, after which a dynamic entry in the Forwarding Database is automatically removed. (The maximum setting of 1000000 seconds is approximately 11 days 13 hours.). The default value is 300 seconds (5 minutes). To set the ageing timer to 180 seconds (3 minutes), use the command: SET SWITCH AGEINGTIMER=180. If the ageing timer ages out all dynamically learned filter entries, and switch learning is disabled, only statically entered MAC source addresses will be used to decide which packets to forward or discard. If the switch finds no matching entries in the Forwarding Database during the Forwarding Process, then all switch interfaces in the VLAN/HVLAN will be flooded with the packet, except the interface on which the packet was received.
364	SET SYSTEM [PROVMODE={MANUAL|AUTO}]	The SET SYSTEM command sets various administrative global attributes. These attributes affect the overall system. All attributes can be displayed using the SHOW SYSTEM command. The SET SYSTEM [PROVMODE={MANUAL|AUTO}] command changes the system provisioning mode from AUTO to MANUAL or vice-versa.
365	SET SYSTEM [TIME=hh:mm:ss] [DATE=yyyy-mm-dd]	The SET SYSTEM command sets various administrative global attributes. These attributes affect the overall system. All attributes can be displayed using the SHOW SYSTEM command. The SET SYSTEM [TIME=hh:mm:ss] [DATE=yyyy-mm-dd] command sets the local time or date on the Telesyn product.

No.	Syntax	Description
366	SET SYSTEM { CONTACT=contact | LOCATION=location | NAME=name | HOSTNAME=name | GATEWAY=ipaddress | DOMAINNAME=name | DNS=ipaddress-list }	The SET SYSTEM command sets various administrative global attributes. These Attributes affect the overall system. All attributes can be displayed using the SHOW SYSTEM command. Sets the attributes that identify the Telesyn product. Once a DNS server has been provisioned in the system, to delete it use the command SET SYSTEM DNS "". Note: The SET SYSTEM DNS, SET SYSTEM DOMAINNAME, and SET SYSTEM GATEWAY commands attempt to change the specified attributes on a system-wide basis for ALL disabled interfaces. The recommended method of setting the DNS, DOMAINNAME, and, GATEWAY attributes is to use the SET IP INTERFACE command.
367	SET SYSTEM LANGUAGE={EN}	The SET SYSTEM LANGUAGE command allows the user to specify the language settings for the device. The security officer user has the ability to change the system language preference at runtime. Once changed, the language setting affects all CLI sessions (is a system-wide setting), and also affects the management logs. English(EN) is the only language supported currently.
368	SET SYSTEM USERCONFIG { MANAGERPASSWORD={ password | NONE } | SECURITYOFFICERPASSWORD={ password | NONE } } [FORMAT={ CLEARTEXT | MD5 }]	The SET SYSTEM USERCONFIG command is used to modify global security parameters for user authentication. Changes to the minimum password length will affect only new users or future updates to existing user passwords.
369	SET TACPLUS AUTHMODE={ LOGIN | COMMAND }	The SET TACPLUS AUTHMODE command is used to change the authentication mode for use with RADIUS servers. When the TACACS+ authentication mode is set to LOGIN, the user will be logged in with the privilege level assigned by the TACACS+ server. If the authentication mode is set to COMMAND, then the user is always logged in at USER privilege level and must run the ENABLE {MANAGER|SECURITYOFFICER} command to request increased privilege. For TACACS+, the privilege level is determined by examining the priv_lvl field in the authentication reply packet. A priv_lvl less than 7 corresponds to USER, priv_lvl less than 15 and greater than corresponds to 7 corresponds to USER, <= 7 corresponds to MANAGER, and 15 corresponds to SECURITYOFFICER.
370	SET TACPLUS SERVER={ ipaddress-list | hostname-list | ALL } [KEY=key] [PORT=1..65535] [RETRIES=0..10] [TIMEOUT=1..60]	The SET TACPLUS SERVER command allows the user to change the settings of one or more existing configured TACACS+ servers. Users can change the servers' shared secret, port number, retries and timeout values.
371	SET VLAN={vlanname|vid} FORWARDINGMODE={STD|UPSTREAMONLY}	The SET VLAN command toggles the status of interfaces in a Virtual LAN (VLAN) between tagged and untagged. If a group of interfaces is included in the command and the setting of any one of them cannot be performed, the entire operation fails and no interfaces are modified in the VLAN.
372	SETDEFAULTS ALARMS THRESHOLD	This command sets all alarm threshold values back to the factory defaults.
373	SETDEFAULTS ALIAS	The SETDEFAULTS ALIAS is used to clear all existing alias commands and restore the default alias commands. Any aliases created by the user no longer exist and must be re-created, if needed. The default alias commands consist of "showdebug" which references a set of other alias commands, used to display all system information.

No.	*Syntax*	*Description*
374	SETDEFAULTS CLASSIFIER=classifiername [VID] [VPRIORITY] [INNERVID] [INNERVPRIORITY] [ETHFORMAT] [LSAP] [IPDEST] [IPSOURCE] [IPDSCP] [IPPROTOCOL] [IPTOS] [MACDEST] [MACSOURCE] [PROTOCOL] [TCPPORTDEST] [TCPPORTSOURCE] [TCPFLAGS] [UDPPORTDEST] [UDPPORTSOURCE]	The SETDEFAULTS CLASSIFIER command clears the specified user defined match rule (or rules) from the CLASSIFIER. The previous user defined match rule match rule may still exist on the CLASSIFIER as a derived rule if it is required by any of the remaining match rules. For example, if the match rules TCPPORTDEST=45 and IPPROTOCOL= TCP exist on a classifier then clearing IPPROTOCOL will result in that rule being removed as a user defined rule and added back as a derived rule. This command does not remove association of the CLASSIFIER to ACTION(s) or PORT(s). Use DELETE ACTION CLASSIFIER or DELETE CLASSIFIER PORT for those types of changes.
375	SETDEFAULTS EPSR={ epsrdomain-list | ALL } [HELLOTIME] [FAILOVERTIME] [RINGFLAPTIME]	The SETDEFAULTS EPSR command is used to reset the values of hello time, failover time, or ringflap time back to defaults. This operation is only allowed when the EPSR domain is disabled.
376	SETDEFAULTS INTERFACE={ type:id-range | id-range | ifname-list | ALL } ALARM [SEVERITY]	For the Interfaces specified, set the alarms (back) to the default level.
377	SETDEFAULTS LLDP [TXINTERVAL] [TXHOLD] [TXDELAY] [REINITDELAY] [NOTIFYINTERVAL]	Sets the defaults for the global LLDP values. This command would be used to change back to the default values that had been changed by the SET LLDP command.
378	SETDEFAULTS LLDP INTERFACE={ type:id-range | id-range | ifname-list | ALL } [MODE] [NOTIFY]	Controls the default settings for LLDP for the specified interface(s).
379	SETDEFAULTS LOGINBANNER [{ USER | MANAGER | SECURITYOFFICER | ALL }]	The SETDEFAULTS LOGINBANNER is used to restore the login banner back to its default settings for the requested user privilege level. If ALL parameter is provided, all user levels are reset to the default loginbanner. The default loginbanner for each of the user privilege levels is an empty string.
380	SETDEFAULTS MGCP INTERFACE={ type:id-range | id-range | ifname-list | ALL } [CALLAGENT] [CALLAGENTPROFILE] [DISCONNECTTHRESHOLD] [SUSPICIONTHRESHOLD] [INITIALRETRANSMITDELAY] [MAXRETRANSMITDELAY] [IPDSCP] [UDPPORT] [VPRIORITY]	The SETDEFAULTS MGCP command sets MGCP parameters to their default value.
381	SETDEFAULTS PROMPT	The SETDEFAULTS PROMPT command is used to restore the CLI command prompt back to its default settings. When this command is run, the prompt reverts back to the prompt string of "%u %s" which displays the user name and security level of the user of the current session.
382	SETDEFAULTS RTP INTERFACE={ type:id-range | id-range | ifname-list | ALL } [IPDSCP] [VPRIORITY]	The SETDEFAULTS RTP command sets RTP parameters to their default value.
383	SETDEFAULTS TRACE [FORCE]	The SETDEFAULTS TRACE command returns the Trace Log system back to its default configuration. Tracing is disabled, the Trace buffer is set to is initial size, and all logs are cleared.
384	SHOW LOG [CATEGORY=category] [DATE=[op] yyyy-mm-dd [-yyyy-mm-dd]] [FORMAT={ FULL | MSGONLY | SUMMARY }] [REVERSE] [SEQUENCE=0..9999 [-0..9999]] [SEVERITY=[op] { CRITICAL | MAJOR | MINOR | NONE }] [TAIL [=count]] [TIME=[op] hh:mm:ss [-hh:mm:ss]]	The SHOW LOG command is used to display all the stored management logs. Optional parameters are available to display only the management logs matching certain criteria. With no optional parameters specified, all management logs are displayed in order from newest to oldest.
385	SHOW { CONFIG STATUS }	Displays the current status of a current BACKUP CONFIG or RESTORE CONFIG. If there is no configuration in progress, displays the most recent configuration status.

No.	Syntax	Description
386	SHOW { CONFIG }	The current configuration information is generated and displayed to the user. The status information is not saved over reboots of the system.
387	SHOW ALARMS [{ CARD={ slot-list | ALL } | INTERFACE={ type:id-range | id-range | ifname-list | ALL } | SEVERITY={ CRITICAL | MAJOR | MINOR | INFO | ALL } | ALL }] [FULL]	The SHOW ALARMS command displays alarm conditions on system components. The display is filtered according to the given parameters and shown in a tabular output, with one alarm per row. There are 3 columns of output for each alarm consisting of: - the component the alarm is against - a description of the fault or condition - the severity of the alarm
388	SHOW ALARMS [PORT [={ port-list | ALL }]] [FULL]	Shows alarms for a specified set of ports or all ports
389	SHOW ALARMS THRESHOLD	Displays alarm threshold settings for MINOR, MAJOR, CRITICAL port outage alarms.
390	SHOW ALIAS [={ aliasname-list | ALL }]	The SHOW ALIAS command allows the user to view the list of alias commands defined in the system, as requested by the user. If the ALIAS parameter is set to ALL, or no value is provided, then all alias commands are listed. The alias name and its corresponding substitution string is provided.
391	SHOW CARD [={ slot-list | ACTCFC | INACTCFC | ALL }] [{ CPUSTATS [TASKS] | INVENTORY | MEMORY { HEAP | MESSAGEBUFFERS | QUICKHEAP } | PORTS | SOFTWARE }]	The SHOW CARD command displays various information about the provisioned card in the specified slot. Entering the command with no optional parameters displays basic information about the card including: - static provisioning attributes - relationship with provisioning profile (if applicable) - dynamic state attributes - alarms and defect conditions - diagnostic scheduling information (CFC card only) Optional parameters are provided to display additional information including: - current software load information (CFC, ADSL and FE only) - status of ports (ADSL, GE and FE only) - CPU usage statistics (CFC only) - memory usage statistics (CFC only) Card types supported include: CFC6 - 6 Gb CFC (Central Fabric Controller) ADSL16 - 16-port ADSL Service Module ADSL8S - 8-port ADSL Service Module w/ integrated splitters GE1 - 1-port Gb Ethernet (WAN) Compact Module GE3 - 3-port Gb Ethernet (WAN) Compact Module FE10 - 10-port Fast Ethernet Service Module FC7 - Fan Controller (7400 shelf only) The SHOW CARD ALL command displays a summary of cards present in the shelf. Entering SHOW CARD ALL command without the optional INVENTORY parameter displays the following information for each slot in tabular format: - slot number - provisioned card type - current state of the card, in the format of hyphen separated administrative state, operational state, and status attribute (for example, UP-UP-ONLINE) - current faults against the card Entering the SHOW CARD ALL command with the optional INVENTORY parameter displays the following information for each slot in tabular format: - slot number - provisioned card type - model number (read from the IDPROM on the card) - serial number (read from the IDPROM on the card)
392	SHOW CARD={ slot-list | ALL } PORTS	Shows the related port information for the card(s). This will be depreacted after 6.0.
393	SHOW CLASSIFIER COUNTER [{ INTERFACE={ type:id-range | id-range | ifname-list | ALL } }]	See SHOW CLASSIFIER COUNTER PORT={port-list|ALL}
394	SHOW CLASSIFIER={ classifiername-list | ALL } [{ INTERFACE={ type:id-range | id-range | ifname-list | ALL } }] [{ SUMMARY | FULL }]	See SHOW CLASSIFIER={classifiername-list|ALL} [{PORT={port-list|ALL}}] [{SUMMARY|FULL}]
395	SHOW CONNECTIONS [INTERFACE={ type:id-range | ifname-list | ALL }] [FULL]	Show which interfaces are connected
396	SHOW CONTACTALARM [={ 0..2 | ALL }] [STATE={ OPEN | CLOSED | ALL }] [SEVERITY={ CRITICAL | MAJOR | MINOR | INFO | ALL }]	The SHOW CONTACTALARM command displays provisioning information for the specified alarm trigger(s). Parameters are provided to specify information for all triggers, all triggers of a given severity, or individual triggers specified by contact number and state.

No.	Syntax	Description
397	SHOW DATABASE	This command shows the system configuration database utilization information to the user.
398	SHOW DHCPRELAY [={ dhcpname-list | MAIN | ALL }] [INTERFACE={ type:id-range | id-range | ifname-list | ALL }] [FULL]	This command displays information about the DHCP Relay Agent for one or interfaces. If more than one interface is specified (or if no interface is specified) the following information will be displayed, including the list of DHCP Servers, cumulative DHCP Relay Statistics, and list of interfaces that are configured to run DHCP Relay.
399	SHOW DHCPRELAY COUNTER [INTERFACE={ type:id-range | id-range | ifname-list | ALL }] [FULL]	Displays information about the DHCP Relay Agent for one or more interfaces. If more than one interface is specified (or if no interface is specified) the following information will be displayed, which includes the list of DHCP Servers, cumulative DHCP Relay Statistics, and list of interfaces that are configured to run DHCP Relay
400	SHOW DIAGNOSTICS [{ INTERFACE={ type:id-range | id-range | ifname-list | ALL } | CARD={ slot-list | ALL } | ALL }]	The SHOW DIAGNOSTICS command displays the diagnostic results for a card.
401	SHOW EGRESSLIMITER [={ limitername-list | ALL }] [INTERFACE={ type:id-range | id-range | ifname-list | ALL }]	The SHOW EGRESSLIMITER command shows information about EGRESSLIMITERs in the system, and optionally their association to interfaces. See CREATE EGRESSLIMITER for discussion of the use of EGRESSLMITERs.
402	SHOW EPSR [={ epsrdomain-list | ALL }] [FULL]	The SHOW EPSR command is used to display the information about the EPSR domains. SHOW EPSR and SHOW EPSR ALL command displays the summary information about all the provisioned EPSR domains in the system. SHOW EPSR epsrdomain command displays the detailed information about that specific EPSR domain.
403	SHOW IGMPSNOOPING [{ STATUS | MCASTGROUPS [FULL] | COUNTER [{ STANDARD | MESSAGERESPONSE | INTERFACE={ type:id-range | id-range | ifname-list | ALL } | CARD={ slot-list | ALL } }] | INTERFACE={ type:id-range | id-range | ifname-list | ALL } [FULL] | CARD={ slot-list | ALL } [FULL] }]	The SHOW IGMPSNOOPING command is used to display the current status of the IGMP snooping feature, the currently configured value of the IP multicast stream count value, or the set-top box(STB) MAC address(es) that have been configured for a particular port in the switch or for all of the ports in the switch.
404	SHOW INTERFACE [={ type: | type:id-range | id-range | ifname-list | ALL }] [CARD=slot-list] [STATE={ UP | DOWN | ALL }] [DIRECTION={ NETWORK | CUSTOMER | INTERNAL }] [FULL]	The SHOW INTERFACE command displays information about interfaces in the system. Information provided includes interface type, interface ID, interface name, physical ports associated with the interface, interface mode (UP or DOWN) and the last change time (based on the system uptime).
405	SHOW INTERFACE [={ type:id-range | id-range | ifname-list | ALL }] ALARM SEVERITY [={ NONE | INFO | MINOR | MAJOR | CRITICAL | DEFAULT | NONDEFAULT | ALL }]	Lists the interfaces and the alarm severities that are assocaited with them. If the severity is the default level, '(Default)' is shown next to the interface.
406	SHOW INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } COUNTER [{ STATUS | FULL }]	The SHOW INTERFACE COUNTER command displays current statistical Performance Monitoring (PMON) or Remote Monitoring (RMON) counts for selected interfaces as well as status information about the interfaces.
407	SHOW INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } FAULTCOUNT	Displays FAULTCOUNT information about interfaces in the system. Information provided includes interface type, interface ID, interface name, physical ports associated with the interface, interface mode (UP or DOWN) and the last change time (based on the system uptime).
408	SHOW INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL } QUEUECOUNT [STATUS]	Displays QUEUECOUNT information about interfaces in the system. Information provided includes interface type, interface ID, interface name, physical ports associated with the interface, interface mode (UP or DOWN) and the last change time (based on the system uptime).

<table>
<tr><th>No.</th><th>Syntax</th><th>Description</th></tr>
<tr><td>409</td><td>SHOW INTERFACE={ type:id-range | id-range | ifname-list | ALL } COUNTER HISTORY [STATUS] [INTERVAL={ interval-list | ALL }] [BUCKET={ bucket-list | ALL }] [FULL]</td><td>The SHOW INTERFACE COUNTER HISTORY command allows the user to view data collection entries for Remote Monitoring (RMON) as well as bucket data collected for both RMON and Performance Monitoring (PMON).</td></tr>
<tr><td>410</td><td>SHOW IP [INTERFACE [={ MGMT | type:id-range | ifname-list | ALL }] [FULL]]</td><td>The SHOW IP INTERFACE command displays the IP configuration information for the named interface. The information displayed includes the interface name, the IP address and the subnet mask, and status. The following is an example of the output displayed: -- Interface........................... MGMT Status.............................. Enabled IP Address.......................... 172.16.8.10 Subnet Mask......................... 255.255.255.0 --</td></tr>
<tr><td>411</td><td>SHOW IP ARP [={ ipaddress-list | ALL }] [INTERFACE={ MGMT | type:id-range | ifname-list | ALL }] [FULL]</td><td>This command allows users to display system's ARP table entries for user specified IP addresses or all entries in the ARP table if IP addresses are not specified by the user. The output displays three fields per entry, namely the IP address, MAC address and the reference count that indicates the number of times that ARP entry was accessed.</td></tr>
<tr><td>412</td><td>SHOW IP CONNECTIONS [={ TCP | UDP }]</td><td>The SHOW IP command without an option displays both TCP and UDP information available. With one option supplied, this command displays the appropriate information. Example SHOW IP TCP will display the connections on the system. This includes local port, local IP address, destination port and destination IP address. The SHOW IP COUNTER displays one of the three TCP,UDP,ICMP protocol related counters based on the option specified by the user. Example SHOW IP COUNTER TCP will display TCP protocol-related counters available in the system.</td></tr>
<tr><td>413</td><td>SHOW LLDP [INTERFACE [={ type:id-range | id-range | ifname-list | ALL }] [FULL]]</td><td>Shows the attributes of how LLDP has been set on the system.</td></tr>
<tr><td>414</td><td>SHOW LLDP COUNTER [INTERFACE={ type:id-range | id-range | ifname-list | ALL }] [FULL]</td><td>Allows the user to view the runtime data (local system LLDP counters) for each interface specified. Packets counted include frames as well as Type-Lenght-Value (TLV) information elements, which are variable in length.</td></tr>
<tr><td>415</td><td>SHOW LOGINBANNER</td><td>The SHOW LOGINBANNER command allows the user to view the login banner settings for each user. This command shows the text that will be displayed to the user upon login.</td></tr>
<tr><td>416</td><td>SHOW MEDIA [={ unit-list | ALL }] [FULL]</td><td>This command is used to display the properties of the media card(s) specified. The attributes displayed for individually specified media cards are: - Parent Card Slot Number - Media Card Type - Media Card State - Media Card Status - Model - Serial Number - Firmware Version - Number of sectors - Number of bytes per sector</td></tr>
<tr><td>417</td><td>SHOW MGCP COUNTER [INTERFACE={ type:id-range | id-range | ifname-list | ALL }] [FULL]</td><td>The SHOW MGCP COUNTER command allows the user to view Media Gateway Control Protocol (MGCP) statistics on a per-interface basis. Both summary and detailed statistical views are available.</td></tr>
<tr><td>418</td><td>SHOW MLPPP [={ mlpppname-list | ALL }] [INTERFACE={ type:id-range | id-range | ifname-list | ALL }] [FULL]</td><td>Shows attributes of the MLPPP(s), including its state and its associated PPP(s). The FULL option displays more details.</td></tr>
<tr><td>419</td><td>SHOW ONU [={ onuname-list | ALL }] [ONUID={ 0..15 | ALL }] [INTERFACE={ type: | type:id-range | id-range | ifname-list | ALL }] [MACADDRESS={ macaddress | ALL }] [FULL]</td><td>Requests to display ONU interface(s). Shows details of the ONU interface. You can ID by interface name/id or by MAC address. INTERFACE should be able to SHOW based on the ONU or EPON interface.</td></tr>
<tr><td>420</td><td>SHOW PPP [INTERFACE={ type:id-range | id-range | ifname-list | ALL }] [FULL]</td><td>List the PPP attributes for the selected interface(s)</td></tr>
</table>

No.	Syntax	Description
421	SHOW PROFILE [={ name-list | NAMES | ALL }] [{ cardtype | porttype }] [FULL]	Shows the profiles for the system. These can be for a profile name, all NAMES, or ALL. It can also be specified for a card type or a card port. For release 7.0, cardtypes are ADSL16B, ADSL16, ADSL24, ADSL8S, ADSL24A, ADSL24B, ADSL24C, CES8, CFC24, CFC4, CFC6, FE10, FE2, FX10, GE1, GE2, GE3, POTS24, SHDSL16, SHDSL24, and NTE8. Port types are ADSLPORT, DS1PORT, E1PORT, FEPORT, FXPORT, GEPORT, POTSPORT, and SHDSLPORT. For release 8.0, new cardtypes are GE8, CFC56, EPON2, VDSL24A, VDSL24B, and XE1. New port types are EPONPORT, VDSLPORT, and XEPORT.
422	SHOW PROFILE [={ name-list | NAMES | ALL }] [{ CES8 | DS1PORT | E1PORT }] [FULL]	Show the profile attributes for the CES8 card or T1 port type
423	SHOW PROFILE [={ name-list | NAMES | ALL }] [FULL]	Shows attributes of Profiles
424	SHOW PROFILE [={ name-list | NAMES | ALL }] { NTE8 | DS1PORT | E1PORT } [FULL]	Show the profile attributes for the NTE8 card or T1 port type
425	SHOW PROFILE [={ name-list | NAMES | ALL }] { XE1 | XEPORT } [FULL]	Shows attributes of Profiles related to XE1 card or XE1 port
426	SHOW PROTECTIONGROUP [={ groupname-list | ALL }]	Show a protection group and which interfaces are associated with it.
427	SHOW PSPAN [={ pspanname-list | ALL }] [{ INTERFACE={ type:id-range | ifname-list } | CARD=slot-list }] [{ JITTERBUFFER | FULL }]	For the INTERFACE parameter here (and in the ENABLE, DISABLE, and DESTROY commands), the user may type "vlan:xxx" to indicate the underlying virtual eth interface, or "pspan:xxx" to indicate a particular PSPAN interface. The command will operate on the intersection of the PSPAN list and the INTERFACE list (one or the other will usually be "ALL").
428	SHOW QOSPOLICY [={ policyname-list | ALL }] [INTERFACE={ type:id-range | id-range | ifname-list | ALL }] [{ BRUUM | IPMC | BIDIRECTIONAL [VLAN={ vlanname-list | vid-range | ALL }] | ALL }] [FULL]	Requests to display QOSPOLICY info. - INTERFACE should accept EPON, ONU or ETH - The command shows QOSPOLICYs and their usage in VLAN / interface associations. - ETHs that do not support QOSPOLICYs will not be displayed, or will indicate "N/A".
429	SHOW RTP COUNTER [INTERFACE={ type:id-range | id-range | ifname-list | ALL }] [FULL]	The SHOW RTP COUNTER command allows the user to view Real Time Protocol (RTP) statistics on a per-interface basis. Both summary and detailed statistical views are available.
430	SHOW RTP INTERFACE={ type:id-range | id-range | ifname-list | ALL } [FULL]	The SHOW RTP INTERFACE command displays the RTP parameters and their values.
431	SHOW STP [{ [INSTANCE={ stpname | mstid | MAIN | ALL }] [INTERFACE={ type:id-range | id-range | ifname-list | ALL }] [FULL] | COUNTER }]	The SHOW STP command displays the system wide STP information for the bridge.
432	SHOW SWITCH INTERNALMAC [{ INTERFACE={ type:id-range | id-range | ifname-list | ALL } | CARD={ slot-list | ALL } }] [ADDRESS=macaddress]	
433	SHOW TECHSUPPORT FILE=filename [FORCE]	Customers can use this command while working with Allied Telesyn Technical Support. When this command is run using the (encrypted) file supplied by Allied Telesyn, the output (sent to the terminal) is placed in a file and sent to Allied Telesyn Support for further study.
434	SHOW TELNET [{ SERVER | SESSIONS }]	Displays the Telnet Client configuration information, indicating the settings for InsertNull and Terminal Type. The SHOW TELNET SERVER command displays the state of the telnet server, indicating if it is ENABLED or DISABLED. The SHOW TELNET SESSIONS command displays the current telnet client sessions, indicating if there are any connections to remote systems, the CLI Session Id that requested the connection, the source and destination IP addresses of the telnet connection, and the time at which the connection was made.

No.	Syntax	Description
435	SHOW TRACE [{ STATUS | BUFFER [DATE=[op] yyyy-mm-dd [-yyyy-mm-dd]] [FORMAT={ FULL | SUMMARY }] [REVERSE] [SEQUENCE=seqnum [-seqnum]] [TAIL [=count]] [TIME=[op] hh:mm:ss [-hh:mm:ss]] }]	The SHOW TRACE command is used to view Trace logs stored in the Trace buffer or to show the status of the Trace system. SHOW TRACE BUFFER is used to view the Trace logs in the buffer. Options control which logs should be displayed and in what order. Multiple options can be used together to further control how the logs are displayed. For example: SHOW TRACE BUFFER DATE=2004-06-04 TIME=>04:15:00 would show logs from June 4, 2004 on or after 4:15a. SHOW TRACE STATUS is used to view the Trace system settings. This includes the state of the Trace system (enabled/disabled) and what Trace options are set for each of the Trace applications.
436	SHOW TRACE EPSR [={ epsrdomain-list | ALL }] [MESSAGETYPE={ HEALTH | RINGUPFLUSH | RINGDOWNFLUSH | LINKDOWN | ALL }] [INTERFACE={ type:id-range | id-range | ifname-list | ALL }]	Display the status of the trace criteria instances that have been defined for EPSR. Note that this command does not display the actual logs in the trace buffer.
437	SHOW TRACE IGMPSNOOPING [MESSAGETYPE={ REPORTV1 | REPORTV2 | LEAVE | GENERALQUERY | LASTMEMBERQUERY | ALL }] [INTERFACE={ type:id-range | id-range | ifname-list | ALL }] [MACADDRESS={ macaddress | ALL }] [GROUPADDRESS={ ipaddress | ALL }]	This shows the status of what's been enabled for tracing, not the actual trace buffer (which is displayed using SHOW TRACE BUFFER).
438	SHOW TRACE PPP [EVENT={ PORT | LCP | BCP | ECHO | FRAME | TIMER | ERRPROTO | MAIN | ALL }] [INTERFACE={ type:id-range | id-range | ifname-list | ALL }]	Shows collected entries in the Event log for specified LCP event(s) on the specified interface(s).
439	SHOW TRACE VOICECALL [EVENT={ OPENLOOP | CLOSELOOP | MGCPOFFHOOK | MGCPONHOOK | MODEMDETECT | ALL }] [INTERFACE={ type:id-range | id-range | ifname-list | ALL }]	Display the status of the trace criteria instances that have been defined. Note that this command does not display the actual logs in the trace buffer. See SHOW TRACE.
440	SHOW TRANSFER [={ transferid-list | ALL }]	The SHOW TRANSFER command displays current file transfer operations, including those in progress and those that are pending. The information is displayed in a columnar format. For files that are being transferred to or from a network server (as result of a PUT FILE or GET FILE command, the following is displayed: - an ID, which is simply a number associated with a particular file transfer to serve as an identifying tag - the CMD, which is the command that was used to initiate the file transfer. The command is either PUT or GET. - Remote file, which is the name of the file being transferred to or from the network server - Local file, which is the name of the file on the CFC flash file system being transferred to or from the network server - the Server, which is the IP address of the network server - the Mode, which is the protocol being used for the file transfer. Currently, only TFTP is supported. - the Status, which describes the current state of the file transfer operation. The status is either Progress, which means that the transfer is in progress, or Pending, which means that the transfer is delayed and will begin when other transfers are completed. - the MB, which is the number of megabytes that have been transferred, if the associated transfer status is in progress For files that are being transferred from the CFC flash file system to another card in the shelf (as result of a PUT FILE operation), the following is displayed: - the Card, which is the card the file is being transferred to - the CMD, which is the command that was used to initiate the file transfer. Currently, on the PUT command is supported.
441	SHOW VC [={ vcid-range | ALL }] [INTERFACE={ type:id-range | id-range | ifname-list | ALL }]	This command displays information about VCs in the system. Without presence of any optional parameters, this command displays all the VCs present on all the ATM interfaces present in the system

No.	*Syntax*	*Description*
442	SHOW ACCESSLIST={ accesslistname-list | ALL } [INTERFACE={ type:id-range |id-range | ifname-list | ALL }]	The SHOW ACCESSLIST command displays data related to the configuration of ACCESSLISTs and (optionally) associations by INTERFACEs There are two minor variations of this command: one that shows ACCESSLIST data for each ACCESSLIST, and one that shows ACCESSLISTs in the context of their associations to INTERFACEs. In both cases the command displays the ACCESSLIST name, rules, and the action (PERMIT or DENY). The second case (by INTERFACE) shows only ACCESSLISTs associated with the specified INTERFACE(s). It also identifies any RULEs that were not able to be applied to the INTERFACE's hardware, resulting in classifier configuration alarms. ACCESSLIST RULEs are implemented using CLASSIFIERS. The CLASSIFIERS used to implement a specific rule can be seen using the FULL option on the SHOW CLASSIFIERS commands.
443	SHOW ARPFILTER [INTERFACE={type:id-range|id-range|ifname-list|ALL}]	The SHOW ARPFILTER command displays ARP filtering configuration data for the specified interface or interfaces. If the INTERFACE option is omitted then data for ALL interfaces will be displayed.
444	SHOW BOOTSERVER	The SHOW BOOTSERVER command displays the static IP address of the network boot server, and the preferred software load file which is downloaded from the server when all boot attempts for the CFC fail from the CFC flash file system. The preferred software load is set using the command SET CARD=ACTCFC PREFLOAD=filename. In the event the CFC cannot use the preferred load from its own flash filesystem, the preferred load file is transferred from the boot server and written to the flash, replacing any existing preferred load file for the CFC.
445	SHOW CLASSIFIER COUNTER [{PORT={port-list|ALL}}]	Each port has three classification counters: - "Filter Count" - counts packets dropped because of classifiers with both the DROP and COUNT actions. - "Match Count" - counts packets that match a classifier with the COUNT action but no DROP action. - "Policed Count" - counts packets dropped because they exceed a TRAFFICDESCRIPTOR when the NCCOUNT action is ON. See ADD ACTION CLASSIFIER. Note that on the 9x00 series platform both the "Match Count" and the "Filter Count" can be incremented by a single packet that matches both the FORWARD and DROP classifier. On other platforms only count with the higher precedence is incremented.
446	SHOW CLASSIFIER={classifiername-list|ALL} [{PORT={port-list|ALL}}] [{SUMMARY|FULL}]	There are two minor variations of this command: one that shows only CLASSIFIER data (independent of associations to PORT or INTERFACEs), and one that shows CLASSIFIERs in the context of their associations to PORTs or INTERFACEs. In both cases the command displays the CLASSIFIER name, match rules, and actions. The second case shows only CLASSIFIERs associated with the specified PORT(s) or INTERFACE(s). It shows the relative precedence of each CLASSSIFIER on that PORT or INTERFACE. It also identifies any classifiers that were not able to be applied to the PORT's hardware, resulting in classifier configuration alarms. The SUMMARY option shows only CLASSIFIERs that can be managed by the user. The SUMMARY display option is the default. The FULL option shows two additional types of information not shown by the SUMMARY option: - "internal" classifiers, which are added by the system to enable other features (e.g. IGMP snooping), and - "derived" match rules, which match fields implied but not explicitly specified by higher protocol match rules (e.g. rules added to match only IPv4 packets if IPDSCP match rule is specified).

No.	*Syntax*	*Description*
447	SHOW FANMODULE	The SHOW FANMODULE command displays various information about the system fan module, including: - dynamic state attributes - alarms and defect conditions - current fan speeds The following illustrates an example output from the command in a 7400 shelf that has a fan module containing 6 fans: -- No Faults Fan Module.......................... FM7 Administrative State................ UP Operational State................... UP Status.............................. ONLINE Fan #1 Speed........................ 5400 Fan #2 Speed........................ 5640 Fan #3 Speed........................ 5640 Fan #4 Speed........................ 5640 Fan #5 Speed........................ 5520 Fan #6 Speed........................ 5520 -- The following illustrates an example output from the command in a 7700 shelf that has a fan module containing 5 blowers and 2 fans: -- No Faults Fan Module.......................... FAN8 Administrative State................ UP Operational State................... UP Status.............................. ONLINE Blower #1 Speed........................ 4680 Blower #2 Speed........................ 4680 Blower #3 Speed........................ 4680 Blower #4 Speed........................ 4680 Blower #5 Speed........................ 4560 Fan #6 Speed........................ 6720 Fan #7 Speed........................ 6480 --
448	SHOW FEATURE [={ userlabel-list | ALL }]	Future
449	SHOW FEATURE [={ userlabel-list | ALL }] [KEYS]	Future
450	SHOW FILES [FULL]	The SHOW FILES command displays all user manageable files that exist on the CFC flash file system or. The CFC flash file system has 48 megabytes of space allocated for user manageable files. Examples of manageable files include software load files and script files. There are other types of files that are not directly manageable by the user that exist on the CFC flash file system, but are hidden and not displayed by this command. Database and log files are examples of files that are not directly user manageable. The information is displayed in a columnar format, and for each file the following is shown: - the name of the file - the size of the file in kilobytes Additional general information is shown about the CFC flash file system, including: - the total amount of space (in kilobytes) allocated for user manageable files - the total amount of space (in kilobytes) currently in use for user manageable files - the total amount of free space (in kilobytes) available for additional user manageable files When the FULL option is specified, extra information about each file is shown: - the version of the file if it is a software load file; for other types of files this field is left blank - the hardware model number supported by this file if it is a software load file; for other types of files this field is left blank - the date and time that the file was last modified
451	SHOW FILES MEDIA=unit [FULL]	The SHOW FILES command displays files that exist on the specified media card. The information is displayed in a columnar format, and for each file the following is shown: - the name of the file - the size of the file in kilobytes Additional general information is shown about the file system on the specified media card, including: - the total amount of space (in kilobytes) allocated for user manageable files - the total amount of space (in kilobytes) currently in use for user manageable files - the total amount of free space (in kilobytes) available for additional user manageable files When the FULL option is specified, extra information about each file is shown: - the version of the file if it is a software load file; for other types of files this field is left blank - the hardware model number supported by this file if it is a software load file; for other types of files this field is left blank - the date and time that the file was last modified

No.	Syntax	Description
452	SHOW FLASH [INACTCFC]	The SHOW FLASH command displays information about the flash memory on the CFC card. Flash memory is used for storage of user manageable files and other data not manageable by the user. The information displayed by the SHOW FLASH command includes: - the total size of flash memory, in kilobytes - the total size of free flash memory, in kilobytes - the total size of contiguous free flash memory, in kilobytes This command should not be confused with the SHOW FILES command which shows files and memory usage associated only with user manageable file space on the flash memory.
453	SHOW HVLAN[={hvlanname|vid|ALL}] [FULL]	The SHOW HVLAN command displays information about the specified Hierarchical VLAN (HVLAN) If no HVLAN name or identifier is specified, then ALL is assumed. If ALL is used, a summary of all HVLANs is presented.
454	SHOW IP COUNTER={TCP|UDP|ICMP}	The SHOW IP COUNTER displays one of the three TCP,UDP,ICMP protocol related counters based on the option specified by the user. Example SHOW IP COUNTER TCP will display TCP protocol-related counters available in the system.
455	SHOW IP ROUTE[={ipaddress-list|ALL}]	This command displays the routing table for the specified list of comma-separated ipaddresses. If none or all is specified, this command will display the routing table for all ipAddresses on the system.
456	SHOW LAG={ lagname-list | ALL } [{ INFO | STATE | LACPSTATS | MACSTATS }]	The SHOW LAG command displays information pertaining to Link Aggregation Groups (LAGs) configured on the system. Individual LAGs or a list of LAGs can be displayed by specifying the valid LAG IDs. If a valid LAG ID is not known, or if information for all LAGs is desired, use the ALL keyword to display all configured LAGs. The type of LAG information displayed can be selected by using one of the following keywords: INFO - Displays general LAG information such as interface list, speed, select criteria, and admin key. STATE - Displays LACP administrative and operational state information for ports in LAG. LACPSTATS - Displays LACP statistics for the LAG, such as LACP packets transmitted, received, and errored. MACSTATS - Displays MAC statistics for the LAG, such as MAC uni/multi/broad-cast packets received/transmitted, and octets received/transmitted counts. If no keyword is specified, INFO is displayed by default. Also note that the STATE and LACPSTATS keywords are applicable only if LAG mode is set to ACTIVE or PASSIVE (indicating that LACP is configured to run on the system).
457	SHOW LOG FILTER	The SHOW LOG FILTER command displays all the existing management log filters in the system. The log filter name, the log categories filtered, if any, and the severity values filtered are displayed by this command. The following is example output from the command: --- Management Log Filters ------------------------------------ Filter ID Categories Severities -------------------- -------------------- -------------------- FILTER1 n/a Critical Major Minor None FILTER2 ADSL CARD Critical Major Minor None --

No.	*Syntax*	*Description*
458	SHOW LOG OUTPUT	The SHOW LOG OUTPUT command displays all the existing management log output destinations currently defined in the system. The information displayed contains the management log output name, the destination type, the log format type, the associated management log filters, and the status (enabled or disabled). Additional destination-specific information is also displayed. For CLI log output destinations, the user name, IP address and session number information is displayed. For Syslog log output destinations, the Syslog server IP address is shown. The following example shows the output for a configuration containing a CLI and SYSLOG destinations: --- Management Log Output Destinations -------------------------- Output ID........................... DAVIDMG Destination......................... CLI Session Message Type........................ CLI - NORMAL Filters............................. FILTER1 FILTER2 Status.............................. Enabled User name........................... officer Remote IP address................... 90.0.0.254 Session ID.......................... 1 Output ID........................... SYSLOG Destination......................... Syslog Message Type........................ SYSLOG - NORMAL Filters............................. FILTER1 Status.............................. Disabled Syslog server IP address............ 192.168.0.20 ---
459	SHOW PORT={port-list|ALL}	The SHOW PORT command displays various information about the specified port, including: - static provisioning attributes - relationship with provisioning profile (if applicable) - dynamic state attributes - alarms and defect conditions
460	SHOW PROFILE NAMES [{cardtype|porttype}]	Shows the profiles associated with the card type or port type
461	SHOW PROFILE=name { CES8 | DS1PORT | E1PORT }	Shows the Profile used for the CES8 card or port (by type).
462	SHOW QOS	The SHOW QOS command displays the mapping of VLAN priority bits to egress queues. To set the VLAN priority to egress queue mappings use the command(s): SET QOS [VLAN4QUEUEMAP=value-map] [VLAN8QUEUEMAP=value-map] For a description of the use of this mapping, see the description from "HELP SET QOS".
463	SHOW RADIUS	The SHOW RADIUS command displays a table containing information regarding the RADIUS server configuration. The information includes each RADIUS server's hostname or IP address, status (enabled or disabled), port, retries, and timeout values. The shared secret is not displayed for security reasons.
464	SHOW SCRIPT=filename	The SHOW SCRIPT command displays the contents of a Command Line Interface(CLI) script. A script contains CLI command that are executed through the EXECUTE SCRIPT command.
465	SHOW SESSIONS	The SHOW SESSIONS command will display a list of all active (logged in) users, including the login-name, the port or device that the user is logged into, the IP address that the user is logged in from and the login time for the user session. There is also a column that identifies if the user has been scheduled for deactivation and the number of seconds before the session is logged off. This column has a value only if the DEACTIVATE SESSION command was invoked.
466	SHOW SNMP	The SHOW SNMP command displays information about the device's SNMP agent. SNMP configuration and SNMP counters are displayed.

No.	*Syntax*	*Description*
467	SHOW SNMP COMMUNITY [={ name-list | ALL }]	The SHOW SNMP COMMUNITY command displays information about a single SNMP community. The COMMUNITY parameter specifies the name of the community. A community with the specified name must already exist in the device. The following is example output from the SHOW SNMP COMMUNITY command: SNMP community information: Name .... public Access .... read-only Status .... Enabled Traps .... Enabled Open access .... Yes Manager .... 192.168.1.1 Manager .... 192.168.5.3 Trap host .... 192.168.1.1 Trap host .... 192.168.6.23 v2c Traphost 192.168.6.24
468	SHOW SNTP	The SHOW SNTP command shows the following SNTP statistics and information: State: Enabled State of the SNTP client Local IP: The Local IP Address Last Update: The time of the last update (before change) Last Delta: The amount of the change in seconds Last Status: The return message from the last attempt to update SNTP Server: The SNTP Server address SNTP Statistics: Packets In/Out The following is example output for the command: SNTP Configuration --- Status On Local IP 172.16.8.10 UTC Offset -05:00:00 Last Update 2003-03-26 23:08:34 Last Delta +1.03s Last Status Success SNTP Server -- 192.168.0.20 SNTP Statistics --- Requests Sent 101 Responses Received 101
469	SHOW STP COUNTER	The SHOW STP COUNTER command displays all the counters that identify how many Bridge Protocol Data Units (BPDUs) have been transmitted or received by this bridge. BPDUs are Spanning Tree Protocol specific control packets. The counters available include the number of any type BPDU transmitted or received, the number of Configuration BPDUs that are transmitted or received, the number of Topology Change Notification (TCN) BPDUs that are transmitted or received, the total number of received BPDUs that were invalid, the number of BPDUs that were invalid because they were received on an interface with a STP state of disabled, the number of BPDUs that were invalid because they had an invalid protocol identifier field, the number of BPDUs that were invalid because they had an invalid type field, the number of BPDUs that were invalid because the message age field was invalid, the number of Configuration BPDUs that were invalid because the length was not correct, the number of TCN BPDUs that were invalid because the length was not correct, the number of forward transitions made by ports, and the number of Topology Changes that have occurred.
470	SHOW STP INTERFACE={ type:id-range | id-range | ifname-list | ALL }	The SHOW STP INTERFACE command displays the STP state and provisioning information for the specified interface(s). The information displayed includes the STP state of the interface, the port identifier used by the STP algorithm, the provisionable port priority and port path cost; the priority, address, and path cost of the bridge that is viewed as root by the specified port; the priority and address of the bridge that is viewed as the designated bridge for the LAN to which the specified interface is attached, the port ID of the designated port for the LAN to which the specified interface is attached; an indicator of whether or not a Topology Change is currently being acknowledged by the specified interface; and an indicator of whether or not Topology Change detection has been enabled for the specified interface.

No.	Syntax	Description
471	SHOW SWITCH	The SHOW SWITCH command displays configuration information for the switch functions. Parameters displayed in the output of the SHOW SWITCH command are: -- Learning: Whether or not the switch&apos;s dynamic learning and updating of the Forwarding Database is enabled; one of "ON" or "OFF". -- Ageing Timer: Whether or not the ageing timer is enabled; one of "ON" or "OFF". -- Number of LIF Ports: The number of fixed switch downlink LIF interfaces. -- Number of WIF Ports: The number of switch uplink interfaces. -- Ageingtime: The value in seconds of the ageing timer, after which a dynamic entry is removed from the Forwarding Database. -- Number of Standard VLAN: The number of standard 802.1q VLANs in the switch. -- Number of UFO VLAN: The number of upstream forwarding-only VLANs in the switch. In a UFO VLAN, the traffic from downstream interfaces is forwarded only to upstream interface(s).
472	SHOW SWITCH COUNTER	This command displays available CXE Queue Discard (QED) counters on the device. This includes information relating to the following: -- IN Queue Overflow The InQ can buffer four packets on each interface whilst waiting for Address lookup results or for a full link request queue (queuing multicast or broadcast packets waiting to be linked) to empty. If a new packet arrives while the InQ already holds four packets for an interface, the new packet will be discarded, and this counter will be incremented. -- Address Lookup FIFO Overflow The number of packets discarded due to internal buffer memory overflow. -- Buffer Memory OverFlow The number of packets discarded due to internal buffer memory overflow. -- Resource Limiter Internal Discard The number of packets discarded by the internal buffer memory resource guarantee block. -- Resource Limiter External Discard The number of packets discarded by the external memory guarantee block. -- Multicast BroadCast Limit Discard The number of packets discarded due to exceeding the limit on how much of the link memory may be used by multicast (or broadcast) packets. -- Time To Live Scoping The number of multicast packets discarded by the Time To Live (TTL) scoping mechanism. -- Weighted Fair Hashed Bandwidth Distribution The number of packets discarded by WFHBD. -- Medium Access Controller Error The number of packets discarded because the MAC indicated an error (CRC error, length error or pause frame).
473	SHOW SWITCH FDB [INTERFACE={ type:id-range | id-range | ifname-list | ALL}] [ADDRESS=macaddress] [HVLAN={ hvlanname | vid }]	The SHOW SWITCH FDB displays the contents of the Forwarding Database. Parameters displayed in the output of the SHOW SWITCH FDB command are: -- VLAN or HVLAN: The VID Identifier for the VLAN or HVLAN. -- MAC Address: The MAC address as learned from the source address field of a frame, or entered as part of a static filter entry. Example: 00:0C:25:00:13:8C -- Interface: The interface from which the MAC address was learned. To display the contents of the Forwarding Database, use the SHOW SWITCH FDB command.
474	SHOW SWITCH FDB [INTERFACE={ type:id-range | id-range | ifname-list | ALL}] [ADDRESS=macaddress] [VLAN={ vlanname | vid }]	The SHOW SWITCH FDB displays the contents of the Forwarding Database. Parameters displayed in the output of the SHOW SWITCH FDB command are: -- VLAN or HVLAN: The VID Identifier for the VLAN or HVLAN. -- MAC Address: The MAC address as learned from the source address field of a frame, or entered as part of a static filter entry. Example: 00:0C:25:00:13:8C -- Interface: The interface from which the MAC address was learned. To display the contents of the Forwarding Database, use the SHOW SWITCH FDB command.
475	SHOW SYSTEM	The SHOW SYSTEM command displays a terse summary of current configuration information for the shelf.

No.	*Syntax*	*Description*
476	SHOW SYSTEM COOLING	The SHOW SYSTEM COOLING command displays various information about shelf temperature and fan conditions. Information includes: - current readings of the shelf temperature sensors - any current faults related to the temperature sensors - fan module information including dynamic state attributes, alarms and defect conditions, and current fan speeds (the same information as the SHOW FANMODULE output) On the 7400 shelf only, additional information is shown about the FC7 (fan controller) card, including: - dynamic state attributes - alarms and defect conditions (The FC7 information is the same as displayed by the SHOW CARD command for the FC7).
477	SHOW SYSTEM PROVMODE	The SHOW SYSTEM PROVMODE command displays the current provisioning mode for the system.
478	SHOW SYSTEM TIME	The SHOW SYSTEM TIME command displays the current date and time that the system is using.
479	SHOW SYSTEM USERCONFIG	The SHOW SYSTEM USERCONFIG command will display the value of all of the global security parameters and security counters. The security parameters indicate the values set by the SET SYSTEM USERCONFIG command. The security counters are counters maintained to monitor user authentication activity in the system. The counters are persisted at intervals as defined by the PERSISTTIMER parameter of the SET SYSTEM USERCONFIG command or whenever a modification to the system parameters is done. The counters can be reset using the RESET USER command. The security counters are listed below: Logins : Number of successful logins into the system Manager Pwd changes : Number of times a manager or security officer password has been changed. Unknown login names : Number of attempts to login with an invalid login-name Idle session timeouts : Number of idle sessions that have closed due to timeout. Database clears : Number of calls to RESET USER command for global counters. Authentications : Number of successful logins into the system. Manager Pwd fails : Number of unsuccessful logins to manager or security officer accounts. Total Pwd fails : Total number of unsuccessful logins to existing accounts. Login lockouts : Number of times a user or session was locked out due to consecutive failed login attempts. Default account resets: Number of times PURGE USER command was called.
480	SHOW TACPLUS	The SHOW TACPLUS command displays a table containing information regarding the TACACS+ server configuration. The information includes each TACACS+ server's hostname or IP address, status (enabled or disabled), port, retries, and timeout values. The shared secret is not displayed for security reasons.
481	SHOW TRAFFICDESCRIPTOR[={tdname-list|ALL}]	The SHOW TRAFFICDESCRIPTOR command shows information about the specified TRAFFICDESCRIPTORs. This includes any classifiers that are associated with the TRAFFICDESCRIPTORs. To see which interfaces are associated with the TRAFFICDESCRIPTORs, you may use SHOW CLASSIFIER to show ports associated with the associated classifiers. See the CREATE TRAFFICDESCRIPTOR command for help on the use of TRAFFICDESCRIPTORs.

No.	*Syntax*	*Description*
482	SHOW USER[=login-name] [FULL]	The SHOW USER command will display the list of all configured users and their configuration parameters and counters. The configuration parameters indicate the values set by the ADD USER or SET USER command. The counters are counters maintained to monitor user authentication activity in the system for each user configured. The user parameters and counters are listed below: Username : the login-name of the user configured in the database. Description : The short description set by the ADD USER or SET USER command. Privilege : The privilege level of the user. Possible values are SECURITY OFFICER, MANAGER or USER. Status : indicates whether the user account is enabled or disabled. The account could be disabled if the user
483	SHOW VLAN [={ vlanname | vid | ALL }] [FORWARDINGMODE={ STD | UPSTREAMONLY | ALL }] [FULL]	The SHOW VLAN command displays information about the specified Virtual LAN (VLAN) If no VLAN name or identifier is specified, then ALL is assumed. If ALL is used, a summary of all VLANs is presented.
484	SHOW VOICECALL	The SHOW VOICECALL command shows how many calls are active over which interfaces. The user can show a summary of the interfaces for a card using the SHOW INTERFACE command and also use the SHOW VOICECALL command that will easily show which interfaces are active.
485	STOP TEST LCPECHOREQUEST [INTERFACE={ type:id-range | id-range | ifname-list | ALL }]	Stops a TEST LCPECHOREQUEST in progress.
486	STOP TRANSFER={ transferid-list | ALL }	The STOP TRANSFER command aborts an in-progress or pending file transfer. Only transfers to or from a network server can be stopped. File transfers from the CFC flash file system to a card in the shelf cannot be stopped. Stopping a transfer that is in progress deletes the destination file, but does not affect the source file.
487	STOP CONFIG	The STOP CONFIG command allows the user to cancel a BACKUP CONFIG or RESTORE CONFIG command that is currently in progress. If neither is currently in progress, no action is taken.
488	STOP PING	The PING command is used to find other hosts in the same network. The PING command sends ICMP echo packets to the specified host and waits for a response. If a response is received, an indication of success is shown to the user. Once the command operation completes, the user is presented with a summary of the number of packets sent and received along with an indication of the percentage of packets lost. In the event that a user wishes to end a repetitive PING request, the STOP PING command terminates ping operation and presents information regarding the number of packets sent and received.
489	STOP TRACEROUTE	The STOP TRACE command can be used to terminate a currently running TRACEROUTE command assuming there is one. Only the user who initiated TRACEROUTE can terminate it. If the user session that initiated TRACEROUTE is terminated, TRACEROUTE will automatically terminate.
490	SWAP ACTIVITY [FORCE]	The SWAP ACTIVITY command switches activity between the 2 redundant CFCs in a 7700 or 9700 system. Both CFCs must be in the ONLINE status. Sanity checking is performed automatically to ensure a non-service affecting switchover, unless the optional FORCE option is used. The FORCE option bypasses sanity checking and requires no confirmation.
491	TELNET={ ipaddress | hostname }	Allows user to telnet to another device during a CLI session. (If the other device locks up, use CTRL-D to forcibly close any open telnet sessions on the Telesyn.)

No.	Syntax	Description
492	TEST LCPECHOREQUEST INTERFACE={ type:id-range | id-range | ifname-list } [DELAY=1..900] [NUMBER={ 1..65535 | CONTINUOUS }] [TIMEOUT=1..900]	Send Echo-Request(s) out the interface and look for Echo-Reply(s). This gives a highly granular, but quantitative, assessment of the health of transport between the specified interface and the destination.
493	TRACEROUTE={ ipaddress | hostname } [FROM { INTERFACE={ type:id | id | ifname } | IPADDRESS=ipaddress }] [MINTTL=number] [MAXTTL=number] [TIMEOUT=seconds] [TOS=0..255] [NORESOLVE]	The TRACEROUTE command is used to trace the path to a specified destination. It displays intermediate nodes (hops) on this path along with round trip times from source to that node in milliseconds for three ICMP probes. TRACEROUTE command accepts an IP address of a destination in dotted decimal form or a DNS resolvable hostname. In addition, the command allows users to specify several optional traceroute parameters. This includes the minimum time to live (MINTTL), maximum time to live(MAXTTL) the timeout in seconds for ICMP responses (TIMEOUT), the IP Type of Service (TOS) byte and a NORESOLVE flag to indicate that TRACEROUTE must not attempt to DNS resolve IP addresses found along the path. If none of these parameters are specified, defaults will be used.

5. Parameter Reference

5.1 Overview

This Section is a complete parameter listing, and can be used as a standalone Section for understating parameters or as a companion to Section 4, which gives a brief description of a parameter for a specific command.

5.2 Commands Listed by Product

The following table lists the commands as follows:

- **Parameter**
- **Range -** This can be a numeric range or a list of possible numeric or string values**.**
- **Short Description** - This is the same description as given in Section 4, but is useful when using this section as a separate reference.
- **Definition** - This is an extended definition of the parameter.
- **Detail** - This can include additional information about how the system processes the parameter or how a parameter works for different products.
- **Default** - Some parameters have a default value if the parameter is not included in the syntax string.

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
ABSOLUTE	200..400	A direct comparison with the rising and falling threshold	The ABSOLUTE parameter indicates that specified RMON statistic is compared directly to the thresholds at the end of the sampling interval.		300
ACCEPTABLE		The acceptable frame types.	The ACCEPTABLE parameter sets the Acceptable Frame Types parameter, in the Ingress Rules, which controls reception of tagged and untagged frames on the interface. If ALL is specified, then the Acceptable Frame Types parameter is set to Admit All Frames. If VLAN/HVLAN is specified, the parameter is set to Admit Only tagged Frames, and any frame received that carries a null VLAN/HVLAN Identifier is discarded by the ingress rules. Untagged frames admitted according to the ACCEPTABLE parameter have the VLAN/HVLAN Identifier of the VLAN/HVLAN for which the interface is untagged associated with them. The ACCEPTABLE parameter can only be set if the interface is untagged for one VLAN/HVLAN. In this case, the default is ALL, admitting all tagged and untagged frames. If the interface is tagged for all the VLAN/HVLAN to which it belongs, the ACCEPTABLE parameter is automatically set to VLAN or HVLAN, and cannot be changed to admit untagged frames.		
ACCESS		The access setting for the SNMP community	The ACCESS parameter specifies the access mode for the community. If READ is specified, management stations in this community can only read MIB variables from the device. If WRITE is specified, management stations in this community can read and write MIB variables. The default is READ.		READ
ACCESSLIST		The name of the ACCESSLIST being affected.	The name of the ACCESSLIST being affected.		
ACTCFC	NA	ACTCFC - the active CFC, INACTCFC - the inactive CFC.	Entering ACTCFC specifies the active CFC card without having to know which slot it is in.	The CFC that is processing subscriber services. In the 7100, 7400, and 9400, there is only one CFC and it is always active.	
ADDRESS		MAC address of device to display (e.g. 00:0C:25:00:13:8C)	The ADDRESS parameter specifies the MAC address of the device for which the contents of the Forwarding Database are to be displayed. It is an Ethernet six-octet MAC address, expressed as six pairs of hexadecimal digits delimited by colons. An example MAC address is "00:00:cd:00:45:c7".		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
ADDRESS for CLEAR SWITCH FDB		MAC address of device to clear (e.g. 00:0C:25:00:13:8C)	The ADDRESS parameter specifies the MAC address of the device for which the contents of the Forwarding Database are to be cleared. It is an Ethernet six-octet MAC address, expressed as six pairs of hexadecimal digits delimited by colons. An example MAC address is "00:00:cd:00:45:c7".		
ADMINKEY		An 802.3ad admin key.	The ADMINKEY parameter is the 802.3ad admin key value for the Link Aggregation Group (LAG). The admin key is used to identify specific groups of ports capable of aggregation. A default value is set by the system if one is not specified. The valid range of values is 1..1024, with default value of 1. Note that higher values represent lower priority. This parameter is applicable only if LAG mode is set to active or passive (indicating that LACP is configured to run on system).		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
ADMINSTATE		Initial Administrative State	The ADMINSTATE parameter specifies the initial administrative state for the card. The administrative state reflects the user's intent on having the card available for service (ready to process data). Valid states are UP (in service) or DOWN (out of service). Once the card is provisioned, use the ENABLE CARD or DISABLE CARD command to change the state.	Administrative and Operational States determine whether the card or port is available for service and if so whether service is being provided: The Administrative State is controlled by the user and can be set to either UP (available for service) or DOWN (Not available for service). Control of this state is through the ENABLE/DISABLE command. The Operational State is either UP (providing service) or DOWN (not providing service). This state is not user controllable but does depend on the Administrative State: If the Administrative State of a card is UP, the Operational State will be UP if the card/port can provide service. If the Administrative State is DOWN, the Operational State will always be DOWN. The exception to these rules is the FM7 in the Telesyn 9400, for the FANMODULE. This cannot be disabled, and the alarms can be masked while the fan module is removed., UP	
ADSL16		16-port ADSL Service Module(SM)	The ADSL16 parameter identifies the card as a 16-port ADSL card. As an ADSL16 card, only ADSL16 options are available to the user.	Service module (SM). ADSL service with 16 ports. The ADSL16 interfaces the Telesyn 7000/9000 and the downstream equipment. It also translates between the Ethernet packet format and the customer interface format (ADSL). Each SM provides an ADSL interface to a number of customer ports.	

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
ADSL16B		16-port ADSL Service Module(SM), Annex B	The ADSL16B parameter identifies the card as an 16-port ADSL card with Annex B support. As an ADSL16B card, only ADSL16B options are available to the user.		
ADSL24		24-port ADSL Service Module (SM)	The ADSL24 parameter identifies the profile as an 24-port ADSL card Profile. As an ADSL24 card profile, only ADSL24 card options are available to the user.	Service module (SM). ADSL service with 24 ports. The ADSL24 interfaces the Telesyn 7000 and the downstream equipment. It also translates between the Ethernet packet format and the customer interface format (ADSL). Each SM provides an ADSL interface to a number of customer ports.	
ADSL8S		8-port ADSL Service Module(SM)	The ADSL8S parameter identifies the card as an 8-port ADSL card with integrated splitters. As an ADSL8S card, only ADSL8S options are available to the user.	Service module (SM). ADSL service with 8 ports. The ADSL8S interfaces the Telesyn 7000 and the downstream equipment. It also translates between the Ethernet packet format and the customer interface format (ADSL). Each SM provides an ADSL interface to a number of customer ports.,	
ADSLPORT		Selects ADSL port as the component type.	The ADSLPORT parameter displays the attributes in the specified profile name for ADSL ports.		
AGEINGTIMER		The FDB aging timer	AGEINGTIMER is the threshold value, in seconds of the ageing timer, after which a dynamic entry is removed from the Forwarding Database.Default is 300.		300
ALLSTANDARD		All the standard 14 reserved multicast IP addresses.	ALLSTANDARD keyword means all the standard 14 reserved multicast IP addresses. These are: DVMRP, OSPF All Routers, OSPF Designated Routers, RIP2, IGRP, DHCP RELAY, PIM, RSVP, CBT, VRRP, DxCLUSTER, CISCONHAP, HSRP, and MDNS.		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
ALTLOAD		The alternate software load for the card.	The ALTLOAD parameter specifies the name of the alternate software load file for the CFC card, and is only supported for the CFC. This file must reside on the CFC flash file system, and is booted by the CFC only when the preferred load is unusable for any reason. If the alternate load is ever booted then it becomes the preferred load. There is no default value for the alternate load. The command is rejected if the alternate software load specified is not compatible with the specified card. The alternate software load should be a renamed copy of the preferred software load. Creating a renamed copy of the preferred software load is done using the COPY FILE command. Setting of ALTLOAD is not allowed for the inactive CFC; it obtains its altload settings from the active CFC.	Alternate - selected using the ALTLOAD parameter. A load designated as ALTLOAD indicates that this is the alternate load that the specified card will load from. (Control Module Only) A load designated as ALTLOAD indicates that this is the alternate load that the specified card will load from. The ALTLOAD is used when a redundant copy of the preferred load file is made on the control module FLASH file system; it specifies an alternate load preference for the redundant file. Establishing an alternate load provides a backup in the unlikely case the preferred load file is not bootable. For a duplex configuration, any changes made in the ALTLOAD designation apply to both the active and inactive control modules. This parameter is not supported for the service modules because the copy of the service module load stored on the control module FLASH file system is the alternate by default (the preferred is the copy in the service module flash memory). Load preferences for the CFC(s) are stored in the non-volatile RAM (NVRAM) of each CFC, while load preferences for the Service Modules are stored in the configuration database. ,	
AnnexType		The desired annextype for the card. Annex-A or Annex-B.	The annextype specifies regional requirements for SHDSL deployments. Annex A is typically enountered in North American networks, annex B is typical in European networks. The default annextype is B. The user can set this parameter only when the card is disabled (See DISABLE CARD).	Specifies the annex type for ADSL or SHDSL ports as described in ITU-T Recommendation G.992.	

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
APPLICATION		The name of the APPLICATION to match on	The name of the APPLICATION to match on. The APPLICATION is one of several pre-defined match rules. For example, the APPLICATION TELNET matches all packets with TCPPORTDEST=23.		
ARP		Address Resolution Protocol	Address Resolution Protocol to obtain MAC address for the specified IP address.		
ARPFILTER		ARPFILTER describes the kind of DISABLE operation being performed.		A filter that specifically blocks Address Resolution Protocol (ARP) packets.	
ASCENDING		ascending order	Sort the interfaces in ascending order.		
ATUC		Specifies the ATU-C (receive) side of the link	The ATUC parameter indicates that the threshold value should be applied to the counts pertaining to the ATUC side of the link.		
ATUR		Specifies the ATU-R (transmit) side of the link.	The ATUR parameter indicates that the threshold value should be applied to the counts pertaining to the ATUC side of the link.		
AUTHMODE		Authentication mode to be used for RADIUS	The AUTHMODE parameter is used to specify how user privilege level is assigned when user authentication is done using a RADIUS server. When the RADIUS authentication mode is set to LOGIN, the user will be logged in with the privilege level assigned by the RADIUS server. If the authentication mode is set to COMMAND, then the user is always logged in at USER privilege level and must run the ENABLE {MANAGER|SECURITYOFFICER} command to request increased privilege.		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
AUTONEGOTIATION		Auto negotiation of transmission parameters (ON or OFF).	The AUTONEGOTIATION parameter specifies whether automatic negotiation of transmission parameters for GE ports is allowed. The parameter is either ON or OFF. The user may set this parameter only when the port is disabled (See DISABLE PORT). Whether ON or OFF, the port speed is fixed at 1000BASE-X with full duplex. If ON, the port has increased flexibility to communicate with the remote peer. The port has the ability to advertise flow control and to provide single direction fault coverage. The port will drive the link state up and down based on the ability to communicate with the remote peer, triggering on both transmit and receive failures (LOS). If OFF, the port state is driven by receive failure (LOS). Flow control is still provided as long as the FLOWCONTROL parameter is ON. This parameter is only applicable to GE ports. The default value is ON.		ON
BEFORE		The RULE number that the new RULE will be inserted ahead of.	The RULE number that the new RULE will be inserted ahead of.		
BOOTSERVER		A network load file server capable of support TFTP requests	The BOOTSERVER parameter specifies the IP address of the network server that is the source for the preferred CFC software load. Files are transferred from the network server via TFTP.		
BROADCAST		Change alert setting for broadcast packets	The BROADCAST parameter indicates that that the rising/falling threshold values are to be used for the broadcast packets statistical counter.		
BUCKETS		A single instance of collected data	The BUCKETS parameter identifies the collection of historical data. BUCKETs are held so that the most recently collected BUCKET is BUCKET number 1 and when newly collected data is obtained, what used to be BUCKET 1 becomes BUCKET 2, and so on. This parameter allows the user to specify the number of buckets to hold at any one time. BUCKETs are a system wide resource and no more than 2,700 can specified to be held onto at any one time.	Buckets are a system wide resource. For RMON data, the maximum number of buckets that can be configured for a Telesyn product is 2700. If the user tries to add a history that will go over the 2700 limit, the system will allocate what is available and produce a message saying how many buckets were granted. For PMON data, none?.	5
Buffer for TRACE		Set the size of the Trace buffer.	The BUFFERSIZE parameter controls the number of Trace logs that will be stored in the Trace buffer. The buffer is circular so once the buffer is full new logs will overwrite the oldest logs. The maximum size of the buffer is 10,000 logs. The default is 200 logs.		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
BUFFERDELAY		Jitter Buffer Delay in milliseconds (0 to 150 in steps of 10)	The BUFFERDELAY parameter specifies amount of time that the first packet is delayed. This delay is used to smooth out jitter on subsequent arrivals. The default is 30 msec.		30 msec
BUFFERMODE		Jitter Buffer Mode - STATIC or DYNAMIC (Adaptive)	The BUFFERMODE parameter specifies the type of buffering mode to employ. A jitter buffer is used to compensate for the jitter in packet arrival and out-of-order packets. Values are STATIC and DYNAMIC.	The jitter buffer mode. A jitter buffer is used to compensate for the jitter in packet arrival and out-of-order packets. A large jitter buffer causes increase in the delay and decreases the packet loss. A small jitter buffer decreases the delay but increases the packet loss.	STATIC
BUFFERSIZE			The buffer size.		
BUFFERSIZE for TRACE		Set the size of the Trace buffer.	The BUFFERSIZE parameter controls the number of Trace logs that will be stored in the Trace buffer. The buffer is circular so once the buffer is full new logs will overwrite the oldest logs. The maximum size of the buffer is 10,000 logs. The default is 200 logs.		
BURSTSIZE		Maximum size burst of traffic allowed to exceed the RATE.	The BURSTSIZE parameter specifies the maximum size burst of traffic that is allowed to exceed the specified RATE. The value is entered from among an enumerated list of allowable values.	Specifies the allowable burst size for conforming traffic.	
CACHEAGING		The maximum age for SNMP cache contents	The CACEAGEING parameter indicates the amount of time after which the data in the cache are considered invalid or dirty. The cache age is expressed in seconds. The default cache ageing interval is 60 seconds. The maximum ageing interval is 10 minutes (600 seconds).		60
CACHESIZE		The maximum size of the SNMP cache	The CACHESIZE parameter determines the size of the SNMP cache in kilobytes(KB). The default cache size is 128 KB. The maximum cache size is 4MB(4000 KB).		128
CACHING		The cache enabled status	The CACHING parameter is used to disable or enable caching of data retrieved as part of an SNMP GET, GET-NEXT, or GET-BULK operation.		FALSE
CALLAGENT		The network callagent identification.	The CALLAGENT parameter specifies the network call agent that the interface will communicate with.	The identification of the network call agent that the card will communicate with. If not specified, the udp-port is defaulted to 2727.	2727

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
CANCEL		Used to abort a delayed session deactivation.	The CANCEL parameter is used to abort a delayed session deactivation.		
CAPABILITY		Supported Codecs for POTS - PCMU, G726, or ALL (both)	The CAPABILITY parameter specifies the POTS codec which should be employed.		
CARD		The slot number for a card	The CARD parameter specifies the slot number for the card being created.	Specifies a slot number for a specific card (module) in the shelf. The CARD parameter specifies the slot number or list of slot numbers of the cards to enable. The slot-list is either: - a single slot - a comma-separated list of slots - a dash range of slots - a combination of dash and comma-separated slots INACTCFC specifies the inactive CFC card, whichever slot it is in.	
CATEGORY		Comma-separated list of log categories.	The CATEGORY parameter allows the user to specify one or more management log categories to filter. A comma-separated list of categories is accepted. The management log category is taken from the leading 3 or 4 alphabetic characters from the management log name. Comma-separated list of log categories. Valid log categories are: ADSL BDB CARD CFCP CHAS CLI CUC FAN FILE IGMP LOG PORT RDB RMON RSDB SHLF SNTP STP SYS TRAP USER Default is ALL.		
CATEGORY (for SNMP TRAP)		The SNMP trap category	The CATEGORY parameter determines the trap category for which traps are generated. By default, all categories are set to ON.		
CBT		All CBT routers	All Core Based Trees routers.		
CFC24		24 Gb Central Fabric Controller (CFC)	The CFC24 parameter identifies the card as a 24 Gb Central Fabric Controller (CFC) card. As a CFC24 card, only CFC24 options are available to the user. This card is not supported in this software release.	Specifies the CFC24 Control Module. The Control Module (CM) - The CM manages all equipment, configuration, and data transport. It is the central switching fabric for the shelf.,	
CFC4		CFC4	The CFC4 parameter displays the attributes in the specified profile name for 4 Gb CFC cards.		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
CFC6		6 Gb Central Fabric Controller (CFC)	The CFC6 parameter identifies the card as a 6 Gb Central Fabric Controller (CFC) card. As a CFC6 card, only CFC6 options are available to the user.	Specifies the CFC6 Control Module. The Control Module (CM) - The CM manages all equipment, configuration, and data transport. It is the central switching fabric for the shelf.,	
CHANGE		A comparison change between collection intervals and the rising and falling thresholds	The CHANGE parameter indicates that rising and falling thresholds are based on a change between the current and previous sampling intervals for the RMON statistic.		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
CIDFORMAT		The Circuit ID format.	The CIDFORMAT tells what format is to be used for the cid value. The options are AUTOMATIC, IFDESC or BOTH.	CIDFORMAT specifies whether the Circuit ID (CID) should be formed automatically by the DHCP feature or if the user-defined interface description should be used. The CID is used to uniquely identify the subscriber port a DHCP packet is received on. DHCP servers can use the CID for assigning IP ADDRESSES and, in conjunction with the giaddr value, for lease reports/statistics. The CID is used by the RELAY AGENT to direct server responses, DHCPOFFER, DHCPACK, DHCPNACK back to the proper circuit (interface). AUTOMATIC - The default. When specified, the CID value will automatically be generated by the DHCP RELAY AGENT. The benefit of using this format is that the CID is guaranteed to be unique for all ports on the switch. IFDESC - Will use the interface description, entered during OAMP interface provisioning via the SET INTERFACE DESCRIPTION command, as a CID. User-defined string of 1 to 31 ASCII characters. BOTH - The CID format value will concatenate the the auto-generated (AUTOMATIC) and the interface description (IFDESC).	AUTOM ATIC
CISCONHAP		CISCO NHAP			
CLASSIFIER COUNTER		Displays CLASSIFIER COUNTERs on the specified PORT/INTERFACE(s)	If allowed by the syntax, the COUNTER parameter specifies that CLASSIFIER-related counters on the PORT/INTERFACE(s) are displayed.		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
CLASSIFIER SUMMARY		SHOWs SUMMARY data for specified CLASSIFIER(s) and PORT/INTERFACE(s)	If allowed by the syntax, the SUMMARY option SHOWs name, match rule, and action data for specified CLASSIFIER(s) and PORT/INTERFACE(s).		SUMMARY
classifiername		The name of the CLASSIFIER	The name of the CLASSIFIER. A CLASSIFIER name may contain a maximum of 20 characters, and may not be an abbreviation for "PORT" or "INTERFACE". They also may not start with an underscore ("_") character.	A character string, 1 to 32 characters in length. Valid characters are uppercase letters (A-Z), lowercase letters (a-z), and decimal digits (0-9). The string may not contain spaces.	
classifiername-list		A listing of classifier names.	A list of classifier names separated by commas.	Specifies one or more CLASSIFIERs to which the ACTION is being added. The value may be entered as a single CLASSIFIER name, or a comma-delimited list of names.	
CLI		Command Line Interface.	Indicates that log output needs to go to a CLI session. Default is CLI.		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
COLD		Resets and reinitializes the card.	The COLD parameter indicates that a COLD restart is performed. This type of restart resets the card hardware, reboots the software load(if applicable), and reinitializes the configuration data.	For the active CFC, a COLD restart resets the CFC and all other cards in the shelf, reboots and reinitializes the software on the CFC, runs out of service diagnostics on the CFC if previously scheduled, reloads configuration data from the system database, manages recovery of the remaining cards in the shelf. For the inactive CFC, a COLD restart changes the operational state to DOWN, if not already DOWN, performs a hardware reset on the card, reboots and reinitializes the software, runs out of service diagnostics, reloads configuration data, restores the operational state to UP if the administrative state is UP, including data initialization and initiation of defect monitoring. For the ADSL16, ADSL8S, FE10 and FX10 cards, a COLD restart, changes the operational state to DOWN, if not already DOWN, performs a hardware reset on the card, reboots and reinitializes the software, runs out of service diagnostics, reloads configuration data, restores the operational state to UP if the administrative state is UP, including data initialization, initiation of defect monitoring, and restoration of ports. For the GE1 and GE3 cards, a COLD restart changes the operational state to DOWN, if not already DOWN, performs a hardware reset on the card, runs out of service diagnostics, reloads configuration data, restores the operational state to UP if the administrative state is UP, including data initialization, initiation of defect monitoring, and restoration of ports.	COLD

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
COLLISIONS		Change alert setting for packet collisions	The COLLISIONS parameter indicates that that the rising/falling threshold values are to be used for the packet collisions statistical counter.		
COMFORTNOISE			Specifies whether or not to generate Comfort Noise (RFC 3389). To generate background noise to fill silent gaps during calls if voice activity detection (VAD) is activated; the parameter should be ON. If COMFORTNOISEGENERATION is not enabled and VAD is enabled at the remote end of the connection, the user hears dead silence when the remote party is not speaking. Comfort noise affects only the silence generated at the local interface; it does not affect the use of VAD on either end of the connection or the silence generated at the remote end of the connection. To provide silence when the remote party is not speaking and VAD is enabled at the remote end of the connection, the parameter should be turned off. Comfort noise is stopped automatically upon receipt of modem tone. Default is ON.		ON

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
COMFORTNOISEGENERATION		Comfort Noise Generation capability for POTS (ON or OFF)	The COMFORTNOISEGENERATION parameter specifies whether or not comfort noise generation is enabled.	Specifies whether or not to generate Comfort Noise (RFC 3389). To generate background noise to fill silent gaps during calls if voice activity detection (VAD) is activated; the parameter should be ON. If COMFORTNOISEGENERATION is not enabled and VAD is enabled at the remote end of the connection, the user hears dead silence when the remote party is not speaking. Comfort noise affects only the silence generated at the local interface; it does not affect the use of VAD on either end of the connection or the silence generated at the remote end of the connection. To provide silence when the remote party is not speaking and VAD is enabled at the remote end of the connection, the parameter should be turned off. Comfort noise is stopped automatically upon receipt of modem tone. Default is ON.	ON
COMMUNITY		The SNMP community name.	The COMMUNITY parameter specifies the SNMP community name. The community name is a case-sensitive alphanumeric string of 1 to 15 characters. The community must already exist on the device before this command is used (See CREATE SNMP COMMUNITY).		
CONFIGCHANGE		The configuration change trap category	The CONFIGCHANGE parameter is used to allow or suppress delivery of configuration change traps. A value of OFF prevents delivery of configuration change traps to the specified SNMPv1 or SNMPv2 trap host.		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
CONFIGURATION		Dislpay the collection threshold settings.	The CONFIGURATION parameters displays the threshold settings for the specified INTERFACEs. For ADSL interfaces, performance monitoring alarm settings are displayed (See RFC2662 and RFC3440). For Ethernet interfaces, remote monitoring rising and falling alarm settings are displayed (See RFC2819).		
CONSOLE		User's console.	Indicates that log output needs to go to the system console.		
CONTACT		The dry contact input number (0, 1, 2)	The CONTACT parameter specifies the dry contact input number. There are 3 separate dry contact inputs numbered 0, 1 and 2.	Dry Contact connections on the ALM IN alarm points detect the presence of an electrical short. Three alarm points are provided, DC0, DC1 and DC2. Alarms, such as open door, ambient temperature, etc. can be connected to the ALM IN points.,	
COUNT		On a CLASSIFIER match, increment a per-port counter.	On a CLASSIFIER match, increment a per-port counter. If combined with a DROP action, then increment the "Filter Count". If combined with a TRAFFICDESCRIPTOR (for policing), then increment the "Policed Count". Else increment the "Match Count" counter. Current COUNTs are displayed via "SHOW CLASSIFIER PORT port-list COUNTER"	COUNT - count the number of packets that have been forwarded or dropped. These are displayed with the SHOW CLASSIFIER command.,	
COUNT (for CLASSIFIER)		On a CLASSIFIER match, increment a per-port counter	On a CLASSIFIER match, increment a per-port counter. The rules for which counter to increment vary slightly depending on hardware platform. If combined with a DROP action, this action increments the "Filter Count". If Combined with actions that do not include DROP, this action increments the "Match Count" counter. Note that on the 9x00 series platform both the "Match Count" and the "Filter Count" can be incremented by a single packet that matches both the FORWARD and DROP classifier. On other platforms only the count with the higher precedence is incremented. Current COUNTs are displayed via "SHOW CLASSIFIER PORT port-list COUNTER"		
COUNTER		A counter.	If allowed by the syntax, the COUNTER parameter specifies that CLASSIFIER-related counters on the PORT(s) are displayed.		
COUNTER (for IGMP)		Resets the IGMP snooping counters/statistics	The COUNTER parameter indicates the kind of RESET IGMPSNOOPING operation performed.		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
COUNTER (for INTERFACE)		Add information having to do with counters	The COUNTER parameter indicates that this command has to do with statistical counter data.		
COUNTER FAULT OR QUEUE		Specifies the network monitoring system counter	The COUNTER parameter identifies the category of monitoring statistic. Valid values are PMON for ADSL port performance monitoring and RMON for remote monitoring on Ethernet ports, FAULT for port faults and QUEUE for adsl egress counter data.		
COUNTER for IP		Show statistical counts for a protocol IP related Counters	Shows statistical count information related to the protocol (TCP, UDP, or ICMP) specified This option indicates counter data for one of UDP,TCP or ICMP.		
CPU		CPU usage statistics	The CPU parameter displays CPU real-time usage statistics. This parameter is only applicable to the CFC card.	Displays CPU information for the specified card.	
CPUSTATS					
CRCALIGN		Change alert setting for CRC alignment errors	The CRCALIGN parameter indicates that that the rising/falling threshold values are to be used for the CRC alignment statistical counter.		
CRCANOMALIES		CRC anomalies TCA generation threshold	The CRCANOMALIES parameter is used to set a limit on the number allowed CRC anomalies allowed over a fifteen minute interval.		
CRITICAL (for SNMP TRAP)		The critical severity SNMP traps.	The CRITICAL parameter is used to allow or suppress delivery of traps marked as critical by the device. A value of OFF prevents delivery of critical severity traps to the specified SNMPv1 or SNMPv2 trap host.		
Critical for alarm threshold		Minimum number of ports before a critical alarm is raised.	Minimum number of ports before a CRITICAL alarm is raised.		
CUSTOM for IGMPSNOOPING FLOODING		Name of the Custom IGMPSNOOPING FLOODING	Any unique name provided by the user for a reserved multicast IP address other than the standard multicast IP addresses.		
CV					
DATE		The current date	The DATE parameter specifies the current date of the year. The format is yyyy-mm-dd, for example 2003-01-01 for January 1, 2003. NOTE: Setting the system date is immediately reflected in all system output that contains date, such as logs, SNMP traps, etc.		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
Date for TRACE		Date range of logs to display	The DATE parameter causes SHOW TRACE to display only the logs that occurred on a certain date or within a range of dates. There are three possible ways to use the DATE parameter. 1) As a single date, yyyy-mm-dd (e.g., 2003-03-14 to display all logs that occurred on March 14, 2003) 2) As an explicit range of dates, yyyy-mm-dd-yyyy-mm-dd (e.g., 2003-03-14-2003-03-17 to display all logs that occurred between March 14, 2003, and March 17, 2003, inclusive) 3) As an operation-specified range of dates. The following operations are valid: "<" - less-than - displays all logs earlier than or equal to a certain date ">" - greater-than - displays all logs with a date later than or equal to a certain date		
DEFAULT		Reset to defaults.	The DEFAULT parameter resets the STP settings to their defaults. The default settings are as follows: - FORWARDDELAY - 15 seconds. - HELLOTIME - 2 seconds. - MAXAGE - 20 seconds. - PRIORITY - 32768. - FORCE - RSTP.		
DEFAULTCALL					
DEFAULTRULE		The default rule for accesslists.	Rule which defines what to do with packets which don't match any other rules in access list. Can either be PERMIT all or DENY all.		
DELAY		The number of seconds to delay before deactivating the session.	Sets the number of seconds to wait between PING requests. (Default: 1 second).		
DELAY (for PING)		The amount of time to wait before sending the PING packet	The DELAY parameter sets the number of seconds to wait between PING requests. (Default: 1 second)		
DELAY OF SESSION		The number of seconds to delay before deactivating the session.	The DELAY parameter provides a means to schedule the session deactivation for 1 to 600 seconds in the future. If the targeted users need to be informed about the pending deactivation request, the MESSAGE option must also be used.		
DENY		Do not allow packets matching this RULE to pass	Do not allow packets matching this RULE to pass		
DENYUSERS		Add list of users to the DENY list	List of users to be added to the DENY list. Maximum of 64 users can be in the DENY list. There must be at least one enabled SECURITY OFFICER user that is NOT denied access.		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
DESCENDING		descending order	Sort the interfaces in descending order.		
DESCRIPTION		The interface description	The DESCRIPTION parameter provides a description for the interface. If the description contains space characters, the description must be specified in quote (") characters.		
DESCRIPTION OF PORT		a text description for the port	The DESCRIPTION parameter specifies a text description for the port. This is an optional parameter.		
DESCRIPTION OF USER ACCOUNT		The description of user id - max 23 characters	The DESCRIPTION parameter provides a description of the account created. This value is typically the name of the user associated with the account. If the description contains spaces, it must be enclosed in quote characters.		
destinationfile		Destination file name.	The TO parameter specifies the name of the destination file on the CFC flash file system. If the file is on a media card then it should be preceded by the media name, as in CFLASH9:myfile.	destinationfile - the name given to the new file.	
DESTMASK		Optional destination IP address mask (e.g. 255.255.255.0)	The optional DESTMASK works with the IPDEST match rule field to match on any IPv4 packet with the specified IP destination address. The value is specified as a mask for the IPDEST field. For example, an IPDEST of 192.168.1.0 with a DESTMASK of 255.255.255.0 matches 192.168.1.0 to 192.168.1.255. If no mask is provided then 255.255.255.255 is assumed. The DESTMASK must be a contiguous series of bits starting with the MSB. For example, 255.255.240.00 would be valid but 255.0.255.0 would not.		
DHCPRELAY			The DHCPRELAY parameter indicates the kind of operation performed.		
DHCPRELAY COUNTER		A DHCP packet counter.	The Counters for all the DHCP packets types exchanged between client, agent and the DHCP server.	The DHCP Relay packet counts on the specified interface. If an interface is not specified, the cumulative DHCP Relay counter will be reset, as well as all individual interface DHCP Relay counters.	
DISCONNECTTHRESHOLD		The disconnect threshold.	The DISCONNECTTHRESHOLD parameter specifies the number of unacknowledged packet retransmissions before beginning a disconnect procedure if no other call agent addresses are available.		7

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
DNS		The domain name server(DNS) for the system.	The DNS parameter designates the IP addresses for domain name servers for the system. DNS allows the translation of host names to IP addresses. A maximum of 3 addresses can be entered. Multiple addresses should be separated by commas.		
DNS for IP INTERFACE		The domain name server(DNS) for the ip interface	The DNS parameter designates the IP addresses for domain name servers for the ip interface. DNS allows the translation of host names to IP addresses. A maximum of 3 addresses can be entered, except for Pots ip interfaces where the maximum is 2. Multiple addresses should be separated by commas.		
DOMAINNAME		The domain name to which the system belongs	The DOMAINNAME parameter designates the domain name to which the system belongs.		
DROP		Drop the packet.	On a CLASSIFIER match, drop the packet. The DROP ACTION conflicts with all ACTIONs except COUNT.	DROP - discard the packet at the card. This action excludes the packet,	
DROPEVENTS		Change alert setting for dropped packet events	The DROPEVENTS parameter indicates that that the rising/falling threshold values are to be used for the dropped packet event statistical counter.		
DUPLEX		Duplex setting for an FE port.	The DUPLEX setting specifies the desired duplex for an FE port. The valid values are HALF, FULL or AUTONEGOTIATE. The default value is AUTONEGOTIATE. The user can set this parameter only when the port is disabled (See DISABLE PORT). This parameter is only applicable to FE ports.		AUTONEGOTIATE
DUPREPORTTIMER		Time delay before sending duplicate IGMP reports to multicast router(s)	Multiple subscriber devices may send up duplicate multicast group information in an IGMP report (i.e., EPG), after a general query is received. Usually, ALL of these reports would be sent to the multicast router(s). This option controls the time delay, which is used to determine when another duplicate report would be sent to the multicast router(s). So another received duplicate report would be sent to the multicast router(s), if it's received after the time delay has passed. This option is used to control the number of duplicate reports hammering the multicast router(s). Default is 10 seconds.		10 seconds
DVMRP		DVMRP routers	Distance Vector Multiple Routing Protocol routers.		
DXCLUSTER		Dx CLUSTER			

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
EARLYPACKETS					
EC		Echo cancellation for ADSL ports (either ON or OFF)	The EC parameter specifies whether echo cancellation is utilized on ADSL ports running G.DMT mode as per ITU-T Recommendation G.992.1. If set ON, the port uses overlapping spectrum operation to more effectively use bandwidth between the upstream and downstream frequencies, thus boosting the connect rate. A Setting of ON is only valid for a MODE of GDMT. The default value is OFF. The user can set this parameter only when the port is disabled (See DISABLE PORT). This parameter is only applicable to ADSL ports.		ON
ECHOCANCELLATION for POTS24		Echo Cancellation capability for POTS (ON or OFF)	The ECHOCANCELLATION parameter specifies whether or not echo cancellation capability is advertised to the call agent.	Specifies whether or not Echo Cancellation capability is advertised to the Call Agent. ON: echo cancellation is supported. This is the default.	ON
EDGEPORT		Port connection to edge of network.	True/False indication of port connectivity to single end user (default = False).	Allows the user to specify a port as an “Edge Port” when it is expected that a port will be directly connected to a host (i.e., a port at the “edge” of the Bridged LAN). Additional processing is associated with the use of this parameter to verify that a port identified as an “Edge Port” by the user is not actually connected to another bridge. This parameter and its associated processing can facilitate a port state transition directly to the forwarding state as part of the RSTP processing.	FALSE
EGRESSLIMITER		The identifier(s) of EGRESSLIMITER(s) , or "ALL".	The name of the EGRESSLIMITER to associate with the INTERFACE(s).	The EGRESSLIMITER parameter specifies the name(s) of the EGRESSLIMITER(s). The value may be entered as a single EGRESSLIMITER name, or a comma-delimited list of names. The value "ALL" specifies all EGRESSLIMITERs.	

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
ENCAPSULATIONTYPE		Encapsulation type for an ADSL port	The ENCAPSULATIONTYPE parameter specifies the ATM data encapsulation protocol used by an ADSL port, as defined in IETF RFC-1483. Values allowed are: - LLCSNAP : LLC/SNAP (Logical Link Control with Subnetwork Attachment Point) - VCMUX : VC Mux (Virtual Circuit Based Multiplexing) The default is LLCSNAP. The user can set this parameter only when the port is disabled (See DISABLE PORT) This parameter is only applicable to ADSL ports.		LLCSNAP
EPSR		EPSR Interface/Vlan	The EPSR parameter indicates the kind of ADD operation performed.		
ES		Errored Seconds TCA generation threshold	The ES parameter is used to set a limit on the number of allowed errored seconds over a fifteen minute interval.		
ETHFORMAT		The Ethernet encapsulation type to match.	The ETHFORMAT match rule matches on any packet with the specified Ethernet encapsulation type. Possible values are: - 802.3TAGGED : matches IEEE 802.3 format with a VLAN tag. - 802.3UNTAGGED : matches IEEE 802.3 format without a VLAN tag. - 802.3 : matches IEEE 802.3 format regardless of tags. - ETHIITAGGED : matches Ethernet II format with a VLAN tag. - ETHIIUNTAGGED : matches Ethernet II format without a VLAN tag. - ETHII : matches Ethernet II format regardless of tags. - ANY : matches any Ethernet encapsulation.	If an ETHFORMAT is specified, the PROTOCOL parameter must be used, specifying the protocol-type.	
EVENT		The event trace to add (default ALL)	OPENLOOP: the subscriber loop is open (on hook) CLOSELOOP: the subscriber loop is closed (off hook) MGCPOFFHOOK: an off hook indication has been sent to the call agent MGCPONHOOK: an on hook indication has been sent to the call agent MODEMDETECT: modem tone has been detected ALL: all of the above Note: ALL counts as a separate event instance and is the default.		ALL
FAILEDFASTRETRAIN		Failed Fast Retrain TCA generation threshold	The FAILEDFASTRETRIAIN parameter is used to set a limit on the number of allowed failed fast retrains over a fifteen minute interval.		
FailOverTime		The Failover time	Time for which the master node waits before declaring that it has detected a break in the ring for this EPSR domain		
FALLINGTHRESHOLD		The value for the RMONSTATISTIC falling threshold.	The FALLINGTHRESHOLD parameter specifies the lower limit of a monitored statistic before an event is generated. When the falling threshold is crossed, a management log is generated along with an SNMP trap (assuming SNMP support is configured for the system).		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
FAST		Specifies that fast linetype is used for an ADSL port	The FAST parameter specifies the ADSL line type as using the fast path as described in ITU G.992. The fast path provides low latency.		
FASTRATEDOWN		Fast Rate Down TCA generation threshold	The FASTRATEDOWN parameter indicates that the threshold value should be applied to either the adslAtucThreshFastRateDown or adslAturThreshFastRateDown statistic based on whether ATUC or ATUR were entered.		
FASTRATEUP		Fast Rate Up TCA generation threshold	The FASTRATEUP parameter indicates that the threshold value should be applied to either the adslAtucThreshFastRateUp or adslAturThreshFastRateUp statistic based on whether ATUC or ATUR were entered.		
FAULT		The fault trap category	The FAULT parameter is used to allow or suppress delivery of fault traps. A value of OFF prevents delivery of fault traps to the specified SNMPv1 or SNMPv2 trap host.	Used to allow or suppress delivery of fault traps. A value of OFF prevents delivery of fault traps to the specified SNMPv1 or SNMPv2 trap host.	
FAULTCOUNT		Port fault counters	Refers to the current fault counts for all interfaces identified with the INTERFACE parameter.		
FAULTCOUNT|QUEUECOUNT		Fault counts for the interface and the egress queue count information for the interface.	The FAULTCOUNT parameter is used to specify the current fault counts for all interfaces identified with the INTERFACE parameter		
FE		Specifies that FE port(s) are being modified	The FE parameter specifies that the port to modify is an FE (Fast Ethernet) port on an FEn (FE10, FE2, etc) card, and sets the context for the specified attribute values.		
FE10		10-port Fast Ethernet (FE) Card.	The FE10 parameter identifies the profile as a 10-port Fast Ethernet(FE) card. As an FE10 card, only FE10 card options are available to the user.	Service module (SM). Fast Ethernet service with 10 ports. Provides Fast Ethernet connections to downstream devices,	
FE2		Show profile names for FE2 ports	Fast Ethernet 2 port.		
FEPORT		Selects FE PORT as the component type	The FEPORT parameter identifies the profile as a Fast Ethernet(FE) port profile. As an FE port profile, only FE port options are available to the user.	Fast Ethernet ports.	

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
FILE		Name of the file that contains the configuration	The FILE parameter indicates the name of the file that contains the output from the BACKUP CONFIG command. The value for this parameter may also include a unit: prefix, to indicate the name of the flash unit where the file resides. The maximum length of the filename is 100 characters.		
filename		File name.	A descriptive file name.	The alphanumeric name of the file.	
FILTER		DHCP IP filtering	Set DHCP filtering ON or OFF for the specified interface.	When enabled, a maximum of 5 IP filters will be applied to the interface based on the number of learned MAC addresses that have been assigned IP addresses from the DHCP servers. IP filtering is off by default for interfaces with DHCP RELAY AGENT enabled. Additionally, setting filtering to ON is applicable only when DHCP RELAY is enabled on the interface.	OFF
FILTER (for LOG)		Names of filters to be added	The FILTER parameter identifies the name of the management log filters to add. The log filters specified must already exist (See CREATE LOG FILTER)		
filterid		Filter ID	The FILTER parameter provides the name of the management log filter to change.	Identifies the name of the management log filters to add. The log filters specified must already exist (See CREATE LOG FILTER). This value is an alphanumeric string between 1 and 23 long. ALL adds all log filterids.	
FLOODINGMODE OF SYSTEM		The forwarding mode of the device	This FORWARDINGMODE parameter indicates which configuration scheme is used. The following are the valid settings: - STD - standard - UPSTREAMONLY - upstreamonly forwarding		
FLOODUNKNOWNS		Flood unknown multicast packets	The FLOODUNKNOWNS parameter indicates if the unknown multicast packets will be flooded or dropped.		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
FLOWCONTROL		Flow control (ON or OFF)	The FLOWCONTROL parameter specifies whether flow control is enabled for GE and FE ports. For GE ports, the parameter can either be ON or OFF. If ON, the port can generate and respond to pause signals with the remote peer. If OFF, pause is ignored and not generated, and potential for packet loss is increased. FLOWCONTROL is independent of AUTONEGOTIATION. The default value is OFF. The user can set this parameter only when the port is disabled. (See DISABLE PORT) For FE ports, the parameter can either be ON or OFF or AUTONEGOTIATE. The default value is AUTONEGOTIATE. The user can set this parameter only when the port is disabled. (See DISABLE PORT)	Note: For Telesyn 7700s, Flow Control must be set to ON for the GE1s. This is true regardless of which CFC (TN-400-A or TN-400-B) is being used.	AUTONEGOTIATE
FORCE		The FORCE parameter suppresses the warning and bypasses the confirmation.	The FORCE parameter suppresses the warning message and bypasses the confirmation normally required for the command.	Suppresses the user warning and bypasses the confirmation, such as: “Service may be affected, are you sure (Y/N)?”. The command is executed.	No Force
FORMAT		The format of password entered. Default is CLEARTEXT.	The FORMAT parameter defines the type of password specified. If the FORMAT parameter is not provided, the password is assumed to be clear text. If MD5 is specified for the format, the password is assumed to be pre-encrypted as a 32 character MD5 digest.		
FORMAT for TRACE		The format the logs will be displayed in.	The FORMAT parameter allows users to specify the format of the Trace logs as they are displayed. Valid formats are: FULL - Displays the entire contents of the Trace log including log type, date and time, the slot where the log was generated, sequence number and the full message body. SUMMARY - Displays a one-line summary of the management log. The summary includes the log type, time, and the first line of the message body.		
FORMAT OF LOG		The format of the management logs.	Allows users to specify the format of the management logs for logs destined for a CLI destination. Valid formats include the following: FULL - Displays the entire contents of the management log including log type, date and time, severity, sequence number and message body. MSGONLY - Displays only the management log bodies. SUMMARY - Displays a one-line summary of the management log. The summary includes the log type, date and time and log sequence number. This parameter applies to CLI log output destinations only. The format for Syslog is fixed. Default is FULL.		

Parameter	*Range*	*Short Description*	*Definition*	*Detail*	*Default*
FORWARD		Forward the packet through the system.	On a CLASSIFIER match, forward the packet through the system. The FORWARD ACTION conflicts with the DROP ACTION.	FORWARD - allow traffic to be forwarded. This action includes the packet,	
FORWARDDELAY		A change to the forwarding delay	The FORWARDDELAY parameter is used to prevent temporary loops in the network occurring in the briefly unstable topology while a topology change is propagated through the network. The value of FORWARDDELAY determines how long the ports remains in each of the Listening and Learning states before moving on to the Forwarding state in the active topology. FORWARDDELAY should be at least half the time it takes for a topology change message to reach the whole network.	FORWARDDELAY - prevents temporary loops in the network occurring in the briefly unstable topology while a topology change is propagated through the network. When a port that has been in the Blocking state in a particular STP topology is to move into the Forwarding state after a topology change, it must first pass through the Listening and Learning states, during which it cannot receive or transmit packets. The FORWARDDELAY parameter determines how long the ports remain in each of the Listening and Learning states before moving on to the Forwarding state in the active topology, that is, half the time between when it is decided that the port will become part of the spanning tree, and when it is allowed to forward traffic. The FORWARDDELAY parameter should be at least half the time it takes for a topology change message to reach the whole network. A value that is too short risks the temporary creation of loops, which can seriously degrade switch performance. A longer value can result in delays in the network after topology changes. (default: 15 seconds)	15

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
FORWARDING		A forwarding mode for the interfaces	The FORWARING parameter is only applicable when the VLAN is in UPSTREAMONLY forwarding mode. The FORWARDING parameter specifies the interface's role for the VLAN: UPSTREAM, DOWNSTREAM, RING, or PROTECTIONLINK. Each VLAN that is in UPSTREAMONLY mode can have a different UPSTREAM interface. On the 7100 and 9x00 systems, there can only be one interface per VLAN that is defined as UPSTREAM. On the 7400/7700, one or both of the GE interfaces can be defined as UPSTREAM. If an interface (for a given VLAN) is defined as UPSTREAM, then all frames that are received on the other interfaces will be sent out this interface. If an interface is defined as DOWNSTREAM, then only frames that was received over the UPSTREAM interface may be switched to the DOWNSTREAM interface. If the interface is defined as RING, then either STP/RSTP or EPSR must be enabled and the enabled protocol will dynamically determine the UPSTREAM interface. If one or more interfaces are defined as PROTECTIONLINK, then the first interface that becomes operational will be the UPSTREAM interface.	For the purposes of configuring ring network topologies, pecified interfaces of a layer-2 virtual network can be configured using parameters UPSTREAM, DOWNSTREAM, RING, or PROTECTIONLINK.	
FORWARDINGMODE		Specifies the forwarding mode for a virtual network(VLAN).	The FORWARDINGMODE parameter specifies the forwarding mode for a VLAN. It can be 'Standard' or 'Upstream Forwarding Only'. In Standard mode the traffic from Service Module(SM) interfaces can go both to the other SM interfaces and the Network Module(NM) interfaces. But in Upstream Forwarding mode, the traffic from SM interfaces can only be forwarded to the UPSTREAM NM interfaces.		
FRAGMENTS		Change alert setting for fragmented packets	The FRAGMENTS parameter indicates that the rising/falling threshold values are to be used for the fragments statistical counter.		
Frame		A tagged or untagged frame header.	The FRAME parameter specifies whether a VLAN tag header is included in each frame transmitted on the specified interfaces. If TAGGED is specified, a VLAN tag is added to frames prior to transmission. The interface is then called a tagged interface for this VLAN. If UNTAGGED is specified, the frame is transmitted without a VLAN tag. The interface is then called an untagged interface for this VLAN.		
FROM for PING		That the PINGs are to be sent from somewhere other than the CFC	Followed by an INTERFACE, where the PING requests are to originate.		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
FTP SERVER		Get the file via the FTP protocol.	The FTP parameter specifies that the file should be retrieved using the FTP protocol. The SERVER parameter specifies the IP address or hostname of the host server to transfer the file from. The command fails if the specified server cannot be reached.	Abbreviation of File Transfer Protocol, a form of the File Transfer Protocol (FTP). TFTP uses the User Datagram Protocol (UDP).	
FULL		Show extra information.	The FULL parameter specifies that extra information is shown for the specified command entered.		
FULL for SHOW ALARMS		Show all alarms regardless of masking.	The FULL parameter makes SHOW ALARMS show all alarms regardless of whether or not they are masked.		
FX		Specifies that FX port(s) are being modified	The FX parameter specifies that the port to modify is a FX port on an optical fast ethernet card, and sets the context for the specified attribute values.		
FX10		10-port Optical Fast Ethernet (FX) Card.	The FX10 parameter identifies the profile as a 10-port Optical Fast Ethernet(FE) card. As an FX10 card, only FX10 card options are available to the user.	Optical Fiber-based Fast Ethernet interface (10 Ports). Provides 100 Base Fast Ethernet service for 10 ports.	
FXPORT		Set attributes for the FX (optical fast ethernet) port profile	The FXPORT parameter identifies the profile as a Optical Fast Ethernet(FX) port profile. As an FX port profile, only FX port options are available to the user.		
GATEWAY		The IP address of a gateway device.	The GATEWAY parameter specifies the address of a gateway device for the system. A gateway is needed when connecting to an external network.		
GE		Specifies that GE port(s) are being modified	The GE parameter specifies that the port to modify is a GE (gigabit ethernet) port on a gigabit ethernet card, and sets the context for the specified attribute values.		
GE1		1-port Gigabit Ethernet (GE) Card.	The GE1 parameter identifies the profile as a 1-port Gigabit Ethernet card. As a GE1 card, only GE1 card options are available to the user.	Network Module (NM). Gigabit Ethernet service 1 port. The NM interfaces the upstream equipment. The GE1 card interfaces to an upstream Ethernet switch or router over a 1 Gigabit link. ,	
GE2		Attributes for the GE2 card profile	The GE2 parameter identifies the profile as a 2-port Gigabit Ethernet(GE) card profile. As a GE2 card profile, only GE2 card options are available to the user.		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
GE3		3-port Gigabit Ethernet (GE) Card.	The GE3 parameter identifies the profile as a 3-port Gigabit Ethernet card. As a GE3 card, only GE3 card options are available to the user.	Network Module (NM). Gigabit Ethernet service 3 port. The NM interfaces the upstream equipment. The GE3 card interfaces to an upstream Ethernet switch or router over three 1-Gigabit links. Provides multiple (more than 2) upstream links, which can be used with features that require multiple links, such as LAG and STP.,	
GENQUERYTIMER	5..120	Timeout before cleaning up IGMP multicast groups from the switch	The IGMP general query timeout setting allows you to specify how long after an IGMP general query is received, before the switch cleans up any non-IGMP reporting subscriber devices. Default is 20 seconds.		20 seconds
GEPORT		Selects GE port as the component type	The GEPORT parameter identifies the profile as an Gigabit Ethernet(GE) port profile. As an GE port profile, only GE port options are available to the user.	Gigabit Ethernet port.	
GLOBAL		The global counters for the User Authentication Facility are reset.	If GLOBAL is specified, the global counters for the User Authentication Facility are reset.		
GROUP for IGMPSNOOPING TRACE			Future		
GROUPADDRESS		IP address of the reserved multicast address	IP address of the reserved multicast address being added by the user.		
GRPLIMIT		A group limit.	The GRPLIMIT parameter is used to specify the multicast group limit configured for all the line cards in the system.		
HEAP		Memory heap usage statistics	The HEAP parameter displays memory heap usage statistics. This parameter is only supported for the CFC card.	Displays memory heap usage statistics. This parameter is only supported for the CFC card.,	

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
HELLOTIME		The Hello time	The hello time for the EPSR domain.	The HELLOTIME parameter determines how often the switch sends Hello messages containing spanning tree configuration information if it is the root bridge, or is trying to become the root bridge in the network. This value determines how often the switch sends hello messages if it is the root bridge, or if it is trying to determine the root bridge identity in the network. Setting a shorter value makes the network more robust, in that network changes can be detected more rapidly. Setting a longer value reduces network traffic and processing overhead.MAXAGE (default 20 sec.) - determines the maximum time that dynamic STP configuration information is stored in the switch, before it is considered too old, and discarded. The value can be set at approximately two seconds for every hop across the network. If this value is too small, the STP may sometimes configure unnecessarily. If it is too long, there can be delays in adapting to a change in the topology, for instance when a fault occurs., 2 seconds	2
HelloTime for EPSR			The rate at which the TAPS protocol Health control message is sent by the master node for this EPSR domain.		
HELLOTIME for STP			Determines how often the switch sends Hello messages containing spanning tree configuration information if it is the root bridge, or is trying to become the root bridge in the network. Setting a shorter value for HELLOTIME than 2 seconds makes the network more robust; setting a longer time uses less processing overhead. (default: 2 seconds)		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
HISTORY		Delete performance history information	The HISTORY parameter indicates the kind of DELETE operation to be performed.		
HISTORY (for INTERFACE)		Add performance history information	The HISTORY parameter indicates the kind of ADD operation to be performed.		
hostname		The host name assigned to device.	The HOSTNAME parameter specifies a host name for the system. The host name is a character string up to 64 characters in length. The host name is translated to an IP address using a DNS server. The hostname allows users to connect to the system without having to remember the IP address associated with the management interface. The management IP address is associated with the system using the ADD IP INTERFACE command. Valid hostnames start with an alpha or digit and may contain hyphens.	The user-defined name of a network device.	
HSRP		HSRP	Hot Standby Router Protocol.		
HVLAN		An Hierarchical Virtual LAN (HVLAN) name or ID.	The HVLAN parameter specifies the name or numerical HVLAN identifier. The HVLAN must be created with the CREATE HVLAN command before it can be associated with an interface.		
IFNAME		The Interface name.	The Interface name parameter specifies a name by which the interface is identified. An interface name may not be assigned to the MGMT interface as it is fixed as 'MGMT'		
IGRP		IGRP routers	All Interior Gateway Routing Protocol routers.		
INACTCFC		INACTCFC specifies the inactive CFC card, whichever slot it is in.	INACTCFC specifies the inactive CFC card, whichever slot it is in	Inactive central fabric controller. In other words, the inactive Control Module. INACTCFC is only available in duplex systems.	
INBAND		Inband interface.	TO BE SUPPLIED	TO BE SUPPLIED	

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
INFILTERING		The ingress filtering settings.	The INFILTERING parameter enables or disables Ingress Filtering of frames admitted according to the ACCEPTABLE parameter, on the specified interfaces. Each interface on the switch belongs to one or more VLANs/HVLANs. If INFILTERING is set to ON, Ingress Filtering is enabled: any frame received on a specified interface is only admitted if the interface belongs to the VLAN/HVLAN with which the frame is associated. Conversely, any frame received on the interface is discarded if the interface does not belong to the VLAN/ HVLAN with which the frame is associated. Untagged frames admitted by the ACCEPTABLE parameter are admitted, since they have the numerical VLAN/HVLAN Identifier of the VLAN/HVLAN for which the interface in an untagged member. If OFF is specified, Ingress Filtering is disabled, and no frames are discarded by this part of the Ingress Rules. The default setting is ON.		ON
Info		Information.	The INFO parameter is used to specify that the STATUS, GRPLIMIT and MACADDRESS parameters configured for a port or ALL ports should be shown (displayed).		
INFO (for SNMP TRAP)		The informational severity SNMP traps.	The INFO parameter is used to allow or suppress delivery of traps marked as informational by the device. A value of OFF prevents delivery of informational severity traps to the specified SNMPv1 or SNMPv2 trap host.		
INFO for LAG		LAG information	The INFO parameter displays general LAG information such as interface list, speed, select criteria, and admin key. If no keyword is specified, the INFO parameter data is displayed by default.		
INITIALRETRANSMIT DELAY	100 msec	The initial retransmit delay.	The INITIALRETRANSMITDELAY parameter specifies the initial delay in milliseconds before any packet retransmission is down towards the call server.	The initial delay before any packet retransmission is done towards the call server. Units are in msec. The default value is 200 milliseconds. Note that INITIALRETRANSMITDELAY must be less than MAXRETRANSMITDELAY.	200 msec
INNERVID		The value of the inner VID to match.	The INNERVID match rule field matches on any packet with the specified value in the INNERVID identifier field of a double tagged packet. Matching on the outer VID requires use of the VID match rule.	When the HVLAN feature is used, this is the VLAN ID of the customer-based VLAN.	

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
INNERVPRIORITY		The value of the inner VLAN priority field to match.	The INNERVPRIORITY match rule field matches on any packet with the specified value in the inner VLAN priority field. Matching on the outer priority required use of the VPRIORITY match rule.	When the HVLAN feature is used, this is the value of the User Priority frame of the customer-based VLAN.	
INSERTNULL					
INSERVICE		In service diagnostics are not currently supported.	The INSERVICE parameter specifies that in-service diagnostics are performed. A card that is INSERVICE has an administrative and operational state of UP. Since the card is actively processing data, the tests run are nondestructive (not service affecting). This INSERVICE parameter is currently not supported.	Specifies that in-service diagnostics are performed. A card that is INSERVICE has an Administrative and Operational state of UP and is actively processing data. Therefore, the tests executed when this parameter is selected are nondestructive (not service affecting). INSERVICE is not currently supported.,	

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
INTERFACE		A logical representation of a port.	An Interface parameter specifies the type of physical port. Interfaces can be of various types like, ETH, PSPAN, ADSL, ATM, AAL5 or LAG. LAG type of interface can have more than one physical ports associated with it. Interfaces can be queried by using 'type:id-range', 'name-list' or 'ALL' options. For example, 'ETH:2.0', 'ETH:2.1-2.4', where 2.0,2.1 etc are the actual physical ports and are used as the interface Id's in this representation.	An interface is a capability associated with a physical port or one/many interfaces; the interface therefore provides a logical representation of one or many physical ports. A specific instance of an interface has an identifier which can be used to when configuring these capabilities. Specifies the interface or interfaces for which RMON data is to be collected. A single interface is identified using type:id (ETH:7.0), a range using type:id-range (ETH:8.0-8.9, for an FE10), or the keyword ALL may be used to specify the same historical data collection parameters on all applicable interfaces in the system. For ADD IP INTERFACE, The INTERFACE parameter specifies an existing interface on the system that carries data packets. The following are the supported interface types: - MGMT - signifies the management Ethernet port on the CFC faceplate. - type:id - signifies a virtual (switched) interface: type is vlan; and id may be either a VID or VLAN name	
INTERLEAVE		Specifies that interleaved linetype is used for a port	The INTERLEAVE parameter specifies the ADSL line type as using the interleaved path as described in ITU G.992. The interleaved path provides a low error rate but greater latency than the fast path. This parameter is only applicable to ADSL ports.		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
INTERLEAVEDELAY		Maximum interleave delay (in milliseconds)	The INTERLEAVEDELAY parameter specifies the maximum interleave delay in milliseconds used when the ADSL linetype is set to INTERLEAVE. The valid range is from 1 to 64. The default is 32. This parameter is only applicable to ADSL ports.	Specifies the maximum interleave delay in milliseconds used when the ADSL linetype is set to INTERLEAVE. The valid range is from 1 to 64. 32 is the default.	32
INTERLEAVERATEDOWN		Interleave Rate Down TCA generation threshold	The INTERLEAVERATEDOWN parameter indicates that the threshold value should be applied to either the adslAtucThreshInterleaveRateDown or adslAturThreshInterleaveRateDown statistic based on whether ATUC or ATUR were entered.		
INTERLEAVERATEUP		Interleave Rate Up TCA generation threshold	The INTERLEAVERATEUP parameter indicates that the threshold value should be applied to either the adslAtucThreshInterleaveRateUp or adslAturThreshInterleaveRateUp statistic based on whether ATUC or ATUR were entered.		
INTERVAL		The period of time between data collections in seconds (2..3600)	The INTERVAL parameter specifies the number of seconds that are to elapse between collecting one BUCKET and the next. There can be at most one data collection entry for a given interface with a specified interval value. INTERVALs may be entered as a single value for the interface(s) or a number of data collection entries may be created at one time by providing a list of intervals. Intervals can have a duration from 2 to 3600 seconds. NOTE: ALL is not a valid value for this parameter for this command.	Specifies the number of seconds that are to elapse between collecting one BUCKET and the next.	
INVENTORY		Hardware inventory for all slots.	The INVENTORY parameter specifies that hardware information is displayed for each card. The information is read from the IDPROM on the card. This parameter is useful in determining what hardware exists in the shelf regardless of whether it is provisioned in software.		
IP		Internet Protocol.	The IP parameter signifies the Internet Protocol. The CFC processor runs an IP software stack for network management communication.		
IP COUNTER		Show statistical counts for a protocol.	Shows statistical count information related to the protocol (TCP, UDP, or ICMP) specified This option indicates counter data for one of UDP,TCP or ICMP.		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
ipaddress		An IP address or list of IP addresses.	The Internet Protocol address assigned to a network entity.	Internet Protocol address assigned to a network entity. A unique identifier for a TCP/IP network element. For networks using the TCP/IP protocol, messages are routed according to the IP address of the destination.,	
IPDEST		The destination IP address to match (e.g. 10.1.1.1), or ANY.	The IPDEST match rule field matches on any IPv4 packet with the specified IP destination address. The mask field is entered separately with DESTMASK. The value ANY matches any IPv4 packet.	The destination IP address (either host or subnet) of the IP packet. IP address ranges are specified using a valid IP address or valid subnet and mask. A range is specified using a '/' character (such as 1.0.0.0/8).	
IPDSCP		The IP DSCP field value to match.	The IPDSCP match rule field matches on any IPv4 packet with the specified value in the Code Point field of the DiffServ byte of an IP packet. The value ANY matches any IPv4 packet. The IP DSCP field occupies the same location as the IP TOS field, so IPDSCP match rule conflicts with IPTOS match rule. Default is ANY.	The code point field with the DiffServ byte of an IP packet. This parameter cannot be specified with the IPTOS parameter.	ANY
IPDSCP for MGCP		The IP Differentiated Services Code Point.	The IPDSCP parameter specifies the DSCP (Differentiated Services Code Point) value for packets transmitted from the POTS card.		34
IPDSCP for PSPAN	0..63				46
IPPROTOCOL		The IP protocol field value (e.g. TCP, UDP, IGMP) to match.	The IPPROTOCOL match rule field matches on any IPv4 packet with the specified value in the protocol field of an IP packet. Any value may be specified by number. Certain common protocol values may be specified by name (TCP, UDP, ICMP, and IGMP). The value ANY matches any IPv4 packet.	The layer 4 IP protocol of the IP packet. If the command specifies a TCP/IP packet matching rule, (e.g. TCPPORTDESC is specified), then the value for this parameter will be TCP. If the command specifies a UDP/IP packet matching rule, (e.g. the UDPPORTDESC parameter is specified), then the value for this parameter will be UDP. ipprotocol-number is expressed a one byte hexadecimal or decimal number.	

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
IPSOURCE		The source IP address to match (e.g. 192.168.1.1), or ANY.	The IPSOURCE match rule field matches on any IPv4 packet with the specified IP source address. The mask field is entered separately with SOURCEMASK. The value ANY matches any IPv4 packet.	The source IP address (either host or subnet) of the IP packet. IP address ranges are specified using a valid IP address or valid subnet and mask. A range is specified using a '/' character (such as 1.0.0.0/8).	
IPTOS		The IP TOS field value to match.	The IPTOS match rule field matches on any IPv4 packet with the specified value in the "precedence" bits of the TOS field of an IP packet. The "DTR" bits of the TOS field cannot be compared using this match rule. Use IPDSCP instead. The value ANY matches any IPv4 packet. The IP TOS field occupies the same location as the IP DSCP field, so IPDSCP match rule conflicts with IPTOS match rule. Default is ANY.	The value of the precedence field within the TOS byte of an IP packet. This parameter cannot be used with the IPDSCP parameter. ANY means to accept any IPv4 packets but not other types, such as ARP. If no IPTOS (including ANY) is specified, there are no checks for the packet being an IPv packet, and so other packet types such as ARP are allowed.	ANY
JABBERS		Change alert setting for jabbers	The JABBERS parameter indicates that that the rising/falling threshold values are to be used for the jabbers statistical counter.		
JITTERBUFFER		Size of the jitter buffer in msec.			6000
KEY		TACACS+ shared key	The KEY parameter is used to specify the key that is shared with the TACACS+ server for use in authentication requests. The secret must be an alphanumeric string of 64 characters or less in length.		
L2VN		A layer-2 virtual network name or id	The L2VN parameter specifies the L2VN name or identifier. The name is case insensitive. The L2VN must already exist.		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
l2vnname|l2vnid		L2VN name.	The L2VN parameter specifies a unique name for the L2VN. The L2VN name provides a more meaningful representation than the L2VNID. The L2VN name is only used within the switch and is not transmitted to other VLAN-aware devices. In addition, the L2VN name is not used in the Forwarding Process or stored in the Forwarding Database. The L2VNID parameter specifies a unique L2VN identifier for the L2VN. If tagged ports are added to this VLAN type of L2VN, the specified L2VNID is used in the VID field of the tag in outgoing frames. If untagged ports are added to this VLAN, the specified L2VNID only acts as an identifier for the VLAN in the Forwarding Database. The default port based L2VN has a L2VNID of 1.		
LACPSTATS		LACP statistics	The LACPSTATS parameter displays LACP statistics for the LAG, such as LACP packets transmitted, received, and errored. This keyword is applicable only if LAG mode is set to active or passive (indicating that LACP is configured to run on system).		
LAG		A link aggregation group identifier	The LAG parameter identifies the Link Aggregation Group(LAG) associated with an interface. The LAG is comprised of N parallel, full duplex, point-to-point links operating at the same speed. MAC Clients then utilize the LAG as if it were a single link. The LAG is identified by a LAG ID, which can be specified at LAG creation time. If the user does not specify a LAG ID, a system-generated ID is used. To query all configured LAGs in the system, use the SHOW LAG ALL command. Select the desired LAG ID from this list to update the LAG configuration or query LAG data.		
LAG COUNTER		A link aggregation group identifier statistical counter.	The LAG parameter identifies the Link Aggregation Group(LAG) associated with a port. The LAG is comprised of N parallel, full duplex, point-to-point links operating at the same speed. MAC Clients then utilize the LAG as if it were a single link. The LAG is identified by a LAG ID, which can be specified at LAG creation time. If the user does not specify a LAG ID, a system-generated ID is used. To query all configured LAGs in the system, use the SHOW LAG ALL command. Select the desired LAG ID from this list to update the LAG configuration or query LAG data. The COUNTER parameter is specified to indicate the type of statistical counter to reset. The user can reset the Link Aggregation Control Protocol (LACP) counter, Medium Access Control (MAC) counter, or all counters.		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
LAG INFO		LAG information	The INFO parameter displays general LAG information such as interface list, speed, select criteria, and admin key. If no keyword is specified, the INFO parameter data is displayed by default.		
LAG STATE		The LACP state	The STATE parameter displays LACP administrative and operational state info for interfaces in a LAG. This keyword is applicable only if LAG mode is set to active or passive (indicating that LACP is configured).		
lag-list		A link aggregation group identifier	The LAG parameter identifies the Link Aggregation Group(LAG) associated with a port. The LAG is comprised of N parallel, full duplex, point-to-point links operating at the same speed. MAC Clients then utilize the LAG as if it were a single link. The LAG is identified by a LAG ID, which can be specified at LAG creation time. If the user does not specify a LAG ID, a system-generated ID is used. To query all configured LAGs in the system, use the SHOW LAG ALL command. Select the desired LAG ID from this list to update the LAG configuration or query LAG data.		
LAG_ID		A link aggregation group identifier	The LAG parameter identifies the Link Aggregation Group(LAG) associated with a port. The LAG is comprised of N parallel, full duplex, point-to-point links operating at the same speed. MAC Clients then utilize the LAG as if it were a single link. The LAG is identified by a LAG ID, which can be specified at LAG creation time. If the user does not specify a LAG ID, a system-generated ID is used. To query all configured LAGs in the system, use the SHOW LAG ALL command. Select the desired LAG ID from this list to update the LAG configuration or query LAG data.		
LANGUAGE		The system CLI language.	The system language displayed on the console.		
LATEPACKETS					
LEARNLIMIT		A learnlimit setting operation.	The LEARNLIMIT parameter specified the maximum number of MAC addresses can be learned for an interface.		
LENGTH		The size of the ICMP echo packet	Sets the size of the ICMP packet, in bytes, sent as part of the ping request (Default: 64 bytes).		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
LINEBUILDOUT	LONGHAUL = 0.0DB | -7.5DB | -15.0DB | -22.5DB SHORTHAUL = 133FT | 266FT | 399FT | 533FT | 655FT	Indicates that the port line build out is being set.	LONGHAUL - This parameter specifies that the LINEBUILDOUT being specified will be for a longer length and will be specified in DB. SHORTHAUL - This parameter specifies that the LINEBUILDOUT being specified will be for a shorter length and will be specified in FT.		0.0DB
LINEENCODING	B8Zs|AMI	The line encoding scheme for this port	DS1 uses B8Zs, E1 uses AMI		B8ZS
LINEQUALITYMONITOR		Desired ADSL line quality	The LINEQUALITYMONITOR parameter specifies a level of quality (amount of errors) acceptable for the ADSL or SHDSL port. If an unacceptable number of errors occurs, the port will automatically retrain. Allowed values include: - Low: Port is monitored for Data applications (approx. 10^-7 bit errors) - Medium: Port is monitored for Video applications (approx. 10^-9 bit errors) - High: Port is monitored for High Quality applications (approx. 10^-10 bit errors) The default is Medium for ADSL ports and Low for SHDSL ports. The user can set this parameter only when the port is disabled (See DISABLE PORT) This parameter is only applicable to ADSL and SHDSL ports.		MEDIUM or LOW
LINETYPE		ADSL line type	The LINETYPE parameter specifies the ADSL line type as per ITU G.992. Allowed values are FAST and INTERLEAVE, although FAST is not allowed if the MODE is GLITE. The default is INTERLEAVE. This parameter is only applicable to ADSL ports.		INTERLEAVE

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
LOCATION		Descriptive text for where the system is located.	The LOCATION parameter specifies the location information for the system. The information is a string of descriptive text for where the system is located. The maximum length is 80 characters. Valid characters are any printable character. If the string includes spaces it must be enclosed in double quotes.		
LOCKOUTPD		The number of seconds to lockout users	The LOCKOUTPD parameter sets the number of seconds to lockout a user or session after the maximum number of consecutive failed login attempts were made. The maximum number of consecutive failed logins is defined by the LOGINFAIL parameter.		
LOFS		Loss of Frame TCA generation threshold	The LOFS parameter is used to set a limit on the number of seconds loss of framing(LOF) is permitted over a fifteen minute interval before an alert is sent.		
logfile		The log file name	The name of the file where the restore logs will be written to.	Syntax is OUTPUT=	
LOGIN		The enable or disable login setting for this user. Default is YES.	The LOGIN parameter specifies whether or not the account is accessed via direct login or not. By default, the login setting is set to YES which means the account can be used immediately after it is created. A value of NO, FALSE, or OFF means that the account cannot be used to access the system.		YES
login-name			Identifies the name of the account created. It is a character string, 1 to 32 characters in length. Valid characters are uppercase letters (A-Z), lowercase letters (a-z), and decimal digits (0-9). The string may not contain spaces. The login name is case insensitive.		
LOGINFAIL		The maximum number of consecutive login failures before lockout.	The LOGINFAIL parameter determines the maximum number of consecutive login failures allowed before locking out a user or session.		
LOLS		Loss of Link TCA generation threshold	The LOLS parameter is used to set a limit on the number of seconds loss of link(LOL) is permitted over a fifteen minute interval before an alert is sent.		
LOOPBACK	NONE|INWARD|LINE	Specifies the loopback setting for this port.			NONE
LOPS					

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
LOSS		Loss of Signal TCA generation threshold	The LOSS parameter is used to set a limit on the number of seconds loss of signal(LOS) is permitted over a fifteen minute interval before an alert is sent.		
LOSTPACKETS					
LOSWS		Loss of Sync Word TCA generation threshold	The LOSWS parameter is used to set a limit on the number of seconds loss of sync word(LOSW) is permitted over a fifteen minute interval before an alert is sent.		
LPRS		Loss of Power TCA generation threshold	The LPRS parameter is used to set a limit on the number of seconds loss of power(LPR) is permitted over a fifteen minute interval before an alert is sent.		
LSAP		LSAP value to match (e.g. NETBIOS or 0x0a0a)	The LSAP match rule field matches on any packet with the specified LSAP value. LSAP refers to the combination of the SSAP and DSAP octets in an 802.3 Ethernet frame. The value may be entered in decimal or in hex but must be less than or equal to 4095 (a 16-bit value). The value "NETBIOS" can be used to specify the LSAP value for that protocol (0xF0F0). The value "ANY" matches any LSAP value.		
MACADDRESS		MACADDRESS - The MAC (Media Access Control (MAC) address) addresses assigned to the port(s).	A MAC address is a unique serial number that identifies a network element from all others. The MACADDRESS parameter is used to specify the Set Top Box (STB) MAC address for a given port. Anywhere from one to three MAC addresses can be specified.	An Ethernet six-octet MAC address, expressed as six pairs of hexadecimal digits delimited by colons. An example MAC address is "00:00:cd:00:45:c7".	
MACDEST		MAC destination address to match (e.g. 00:0C:25:00:13:8C)	The MACDEST match rule field matches on any packet with the specified MAC destination address. The value must be entered as a sequence of 6 bytes (2 hex digits each) separated by colons (e.g. 00:0C:25:00:13:8C). The "MULTICAST" can be used to match only multicast MAC addresses. The value "ANY" matches any MAC destination address.	The destination MAC address for the packet.	ANY
MACSOURCE		MAC source address to match (e.g. 00:0C:25:00:13:8C	The MACSOURCE match rule field matches on any packet with the specified MAC source address. The value must be entered as a sequence of 6 bytes (2 hex digits each) separated by colons (e.g. 00:0C:25:00:13:8C). The value "ANY" will match any MAC source address. Default is ANY.	The source MAC address.	ANY

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
MACSTATS		MAC statistics	The MACSTATS parameter displays MAC statistics for the LAG, such as MAC uni/multi/broad-cast packets received/transmitted, and octets received/transmitted counts.		
MAJOR (for SNMP TRAP)		The major severity SNMP traps.	The MAJOR parameter is used to allow or suppress delivery of traps marked as major by the device. A value of OFF prevents delivery of major severity traps to the specified SNMPv1 or SNMPv2 trap host.		
Major for Alarm Threshold		Minimum number of ports before a MAJOR alarm is raised.	Minimum number of ports before a MAJOR alarm is raised.		
MANAGER		The address of a trusted host.	Specifies a management station for this SNMP community. This is the IP address of a device from which SNMP requests with the community name are deemed to be authentic. A community may have more than one management station. IP address must be specified in dotted decimal format. A list of IP addresses can be specified as a comma separated list.		
MANAGER for LOGINBANNER		Set the loginbanner for all MANAGER users.	The MANAGER parameter indicates that the loginbanner is to be set for all MANAGER users.		
MANAGERPASSWORD		Manager ENABLE password	The MANAGERPASSWORD parameter is used to set a global password that can be used to obtain MANAGER level privileges when authenticating against the local database using the ENABLE MANAGER command. If there are RADIUS or TACACS+ servers configured and enabled, privilege escalation requests are sent to those servers first.		
MANPWDFAIL		Not currently supported	The MANPWDFAIL parameter is not currently supported.		
MASTER		The Master node type	The Master node designation in an EPSR domain. The Master node is responsible for the management of the EPSR domain.		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
MAXAGE		A change to the maximum age	The MAXAGE parameter determines the maximum time that dynamic STP configuration information is stored in the switch, before it is considered too old, and discarded. . - MAXAGE - determines the maximum time that dynamic STP configuration information is stored in the switch, before it is considered too old, and discarded. The value can be set at approximately two seconds for every hop across the network. If this value is too small, the STP may sometimes configure unnecessarily. If it is too long, there can be delays in adapting to a change in the topology, for instance when a fault occurs. (default: 20 seconds).	This value determines the maximum “age” of dynamic spanning tree configuration information (i.e. the root bridge ID, designated ports, and root ports). If this information has not been refreshed by hello messages before the timer expires, the information is discarded and the spanning tree must reconverge. If this timer is too short, the spanning tree will undergo reconvergence unnecessarily, resulting in network outages. If the timer is too long, the spanning tree may be slow to react to changes in network topology., 20 seconds, 20 seconds. The FORWARDDELAY, MAXAGE and HELLOTIME parameters should be set according to the following formulae, as specified in IEEE Standard 802.1D: 2 x (FORWARDDELAY - 1.0 seconds) >= MAXAGE MAXAGE >= 2 x (HELLOTIME + 1.0 seconds) To modify the parameters controlling these time intervals, use the command: SET STP [FORWARDDELAY=4..30] [HELLOTIME=1..10] [MAXAGE=6..40]	20
MaxConnectRate		The maximum connection bit rate to attain (in kilobytes(Kb))	The MAXCONNECTRATE parameter specifies the maximum downstream bit rate to attain for a SHDSL port. The valid range for this parameter for a port in 2-wire configuration is from 72Kb to 2312Kb in increments of 64Kb. The default is 2312Kb. This parameter is only applicable to SHDSL ports. Defines the desired maximum connection rate to attain (in Kbps). The allowed range of values are the same as for the MinConnectRate, with the additional restriction that the MaxConnectRate must be larger than the MinConnectRate. The default is 2312.		2312

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
MAXDOWNSTREAMRATE		The maximum downstream bit rate to attain (in kilobytes(Kb))	The MAXDOWNSTREAMRATE parameter specifies the maximum downstream bit rate to attain for an ADSL port. The valid range for this parameter is from 32Kb to 16128Kb for all line modes except GLITE. If the MODE is set to GLITE, then the valid range is from 32Kbto 1536Kb. The default is 10016Kb. This parameter is only applicable to ADSL ports		10016Kb
MAXPACKETIZATION		Max packetization supported in milliseconds (10..30 in steps of 10)	The MAXPACKETIZATION parameter specifies maximum number of milliseconds of voice data that can be encoded in a data packet. This value is advertised to the call agent. The maximum number of milliseconds of voice data that can be encoded in a data packet. This value is advertised to the Call Agent. The default is 20 msec. Note: To support Call Waiting with Caller ID, this attribute should be set to 10 milliseconds.	The maximum number of milliseconds of voice data that can be encoded in a data packet. This value is advertised to the Call Agent. The default is 20 msec. Note: To support Call Waiting with Caller ID, this attribute should be set to 10 milliseconds.	20 msec
MAXPROPAGATIONDELAY			Deleted in Rel 4.0.		
MAXRETRANSMITDELAY		The maximum retransmit delay.	The MAXRETRANSMITDELAY parameter specifies the maximum amount of time in milliseconds to wait for an acknowledgement from the call agent before retransmitting a packet.	Also known as RTO-MAX in RFC 3435, this is the maximum amount of time to wait for an acknowledgement from the call agent before retransmitting a packet. The default value is 20 seconds (20000 msec).	20 seconds
MAXTTL		The maximum Time To Live field in the IP header	The MAXTTL parameter in the IP header indicates maximum hops TRACEROUTE should take before terminating. Default MAXTTL is 30. Acceptable range is 1-30.		
MAXUPSTREAMRATE		The maximum upstream bit rate to attain (in kilobytes(Kb))	The MAXUPSTREAMRATE parameter specifies the maximum upstream bit rate to attain for an ADSL port. The valid range for this parameter is from 32Kb to 1024Kb for all line modes except GLITE. If the MODE is set to GLITE, then the valid range is from 32Kb to 512Kb. The default is 1024Kb. This parameter is only applicable to ADSL ports.		1024Kb

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
MCASTGROUPLIMIT		Multi-cast group limit alarm	The MCASTGROUPLIMIT parameter signifies the alarm condition associated with exceeding the threshold on the number of multicast groups allowed to be active on a card. When the threshold is exceeded, this alarm is raised against the card, and is only cleared by executing this command. The number of multicast groups for a card is configured using the SET IGMPSNOOPING command with the GRPLIMIT parameter, and is displayed using the SHOW IGMPSNOOPING command with the GRPLIMIT parameter.	Clears the Multicast Group Limit alarm., The MCASTGROUPLIMIT parameter signifies the alarm condition associated with exceeding the threshold on the number of multicast groups allowed to be active on a card. When the threshold is exceeded, this alarm is raised against the card, and is only cleared by executing this command. The number of multicast groups for a card is configured using the SET IGMPSNOOPING command with the GRPLIMIT parameter, and is displayed using the SHOW IGMPSNOOPING command with the GRPLIMIT parameter. MCASTGROUPLIMIT, MCASTGROUPLIMIT	
MCASTGROUPLIMIT for ALARMS		Multi-cast group limit alarm	The MCASTGROUPLIMIT parameter signifies the alarm condition associated with exceeding the threshold on the number of multicast groups allowed to be active on a card. When the threshold is exceeded, this alarm is raised against the card, and is only cleared by executing this command. The number of multicast groups for a card is configured using the SET IGMPSNOOPING command with the GRPLIMIT parameter, and is displayed using the SHOW IGMPSNOOPING command with the GRPLIMIT parameter.		
MCASTGROUPLIMIT for IGMP		A multicast group limit to use for the card(s)	The MCASTGROUPLIMIT parameter is used to configure the number of multicast IP streams that can be directed towards a line card.		
MCASTGROUPS		Displays the currently subscribed multicast group(s)	The MCASTGROUPS parameter is used to display the current multicast group(s) that are subscribed either for the entire switch.		
MDNS			Multicast Domain Name Server.		
MEDIA		CFLASH#, where # is the slot number of the parent card.	The compact flash card to be formatted, specified using the format CFLASH#, where # is the slot number of the parent card.		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
MEMORY		Memory usage statistics	The MEMORY parameter displays memory usage statistics. This parameter is only supported for the CFC card.	This parameter is only supported for the CFC card.	
MESSAGE		Text description for the alarm associated with the trigger	The MESSAGE parameter specifies a text description for the alarm associated with the trigger. This text is used in log output and is shown in the SHOW ALARMS command.	Specifies a text description for the alarm associated with the trigger. This text is used in log output and is shown in the SHOW ALARMS command. Place the message within quotes (“). For example “Open Door”.,	
MESSAGE for CONTACTALARM		Text description for the alarm associated with the trigger	The MESSAGE parameter specifies a text description for the alarm associated with the trigger. This text is used in log output and is shown in the SHOW ALARMS command.		
MESSAGE for DEACTIVATE SESSION		The message text to send to user scheduled for deactivation.	The MESSAGE parameter provides a text message for scheduled deactivation requests. The message is a quoted string that explains why deactivation is occurring. (e.g. MESSAGE="Log off now for system maintenance")		
MESSAGE TEXT		The text string to be sent to the destination session windows.	The MESSAGE parameter has an associated text string that is displayed on sessions listed in the SESSION parameter. Any printable character allowed with the exception of '#', which is identified as a comment character.		None
MESSAGEBUFFERS		Memory message buffer usage statistics	The MESSAGEBUFFERS parameter displays memory message buffer statistics. This parameter is only supported for the CFC card.	Displays memory message buffer statistics. This parameter is only supported for the CFC card.,	
MESSAGERESPONSE		Resets the IGMP snooping 'message response' counters/statistics	Resets the IGMP snooping 'message response' counters/statistics, these counter/statistics help in determining channel change response time.		
MESSAGETYPE for EPSR Trace					
MESSAGETYPE for IGMPSNOOPING TRACE		IGMPSNOOPING TRACE message type.		One of REPORT, LEAVE, QUERY, OSPFMCHELLO, DVMRP, PIMV1, PIMV2, ALL.	

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
MGMT		Management	Management. Signifies the management Ethernet port on the CFC faceplate.	The MGMT Ethernet interface that transports only management data packets.	
MinConnectRate		The minimum connection bit rate to attain (in kilobytes(Kb))	The MINCONNECTRATE parameter specifies the minimum downstream bit rate to attain for a SHDSL port. The valid range for this parameter for a port in 2-wire configuration is from 72Kb to 2312Kb in increments of 64Kb. The default is 72Kb. This parameter is only applicable to SHDSL ports.	Defines the desired minimum connection rate to attain (in Kbps). The allowed range of values in 2-wire configuration is 72 to 2312, in increments of 64.	72
MINDOWNSTREAMRA TE		The minimum downstream bit rate to attain (in kilobytes(Kb))	The MINDOWNSTREAMRATE parameter specifies the minimum downstream bit rate to attain for an ADSL port. The valid range for this parameter is from 32Kb to 16128Kb for all line modes except GLITE. If the MODE is set to GLITE, then the valid range is from 32Kb to 1536Kb. The default is 32Kb. The MINDOWNSTREAMRATE must be less than the MAXDOWNSTREAMRATE. This parameter is only applicable to ADSL ports..		32
MINOR (for SNMP TRAP)		The minor severity SNMP traps.	The MINOR parameter is used to allow or suppress delivery of traps marked as minor by the device. A value of OFF prevents delivery of minor severity traps to the specified SNMPv1 or SNMPv2 trap host.		
MINOR for Alarm Threshold		Minimum number of ports before a MINOR alarm is raised.	Minimum number of ports before a MINOR alarm is raised. Setting minor to anything greater than one is allowed but not recommended. That means that (MINOR - 1) ports can be out of service before the threshold alarm is raised.		
MINPACKETIZATION		Min packetization supported in milliseconds (10..30 in steps of 10)	The MINPACKETIZATION parameter specifies the minimum number of milliseconds of voice data that can be encoded in a data packet. This value is advertised to the call agent.	The minimum number of milliseconds of voice data that can be encoded in a data packet. This value is advertised to the Call Agent. The default is 20 msec. Note: To support Call Waiting with Caller ID, this attribute should be set to 10 milliseconds.	20 msec
MINPWDLEN		The minimum password length 6 to 23 characters.	The MINPWDLEN parameter specifies the minimum number of characters a user password is allowed to contain. This parameter affects setting of password in CLEARTEXT format or via the SET PASSWORD command.		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
MINTTL		The Minimum Time To Live in the IP header	The MINTTL parameter indicates that data after MINTTL hops must be displayed back to the user. Default MINTTL is 1. Acceptable range is a value in the range 1-30.		
MINUPSTREAMRATE		The minimum upstream bit rate to attain (in kilobytes(Kb))	The MINUPSTREAMRATE parameter specifies the minimum upstream bit rate to attain for an ADSL port. The valid range for this parameter is from 32Kb to 1024Kb for all line modes except GLITE. If the MODE is set to GLITE, then the valid range is from 32Kb to 512Kb. The default is 32Kb. The MINUPSTREAMRATE must be less than the MAXUPSTREAMRATE. This parameter is only applicable to ADSL ports.		32kB
MODE		The ADSL line mode	The MODE parameter specifies the ADSL line mode standard. Allowed values include: - ADSL2+ : ADSL2+ (ITU G.992.5) - GLITE : G.Lite (ITU G.992.2) - GDMT : G.DMT (ITU G.992.1) - T1.413 : ANSI T1.413 Issue 2 - AUTO : multimode, where the choice of G.lite, G.dmt, or T1.413 is auto negotiated with the remote peer The default is AUTO. The user can set this parameter only when the port is disabled (See DISABLE PORT) This parameter is only applicable to ADSL ports.		Auto
MODE of LAG		A Link Aggregation Group mode	The MODE parameter controls behavior of the Link Aggregation Group (LAG). The following describes each of the modes: - OFF - disables aggregation for the interfaces in the LAG. This is the default LAG mode. - ON - specifies that the interfaces belonging to the LAG do not have the Link Aggregation Control Protocol (LACP) running. For aggregation to work, the interfaces in the LAG must be connected to interfaces in a LAG on the other end, that is also in the ON mode. This is "statically configured link aggregation". - PASSIVE - causes the interfaces in the LAG to respond to LACP packets, but does not initiate LACP negotiation. The interfaces will speak LACP only when spoken to. This is "passive dynamically configured link aggregation". - ACTIVE - causes interfaces in the LAG to initiate LACP negotiation with the interfaces in the LAG it is connected to, by sending LACP packets. This is "dynamically configured link aggregation".		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
MOVEPRIOTOTOS		On a match, copy the outer VLAN priority field to the IP TOS field.	On a CLASSIFIER match, copy the outer VLAN priority field to the IP TOS field. This action conflicts with the SETIPTOS and SETIPDSCP ACTIONs, because they both modify the same location in the IP packet. This action also implies a FORWARD ACTION, and so it conflicts with the DROP ACTION. This action requires that one or more of the match rules on the classifier qualifies the packet as an IP packet.	MOVEPRIOTOTOS copies the 802.1q priority field to the IP TOS field,	5
MOVETOSTOPRIO		On a match, copy the IP TOS field to the outer VLAN priority field.	On a CLASSIFIER match, copy the IP TOS field to the outer VLAN priority field. This action conflicts with the SETVLANPRIORITY ACTION, because they both modify the same field in the packet. Also implies a FORWARD ACTION, and so it conflicts with the DROP ACTION. This action requires that one or more of the match rules on the classifier qualifies the packet as an IP packet.	MOVETOSTOPRIO copies the IP TOS field to the 802.1q priority field. This new value will determine selection of the egress CoS queue.,	
MSG		Message	Used by STP debug for messaging.	STP debug message parameter	
MULTICAST		Change alert setting for multicast packets	The MULTICAST parameter indicates that that the rising/falling threshold values are to be used for the multicast packets statistical counter.		
NAME		Descriptive text for the name of the system.	The NAME parameter specifies a string defining the name of the system. The name can be a maximum of 80 characters. If the string includes spaces it must be enclosed in double quotes. By convention, this is the full domain name of the IP entity ("hostname.domainname").		
NCCOUNT		Count (ON) or not count (OFF) non-conforming packets.	When NCCOUNT is ON, any packets identified by the CLASSIFIER that exceed the limits of the TRAFFICDESCRIPTOR increment the "Policed Count". This value defaults to OFF.		
NCDROP		Action to drop non-conforming packets.	Adds the ability to drop all non-conforming packets to the traffic descriptor.		
NCFORWARD		Action to forward non-conforming packets.	Instructs the traffic descriptor to forward all non-conforming packets.		
NODIAGS		Do not perform out of service diagnostics.	The NODIAGS parameter signifies that out of service diagnostics will not run during the enable sequence. Out of service diagnostics are run by default unless this parameter is provided.	Out of service diagnostics will not run during the enable sequence. Out of service diagnostics are run by default unless this parameter is provided. Default is DIAGS.	

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
NORESOLVE		Do not DNS resolve	The NORESOLVE parameter if specified indicates to TRACEROUTE that DNS resolution of ip addresses to hostnames is not required. This can speed up the TRACEROUTE program. The default is to DNS resolve.		DNS resolve
NUMBER		The number of ping requests to perform	Indicates the number of ping requests to send to the specified host. To stop the ping operation before all attempts are given or to stop continuous pinging, use the STOP PING command.		
NUMBYTES	16..1023	Number of bytes per packet	Default is 192 (DS1), 256 (E1)		
OCTETS		Change alert settings for octets	The OCTETS parameter indicates that the rising/falling threshold values are to be used for the octets statistical counter.		
OFF (for INTERFACE COUNTER)		Disables network monitoring	The OFF parameter indicates that network monitoring is to be disabled for the specified interface or interfaces. This only affects network monitoring and in no way changes the state of the interface itself.		
ON (for INTERFACE COUNTER)		Enables network monitoring	The ON parameter indicates that network monitoring is to be enabled for the specified interface or interfaces. This only affects network monitoring and in no way changes the state of the interface itself.		
OPEN		The trusted host setting for the SNMP community	The OPEN parameter when set to ON allows access using this community from any management station. When set to ON, the agent will accept requests from any host (the trusted host list is ignored). When set to OFF, the device performs the trusted host check and only MANAGERs associated with the community are allowed access (assuming the community is enabled). ON, TRUE and YES are equivalent. OFF, FALSE and NO are equivalent.		OFF
OSPFALL		All OSPF routers	All OSPF routers		
OSPFDESIGNATED		Designated OSPF routers	Designated OSPF routers		
OTHER		The unclassified SNMP trap	The OTHER parameter is used to allow or suppress delivery of traps that are otherwise uncategorized. A value of OFF prevents delivery of uncategorized traps to the specified SNMPv1 or SNMPv2 trap host.		
OTHER (for SNMP TRAP)		The unclassified SNMP traps	The OTHER parameter is used to allow or suppress delivery of traps that are otherwise uncategorized. A value of OFF prevents delivery of uncategorized traps to the specified SNMPv1 or SNMPv2 trap host.		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
OUTOFSERVICE		Out of service	The OUTOFSERVICE parameter specifies that out of service diagnostics are performed. A card that is OUTOFSERVICE has an operational state of DOWN.	Specifies that out of service diagnostics are performed. A card that is OUTOFSERVICE has an operational state of DOWN. Default is OUTOFSERVICE.	
OUTPUT				System output.	
OUTPUT for LOG FILTER		The name of output destination	The OUTPUT parameter provides the name of the management log output destination to associate with the management log filter. The output destination specified must already exist (See CREATE LOG OUTPUT)		
outputid		Output ID	The OUTPUT parameter provides the name of the management log output destination to change. This value must be the name of an existing management log output destination.	The output destination specified must already exist. This value must be an alphanumeric string between 1 and 23 characters long. (See CREATE LOG OUTPUT).	
OVERSIZE		Change alert setting for oversize packets	The OVERSIZE parameter indicates that that the rising/falling threshold values are to be used for the oversized packets statistical counter.		
PACKETLOSSCONCEALMENT		Packet Loss Concealment capability for POTS (ON or OFF)	The PACKETLOSSCONCEALMENT parameter specifies whether packet loss concealment is enabled. Packet loss concealment is a technique used on the receive side of the voice packet stream to mask the effect of lost or discarded packets.	If not used, users may report difficulty in understanding speech due to short gaps.	ON
PACKETS		Change alert setting for packets	The PACKETS parameter indicates that that the rising/falling threshold values are to be used for the packets statistical counter.		
PASSWORD		Password for GET FILE.	The PASSWORD parameter is used to specify the password that should be used for retrieving the file.	The User’s password. Note: This parameter is used with database commands.	
PASSWORD FORMAT		The format of password entered. Default is CLEARTEXT.	The FORMAT parameter defines the type of password specified. If the FORMAT parameter is not provided, the password is assumed to be clear text. If MD5 is specified for the format, the password is assumed to be pre-encrypted as a 32 character MD5 digest.		CLEARTEXT

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
PASSWORD OF LOGIN USER		The password in cleartext or MD5 format.	The PASSWORD parameter specifies the initial user password for the account. The password, in conjunction with the login-name, provide the means to access the device. The password may be specified as either clear text or MD5 digest. If an MD5 digest is provided, FORMAT=MD5 must also be specified. Case sensitive.		
PATH		The path on the network server where the preferred software load is located.	The PATH parameter identifies the directory path on the network server from which the preferred software load is retrieved. If the path on the network server includes spaces then the entire PATH must be enclosed in double quotes ("). For example, SET BOOTSERVER PATH "\Program Files\My Loads\"	The explicit directory path to an entity on a network server.	
PATHCOST		Change path cost.	The PATHCOST parameter is used to change the path cost for the interface. The following tables list some standard port speeds and identifies the default path cost value and the range of recommended values as a guide for STP and RSTP modes: STP Mode: Port speed Default PATHCOST Recommended PATHCOST range -- 4 Mbps 250 100 - 1000 10 Mbps 100 50 - 600 100 Mbps 19 10 - 60 1 Gbps 4 3 - 10 RSTP Mode: Port speed Default PATHCOST Recommended PATHCOST range -- 1 Mbps 20000000 2000000 - 200000000 10 Mbps 2000000 200000 - 20000000 100 Mbps 200000 20000 - 2000000 1 Gbps 20000 2000 - 200000	NOTE: when changing protocol modes from RSTP (or STP compatible) to original STP, all path cost values greater than 16-bits in value will be set to 65535 to conform to IEEE Std 802.1d, 1998. Setting the path cost to a larger value on a particular interface is likely to reduce the traffic over the LAN connected to it. This may be appropriate if the LAN has lower bandwidth, or if there are reasons for limiting the traffic across it. To modify the STP interface path cost, use the command: SET STP INTERFACE={type:id-range|id-range|ifname-list|ALL} PATHCOST=path-cost If the path cost of an interface has been explicitly set to a particular value, it can be returned to its self-adjusting default path cost and priority, using the command: SET STP INTERFACE={type:id-range|id-range|ifname-list|ALL} DEFAULT	
PEERIPADDRESS		Matches the IP address the far end of the PSPAN.			

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
PEERUDPPORT		Matches with the peer's UDPPORT attribute, the local transmit ID.	Must be unique within an IP address on a card. This value is placed in the UDP destination port for packets that are transmitted and is expected in the UDP source port for packets that are received for this pseudo-span.		
PERMIT		Allow packets matching this RULE to pass.	Allow packets matching this RULE to pass.		
PERSISTTIMER		The statistic persistence interval	The PERSISTTIMER parameter sets the persistence interval for system counters. The value is specified in minute increments.		
PIM			Protocol Independent Multicast address.		
PKT		Packet	Used by STP debug for packets.	STP debug message parameter	
PKTS1024TO1518OCTETS		Change alert settings for packets that are 1024 to 1518 octets long	The PKTS1024TO1518OCTETS parameter indicates that that the rising/falling threshold values are to be used for the statistical counter for packets 1024 to 1518 octets long.		
PKTS128TO255OCTETS		Change alert settings for packets that are 128 to 255 octets long	The PKTS128TO255OCTETS parameter indicates that that the rising/falling threshold values are to be used for the statistical counter for packets 128 to 255 octets long.		
PKTS256TO511OCTETS		Change alert settings for packets that are 256 to 511 octets long	The PKTS256TO511OCTETS parameter indicates that that the rising/falling threshold values are to be used for the statistical counter for packets 256 to 511 octets long.		
PKTS512TO1023OCTETS		Change alert settings for packets that are 512 to 1023 octets long	The PKTS512TO1023OCTETS parameter indicates that that the rising/falling threshold values are to be used for the etherStatsPkts512to1023Octets statistical counter.		
PKTS64OCTETS		Change alert settings for packets that are up to 64 octets long	The PKTS64OCTETS parameter indicates that that the rising/falling threshold values are to be used for the statistical counter for packets up to 64 octets long.		
PKTS65TO127OCTETS		Change alert settings for packets that are 65 to 127 octets long	The PKTS65TO127OCTETS parameter indicates that that the rising/falling threshold values are to be used for the etherStatsPkts65to127Octets statistical counter.		
PMONALERT		Indicates that this command has to do with PMON Alerts	The PMONALERT parameter indicates that this command is used to set alert entries for PMON.		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
PMONSTATISTIC		The name of a performance monitoring(PMON) statistic.	The PMONSTATISTIC parameter identifies the name of a performance monitoring(PMON) statistic which is already monitored. The following are valid values for a PMONSTATISTIC name: - adslAtucThresh15MinLOFs - adslAtucThresh15MinLOSs - adslAtucThresh15MinLOLs - adslAtucThresh15MinLPRs - adslAtucThresh15MinESs - adslAtucThreshFastRateUp - adslAtucThreshInterleaveRateUp - adslAtucThreshFastRateDown - adslAtucThreshInterleaveRateDown - adslAturThresh15MinLOFs - adslAturThresh15MinLOSs - adslAturThresh15MinLPRs - adslAturThresh15MinESs - adslAturThreshFastRateUp - adslAturThreshInterleaveRateUp - adslAturThreshFastRateDown - adslAturThreshInterleaveRateDown - adslAtucThreshold15MinFailedFastR - adslAtucThreshold15MinSesL - adslAtucThreshold15MinUasL - adslAturThreshold15MinSesL - adslAturThreshold15MinUasL Default is 15 minutes and 24 hours.		
POINT2POINT		Interface connection to be treated as direct vs. shared vs. auto detect which type.	Indication of whether to treat interface as a point-to-point connection vs. shared medium connection vs. apply automatic detection criteria (default = auto detection).		
PORT		A port on a card in slot.port format	The PORT parameter specifies the port or list or ports to disable. A port is identified using slot.port format. For example, port 1.1 signifies port 1 on card 1. The first port on any card is port 0. The port-list is either: - a single port - a comma-separated list of ports - a dash range of ports - a combination of dash and comma-separated ports	Specifies a port on a card in a specific slot on the shelf.	
PORT COUNTER		Specifies the network monitoring system	The COUNTER parameter identifies the category of monitoring statistic. RMON is the only valid value for resetting remote monitoring statistics on Ethernet ports. To reset port faults, use the FAULT option. To reset qos egress counters on ADSL ports, use QUEUE option.		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
PORT, port-list		The port or list of ports.	The PORT parameter specifies the port or list or ports to disable. A port is identified using slot.port format. For example, port 1.1 signifies port 1 on card 1. The first port on any card is port 0. The port-list is either: - a single port - a comma-separated list of ports - a dash range of ports - a combination of dash and comma-separated ports	The convention for specifying a module is by its slot number, and for any associated port by its slot.port number. For example, to specify port 1 on a module in slot 4, use 4.1. Port or port list. The port-list is either: - a single port, in the format slot.port - a comma-separated list of ports - a dash range of ports - a combination of dash and comma- separated ports - all ports	
PORTPRIORITY		Change port priority (see detailed help for ranges)	The PORTPRIORITY parameter is to modify the priority settings for an interface or interfaces.		
PORTS		The status of all ports.	The PORTS parameter displays port status and alarm information. This parameter is only supported for the ADSL, GE, FE, and FX cards.		
PORTTYPE	DS1|E1	The type of port, either DS1 or E1, to be utilized for the card.	All ports on the card will be of the same type. The user must DISABLE the card to change the mode. Changing the PORTTYPE effectively destroys the card and creates a new card with the new port types.		DS1
PRECEDENCE		The PRECEDENCE of this CLASSIFIER on this PORT.	The value of the PRECEDENCE parameter indicates whether actions from this CLASSIFIER are performed when other matching CLASSIFIERS have actions that conflict with the actions on this CLASSIFIER. In this case, actions from the CLASSIFIER with the higher PRECEDENCE (smaller numeric value) are performed, along with any actions from other matching CLASSIFIERs that do not conflict with those actions. Some PRECEDENCE values are reserved for internal use (e.g. for IGMP snooping). CLASSIFIERS for Filtering should use PRECEDENCE values between 51 and 69. CLASSIFIERS for setting fields in the packets should use PRECEDENCE values between 146 and 199.		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
PREFLOAD		The preferred software load for the card.	The PREFLOAD parameter specifies the name of the preferred software load file for the card. This file must reside on the CFC flash file system, and is loaded to the flash memory on the card (if it's not already there) when the card is enabled or reset. (Note that since the GE1 and GE3 do not contain FLASH memory, there is no PREFLOAD option for them.) There is no default value for the prefload. The command is rejected if the preferred software load specified is not compatible with the specified card.	A load designated as PREFLOAD indicates that this is the primary load that the specified card will load from. Preferred - A load designated as PREFLOAD indicates that this is the primary load that the specified card will load from. For system integrity reasons, load files designated as PREFLOAD cannot be renamed or deleted. Any changes made in load designations, for a system configured for duplex operation, while the system is operating in sync, will be reflected on both the ACTCFC and INACTCFC. Load preferences for the CFC(s) are stored in the non-volatile RAM (NVRAM) of each CFC, while load preferences for the Service Modules are stored in the configuration database.	

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
PRIORITY		A change to bridge priority	The PRIORITY parameter is used to set the writable portion of the bridge ID.	The value of the PRIORITY parameter is used to set the writable portion of the bridge ID, i.e. the first two octets of the (8-octet long) Bridge Identifier. The remaining 6 octets of the bridge IDs are given by the MAC address of the switch. The Bridge Identifier parameter is used in all Spanning Tree Protocol packets transmitted by the switch. The first two octets, specified by the PRIORITY parameter, determine the switch's priority for becoming the root bridge or a designated bridge in the network, with a lower number indicating a higher priority. In fairly simple networks, for instance those with a small number of switches in a meshed topology, it may make little difference which switch is selected to be the root bridge, and no modifications may be needed to the default PRIORITY parameter, which has a default value of 32768. In more complex networks, one or more switches are likely to be more suitable candidates for the root bridge role, for instance by virtue of being more central in the physical topology of the network. In these cases the STP PRIORITY parameters for at least one of the switches should be modified.	

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
PRIVILEGE		Privilege level of the user.	The PRIVILEGE parameter determines the access rights given to the user. There are three privilege levels available. The levels are identified as follows: USER - Basic access to read/view information but can only effect changes on his/her session MANAGER - Has all of the privileges of USER but has the added ability to change system settings and configuration. A MANAGER cannot, however, perform any actions that affect system security. SECURITYOFFICER - Has the ability to perform any action on the system including those that affect system security		
PROFILE		The profile to use in setting attributes for the card and its ports	The PROFILE parameter specifies the name of the profile used to provision the card. A profile contains a set of pre-defined provisioning attributes. The contents of a profile can be displayed (SHOW PROFILE) and changed (SET PROFILE). For this release, only the AutoProv profile for autoprovisioning is supported.	A profile is a template that contains the provisioning data. In this release, there is one only one profile, called AUTOPROV (for Auto-provisioning), which contains at first the factory defaults, but any or all attributes can be changed. This is the profile used for the Auto Provisioning Mode. When the system is first initialized, the system's PROVMODE is set to AUTO, and all Modules come up with the profile name AUTOPROV. Modification of a profile does not change the attributes of a card/port that has already been provisioned., AUTOPROV	
PROGRESSINDICATION		The progress indication trap category	The PROGRESSINDICATION parameter is used to allow or suppress delivery of progress indication traps. A value of OFF prevents delivery of progress indication traps to the specified SNMPv1 or SNMPv2 trap host.		
PROTECTIONGROUP		Name of the protection group.	Name of the protection group, any text string except for ALL.		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
PROTOCOL		Protocol Version to run (i.e., STP or RSTP)	The PROTOCOL parameter identifies which version of the Spanning Tree Protocol to run - original STP, Rapid Spanning Tree (RSTP), or an STP compatible version of RSTP. [default = RSTP	The choice of protocol version should be made based upon what version of Spanning Tree is being run on all the other bridges in the network. RSTP should be used when most of the other bridges in the network are also running RSTP and rapid convergence is desired following changes to the network topology. One of the two STP choices should be selected when most of the bridges in the network are NOT running RSTP, or when at least one of the bridge in the network that is running STP does not appear to be working correctly. The difference between the two STP choices is that the "original STP" protocol is based upon IEEE 802.1D, 1998 edition "The Spanning Tree Algorithm and Protocol", whereas STP compatible RSTP is based upon IEEE P802.1D/D3, June 11, 2003. These two choices should be functionally equivalent. note: The original STP is currently being maintained to provide an additional configuration setup option for communicating with older versions of the Spanning Tree Protocol.	RSTP
PROTOCOL (for ACCESSLIST)		The value of the layer 2 "protocol" field to match.	The PROTOCOL match rule field matches on any packet with the specified layer 2 "protocol" field value. The value of this field indicates which layer 3 protocol is being carried. Any value may be specified as a number. However, certain common protocols (e.g. IPV4, IPV6) may be entered by name.		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
PROTOCOL OF CLASSIFIER		The value of the layer 2 "protocol" field to match.	The PROTOCOL match rule field matches on any packet with the specified layer 2 "protocol" field value. The value of this field indicates which layer 3 protocol is being carried. Any value may be specified as a number. However, certain common protocols (e.g. IPV4, IPV6) may be entered by name.	The type field of the payload.	
PROVMODE		The system provisioning mode.	The PROVMODE parameter specifies the system provisioning mode. The provisioning mode determines how hardware devices are introduced to the system software. There are two different provisioning modes allowed: - AUTO: In auto provisioning mode, removable hardware devices are automatically discovered and provisioned either upon insertion or upon system startup. The provisioning is persisted in the CFC database until manually destroyed using CLI commands (DESTROY CARD for example). Auto provisioning is the default mode for the system. - MANUAL: In manual provisioning mode, all provisioning is performed through the use of CLI commands (CREATE CARD for example). Hardware devices are not automatically provisioned upon card insertion or upon system startup. The manually entered provisioning data is persisted in the CFC database until manually destroyed using CLI commands (DESTROY CARD for example).	NOTE: some cards (active CFC and FC) are automatically provisioned even in manual mode, and cannot be destroyed using CLI commands.	
PSPAN					
PSPANID	The ID withign the IP interface	The number (up to 8) of PSPANs that can be created withing the IP interface.			
PUBLICKEY		n/a	n/a	n/a	
QUEUECOUNT		ADSL egress queue counts	Refers to the current egress queue counts for all ADSL interfaces identified with the INTERFACE parameter. This option has no effect on non-ADSL interfaces.		
QUICKHEAP		Memory quick heap usage statistics	The QUICKHEAP parameter displays memory quick heap usage statistics. This parameter is only supported for the CFC card.	Displays memory quick heap usage statistics. This parameter is only supported for the CFC card.,	

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
Rate		The RATE to which traffic must be limited (in bits per second).	The RATE parameter specifies the rate to which transmitted traffic must be limited (in bits per second). The rate may exceed this value for up to the specified BURSTSIZE for a brief time. The value must be a non-zero multiple of 8K bits-per-second. The value may have a suffix of "K" (meaning times 1,000) or "M" (meaning times 1,000,000).	Specifies the allowable bandwidth for conforming traffic.	
REMOTEID		The DHCP Relay agent's remote Id.	The REMOTEID is used by DHCP Servers to identify the Relay Agent.	Used by DHCP servers to identify a RELAY AGENT. Setting this parameter is optional. The default is the MAC address of the switch the RELAY AGENT is running on. The user can specify the REMOTEID by entering a string of 1 to 31 ASCII characters.	
RETRANSMITDELAY			Changed to INITIALRETRANSMITDELAY.		
RETRIES		Number of reties for each authentication request	The RETRIES parameter specifies the number of times a user authentication request should be retried. Once the maximum number of retries has been reached without a response from the RADIUS server, the next RADIUS or TACACS+ server or local database is consulted to determine the validity of the authentication attempt.		
REVERSE		Reverses the normal order of management log display	Reverses the normal order of management log display, displaying the management logs in oldest to newest order.		
RINGFLAPTIME		For future use.	For future use.		
RIP2			Routing Information Protocol 2.		
RISINGTHRESHOLD		The value for the RMONSTATISTIC rising threshold.	The RISINGTHRESHOLD parameter specifies the upper limit of a monitored statistic before an event is generated. When the rising threshold is crossed, a management log is generated along with an SNMP trap (assuming SNMP support is configured for the system).		
RMONALERT		Indicates that this command has to do with RMON Alerts	The RMONALERT parameter indicates that this command is used to create alert entries for RMON.		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
RMONSTATISTIC		The name of a remote monitoring(RMON) statistic.	The RMONSTATISTIC parameter identifies the name of the remote monitoring statistic to add. The following are valid remote monitoring statistic names: - etherStatsDropEvents - etherStatsOctets - etherStatsPkts - etherStatsBroadcastPkts - etherStatsMulticastPkts - etherStatsCRCAlignErrors - etherStatsUndersizePkts - etherStatsOversizePkts - etherStatsFragments - etherStatsJabbers - etherStatsCollisions - etherStatsPkts64Octets - etherStatsPkts65to127Octets - etherStatsPkts128to255Octets - etherStatsPkts256to511Octets - etherStatsPkts512to1023Octets - etherStatsPkts1024to1518Octets		
ROUTE		The IP Routing Table.	Allows the user to specify which IP Routes they want to see either by entering a comma separated list of IP Addresses, or the key-word ALL. Not entering anything after the "ROUTE" parameter is the same as using the ALL key-word. This option displays the routing table available.		
ROUTERAGEINGTIMER		Timeout before cleaning up a learned IGMP multicast router from the switch	The IGMP multicast router timeout setting specifies how long to wait before cleaning up ALL IGMP related information associated with a learned multicast router. If no multicast related packets have been received, on the port we learned the router on, (IGMP general query packets, OSPF multicast hello, PIMv1/PIMv2, or DVMRP), all associated IGMP information will be cleaned up. Default is 300 seconds (5 min).		300 sec.
RSTPCHECK		RSTP Check	The RSTPCHECK parameter indicates that migration check for RSTP protocol is enabled for the specified interfaces.		
RSVP			Resource Reservation Protocol.		
RTP	ON|OFF	Whether the RTP header is included or not			ON
RULE		Add a RULE to this ACCESSLIST	The RULE field is followed by an action (PERMIT or DENY) and the match rule to act on.		
SCRIPT		A command line interface(CLI) script	The SCRIPT parameter identifies the name of a file that contains CLI commands.		
SECRET		RADIUS shared secret	The SECRET parameter is used to specify the secret that is shared with the RADIUS server for use in authentication requests. The secret must be an alphanumeric string of 64 characters or less in length.		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
SECUREDELAY		The number of minutes for session idle time timeout	The SECUREDELAY parameter specifies the number of minutes that a user session can remain idle before it is automatically timed out.		
SECURITYOFFICER for LOGINBANNER		Set the loginbanner for all SECURITYOFFICER users.	The SECURITYOFFICER parameter indicates that the loginbanner is to be set for all SECURITYOFFICER users.		
SECURITYOFFICERPASSWORD		Securityofficer ENABLE password	The SECURITYOFFICERPASSWORD parameter is used to set a global password that can be used to obtain SECURITYOFFICER level privileges when authenticating against the local database using the ENABLE MANAGER command. If there are RADIUS or TACACS+ servers configured and enabled, privilege escalation requests are sent to those servers first.		
SELECT		The select criteria for hashing.	The SELECT parameter specifies the select criteria used by the internal hashing algorithm to determine frame distribution among interfaces in the LAG. Frames are distributed based on one of the following sources: - MACSRC - Source Medium Access Control (MAC) address - MACDEST - MAC destination address - MACBOTH - Combination of MAC source and MAC destination addresses - IPSRC - Internet Protocol (IP) source address - IPDEST - IP destination address - IPBOTH - Combination of IP source and IP destination addresses - PORTSRC - Source port number - PORTDEST - Destination port number		
SEQUENCE		Management logs sequence number.	Allows for the display of management logs that match the specified range of sequence numbers. Sequence number ranges can be either a single sequence number, an explicit range of sequence numbers (e.g., 100-200) or an operation-specified range of sequence numbers (e.g., < - less-than - displays all logs with a sequence number less than or equal to the given sequence number. > - greater-than - displays all logs with a sequence number greater than or equal to the given sequence number.		
SERVER		A DHCP server	A DHCP server IP address where DHCP messages from the client will be forwarded by the relay agent.	The IP address or hostname of the server.	
SERVER (for RADIUS)		IP address(es) or hostname(s) of RADIUS servers to add	The SERVER parameter is used to specify one or more IP addresses or hostnames to send RADIUS authentication requests to.		
SERVER (for SNTP)		IP address or hostname of the SNTP server	The SERVER parameter specifies the IP address or hostname of the SNTP server.		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
SERVER (for TACPLUS)		IP address(es) or hostname(s) of TACACS+ servers to add	The SERVER parameter is used to specify one or more IP addresses or hostnames to send TACACS+ authentication requests to.		
serverpath		Absolute path to the server			
SES		Severely Errored Seconds TCA generation threshold	The SES parameter is used to set a limit on the number of allowed severely errored seconds over a fifteen minute interval.		
session-list		The list of session id numbers to send the message to.	The SESSION parameter identifies the list of session id numbers to which messages are sent. Valid session id numbers are found by running the SHOW SESSIONS command. A message will is sent to the session that invoked this command.		
SETIPDSCP		On a match, set the IP DSCP field to a specified value.	On a CLASSIFIER match, set the IP DSCP field to a specified value. This action conflicts with the SETIPTOS and MOVEPRIOTOTOS ACTIONs, because they both modify the same location in the IP packet. This action requires that one or more of the match rules on the classifier qualifies the packet as an IP packet. Also implies a FORWARD ACTION, and so it conflicts with the DROP ACTION.	SETIPDSCP sets the IP DiffServ CodePoint field. Set the IP TOS and IP DSCP fields - These can be set as follows: The values can be set directly. The value is set using the 802.1Q priority field.,	
SETIPTOS		On a match, set the IP TOS field to a specified value.	On a CLASSIFIER match, set the IP TOS field to a specified value. This action conflicts with the SETIPDSCP and MOVEPRIOTOTOS ACTIONs, because they both modify the same location in the IP packet. This action requires that one or more of the match rules on the classifier qualifies the packet as an IP packet. Also implies a FORWARD ACTION, and so it conflicts with the DROP ACTION.	SETIPTOS sets the IP TOS field. Set the IP TOS and IP DSCP fields - These can be set as follows: The values can be set directly. The value is set using the 802.1Q priority field.,	
SETVPRIORITY		On a match, set the VPRIORITY field to a specified value.	On a CLASSIFIER match, set the VPRIORITY field to a specified value. This action conflicts with the MOVETOSTOPRIO ACTION, because it modifies the same location in the packet. Also implies a FORWARD ACTION, and so it conflicts with the DROP ACTION.	SETVPRIORITY sets the 802.1p bits to the specified value. This value will impact selection of the egress CoS queue. ,	

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
SEVERITY		Severity of the alarm: critical, major, minor, info	The SEVERITY parameter indicates the severity level to filter the display with. Severity indicates the degree of service impact associated with an alarm condition. The following severities are defined: - CRITICAL: A critical alarm is used to indicate that a severe, service-affecting condition has occurred and that immediate corrective action is imperative. - MAJOR: A major alarm is used to indicate a serious disruption of service or the malfunctioning or failure of important circuits. These troubles require immediate attention and response by the craftsperson to restore or maintain system capability. The urgency is less than critical situations because of lesser immediate or impending effect on service or system performance. - MINOR: Minor alarms are used for troubles that do not have serious effect on service to customers or for troubles that do not effect essential system operation. - INFO: Represents an informational message. No explicit action is required of the craftsperson.	,	
SEVERITY OF LOG		Indicates the severity of log(s).	The SEVERITY parameter allows for the display of management logs that have only a certain sequence number values. A single severity value may be specified or an operation-specified range of severities. Valid severities are CRITICAL, MAJOR, MINOR or NONE. These severity values can be combined with an optional operator to include a range of severities. The valid operators are the following: < - less-than - match all logs with a severity less than or equal to the specified severity threshold > - greater-than - match all logs with a severity greater than or equal to the specified severity threshold ! - not-equal - match all logs with a severity less than or equal to the specified severity threshold Valid log categories are: ADSL BDB CARD CHAS CLI CUC FAN FILE IGMP LOG PORT RDB RMON RSDB SHLF SNTP SYS TRAP USER		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
SEVERITY OF SNMPTRAPFILTER		The trap severity filter	The SEVERITY parameter is indicates that filtering is performed based on trap severity. Trap severity is classified as CRITICAL, MAJOR, MINOR, and INFO. The CRITICAL parameter is used to allow or suppress delivery of traps marked as critical by the device. A value of OFF prevents delivery of critical severity traps to the specified SNMPv1 or SNMPv2 trap host.The MAJOR parameter is used to allow or suppress delivery of traps marked as major by the device. A value of OFF prevents delivery of major severity traps to the specified SNMPv1 or SNMPv2 trap host. The MINOR parameter is used to allow or suppress delivery of traps marked as minor by the device. A value of OFF prevents delivery of minor severity traps to the specified SNMPv1 or SNMPv2 trap host. The INFO parameter is used to allow or suppress delivery of traps marked as informational by the device. A value of OFF prevents delivery of informational severity traps to the specified SNMPv1 or SNMPv2 trap host.		
SLOT		The slot number for a card	The SLOT parameter is used to specify a card slot. This parameter can be a single slot or can mean all slots when ALL is specified.	A card slot number. The convention for specifying a card is by its slot number, and for any associated port by its slot.port number. For example, to specify port 1 on a module in slot 4, use 4.1. A comma-separated list of card slots.	
slot-list		The slot number(s) for the card(s)	The CARD parameter specifies the slot number or list of slot numbers of the cards to destroy. The slot-list is either: - single slot - a comma-separated list of slots - a dash range of slots - a combination of dash and comma-separated slots	A comma-separated list of card slots. ALL is for all slots.,	
SOFTWARE		Software load information	The SOFTWARE parameter displays software load information. This parameter is only supported for the CFC, ADSL, FE, and FX cards.	Displays software load information. This parameter is only supported for the CFC, ADSL, FE, and FX cards.	
SORTBY		Field to sort by.	The output is sorted by type, id, name, state, lastchange relative to system up time in ascending or descending order. Default is ascending order.		ascending
sourcefile		Souerce file name.	The FILE parameter specifies the name of the existing file to copy. If the file is on a media card then it should be preceded by the media name, as in CFLASH9:myfile.	sourcefile - the name of file the user wishes to copy.	

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
sourcefilename		The source file name			
SOURCEMASK		Optional source IP address mask (e.g. 255.255.255.0)	The optional SOURCEMASK works with the IPSOURCE match rule field to match on any IPv4 packet with the specified IP source address. The value is specified as a mask for the IPSOURCE field. For example, an IPSOURCE of 192.168.1.0 with a SOURCEMASK of 255.255.255.0 matches 192.168.1.0 to 192.168.1.255. If no mask is provided then 255.255.255.255 is assumed. The SOURCEMASK must be a contiguous series of bits starting with the MSB. For example, 255.255.240.00 would be valid but 255.0.255.0 would not.		
SPEED		Speed of an FE port (in Mbps).	The SPEED parameter specifies the speed of this FE port in Mbps. The valid values are 10 or 100 or AUTONEGOTIATE. The default value is AUTONEGOTIATE. The user can set this parameter only when the port is disabled (See DISABLE PORT). This parameter is only applicable to FE ports.	The port speed. Defines the port speed. One of: - 10Full – 10Mbits, full duplex - 100Full – 100 Mbits, full duplex - 10Half – 10Mbits, half duplex - 100Half – 100 Mbits, half duplex - Auto – the choice of speed and duplex is automatically negotiated with the remote peer. This is the default.	AUTONEGOTIATE
SSH				Secure Shell	
STANDARD		Resets the IGMP snooping 'standard' counters/statistics	Resets the IGMP snooping standard counters/statistics, example statistics are IGMP report/leave/general query, etc.		
STATE		the physical state of the contact that triggers an alarm	The STATE parameter specifies the condition of the dry contact input when an alarm is to be triggered. The dry contact input can either be OPEN or CLOSED.	Note: The STATE parameter cannot be changed using the SET CONTACTALARM command. The alarmtrigger must be destroyed and reentered to change the STATE of OPEN or CLOSED.,	
STATE of Interface		The state of the interface(s). Show only interfaces in the specified state.	The STATE parameter is used to specify that only interfaces in the given state should be displayed.		
STATE of LAG		The LACP state	The STATE parameter displays LACP administrative and operational state info for interfaces in a LAG. This keyword is applicable only if LAG mode is set to active or passive (indicating that LACP is configured).		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
STATECHANGE		The state change trap category	The STATECHANGE parameter is used to allow or suppress delivery of state change traps. A value of OFF prevents delivery of state change traps to the specified SNMPv1 or SNMPv2 trap host.	Used to allow or suppress delivery of state change traps. A value of OFF prevents delivery of state change traps to the specified SNMPv1 or SNMPv2 trap host.	
STATUS		Status information.	The STATUS parameter is used to indicate that the current status of the IGMP snooping feature is desired. The current status is either that the snooping feature is enabled or disabled for a port or ports or for the whole system.		
STATUS (of INTERFACE COUNTER)		Display collection status information for interfaces	The STATUS parameter, when present, indicates that the user wishes to view a shorter view of the data geared more towards the status of the interfaces in question rather than a view oriented more towards current statistical counter data.		
STATUS for TRACE		Show the status of the Trace system.	The STATUS parameter is used to show the settings of the Trace system. The settings include the state of the Trace system (enabled/disabled) and the enabled settings for each Trace application.		
STP PROTOCOL			Identifies which version of the Spanning Tree Protocol to run - original STP, Rapid Spanning Tree (RSTP), or an STP compatible version of RSTP. [default = RSTP] The choice of protocol version should be made based upon what version of Spanning Tree is being run on all the other bridges in the network. RSTP should be used when most of the other bridges in the network are also running RSTP and rapid convergence is desired following changes to the network topology. One of the two STP choices should be selected when most of the bridges in the network are NOT running RSTP, or when at least one of the bridge in the network that is running STP does not appear to be working correctly. The difference between the two STP choices is that the "original STP" protocol is based upon IEEE 802.1D, 1998 edition "The Spanning Tree Algorithm and Protocol", whereas STP compatible RSTP is based upon IEEE P802.1D/D3, June 11, 2003. These two choices should be functionally equivalent. note: The original STP is currently being maintained to provide an additional configuration setup option for communicating with older versions of the Spanning Tree Protocol.		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
STRING		The loginbanner to be displayed upon login.	The STRING parameter contains the string that is to be displayed to the user upon login to the system. Maximum of 255 characters.		
String for ALIAS		Substitute text string replacing the CLI command.	Substitution string containing a semicolon separate list of commands and/or other alias commands. Maximum of 1024 characters.		
STUC for SHDSL		Specifies the STU-C (receive) side of the SHDSL link.	The STUC parameter indicates that the threshold value should be applied to the counts pertaining to the STUC side of the link.	STUC - CO terminal unit, LOSS - Loss of Signal Seconds, LPRS - Loss of Power Seconds, LOSWS - Loss of Sync Word Seconds, LOLS - Loss of Link Seconds, ES - Errored Seconds, SES - Severly Errored Seconds, - UAS - UnAvailable Seconds,	
STUR for SHDSL		Specifies the STU-R (transmit) side of the SHDSL link.	The STUR parameter indicates that the threshold value should be applied to the counts pertaining to the STUR side of the link.	STUR - CPE terminal unit, LOSS - Loss of Signal Seconds, LPRS - Loss Of Power Seconds , LOSW - Loss of Sync Word , ES - Errored Seconds.	
SUBNETMASK		The subnet mask for this interface	The SUBNETMASK parameter specifies the subnet mask to associate with the given interface.		
SUMMARY		Summary information.	Shows SUMMARY data.		
SUSPICIONTHRESHOLD		The suspicion threshold	The SUSPICIONTHRESHOLD parameter specifies the number of unacknowledged packet retransmissions toward the call agent that are allowed before suspecting that the call agent is unreachable. The default value is 5.	Also known as Max1 in RFC 3435, this is the number of unacknowledged packet retransmissions toward the call agent that are allowed before suspecting that the call agent is unreachable, which triggers the MGCP application running in the POTS24 card to use alternate addresses for the agent or initiate a new DNS query to verify the call agent address.	5
SWITCH COUNTER		Switch Counters	The COUNTER parameter refers to CXE switch counters available.		
SYSLOG SERVER		Identity of the Syslog server.	Indicates that output is directed to a Syslog server. The SERVER parameter specifies the IP address or hostname of the Syslog server		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
SYSTEM CONTACT		The name of a contact person.	The CONTACT parameter specifies the contact information for the system. The information is a string of descriptive text for whom to contact. The maximum length is 80 characters. Valid characters are any printable character. If the string includes spaces is must be enclosed in double quotes.		
TAGALL		Double tagging control operation	The state of TAGALL parameter: one of "ON" or "OFF".		
TAIL		The end of the management log stream, the latest logs.	Allows for the display of a certain number of the newest logs. If a numeric argument is not supplied, the newest 20 logs are displayed, otherwise the optional numeric argument is taken as the number of logs to display, if that number of logs exists.		
TARGETSNRMARGIN		Target signal-to-noise ratio margin (in dB) to achieve.	The TARGETSNRMARGIN parameter specifies the target signal-to-noise ratio (in dB) to achieve on an ADSL or SHDSL port. The valid range is from 0 to 15 for an ADSL port and from 0 to 10 for a SHDSL port. The default value is 8 for an ADSL port and 5 for a SHDSL port. This parameter is only applicable to ADSL and SHDSL ports.		8 or 5
TCA		The threshold crossing alert trap category	The TCA parameter is used to allow or suppress delivery of threshold crossing alerts(TCAs) for performance and remote monitoring traps. A value of OFF prevents delivery of TCA traps to the specified SNMPv1 or SNMPv2 trap host.		
TCP				TCP connection	
TCPFLAGS		The value of the TCP flags to match.	The TCPFLAGS match rule field matches on any TCP packet where the specified TCP flags are set, and any TCP flags not specified are not set. Values are entered as a comma-separated list of flag names. The value ANY matches any TCP packet regardless of flag values.	The control bytes used in the TCP header. (Refer to RFC793.) - URG: Urgent Pointer field significant, - ACK: Acknowledgment field significant, - RST: Reset the connection, - SYN: Synchronize sequence numbers, - FIN: No more data from sender, - PSH: Push Function	
TCPPORTDEST		The value of the TCP destination port to match, in decimal or hexadecimal format.	The TCPPORTDEST match rule field matches on any TCP packet with the specified value in the destination port field. The value may be entered in decimal (10) or hexadecimal (0xa) format. Multiple values (separated by commas) can be entered. The value ANY matches any TCP packet.	The TCP destination port of a TCP/IP packet.	ANY

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
TCPPORTSOURCE		The value of the TCP source port to match, in decimal or hexadecimal format.	The TCPPORTSOURCE match rule field matches on any TCP packet with the specified value in the source port field. The value may be entered in decimal (10) or hexadecimal (0xa) format. The value ANY matches any TCP packet.	The TCP source port of a TCP/IP packet	ANY
TELNET		Set Telnet access for the user	The TELNET parameter allows telnet access to be enabled or disabled for the user being added. If the value is YES, then the user has access via telnet. If the value is NO, then the user will only be able to connect via serial port.		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
TEMPLOAD		The temporary software load for the card.	The TEMPLOAD parameter specifies the name of the temporary software load file for the card, and is intended for use during load upgrades to temporarily try out a new software release. This file must reside on the CFC flash file system. The temporary load overrides the preferred load for a single restart. After the temporary load is used for a single restart, the TEMPLOAD parameter is automatically cleared (although the file remains intact on the CFC flash file system) and the card reboots using its preferred load during any subsequent restarts. After a restart using a temporary load, the system is normally in upgrade mode. To get out of upgrade mode, the user can perform another restart to revert back to the preferred load if they want to retain the previous software release, or they can commit to the new release by setting the preferred load to the new release (the same file as the temporary load they just booted). There is no default value for the temporary load. The command is rejected if the temporary software load specified is not compatible with the specified card.	Temporary - A load designated as TEMPLOAD indicates that this is the load that the specified card will load from, one time, during the next loading process. The TEMPLOAD designation is used during the software upgrade procedure. A load designated as TEMPLOAD indicates this is the load that the specified card will load from, one time, during the next loading process. TEMPLOAD designation results in two things. First, if for any reason the new load file is unusable, the system will erase the designation of TEMPLOAD for the new file and revert back to using its original load, allowing the system to automatically recover from an initialization failure of the TEMPLOAD. Second, setting a load as TEMPLOAD puts the configuration into the upgrade mode. For upgrade purposes, changes made to the designation of temporary are independent of system synchronization status. Load preferences for the CFC(s) are stored in the non-volatile RAM (NVRAM) of each CFC, while load preferences for the Service Modules are stored in the configuration database.	
TERMTYPE					
TFTP SERVER		The Trivial File Transfer Protocol server.	The TFTP parameter specifies that the file should be retrieved using the TFTP protocol. The SERVER parameter specifies the IP address or hostname of the host server to transfer the file from. The command fails if the specified server cannot be reached.	Abbreviation of Trivial File Transfer Protocol, a form of the File Transfer Protocol (FTP). TFTP uses the User Datagram Protocol (UDP).	

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
THRESHOLD		The threshold value of the statistic.	The THRESHOLD parameter specifies the threshold at which a threshold crossing alert(TCA) is generated. The threshold parameter only applies to PMONSTATISTIC settings.		
TIME		The current local time of day for the system	The TIME parameter specifies the current local time of day. The format for the time is hh:mm:ss, for example 08:30:00 for 8:30 AM and 20:30:00 for 8:30 PM. Note that the time set using this command is potentially changed by enabling an SNTP server. NOTE: Setting the system time is immediately reflected in all system output that contains time, such as logs, SNMP traps, network monitoring statistics, etc.		
TIMEOUT		The amount of time to wait for a response	Specifies the amount of time, in seconds, to wait for a response from the remote host. If the timeout delay expires, the ICMP response packet is considered lost and the remote host unreachable. (Default: 5 seconds).		
TIMEOUT (for RADIUS)		Timeout in seconds for each RADIUS request	The TIMEOUT parameter is used to specify the number of seconds to wait for a response back from the RADIUS server. If no response is received within the timeout period either the request is retried if there are retries remaining, the next RADIUS or TACACS+ server is contacted or authentication is attempted against the local user database.		
TIMEOUT (for TACACS+ (TACPLUS))		Timeout in seconds for each TACACS+ request	The TIMEOUT parameter is used to specify the number of seconds to wait for a response back from the TACACS+ server. If no response is received within the timeout period either the request is retried if there are retries remaining, the next TACACS+ server is contacted or authentication is attempted against the local user database.		
TIMEOUT for TRACEROUTE		ICMP response wait time.	The maximum time is seconds to wait for an ICMP probe from a intermediate hop. Acceptable range is 1-10. Default is 2 seconds.		
TIMINGREFERENCE	type:id|ifname|INTERNAL	The card-level timing reference.	The card-level timing reference is a common reference for all interfaces on the card		INTERNAL
TIMINGREFERENCE (Port)	SELF|CONNECTION|CARD	This parameter controls the card-level timing reference for this card.			SELF

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
TO		The name of the new file	The TO parameter specifies the name of the destination file on the CFC flash file system. If the file is on a media card then it should be preceded by the media name, as in CFLASH9:myfile.	The destination.	
TO for GET FILE		The optional TO parameter specifies a media card to transfer the file to	The optional TO parameter is used to indicate that the file retrieved from the specified server should be stored on a specified media card rather than in local CFC flash. Its value can either be a combination of the unit name and file name (i.e. CFLASH9:myFile) or just a unit name (CFLASH9: or CFLASH9). If the latter, the file will be stored with the same file name it had on the server.		
TO for PUT FILE		Destination file name or path/filename.	The filename or path/filename to give the transferred file at the destination. Example: TO=myDirectory/myFile		
TOPOLOGYCHANGE		A topology change	The TOPOLOGYCHANGE parameter indicates that topology change detection and notification is disabled for the specified interfaces.	This command also supports the TOPOLOGYCHANGE parameter to control the detection of topology changes on the associated port. This allows the disabling of topology change detection on ports that are known to be connected to single end stations that could cause the Topology Change Notification mechanism to be triggered for the entire network when the end station is power cycled.,	
TOPOLOGYMODE		Controls how the interface(s) are used in a particular topology	Controls how the interface(s) are used in a particular topology, either acting as an UPSTREAM, DOWNSTREAM, OR RING configuration.		
TOS		IP Type of Service	The TOS parameter refers to the Type of Service byte in IP header. Acceptable range is 0-255. Default is 0.		0
TPID		TPID control operation	The value of TPID (Tag protocol identifier).	Used to identify the frame as a tagged frame. The value of the TPID for an 802.1q ethernet tagged frame is 0x8100.	
TRACEROUTE		Trace route to destination	TRACEROUTE to destination displaying hops and their roundtrip times		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
TRACEROUTE TIMEOUT		ICMP response wait time.	The maximum time is seconds to wait for an ICMP probe from a intermediate hop. Acceptable range is 1-10. Default is 2 seconds.		
TRACEROUTE TOS		IP Type of Service	The TOS parameter refers to the Type of Service byte in IP header. Acceptable range is 0-255. Default is 0.		
TRAFFICDESCRIPTOR		Name(s) of TRAFFICDESCRIPTOR(s) or "ALL".	The TRAFFICDESCRIPTOR parameter specifies the name(s) of the TRAFFICDESCRIPTOR(s). The value may be entered as a single TRAFFICDESCRIPTOR name, or a comma-delimited list of names. The value "ALL" means all TRAFFICDESCRIPTORs not associated with classifiers.		
TRANSFER		List of transfer IDs. The file transfer operation to display.	The TRANSFER parameter specifies the file transfer to display. The parameter is in the form of a single ID, a list of IDs, or ALL. The ID is simply a number associated with a particular file transfer to serve as an identifying tag. The ID is output whenever the GET or PUT commands are entered to transfer a file from a network server. Multiple IDs are supported either in a comma separated list format, or a hyphen separated range format. Using the keyword ALL displays all current and pending file transfers.		
TRANSIT		The Transit node type	The Transit node designation in an EPSR domain.		
TRANSLATE		Add VLAN translation.	The TRANSLATE parameter specifies the VLAN identifier from which the VLAN is translated.		
TRAP		Enable SNMP traps.	Used to indicate that SNMP traps are enabled for the community.		
TRAPHOST		The address of a SNMPv1 trap host.	The TRAPHOST parameter specifies an SNMPv1 trap hosts for the SNMP community. These are the IP addresses of devices to which traps are sent. A community may have more than one trap host, The IP address is specified in dotted decimal format. A list of IP addresses can be specified as a comma separated list		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
TXMAX		Maximum number of RSTP specific messages to allow during Hello Time period.	This parameter allows the user to control the amount of message processing that is used by RSTP, in a worst case scenario, to handle protocol specific information by limiting the number of RSTP specific information message transmissions that are allowed during any given Hello Time period.	This parameter allows the user to specify the maximum BPDU transmission rate for any port on the bridge, which therefore determines how much STP control traffic is going into the network. The default value for this parameter is 6, indicating that at most 3 BPDUs can be transmitted from any port in a given Hello Time period (i.e., 2 seconds by default). In the SET STP command, the parameter is TXMAX; the range is 1 to 10 (with the default of 6)., 6	6
TXPEAKCELLRATE	0-MAX	Enter the transmitting peak-cell-rate for the VC.	This parameters is the transmitting peak-cell-rate for this VC. The unit for rate is entered in Cells-per-second. MAX is also a valid option for this parameter. MAX means that the transmit rate will not be constrained by a PCR. The VC will transmit data at a rate up to the actual line rate. In all cases, the VC traffic class of service is UBR(Unspecified Bit Rate).		
TYPE		Layer-2 virtual network type.	Layer-2 virtual network type. Specifies a L2VN type. There are six types of L2VN types which are VLAN, HVLAN, VLLP, VLLV, VPLSP and VPLSV. Only VLAN and HVLAN types are supported.		
TYPE of EPSR		Primary of Secondary	The type of EPSR, either primary or secondary.		
TYPE of EPSR VLAN		The type of EPSR VLAN.	The type of EPSR VLAN, either CONTROL or DATA .		
TYPE OF LOG		Type of log	Specify the type of logs to transfer off the device. Valid values include the following: MGMT - management logs - logs generated during the normal course of system operation that may indicate system status, state or error conditions. ERROR - error logs - logs used for field support and debugging that may assist in troubleshooting. TRACE - trace logs - logs used for field support and debugging that may assist in troubleshooting. CRASH - crash logs - logs used for field support and debugging in cases where the system has experienced an unhandled exception condition. By default, logs with the TYPE of ERROR are placed in the file. Default is for ALL log types to be included.		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
UAS		Unavailable Seconds TCA generation threshold	The UAS parameter is used to set a limit on the number of allowed unavailable seconds over a fifteen minute interval.		
UDP				UDP connection	
UDPPORT for MGCP		The UDP port number.	The UPDPORT parameter specifies the UDP (User Datagram Protocol) port the MGCP application will use for receiving packets.	Specifies the UDP (User Datagram Protocol) port the MGCP application in the POTS24 card will use for receiving packets. The default value is 2427.	2427
UDPPORT for PSPAN		The UDP port of the near end interface, the local receive ID.	This value is placed in the UDP source port for packets that are transmitted and is expected in the UDP destination port for packets that received for this pseudo-span.		
UDPPORTDEST		The value of the UDP destination port to match, in decimal or hexadecimal format.	The UDPPORTDEST match rule field matches on any UDP packet with the specified value in the destination port field. The value may be entered in decimal (10) or hexadecimal (0xa) format. Multiple values (seperated by commas) can be entered. The value ANY matches any UDP packet.	The UDP destination port of a UDP packet.	ANY
UDPPORTSOURCE		The value of the UDP source port to match, in decimal or hexadecimal format.	The UDPPORTSOURCE match rule field matches on any UDP packet with the specified value in the source port field. The value may be entered in decimal (10) or hexadecimal (0xa) format. The value ANY matches any UDP packet. Default is ANY.	The UDP source port of a UDP packet.	ANY
UNDERSIZE		Change alert settings for undersize packets	The UNDERSIZE parameter indicates that that the rising/falling threshold values are to be used for the undersize packet statistical counter.		
unit:		CFLASH#, where # is the slot number of the parent card	The compact flash card, specified using the format CFLASH#, where # is the slot number of the parent card.		
unit:destinationfile		Destination file name that resides on CFLASH.	The TO parameter specifies the name of the destination file on the CFC flash file system. If the file is on a media card then it should be preceded by the media name, as in CFLASH9:myfile.		
unit:filename		Introduces the use of Compact FLASH (CFLASH)	Designates a Compact FLASH unit which is the same as the CFC slot number.	UNIT specifies the shelf slot number for a CFC. FILENAME is the name of the file. For example, CFLASH12 means the CFLASH unit on the CFC in slot 12.	

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
unit:logfile		The CFLASH unit and log file name	unit is the name of the CFC24 CFLASH unit where the log file will be recorded. logfile is the name of the file where the restore logs will be written to.	Syntax is OUTPUT=. Example: OUTPUT=CFLASH12:rest_file_logs	
unit:sourcefile		Source file name that resides on CFLASH.	The FILE parameter specifies the name of the existing file to copy. If the file is on a media card then it should be preceded by the media name, as in CFLASH9:myfile.		
UPSTREAM		The topology setting for a port.	YES - implies that the topology is upstream. NO - implies that the topology is not upstream, rather downstream. RING - implies that this is a RING topology.	When converting a single shelf system to a linear, star, or ring topology, the user can configure the network module ports to be upstream, non-upstream (downstream) or ring.	Upstream = Yes
User		The login name of the user. Case insensitive.	The USER parameter identifies the name of the account to change. It is a character string, 1 to 32 characters in length. Valid characters are uppercase letters (A-Z), lowercase letters (a-z), and decimal digits (0-9). The string may not contain spaces. The login name is case insensitive.	The user ID.	
USER COUNTER		The type of counters to be reset. Default is USER.	Determines the type of counters to be reset. (default: USER)		USER
USER for LOGINBANNER		Set the loginbanner for all USER users.	The USER parameter indicates that the loginbanner is to be set for all USER users.		
USER of BACKUP DATABASE		User Id for DATABASE BACKUP	The USER parameter is used to specify the User Id that should be used for backing up the database.		
UTCOFFSET		The UTC offset (-23:59 .. +23:59).	The UTCOFFSET parameter specifies the number of hours and minutes difference there is between Universal Time/Greenwich Mean Time and local time for the device.	Allows the user to specify the UTC offset for the device. The UTC offset indicates the number of hours and minutes difference between Universal Time/Greenwich Mean Time and local time for the device. Note: This change affects every command in the system that displays time. The UTC offset from Universal Time is specified as a value from -23:59 to +23:59. For example, the UTC offset for Eastern Standard Time for the US and Canada is -5:00.	

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
V2CTRAPHOST		The address of a SNMPv2c trap host.	The V2CTRAPHOST parameter specifies an SNMP v2c trap hosts for the SNMP community. Just like the TRAPHOST parameter, these are hosts to which traps are sent. The format of the parameter is the same as TRAPHOST parameter.		
VAD			VOICEACTIVITYDETECTION - Specifies whether to advertise Voice Activity Detection (VAD) capability to the Call Agent. VAD is used for silence suppression, and will reduce the transmission rate during inactive speech periods while maintaining an acceptable level of output quality. ON: VAD is supported. This is the default.	Values are: ON: VAD is supported. This is the default. VAD_LIGHT is used between the POTS24 card and the Call Agent in this case. Silence interval description packets are sent with noise level value. Reflection coefficient is not included. OFF: VAD is not supported	ON
VC		The VC ID for this VC.	Enter the VC ID for this VC. The VC-ID valid range depends on the capability of interface to which the VC is being added. Since VCID=0 is a default VC which is system generated and user can only change its configuration parameters.		
VCI		Virtual Channel Identifier, value for the ATM virtual channel identifier	The VCI parameter specifies the value for the ATM virtual channel identifier on an ADSL or SHDSL port. The valid range for this parameter is from 32 to 65535. The default is 35. This parameter is only applicable to ADSL or SHDSL ports. The user can set this parameter only when the port is disabled (See DISABLE PORT) This parameter is only applicable to ADSL or SHDSL ports.		35
VERBOSE		Updates the user with progress of the card enable command.	The VERBOSE parameter will cause the prompt to be held for the duration of the enable card command. The user is updated with the progress of the card enable sequence as the card transitions between states, through to the final state.	Updates the user with progress of the card enable command. VERBOSE lists the change in card status as the card is enabled. (Logs, however, are always produced even if this option is not used.),	
VID		The value of the VLAN identifier.	The VID parameter specifies a unique identifier for the VLAN/HVLAN. If tagged interfaces are added to this HVLAN, the specified VID is used in the VID field of the tag in outgoing frames. If untagged interfaces are added to this HVLAN, the specified VID only acts as an identifier for the HVLAN in the Forwarding Database. The default interface based VID has a VID of 1.		

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
VID for CREATE CLASSIFIER		The value of the outer VLAN identifier to match.	The VID match rule field matches on any packet with the specified value in the outer VLAN identifier field. If the port's service configuration adds tags to the packet, or translates VLAN IDs, then this comparison is to the newly added VLAN tag, after translation.		
VLAN		A Virtual LAN (VLAN) name or Id.	The VLAN parameter specifies the name or numerical VLAN identifier. The VLAN must be created with the CREATE VLAN command before it can be associated with an interface.		
VLAN4QUEUEMAP		Comma-delimited list of 4 egress queues (0-3); one for each potential	Mapping of VLAN priority bits to egress queue numbers.		
VLAN8QUEUEMAP		Comma-delimited list of 8 egress queues (0-7); one for each potential	Mapping of VLAN priority bits to egress queue numbers.		
VLANQUEUEMAP		Comma-delimited list of 8 egress queues; one for each potential VLAN priority field value.	Mapping of VLAN priority bits to egress queue numbers.	Comma-delimited list of 8 egress queues; one for each potential VLAN priority field value. Mapping of VLAN priority bits to egress queue numbers. The priority value. Valid values are 0,p1,p2,p3,p4,p5,p6, and p7. Where p0,p1,p2,p3,p4,p5,p6,p7 is the queue number that 802.1p user priority 0,1,2,3,4,5,6,7 will map to respectively. For Systems that only support 4 queues, p0-p7 is limited to 0,1,2,3.	
VOICEACTIVITYDETECTION		Voice Activity Detection capability for POTS (ON or OFF)	The VOICEACTIVITYDETECTION parameter specifies whether to advertise Voice Activity Detection (VAD) to the call agent. VAD is used for silence suppression.	VOICEACTIVITYDETECTION - Specifies whether to advertise Voice Activity Detection (VAD) capability to the Call Agent. VAD is used for silence suppression, and will reduce the transmission rate during inactive speech periods while maintaining an acceptable level of output quality. ON is the default.	ON

Parameter	***Range***	***Short Description***	***Definition***	***Detail***	***Default***
VPI		Virtual Path Identifier, value for the ATM virtual path identifier	The VPI parameter specifies the value for the ATM virtual path identifier on an ADSL or SHDSL port. The valid range for this parameter is from 0 to 255. The default is 0. This parameter is only applicable to ADSL and SHDSL ports. The user can set this parameter only when the port is disabled (See DISABLE PORT) This parameter is only applicable to ADSL and SHDSL ports.		0
VPRIORITY		The value of the outer VLAN priority field to match.	The VPRIORITY match rule field matches on any packet with the specified value in the outer VLAN priority field. If the port's service configuration adds tags to the packet, this comparison is to the priority field of the newly added VLAN tag, which is always 0.	This matches the VLAN ID specified with the User Priority frame. This match rule is used to set up the class of service queues.	
VPRIORITY for MGCP		The priority bit setting.	The VPRIORITY parameter specifies the 802.1p priority bit setting for MGCP packets transmitted from the POTS card.	The 802.1p priority bit setting for MGCP packets transmitted from the POTS24 card. The default value is 5.	5
VRRP			Virtual Router Redundancy Protocol.		
WETTINGCURRENT		The WETTINGCURRENT setting for the card.	The WETTING CURRENT (also known as "sealing current") setting controls whether a low level DC current is applied to the loop to maintain cable splice integrity and physical line loop quality. The default value is OFF. Note that WETTINGCURRENT is not supported in Release 4.0.	Also known as sealing current, is a low-level DC current (less than 20 mA) applied to the loop. It is used to maintain cable splice integrity and physical line loop quality. Allowed values are: On - current is being applied to all lines. Off - current is not being applied to any lines. This is the default.	
WITH LAG		Indicating that a LAG is associated with the port	The WITH parameter is used to indicate that something needs to be associated with the port.		
ZMODEM		Get the file via the ZMODEM protocol.	The ZMODEM parameter specifies that the file should be retrieved using the ZMODEM protocol.	ZMODEM transfer protocol.	