CONEXANT®

Preliminary

Viking™ Chip Set Family
CLI Reference Manual

A detailed reference of CLI commands, parameters, and output for Conexant's Viking family of ADSL-Ethernet bridge/router chip sets

Document #: DO-300171-TC, Issue 7

Date: March 12, 2004

For additional information, contact Conexant Systems, Inc. (together with its subsidiaries, “Conexant”) at **1-888-855-4562** (toll-free within the U.S. and Canada) or **1-732-345-7500**, or visit the Conexant internet site at www.conexant.com.

IMPORTANT NOTICE TO OUR VALUED CUSTOMERS: Conexant has taken all commercially reasonable effort to ensure that the information contained in this document is accurate, however we realize that errors do occur. Conexant continually strives to improve the quality of its products and documentation and, as such, may make changes to this document at any time without notice. A more recent version of this document may exist on the Licensee Server. If you find errors, or information that may be missing, please contact your Conexant Support Representative. Readers of this document who are designers remain responsible for their own system designs and for ensuring that their overall system design satisfies their design objectives, taking due account of the specifications of all equipment and software which may be incorporated into their design. Please be reminded that differences in system hardware and software design or configuration may affect actual performance.

No licenses to patents, copyrights, trade secrets or other intellectual property of Conexant or any of its subsidiaries are granted by this document. Conexant assumes no liability whatsoever, and disclaims any express or implied warranty relating to the sale or license of the products described in this document, including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement. This Conexant proprietary document is intended only for use as specified in a non-disclosure agreement with the company or one of its subsidiaries.

This document is the property of Conexant. No part of this document may be copied, reproduced, stored in a retrieval system, translated, or transmitted in any form, or by any means, nor may any part of this document be used as the basis for manufacture or sale of any items or software without the express written consent of Conexant.

Viking is a proprietary trademark of Conexant. Third party brands, names, and marks are the property of their respective owners.

Table of Contents

1 About this Manual

1.1 Who Should Read this Manual

This manual is intended for the manufacturer, who will use this to refer to the CLI commands in detail, while configuring the modem using the CLI interface.

1.2 How to Use this Manual

The document is organized as follows:

Chapter 1, About this Manual, describes the target audience of this document, lists document conventions and related documents.

Chapter 2, Command Reference, broadly groups all the CLI commands based on features.

Chapter 3, Command Listing, describes each CLI command, parameters and output fields in detail, with examples.

Chapter 4, Quick Reference helps you look up commands at a glance, with a quick look at the related parameters.

1.3 Revision History

Revision	Date	
Issue 7	March, 2003	Updated for software release 2.1
Issue 6	September, 2003	Updated for 1.38.030917a release
Issue 5	February, 2003	Updated for 1.38 release
Issue 4	December 2002	Updated for 1.38.021206a release
Issue 3 (b.)	August 2002	Updated for 1.37 software release.
Issue 1 (Rev 0.5)(a.)	May 2002	Updated for 1.35 software release.

a. As of the May 2002 release, the previous document number (GIUM-0005) and revision number (0.5) were changed to DO-300171-TC and Issue 1, respectively.
b. Issue 2 was bypassed; all changes are reflected in Issue 3.

1.4 Document and Notational Conventions

- Keywords (words you must enter exactly as shown) are represented in Bold Italic.
- User specified values in a command are shown in regular typeface (that is, they are not bold and not italic). For example,

  create alg port portno `port-no` ***[prot {any|tcp|udp|***`<prot-number>`***}] algtype {ftp|snmp|ra|rcmd|l2tp|mirc|icq|cuseeme|h323_q931|h323_ras}***

  Here, “port-no” will carry the user specified value.
- Parameter values enclosed in < > must be specified.
- Parameters enclosed in [ ] are optional.
- Parameter values are separated by a vertical bar (|) when only one of the specified values value can be used (you can use only one).
- Parameter values are enclosed in { } when you *must* use one of the values specified.
- Parameters are enclosed in [ ]+ to indicate that you can specify the parameter one or more times on the command line.
- Parameters are enclosed in [ ] * to indicate that you can specify no values, one value, or multiple values.
- An asterisk (*) symbol in the description table for parameters indicates a configuration-dependent maximum value. For example, in the command `create atm trfdesc`, the parameter `trfindex traffic-descriptor-index` has a valid value range of 1 - *. Here, * indicates a configuration-dependent maximum value.

2 CLI Command Reference

This section lists commands according to features.

2.1 ALG Commands

Category	Commands
ALG Type	`get alg type`

Port ALG	`create alg port`
	`delete alg port`
	`get alg port`

2.2 ATM Commands

Category	Commands
1483 Statistics	`get atm 1483 stats`
AAL5 VC Statistics	`get atm aal5 stats` `reset atm aal5 stats`

IP over ATM Interface	`create ipoa intf`
	`delete ipoa intf`
	`get ipoa intf`
	`modify ipoa intf`

OAM Loopback	`get oam lpbk vc` `modify oam lpbk vc`
OAM F5CC	`modify oam cc vc` `get oam cc vc`

Switched Virtual Connection	`create atm svccfg`
	`delete atm svccfg`
	`get atm svccfg`
	`modify atm svccfg`

Traffic Descriptor	`create atm trfdesc`
	`delete atm trfdesc`
	`get atm trfdesc`

Virtual ATM Port	Interface: `create atm port`
	`delete atm port`
	`get atm port`
	`modify atm port`
	Statistics: `get atm stats`
	`reset atm stats`

Category	Commands
Virtual Circuit	Interface: *create atm vc intf* *delete atm vc intf* *get atm vc intf* *modify atm vc intf* Statistics: *get atm vc stats* *reset atm vc stats*

2.3 AutoDetect Commands

Category	Commands
Global Configuration	*get autodetect cfg* *modify autodetect cfg*
Status	*get autodetect status* *modify autodetect status*

2.4 Bridge Commands

Category	Commands
Global Configuration	*get bridge mode* *modify bridge mode*
Forwarding Table	*get bridge forwarding*
Information	*get bridge tbg info* *modify bridge tbg info* *reset bridge tbg stats*
Ports	Interface: *create bridge port intf* *delete bridge port intf* *get bridge port intf* Statistics: *get bridge port stats* *reset bridge port stats*
Static Entries	*create bridge static* *delete bridge static* *get bridge static* *modify bridge static*
STP	Global Configuration: *get stp global* *modify stp global* Port Configuration: *get stp port* *modify stp port* *reset stp stats* *reset stp port stats*

2.5 Bridge Router Autosense (BRAS) Commands

Category	Commands
Configuration	***get bras cfg*** ***modify bras cfg***

2.6 DDNS Commands

Category	Commands
Host Name	***create ddns hostname*** ***delete ddns hostname*** ***get ddns hostname***
Service Configuration	***create ddns intf*** ***delete ddns intf*** ***get ddns intf***

2.7 DHCP Client Commands

Category	Commands
Information	***get dhcp client info***
Statistics	***get dhcp client stats***

2.8 DHCP Relay Commands

Category	Commands
Global Configuration	***get dhcp relay cfg*** ***modify dhcp relay cfg***
Interface Table	***create dhcp relay intf*** ***delete dhcp relay intf*** ***get dhcp relay intf***
Statistics	***get dhcp relay stats*** ***reset dhcp relay stats***

2.9 DHCP Server Commands

Category	Commands
Address Table	`get dhcp server address`
Global Configuration	`get dhcp server cfg` `modify dhcp server cfg`

Pool Exclusion Table	`create dhcp server exclude`
	`delete dhcp server exclude`
	`get dhcp server exclude`

Host Table	`create dhcp server host`
	`delete dhcp server host`
	`get dhcp server host`
	`modify dhcp server host`

Pool Table	`create dhcp server pool`
	`delete dhcp server pool`
	`get dhcp server pool`
	`modify dhcp server pool`

Statistics	`get dhcp server stats` `reset dhcp server stats`

2.10 DNS Commands

Category	Commands

Configuration	`modify DNS relay`
	`get DNS relay`
	`create dns servaddr`
	`delete dns servaddr`
	`get dns servaddr`

Statistics	`get dns relay stats` `reset dns relay stats`

2.11 DSL Commands

Category	Commands

Configuration	`modify dsl config`
	`get dsl config`
	`get dsl params`

Statistics	`get dsl stats cntrs`
	`get dsl stats curr`
	`get dsl stats hist`
	`reset dsl stats cntrs`
	`get dsl stats flrs`
	`reset dsl stats flrs`

2.12 EoA Commands

Category	Commands
Configuration	***create eoa intf*** ***get eoa intf*** ***delete eoa intf*** ***modify eoa intf***

2.13 Ethernet Commands

Category	Commands
Configuration	***create ethernet intf*** ***delete ethernet intf*** ***get ethernet intf*** ***modify ethernet intf***
Statistics	***get ethernet stats*** ***reset ethernet stats***

2.14 Firewall Commands

Category	Commands
Configuration	***get fwl blacklist*** ***delete fwl blacklist*** ***modify fwl global*** ***get fwl global***
Statistics	***get fwl stats*** ***reset fwl stats***

2.15 HDLC Commands

Category	Commands
Configuration	***get hdlceoc cfg*** ***modify hdlceoc cfg***
Statistics	***get hdlceoc stats***

2.16 ICMP Commands

Category	Commands
Statistics	***get icmp stats***

2.17 IGMP Commands

Category	Commands
Configuration	*create igmp intf* *delete igmp intf* *get igmp intf* *get igmp groups*

2.18 ILMI Commands

Category	Commands
Configuration	*create ilmi intf* *get ilmi access protocol* *modify ilmi access protocol* *get ilmi intf* *modify ilmi intf* *trigger ilmi*

2.19 IP Commands

Category	Commands
Address Table	*get ip address*
ARP Table	*create arp* *delete arp* *get arp*
Global Configuration	*get ip cfg* *modify ip cfg*
Routing	*create ip route* *delete ip route* *get ip route*
Statistics	*get ip stats* *get host info*

2.20 IP Filtering Commands

Category	Commands
Filtering Rules	Configuration: ***create ipf rule entry*** ***delete ipf rule entry*** ***get ipf rule entry*** ***modify ipf rule entry*** Statistics: ***get ipf rule stats*** ***reset ipf rule stats***
Statistics	***get ipf session*** ***reset ipf session*** ***delete ipf session***
Global IP Filtering Setup	***get ipf global*** ***modify ipf global*** ***get ipf stats*** ***reset ipf stats***

2.21 L2TP Commands

Category	Commands
Configuration/Statistics	***get l2tp tunnel config*** ***delete l2tp tunnel config*** ***get l2tp tunnel config*** ***get l2tp global config*** ***modify l2tp global config*** ***modify l2tp tunnel config*** ***get l2tp udp stats*** ***reset l2tp tunnel stats*** ***get l2tp tunnel stats*** ***get l2tp global info*** ***get l2tp session stats*** ***reset l2tp session stats***

2.22 L2Wall Commands

Category	Commands
Configuration	***get l2wall cfg*** ***modify l2wall cfg***

2.23 Management Control Commands

Category	Commands
Allowed IP	***create mctl iplist*** ***delete mctl iplist*** ***get mctl iplist***
Access Configuration	***get mctl access*** ***modify mctl access***

2.24 NAT Commands

Category	Commands
Global Configuration	***get nat global*** ***modify nat global***
Global Statistics	***get nat stats*** ***reset nat stats***
Rule	Rule Statistics: ***get nat rule stats*** ***reset nat rule stats*** Status: ***get nat rule status*** Table: ***create nat rule entry*** ***delete nat rule entry*** ***get nat rule entry***
Translation Table	***get nat translation***
Status	***get nat status***

2.25 Pfraw Commands

Category	Commands
Rule and Subrule	*create pfraw rule entry* *create pfraw subrule entry* *delete pfraw rule entry* *delete pfraw subrule entry* *get pfraw rule info* *get pfraw rule entry* *get pfraw subrule entry* *modify pfraw rule entry* *modify pfraw subrule entry*
Global Configuration	*modify pfraw global* *get pfraw global*
Statistics	*get pfraw stats* *get pfraw rule stats* *reset pfraw rule stats* *reset pfraw stats*
Protocol Blocking	*get pfraw block* *modify pfraw block*

2.26 PPP Commands

Category	Commands
IP Status	*get ppp ipinfo*
Link Configuration	*create ppp intf* *delete ppp intf* *get ppp intf* *modify ppp intf*
Link Status	*get ppp lstatus* *reset ppp lstatus*
Global Configuration	*get ppp global* *modify ppp global*
Security Secrets	*create ppp security* *delete ppp security* *get ppp security* *modify ppp security*

2.27 PPPoE Commands

Category	Commands
AC Service Name Support	***get ppe acserv***
Global Configuration	***modify ppe cfg*** ***get ppe cfg***
Policy Configuration	***create ppe pconf*** ***delete ppe pconf*** ***get ppe pconf***
Statistics	Global: ***get ppe stats global*** Session: ***get ppe stats session***

2.28 RADIUS Commands

Category	Commands
Radius Accounting Server Configuration	***create radius acctserv config*** ***delete radius acctserv config*** ***get radius acctserv config*** ***get radius acctserv stats*** ***modify radius acctserv config*** ***reset radius acctserv stats***
Radius Authentication Server Configuration	***create radius authserv config*** ***delete radius authserv config*** ***get radius authserv config*** ***get radius authserv stats*** ***modify radius authserv config*** ***reset radius authserv stats***
Radius Global Configuration	***get radius global config*** ***get radius global stats*** ***modify radius global config***

2.29 RIP Commands

Category	Commands
Global Configuration	***get rip global*** ***modify rip global***
Interface	***create rip intf*** ***delete rip intf*** ***get rip intf*** ***modify rip intf***
Statistics	***get rip stats*** ***reset rip stats***

2.30 RMON Commands

Category	Commands
Event Group	*get rmon eventgrp*
Memory Pool	*get rmon mpool*
Queue	*get rmon queue*
Semaphore	*get rmon semaphore*
Task	*get rmon task*

2.31 SNMP Commands

Category	Commands
Community	*create snmp comm* *delete snmp comm* *get snmp comm*
Host	*create snmp host* *delete snmp host* *get snmp host*
Statistics	*get snmp stats*
Traps	*get snmp trap* *modify snmp trap*

2.32 SMTP Commands

Category	Commands
Configuration	*modify smtp servaddr* *get smtp servaddr*

2.33 SNTP Commands

Category	Commands
Configuration	*create sntp servaddr* *delete sntp servaddr* *get sntp servaddr* *modify sntp cfg* *get sntp cfg*
Statistics	*get sntp stats* *reset sntp stats*

2.34 Surfing Profile

Category	Commands
Configuration	*reset surf profile reg*

2.35 TCP Commands

Category	Commands
Connection Table	***delete tcp conn*** ***get tcp conn***
Statistics	***get tcp stats***

2.36 UDP Commands

Category	Commands
Listener Table	***get udp listen***
Statistics	***get udp stats***

2.37 UNI Commands

Category	Commands
Configuration	***create atm uni*** ***delete atm uni*** ***get atm uni***

2.38 Usage Control Commads

Category	Commands
Configuration	***get usagectrl*** ***modify usagectrl*** ***get datauserslist*** ***reset datauserslist***

2.39 UPnP Commands

Category	Commands
Configuration	***get upnp cfg*** ***modify upnp cfg***

2.40 USB Commands

Category	Commands
Configuration	***create usb intf*** ***delete usb intf*** ***get usb intf*** ***modify usb intf***
Statistics	***get usb stats***

2.41 ZIPB Commands

Category	Commands
Configuration	***modify zipb cfg enable***

2.42 802.11 Interface Commands

Category	Commands
Configuration	***create wlan intf*** ***delete wlan intf*** ***get wlan intf*** ***modify wlan intf***
Wired Equivalent Privacy Keys	***create wlan key*** ***delete wlan key*** ***get wlan key*** ***modify wlan key***
Firmware Information	***get wlan fwinfo***
Statistics	***get wlan stats***

2.43 802.1x Commands

Category	Commands
Global configuration	*get 8021x global* *modify 8021x global*
Interface configuration	*create 8021x intf* *delete 8021x intf* *modify 8021x intf* *get 8021x intf*
Supplicant Interface	*create 8021x supp* *modify 8021x supp* *get 8021x supp* *delete 8021x supp*
Statistics	*reset 8021x authstats* *get 8021x sessstats* *reset 8021x sessstats*

2.44 Other Commands

apply
alias
commit
create user
delete user
do getserialize
do getver
do serialize
download
get autoupdate
get interface stats
get nbsize
get sizeinfo
get system
get trace cfg
get trace stats
get traps
get trapprints
get user
help
list
logout
modify autoupdate
modify nbsize
modify system
modify trace cfg
modify trapprints
passwd
ping
prompt
reboot
remove
reset traps
size
traceRoute
unalias
verbose

3 Command Listing

This chapter lists all commands in detail. All commands are arranged in an alphabetical order.

3.1 alias

Description Use this command to create an alias for any CLI command. You can later call this command by using the alias-string along with any additional parameters, which you need to specify. It will display a list of all the aliases currently defined if no parameter is given.

Command Syntax ***alias [alias-string = aliased-command]***

Parameters

Name	Description
alias-string	The string which you will use to refer to the aliased command henceforth. **Type:** Optional **Valid values:** string of up to 14 characters ('A'-'Z', 'a'-'z', '0'-'9', '-', '_')
aliased-command	This is the total CLI command length (512 characters). **Type:** Mandatory **Valid values:** Any string (all printable characters except ';') as long as the total CLI Command length is not exceeded.

Mode Super-User, User

Example With Parameters:

```
$alias abc = create dhcp server pool
Set Done
$abc start-ip 192.168.1.1 end-ip 192.168.1.5 mask 255.255.255.0
Entry Created
Pool Id:     0
```

Without Parameters:

```
$alias
Alias               Command
--------------------------
abc                 create dhcp server pool
```

Output field description

Field	Description
Alias	This is the new abbreviated command which you may use in place of the string specified in Command
Command	The command string which has been aliased

Caution Alias Name should not match any CLI keyword. In this case the alias creation will be successful but the alias will not work. It will prompt an error.

References

- *unalias* command.

3.2 apply

Description Use this command to apply a configuration (.cfg) or shell script (.sh) file that is stored on the modem but has not yet been made active. (This command does not work with binary files, which are activated in RAM when they are uploaded.)

Command Syntax ***apply fname*** file-name ***[besteffort true|false] [sparams "<params>"]***

Parameters

Name	Description
fname file-name	This specifies the file name which needs to be applied. **Type:** mandatory **Valid values:** string of up to 128 characters: ('A'-'Z', 'a'-'z', '0'-'9', '-', '_')
besteffort true|false	If the besteffort flag is false, command execution (as specified in "file-name" file) stops immediately after a command returns an error. If the besteffort flag is true, command execution (as specified in "file-name" file) continues even if a command returns an error. **Type:** Optional **Valid values:** *true* or *false* **Default value:** *false*
sparams "<params>"	Params is space-separated list of parameters used as input in case of shell script files. **Type:** Optional **Valid values:** quoted string.

Mode Super-User

Example ***$ apply fname myconfig.cnf***

Output The output of the command is determined by the contents of myconfig.cnf.

Example 1:

The file *myconfig.cnf* has the following commands:

```
verbose on
create atm port ifname atm-0
```

The output would be:

```
  Entry Created

  If-Name          : atm-0              MaxVccs          : 2
  CBRPriority      : 5                  UBRPriority      : 1
  RTVBRPriority    : 4                  NRTVBRPriority   : 3
  GFRPriority      : 2                  Latency          : Interleaved
  MaxConfVccs      : 0
  OAMSrc           : 0xffffffffffffffffffffffffffffffff
  Oper Status      : Up                 Admin Status     : Up
```

Example 2:

The file *myconfig.cnf* has the following commands:

```
create atm port ifname atm-0
```

The output would be:

```
Entry Created
```

Output field description None.

Caution None.

References

- *modify autoupdate* command
- *set autoupdate* command
- *remove* command
- *list* command
- *download* command

3.3 commit

Description Use this command to commit the active configuration to the flash.

Command Syntax ***commit***

Parameters None.

Mode Super-User, User

Example ***$ commit***

Output

```
Set Done
```

Output field description None.

Caution None.

References

- *reboot* command
- *download* command

3.4 create alg port

Description Use this command to create an ALG port.

Command Syntax

create alg port portno port-no ***[prot {any|tcp|udp|icmp|esp|num*** <prot-number>***}] algtype {ftp|snmp|cuseeme|l2tp|ra|rcmd|mirc|h323_q931|h323_ras|pptp|rtsp|timbuktu|ldap|sgicompcore|msnmsgr|ike|esp|SIP|t120|icq}***

Parameters

Name	Description
portno port-no	The Port number on which the ALG should run. The port here is the destination port of the untranslated packet **Type:** Mandatory **Valid values:** *0 – 65535*
prot any|tcp|udp|icmp|esp|num< prot-number>	This specifies the protocol type for which the ALG should run. **Type:** Optional **Valid values:** any, tcp, udp, icmp, esp or 0-255 (valid IANA-specified protocol) **Default value:** a*ny*
algtype ftp|snmp|cuseeme|l2tp|ra|rcmd|mirc|h323_q931|h323_ras|pptp|rtsp|timbuktu|ldap|sgicompcore|msnmsgr|ike|esp|sip|t120|icq	This specifies the ALG which has to be applied to this port. **Type :** Mandatory **Valid values :** ftp, snmp, cuseeme, l2tp, ra, rcmd, mirc, h323_q931, h323_ras, pptp , rtsp, timbuktu, ldap, sgicompcore, msnmsgr, ike, esp, sip, t120, icq.

Mode Super-User

Example ***$ create alg port portno*** 21 ***prot tcp algtype ftp***

Output Verbose Mode On:

```
Entry Created
Port Num                Protocol                ALG Type
-------------------------------------------------------------
21                      Tcp                     FTP
```

Verbose Mode Off:

```
Entry Created
```

Output field description

Field	Description
Port Num	The port number on which the ALG will operate. The port here is the destination port of the untranslated packet.

Field	Description
Protocol	The protocol for which this ALG will run.
ALG type	This specifies the ALG with has to be applied to this port. It may be: *ftp, snmp, cuseeme, l2tp, ra, rcmd, mirc, h323_q931, h323_ras, pptp, rtsp, timbuktu, ldap, sgicompcore, msnmsgr, IKE,ESP, ICQ*

Caution None.

References

- *delete alg port* command
- *get alg port* command
- *get alg type* command.

3.5 create arp

Description This command is used for creating a static entry in ARP table.

Command Syntax ***create arp ip*** ip-address ***macaddr*** mac-address

Parameters

Name	Description
ip ip-address	IP address corresponding to the media-dependent “physical” address **Type:** Mandatory **Valid values:** Any valid class A/B/C IP address
macaddr mac-address	The media-dependent “physical” address **Type:** Mandatory **Valid values:** *0:0:0:0:0:1 - ff:ff:ff:ff:ff:fe*

Mode Super-User

Example ***$ create arp ip 192.168.1.1 macaddr 11:11:11:11:11:11***

Output Verbose Mode On:

```
Entry Created

If Name    Type         Mac Address              Ip Address
-------------------------------------------------------------
veth-0     Static      11:11:11:11:11:11         192.168.1.1
```

Verbose Mode Off:

```
Entry Created
```

Output field description

Field	Description
If Name	This specifies the physical interface for the media. It may be: *eth-0* or *veth-4* to *veth-1*
Type	This defines the type of mapping in use. The value *Invalid* has the effect that this entry is not used. It may be: *Static, Dynamic, Other*
Mac Address	The media-dependent “physical” address
Ip Address	IP address corresponding to the media-dependent “physical” address

Caution The specified interface should exist. Please refer to the *create ethernet intf* command.

References

- *delete arp* command
- *get arp* command
- *create ethernet intf* command
- *ip stats* related commands
- *ip route* related commands
- *ip address* related commands
- *ip cfg* related commands

3.6 create atm port

Description Use this command to create an ATM Port.

Command Syntax ***create atm port ifname*** interface-name ***[maxvc*** max-num-vccs***]*** ***[fast|interleaved]*** ***[oamsrc*** oam-src-id***]*** ***[cbrpriority*** cbr-priority***]*** ***[rtvbrpriority*** rtvbr-priority***]*** ***[nrtvbrpriority*** nrtvbr-priority***]*** ***[gfrpriority*** gfr-priority***]*** ***[ubrpriority*** ubr-priority***]*** ***[enable|disable]***

Parameters

Name	Description
ifname interface-name	This specifies the name of the ATM port **Type:** Mandatory **Valid values:** *atm-0*
maxvc max-num-vccs	This specifies the maximum number of VCCs (PVCCs and SVCCs) supported at this ATM interface **Type:** Optional **Valid values:** 1 - up to maxvc given in size command **Default value:** 2
fast|interleaved	Type of DSL channel in use on the underlying DSL port **Type:** Optional **Default value:** *interleaved*
oamsrc oam-src-id	Loop back source id assigned to the ATM port. The ATM port will respond to all loopback cells which carry this OAM id. **Type:** Optional **Valid values:** 0x followed by 32 hex digits **Default value:** *0xffffff ffff ffff ffff ffff ffff ffff*
cbrpriority cbr-priority	Priority of the CBR class. The higher the value, the higher the priority The priority can be changed at run time. **Type:** Optional **Valid values:** *1-5* **Default value:** *5*
rtvbrpriority rtvbr-priority	Priority of RT-VBR service category. The higher the value, the higher the priority. The priority can be changed at run time. **Type:** Optional **Valid values:** *1-5* **Default value:** *4*
nrtvbrpriority nrtvbr-priority	Priority of NRT-VBR service category. The higher the value, the higher the priority. The priority can be changed at run time. **Type:** Optional **Valid values:** *1-5* **Default value:** *3*

Name	Description
gfrpriority gfr-priority	This specifies the priority of GFR class. Value 1 means minimum priority is assigned to this traffic class. The higher the value, the higher the priority. It can be changed at run time. **Type:** Optional **Valid values:** *1-5* **Default value:** *2*
ubrpriority ubr-priority	Priority of the best effort traffic. Value 1 means minimum priority is assigned to this traffic class. The higher the value, the higher the priority. It can be changed at run time. **Type:** Optional **Valid values:** *1-5* **Default value:** *1*
enable | ***disable***	Admin status of the ATM port **Type:** Optional **Default value:** *enable*

Mode Super-User

Example `$ create atm port ifname atm-0 maxvc 4 fast`

Output Verbose Mode On:

```
Entry Created

If-Name          : atm-0          MaxVccs          : 4
CBRPriority      : 5              UBRPriority      : 1
RTVBRPriority    : 4              NRTVBRPriority   : 3
GFRPriority      : 2              Latency          : fast
MaxConfVccs      : 0
OAMSrc           : 0xffffffffffffffffffffffffffffffff
Oper Status      : Up             Admin Status     : Up
```

Verbose Mode Off:

```
Entry Created
```

Output field description

Field	Description
If-Name	This specifies the name of the ATM port: It can be: *atm-0.*
Max Vccs	This specifies the maximum number of VCCs (PVCCs and SVCCs) supported at this ATM interface. It can be: *0-64*.
CBRPriority	Priority of the CBR Class. Value 1 means lowest priority and higher the value higher the priority. It may be *1-5*
UBRPriority	Priority of the best effort traffic. A value *0* means no traffic of this class is supported. The higher the value, the higher the priority. It may be: *1-5.*

Field	Description
RTVBRPriority	Priority of the RT-VBR service category. The higher the value, the higher the priority. It may be: *1-5.*
NRTVBRPriority	Priority of the NRT-VBR service category. The higher the value, the higher the priority. It may be: *1-5.*
GFRPriority	This specifies the priority of GFR class. A value 0 means no traffic of this class is supported. Higher the value higher the priority. It may be: *1-5.*
Latency	Type of DSL channel in use on the underlying DSL port. It may be: *fast, interleaved*
MaxConfVccs	This specifies the current number of VCCs configured on this port. It may be: *0* - Value defined in MaxVccs.
OAMSrc	Loop back source id assigned to the ATM port. The ATM port will respond to all loopback cells which carry this OAM ID.
Oper Status	The actual/current state of the interface. It can be either *Up* or *Down*
Admin Status	The desired state of the interface. It may be either *Up* or *Down*

Caution Execute the **`size`** command before creating an atm port.

References

- `atm trfdesc` related commands
- `atm vc` related commands
- `oam lpbk` command
- `atm port` related commands
- `atm statistics` related commands.

3.7 create atm svccfg

Description Use this command to configure SVC (Switched Virtual Connection).

Command Syntax

create atm svccfg ifname interface-name ***daddr*** dest-atm-address ***[pppoa|eoa|any] [nplan isdn|atmes] [trfindex*** traffic-descriptor-index***] [a5txsize*** aal5-cpcs-tx-sdu-size***] [a5rxsize*** aal5-cpcs-rx-sdu-size***] [vcmux|llcmux|none]***

Parameters

Name	Description
Ifname interface-name	Interface name of the SVC to be configured. **Type:** Mandatory **Valid values:** *aal5-0, aal5-1…*
Nplan isdn|atmes	The Address Plan to which the specified ATM Destination Address (for SVC to be opened) belongs **Type:** Optional **Valid values:** *isdn* | *atmes* **Default value:** *atmes*
daddr dest-atm-address	The ATM address of the destination with which the connection has to be established. **Type:** Mandatory **Valid values:** Valid ATM Address
pppoa|eoa|any	This specifies the protocol that would run on the VC. pppoa – PPP over ATM eoa – Ethernet over ATM Any – Any **Type:** Optional **Valid values:** *ppoa, eoa, any* **Default value:** *any*
Trfindex traffic-descriptor-index	The index of the Traffic Descriptor Table entry whose traffic parameters are desired for the SVC to be opened. **Type:** Optional **Valid values:** *0 - 2* (max VC) **Default value:** 0
a5txsize aal5-cpcs-tx-sdu-size	This specifies the transmit CPCS SDU size to be used **Type:** Optional **Valid values:** *1-65535* **Default value:** *9188*

Name	Description
a5rxsize aal5-cpcs-rx-sdu-size	This specifies the receive CPCS SDU size to be used **Type:** Optional **Valid values:** *1-65535* **Default value:** *9188*
vcmux|llcmux|none	The type of Protocol Multiplexing used over 1483. The value *none* means no data multiplexing is to be done. **Type:** Optional **Valid values:** *vcmux, llcmux, none* **Default value:** *llcmux*

Mode Super-User.

Example

```
$ create atm svccfg ifname aal5-0 nplan atmes daddr
0x47000580ffde000000000001050000000000000000 trfindex 1
a5txsize 200 a5rxsize 200 vcmux pppoa
```

Output Verbose Mode On

```
Entry Created

VC IfName        : aal5-0    AAL5 Encap       : VC Mux
VPI              : 0         VCI              : 0
Numbering Plan   : atmes
Dest Atm Address : 0x47000580ffde000000000001050000000000000000
Trf Descr Index  : 1         Access Protocol  : PPPoA
Aal5 Tx Size     : 200       Aal5 Rx Size     : 200
```

Verbose Mode Off

```
Entry Created
```

Output field description

Name	Description
VC Ifname	Interface name of the configured SVC.
AAL5 Encap	The type of Protocol Multiplexing used over 1483
VPI	The VPI of the ATM VC found towards the specified ATM Destination
VCI	The VCI of the ATM VC found towards the specified ATM Destination
Numbering Plan	The Address Plan to which the specified ATM Destination Address (for SVC to be opened) belongs.
Dest Atm Address	The ATM address of the destination with which the connection is established.
Trf Descr Index	The index of the Traffic Descriptor Table entry whose traffic parameters are for the SVC to be opened.
Access Protocol	This specifies the protocol that runs on the VC

Name	Description
Aal5 Tx Size	This specifies the transmit CPCS SDU size.
Aal5 Rx Size	This specifies the receive CPCS SDU size.

Caution None.

References

- *get atm svccfg* command
- *delete atm svccfg* command

3.8 create atm trfdesc

Description Use this command to create a traffic descriptor entry. Traffic descriptors are used to specify desired traffic characteristics during VC creation.

Command Syntax

create atm trfdesc trfindex traffic-descriptor-index ***[NOCLP_NOSCR|CLP_NOTAG_MCR|NOCLP_SCR|NOCLP_NOSCR_CDVT|NOCLP_SCR_CDVT] [UBR|GFR|CBR|RTVBR|NRTVBR] [pcr*** peak-cell-rate***] [mcr*** minimum-cell-rate***] [scr*** sustained-cell-rate***] [mbs*** maximum-burst-size***][cdvt cell-delay-variation-tolerance]***

Parameters

Name	Description
trfindex traffic-descriptor-index	This identifies the traffic descriptor entry. The traffic descriptor 0 has a special meaning – it is always created by default and is used if the user does not specify a traffic descriptor in the *create atm vc intf* command. **Type:** Mandatory **Valid values:** *0 - **
NOCLP_NOSCR | ***CLP_NOTAG_MCR*** | ***NOCLP_SCR*** | ***NOCLP_NOSCR_CDVT*** | ***NOCLP_SCR_CDVT***	Type of traffic to be used. **Type:** Optional **Valid values:** *NOCLP_NOSCR, CLP_NOTAG_MCR, NOCLP_SCR, NOCLP_NOSCR_CDVT, NOCLP_SCR_CDVT* **Default value:** *NOCLP_NOSCR*
UBR | ***GFR*** | ***CBR*** | ***RTVBR*** | ***NRTVBR***	Service category to be used. *UBR* and *CBR* can be used only with *NOCLP_NOSCR*, *RTVBR, and NRTVBR*. *GFR* can be used with *CLP_NOTAG_MCR*. **Type:** Optional **Valid values:** *UBR, GFR, CBR, RTVBR, NRTVBR* **Default value:** *UBR*
pcr peak-cell-rate	Peak Cell Rate for ATM Traffic **Type:** Optional **Valid values:** *0 – 4294967295* **Default value:** *0*
mcr minimum-cell-rate	Minimum Cell Rate for ATM Traffic **Type:** Optional **Valid values:** *0 – 4294967295* **Default value:** *0*
scr sustained-cell-rate	Sustained Cell Rate for ATM Traffic **Type:** Optional **Valid values:** *0 – 4294967295* **Default value:** *0*

Name	Description
mbs maximum burst size	Maximum Burst Size for ATM Traffic **Type:** Optional **Valid values:** *0 – 4294967295* **Default value:** *0*
cdvt cell-delay-variation-tolerance	Cell delay variation tolerance **Type:** Optional **Valid values:** 0 - 4294967295 **Default value:** 0

Mode Super-User

Example ***$ create atm trfdesc trfindex 2 noclp_noscr ubr***

Output Verbose Mode On:

```
Entry Created

Traffic Descr Id     : 2              Type                 : NOCLP_NOSCR
Service Category     : UBR            Frame Discard        : Enabled
PCR                : 0              MCR                : 0
```

Verbose Mode Off:

```
Entry Created
```

Output field description

Field	Description
Traffic Descr Id	This identifies the traffic descriptor entry which has been created.
Type	This defines the type of traffic used. It may be: *NOCLP_NOSCR, CLP_NOTAG_MCR, or NOCLP_SCR*
Service Category	This specifies the service category to be used. It may be: *UBR, GFR, CBR, RTVBR, NRTVBR*
Frame Discard	It is always *Enabled.* It indicates that the network is requested to treat data for this connection, in the given direction, as frames (e.g. AAL5 CPCS_PDU's) rather than as individual cells. This treatment may for example involve discarding entire frames during congestion, rather than a few cells from many frames.
PCR	Peak Cell Rate for ATM Traffic
MCR	Minimum Cell Rate for ATM Traffic

Caution None.

References

- Other *atm trfdesc* commands
- *atm vc* related commands
- *atm statistics* command
- *atm port* related commands

3.9 create atm uni

Description Use this command to create UNI (User Network Interface).

Command Syntax

```
create atm uni ifname interface-name saddr source-atm-addr
[nplan isdn|atmes] [version uni31|uni40]
```

Parameters

Name	Description
Ifname interface-name	Interface name of the ATM VC over which UNI signaling is to be run. **Type:** Mandatory **Valid values:** *aal5-0, aal5-1…*
Nplan isdn|atmes	The Address Plan to which the specified ATM Source Address belongs **Type:** Optional **Valid values:** *isdn|atmes* **Default value:** *atmes*
Saddr source-atm-address	The self ATM address. It could be a valid hexvalue or decvalue. **Type :** Mandatory **Valid values:** Valid ATM Address
version uni31|uni40	This specifies the version of UNI. **Type:** Optional **Valid Values:** uni31 or uni40 **Default Value:** uni31

Mode Super-User.

Example

```
$ create atm uni ifname aal5-0 nplan atmes saddr
0x39000760ff8900000000000119000000000000000 version uni40
```

Output Verbose Mode On

```
Entry Created

IfName          : aal5-0          ATM Numb Plan : atmes
Status          : Up              Version       : UNI40
Self ATM Address: 0x39000760ff8900000000000119000000000000000
```

Verbose Mode Off

```
Entry Created
```

Output field description

Name	Description
Ifname	Interface name of VC over which UNI signaling is running. It can be: *aal5-0, aal5-1…*
ATM NumbPlan	The Address Plan to which the specified ATM Source Address belongs.

Name	Description
Status	This specifies the status of the Signaling ATM Adaptation Layer (SAAL) layer. The purpose of SAAL is to provide reliable transfer of signaling message between peer UNI entities.
Version	This specifies the version of the UNI used. UNI31 and UNI40 mean UNI3.1 and UNI4.1 respectively.
SelfAtmAddress	The source ATM address.

Caution Create aal5 VC with **none** encapsulation, before creating atm uni.

References

- *get atm uni* command
- *delete atm uni* command

3.10 create atm vc intf

Description Use this command to create a new ATM Virtual Circuit.

Command Syntax

```
create atm vc intf ifname interface-name vpi vpi vci vci
[lowif virtual-atm-port-interface-name]
[enable|disable|lpbk] [trfindex traffic-descriptor-index]
[aal5] [a5txsize aal5-cpcs-tx-sdu-size] [a5rxsize aal5-cpcs-
rx-sdu-size] [vcmux|llcmux|none] [a5maxproto max-protocol-
per-aal5] [vcweight vc-weight]
```

Parameters

Name	Description
ifname interface-name	VC Interface Name **Type:** Mandatory **Valid values:** *aal5-0 - * to aal5-7*
lowif virtual-atm-port-interface-name	Lower interface index. It should correspond to a valid atm port. **Type:** Optional **Valid values:** *atm-0* **Default value:** *atm-0*
vpi	Virtual Path Identifier **Type:** Mandatory **Valid values:** *0-255*
vci	Virtual Circuit Identifier **Type:** Mandatory **Valid values:** *0-65535*
enable | ***disable*** | ***lpbk***	This specifies the Admin Status of the VC. *lpbk* has a special significance. If set to *lpbk*, the VC will loop back whatever cells it receives. **Type:** Optional **Default value:** *enable*
trfindex	This index references an existing traffic descriptor, whose ATM traffic parameters will be used to create the VC. **Type:** Optional **Default value:** *0*
aal5	AAL type to be used for the VC. **Type:** Optional **Default value:** *aal5*
a5txsize	This specifies the transmit CPCS SDU size to be used **Type:** Optional **Valid values:** *1-65535* **Default value:** *9188*
a5Rxsize	This specifies the receive CPCS SDU size to be used **Type:** Optional **Valid values:** *1-65535* **Default value:** *9188*

Name	Description
vcmux*|*llcmux*|*none	This specifies the data multiplexing method to be used over the AAL5 SSCS layer. RFC 1483 defines two methods – VC muxing and LLC muxing. *None* means no data multiplexing is to be done. **Type:** Optional **Default value:** *llcmux*
A5maxproto	This specifies the maximum number of protocols that are supported over the VC. It is relevant and configurable only for an LLC muxed VC. For a VC muxed VC it is always 1. **Type:** Optional **Valid values:** *1-255* **Default value:** *2*
vcweight	This specifies the priority of the VC. Higher value means higher priority. **Type:** Optional **Valid values:** *0-255* **Default value:** *10*

Mode Super-User

Example

```
$ create atm vc intf ifname aal5-0 vpi 10 vci 10 lowif atm-0
enable trfindex 2 aal5 a5txsize 9200 a5rxsize 9200 llcmux
a5maxproto 3 vcweight 40
```

Output Verbose Mode On:

```
Entry Created

LowIf              : atm-0     VPI              : 10         VCI    : 10
VC IfName          : aal5-0    VC Type         : PVC
Admin Status       : Up        Oper Status      : Up
Aal5 Tx Size       : 9200      Aal5 Rx Size     : 9200
AAL Type           : AAL5      AAL5 Encap       : LLC Mux
Max Aal5 Proto     : 3         Trf Descr Index  : 2
VC Weight          : 40
```

Verbose Mode Off:

```
Entry Created
```

Output field description

Field	Description
LowIf	Lower interface index. It is always: *atm-0*
VPI	It is the Virtual Path Identifier.
VCI	It is the Virtual Circuit Identifier.
VC IfName	VC Interface Name. It can be: *aal5-0 - aal5-63*
VC Type	This field specifies whether VC type is PVC or SVC.
Oper Status	The actual/current state of the interface. It can be either *Up* or *Down*

Field	Description
Admin Status	The desired state of the interface. It may be either *Up*, *Down or Loopback. Loopback* has a special significance. A Loopback VC will loop back whatever cells it receives.
Aal5 Tx Size	This specifies the transmit CPCS SDU size to be used
Aal5 Rx Size	This specifies the receive CPCS SDU size to be used
Aal Type	AAL type in use for the VC
Aal5 Encap	This specifies the data multiplexing method to be used over the AAL5 SSCS layer.
Max Aal5 Proto	This specifies the maximum number of protocols that are supported over the VC
Trf Descr Index	This identifies the transmit traffic parameters in use. It corresponds to a valid traffic descriptor entry
VC Weight	This specifies the priority of the VC. Higher value means higher priority

Caution Entry corresponding to the specified trfindex should exist. Please refer to *atm trfdesc* commands.

The specified lower interface should exist. Please refer to the `create atm port` command.

References

- Other *atm vc intf* commands
- *atm trfdesc* related commands
- *oam lpbk* command
- *atm port* related commands
- *atm statistics* command

3.11 create bridge port intf

Description Use this command to create a new bridge port.

Command Syntax ***create bridge port intf ifname*** interface-name

Parameters

Name	Description
ifname interface-name	Specifies the interface name for which the bridge port is to be created. Any valid EoA or ethernet interface may be specified. **Type:** Mandatory **Valid values:** *eoa-0 - *, eth-0*

Mode Super-User

Example ***$ create bridge port intf ifname eth-0***

Output Verbose Mode On:

```
Entry Created

Port     If-Name   Delay-Exceed-Discards    MTU-Exceed-Discards
-----------------------------------------------------------------
1        eth-0     0                        0
```

Verbose Mode Off:

```
Entry Created
```

Output field description

Field	Description
Port	The port number of the interface for which the bridge port has been created.
If-Name	This specifies the Interface name corresponding to the above port. It can be: *eoa-0 - *, eth-0*
Delay-Exceed-Discards	The number of frames discarded by this port due to excessive transit delay through the bridge
MTU-Exceed-Discards	The number of frames discarded by this port due to the frame size being greater than the MTU of the interface

Caution The specified interface should exist.

References

- *delete bridge port intf* command
- *create usb intf* command
- *get bridge port intf* related commands
- *bridge mode* related commands
- *bridge port stats* related commands
- *bridge static* related commands
- *bridge forwarding* related commands
- *create ethernet intf* related commands
- *create eoa intf* related commands.

3.12 create bridge static

Description Use this command to specify the list of interfaces over which frames destined for the given MAC address shall be forwarded.

Command Syntax ***create bridge static macaddr*** mac-address ***inifname*** interface-name|all ***[ifname*** interface-name|all**]+**

Parameters

Name	Description
macaddr mac-address	The destination MAC address in a frame to which this entry's filtering information applies. **Type:** Mandatory **Valid values:** *0:0:0:0:0:1 to FF:FF:FF:FF:FF:FE*
Inifname interface-name|all	Interface from which a frame must be received in order for this entry's filtering information to apply. A value of all indicates that this entry applies on all interfaces of the bridge for which there is no other applicable entry. **Type:** Mandatory **Valid values:** *eth-0, eoa-0 - *, usb-0*
ifname interface-name|all	The interface to which frames destined for the given MAC address are allowed to be forwarded. Any number of such interfaces may be specified together. **Type:** Optional **Valid values:** *eth-0, eoa-0 - ** **Default value:** *all*

Mode Super-User

Example ***$ create bridge static macaddr 1:1:1:1:1:1 inifname veth-0 ifname eth-0 ifname eoa-1***

Output Verbose Mode On:

```
Entry Created

MAC Address      : 01:01:01:01:01:01      Incoming Interface : veth-0
Interfaces       : eoa-0 eoa-1
```

Verbose Mode Off:

```
Entry Created
```

Output field description

Field	Description
MAC Address	The destination MAC address in a frame to which this entry's filtering information applies
Incoming Interface	Interface from which a frame must be received in order for this entry's filtering information to apply. A value of all indicates that this entry applies on all interfaces of the bridge for which there is no other applicable entry.
Interfaces	The interfaces to which frames destined for a specific MAC address are allowed to be forwarded. They may be: *eth-0, eoa-0 - **

Caution Bridge ports must have been created for the interfaces specified in this command.

References

- *delete bridge static* command
- *get bridge static* related commands
- *modify bridge static* related commands
- *bridge port stats* related commands
- *bridge static* related commands
- *bridge forwarding* related commands
- *bridge mode* related commands.

3.13 create ddns hostname

Description Use this command to create Dynamic DNS Host Name Table

Command Syntax ***create ddns hostname ifname*** ifname ***name*** name

Parameter

Name	Description
ifname ifname	Interface name of the public interface for which this entry defines the Dynamic DNS Host Name. **Valid Values :** ppp-0 - ppp-*, ipoa-0 - ipoa-*, eoa-0 - eoa-*, eth-0 - eth-*, usb-0, wlan-0 **Type:** Mandatory
name name	Hostname registered at service provider. **Type:** Mandatory

Mode Super-User

Example ***$ create ddns hostname ifname*** ppp-0 ***name*** www.xyz.com

Output Verbose Mode On

```
Entry Created

Interface  HostName
--------------------------------------------------------------------------------
ppp-0      www.xyz.com
```

Verbose Mode Off:

```
Entry Created
```

Output field description

Field	Description
Interface	Interface name of the public interface for which this entry defines the Dynamic DNS Host Name. Valid Values : ppp-0 - ppp-*, ipoa-0 - ipoa-*, eoa-0 - eoa-*, eth-0 - eth-*, usb-0, wlan-0
HostName	Hostname registered at service provider.

Cautions None.

References

- *get ddns hostname* command
- *delete ddns hostname* command

3.14 create ddns intf

Description Use this command to create Dynamic DNS Service Configuration

Command Syntax

create ddns intf ifname ifname ***srvcname*** tzo | dyndns ***username*** username ***passwd*** passwd ***[system*** dynamic | static | custom ***] [wildcard*** enable | disable ***] [mailexchger*** mailexchger ***] [mailbackup*** enable | disable ***] [offlinesupport*** enable | disable ***]***

Parameter

Name	Description
ifname ifname	Interface name of the public interface for which this entry defines the Dynamic DNS profile. **Valid Values :** ppp-0 - ppp-*, ipoa-0 - ipoa-*, eoa-0 - eoa-*, eth-0 - eth-*, usb-0, wlan-0 **Type:** Mandatory
srvcname tzo | dyndns	This is the name of the Dynamic DNS service provider where the user has registered and has an account.Some examples are www.tzo.com, www.dyndns.org **Type:** Mandatory
username username	Username registered at service provider. The value is to be given in double quotes. **Type:** Mandatory
passwd passwd	Password provided by service provider. **Type:** Mandatory
system dynamic | static | custom	This parameter is valid only when SrvcName is DYNDNS. www.dyndns.org provides 3 kinds of services - Dynamic DNS, Custom DNS and Static DNS. The user can create different domains in these systems. Custom DNS service is a full DNS solution for newly purchased domains or domains you already own. A web-based interface provides complete control over resource records and your entire domain including support for dynamic IPs and automated updates. Static DNS service points a DNS hostname in some domain owned by dyndns.org to the user's ISP-assigned static or pseudo-static (meaning which do not change too frequently) IP address. DynDNS service points a fixed hostname in some domain owned by dyndns.org to the user's ISP-assigned dynamic IP address. This allows more frequent updation of IP addresses than Static DNS. **Type:** Optional **Default value:** dynamic

Name	Description
wildcard enable | disable	This parameter is valid only if SrvcName is DYNDNS. It specifies whether Wildcard CNAME are to be resolved or not. If enabled, addresses *.yourhost.ourdomain.ext are aliased to the same address as yourhost.ourdomain.ext. **Type:** Optional **Default value:** disable
mailexchger mailexchger	This parameter is valid only if SrvcName is DYNDNS. It specifies a Mail Exchanger (MX) for use with the hostname being modified. The specified MX must resolve to an IP address,or it will be ignored.Providing no MX setting (or an MX that doesn't resolve properly to an A record) will cause the hostname's MX record(s) to be removed. **Type:** Optional **Default value:** ""
mailbackup enable | disable	This parameter is valid only if SrvcName is DYNDNS.It specifies whehter mails are to be backed up by the service provider. **Type:** Optional **Default value:** disable
offlinesupport enable | disable	This parameter is valid only if SrvcName is DYNDNS.If enabled, the service provider redirects browsers to its own site if the registered host is currently offline. **Type:** Optional **Default value:** disable

Mode Super-User

Example

```
$ create ddns intf  ifname ppp-0 srvcname dyndns username "Viking" passwd Viking1 system dynamic wildcard enable mailexchger www.IAD1.com mailbackup enable offlinesupport enable
```

Output Verbose Mode On

```
Entry Created

Interface        : ppp-0
Service Provider : dyndns
User Name        : "Viking"
Type of system   : dynamic WildCard        : enable
Mail Exchanger   : www.IAD1.com
Mail Backup      : enable  Offline Support : enable
```

Verbose Mode Off:

```
Entry Created
```

Output field description

Field	Description
Interface	Interface name of the public interface for which this entry defines the Dynamic DNS profile. Valid Values : ppp-0 - ppp-*, ipoa-0 - ipoa-*, eoa-0 - eoa-*, eth-0 - eth-*, usb-0, wlan-0
Service Provider	This is the name of the Dynamic DNS service provider where the user has registered and has an account.Some examples are www.tzo.com,www.dyndns.org
User Name	Username registered at service provider. The value is to be given in double quotes.
Type of system	This parameter is valid only when SrvcName is DYNDNS.www.dyndns.org provides 3 kinds of services - Dynamic DNS, Custom DNS and Static DNS. The user can create different domains in these systems.Custom DNS service is a full DNS solution for newly purchased domains or domains you already own. A web-based interface provides complete control over resource records and your entire domain including support for dynamic IPs and automated updates.Static DNS service points a DNS hostname in some domain owned by dyndns.org to the user's ISP-assigned static or pseudo-static (meaning which do not change too frequently) IP address.DynDNS service points a fixed hostname in some domain owned by dyndns.org to the user's ISP-assigned dynamic IP address. This allows more frequent updation of IP addresses than Static DNS.
WildCard	This parameter is valid only if SrvcName is DYNDNS.It specifies whether Wildcard CNAME are to be resolved or not. If enabled, addresses *.yourhost.ourdomain.ext are aliased to the same address as yourhost.ourdomain.ext.
Mail Exchanger	This parameter is valid only if SrvcName is DYNDNS. It specifies a Mail Exchanger (MX) for use with the hostname being modified. The specified MX must resolve to an IP address,or it will be ignored.Providing no MX setting (or an MX that doesn't resolve properly to an A record) will cause the hostname's MX record(s) to be removed.
Mail Backup	This parameter is valid only if SrvcName is DYNDNS.It specifies whehter mails are to be backed up by the service provider.
Offline Support	This parameter is valid only if SrvcName is DYNDNS.If enabled, the service provider redirects browsers to its own site if the registered host is currently offline.

Cautions None.

References

- *get ddns intf* command
- *delete ddns intf* command

3.15 create dhcp relay intf

Description Use this command to enable the specified interface for DHCP relay.

Command Syntax ***create dhcp relay intf ifname*** interface-name

Parameters

Name	Description
ifname interface-name	This specifies the Interface which is to be enabled for DHCP Relay **Type:** Mandatory **Valid values:** *eth-0, eoa-0 - *, ppp–0 - *, ipoa-0-* and usb-0*

Mode Super-User

Example ***$ create dhcp relay intf ifname*** **eth-0**

Output Verbose Mode On:

```
Entry Created

If-name
-------
eth-0
```

Verbose Mode Off:

```
Entry Created
```

Output field description

Field	Description
If-Name	This specifies an interface which is enabled for DHCP Relay. It can be: *eth-0, ppp-0, ppp-1,…*

Caution None.

References

- *delete dhcp relay intf* command
- *get dhcp relay intf* related commands
- *dhcp relay cfg* related commands
- *dhcp relay stats* related commands
- *create ethernet intf* related commands
- *create ppp intf* related commands.

3.16 create dhcp server exclude

Description Use this command to create an entry in the address exclusion table. While assigning addresses to DHCP clients, the DHCP server does not use the IP addresses that are added in the address exclusion table.

Command Syntax ***create dhcp server exclude ip*** ip-address

Parameters

Name	Description
ip ip-address	The IP address that has to be excluded. The IP Address must belong to a pool **Type:** Mandatory **Valid values:** Any valid class A/B/C IP address

Mode Super-User

Example ***$ create dhcp server exclude ip*** **192.168.1.5**

Output Verbose Mode On:

```
Entry Created

Ip Address
----------
192.168.1.5
```

Verbose Mode Off:

```
Entry Created
```

Output field description

Field	Description
ip Address	This is the IP Address that has been excluded.

Caution The IP Address specified must belong to a pool.

References

- *get dhcp server exclude* command
- *delete dhcp server exclude* related commands
- *dhcp server pool* related commands.

3.17 create dhcp server host

Description

This command is used to create a DHCP static host entry. Whenever a client with the same MAC address as specified in the entry requests an IP address, the server assigns it the address as given in the entry. The client with the given MAC address always gets this same IP address whenever it boots.

Command Syntax

create dhcp server host ip ip-address ***mask*** ip-address ***hwaddr*** hw-address ***[dname*** domain-name***]***
[{pop3|nntp|web|irc|wins|swins|dns|sdns|gwy|smtp} ip-address***]* [dlease*** default-lease-time***] [mlease*** max-lease-time***]***

Parameters

Name	Description
ip ip-address	This specifies the IP address to be provided to this host **Type:** Mandatory **Valid values:** Any valid class A/B/C IP address
mask ip-address	This specifies the subnet mask to be provided to the host **Type:** Mandatory **Valid values:** *128.0.0.0 – 255.255.255.254*
hwaddr hw-address	This specifies the hardware address of the client. **Type:** Mandatory **Valid values:** *0:0:0:0:0:0 – ff:ff:ff:ff:ff:ff*
dname domain-name	Specifies the domain name configured for this host **Type:** Optional **Valid values:** String of length 64 with valid characters ‘a’-‘z’, ’A’-‘Z’, ’0’-‘9’, ’-‘, ’_’and ‘.‘ **Default value:** null
gwy ip-address	This specifies the default gateway IP address **Type:** Optional **Valid values:** Any valid class A/B/C IP address **Default value:** *0.0.0.0*
pop3 ip-address	This specifies the IP address of the POP3 Server **Type:** Optional **Valid values:** Any valid class A/B/C IP address **Default value:** *0.0.0.0*
nntp ip-address	This specifies the IP address of the NNTP Server **Type:** Optional **Valid values:** Any valid class A/B/C IP address **Default value:** *0.0.0.0*
web ip-address	This specifies the IP address of the WWW Server **Type:** Optional **Valid values:** Any valid class A/B/C IP address **Default value:** *0.0.0.0*
irc ip-address	This specifies the IP address of the IRC Server **Type:** Optional **Valid values:** Any valid class A/B/C IP address **Default value:** *0.0.0.0*

Name	Description
wins ip-address	This specifies the IP address of the primary WIN Server **Type:** Optional **Valid values:** Any valid class A/B/C IP address **Default value:** *0.0.0.0*
swins ip-address	This specifies the IP address of the secondary WIN Server **Type:** Optional **Valid values:** Any valid class A/B/C IP address **Default value:** *0.0.0.0*
dns ip-address	This specifies the IP address of the primary Domain Name Server **Type:** Optional **Valid values:** Any valid class A/B/C IP address **Default value:** *0.0.0.0*
sdns ip-address	This specifies the IP address of the secondary Domain Name Server **Type:** Optional **Valid values:** Any valid class A/B/C IP address **Default value:** *0.0.0.0*
smtp ip-address	This specifies the IP address of the SMTP Server **Type:** Optional **Valid values:** Any valid class A/B/C IP address **Default value:** *0.0.0.0*
dlease default-lease-time	This specifies the lease period for which the server assigns an IP address to a client in case the client does not request for a specific lease period itself. **Type:** Optional **Valid values:** *0 -mlease* **Default value:** *2592000 seconds (this equals 30 days)*
mlease max-lease-time	This specifies the maximum period for which the DHCP server can lease out an IP address to a DHCP client. **Type:** Optional **Valid values:** *0 – 4294967295* **Default value:** *31536000* seconds (this equals 1 year)

Mode Super-User

Example

```
$ create dhcp server host ip 192.168.1.7 mask 255.255.255.0
hwaddr 12:34:45:56:3:2
```

Output Verbose Mode On:

```
Entry Created

Host Ip          : 192.168.1.7        Hardware Addr    : 12:34:45:56:03:02
Def Lease(sec)   : 2592000            Max Lease(sec)   : 31536000
Domain Name      :
Subnet Mask      : 255.255.255.0
Gateway Ip       : 0.0.0.0            Smtp Ip          : 0.0.0.0
Dns Ip           : 0.0.0.0            Sec. Dns Ip      : 0.0.0.0
Pop3 Ip          : 0.0.0.0            Nntp Ip          : 0.0.0.0
Www Ip           : 0.0.0.0            Irc Ip           : 0.0.0.0
Wins Ip         : 0.0.0.0             Sec. Wins Ip     : 0.0.0.0
```

Verbose Mode Off:

```
Entry Created
```

Output field description

Field	Description
Host Ip	This specifies the IP address to be provided to this host.
Hardware Addr	This specifies the hardware address of the client
Def Lease	This specifies the lease period for which the server assigns an IP address to a client in case the client does not request for a specific lease period itself.
Max Lease	This specifies the maximum period for which the DHCP server can lease out an IP address to a DHCP client.
Domain Name	Specifies the domain name configured for this host
Subnet Mask	This specifies the subnet mask to be provided to the host
Gateway Ip	This specifies the default gateway IP address
Smtp Ip	This specifies the IP address of the NNTP Server
Dns Ip	This specifies the IP address of the primary Domain Name Server
Sec.Dns Ip	This specifies the IP address of the secondary Domain Name Server
Pop3 Ip	This specifies the IP address of the POP3 Server
Nntp Ip	This specifies the IP address of the SMTP Server
Www Ip	This specifies the IP address of the WWW Serve
Irc Ip	This specifies the IP address of the IRC Server
Wins Ip	This specifies the IP address of the primary WIN Server
Sec. Wins Ip	This specifies the IP address of the secondary WIN Server

Caution None.

References

- *get dhcp server host* command
- *delete dhcp server host* related commands
- *modify dhcp server host* related commands
- *dhcp server* related commands.

3.18 create dhcp server pool

Description Use this command to create a DHCP server pool.

Command Syntax

```
create dhcp server pool [pool-id pool-id] start-ip ip-address
end-ip ip-address mask ip-address [dname domain-name]
{{pop3|nntp|web|irc|wins|swins|dns|sdns|gwy|smtp} ip-
address}* [enable|disable] [lthres low-threshold] [dlease
default-lease-time] [mlease max-lease-time]
```

Parameters

Name	Description
pool-id pool-id	This specifies the Pool Id to be assigned to the newly created pool. If no id is specified then the pool is automatically assigned a pool id which is free. **Type:** Optional **Valid values:** 0-* , where * dependes upon the iad.conf value
start-ip ip-address	The IP address of the first address in the range. The value of range start must be less than or equal to the value of range end **Type:** Mandatory **Valid values:** Any valid class A/B/C IP address
end-ip ip-address	The IP address of the last address in the range. The value of range end must be greater than or equal to the value of range start. **Type:** Mandatory **Valid values:** Any valid class A/B/C IP address
mask ip-address	This specifies the subnet mask provided to any client offered an address from this range **Type:** Mandatory **Valid values:** *128.0.0.0 – 255.255.255.254*
dname domain-name	Domain name used per subnet. **Type:** Optional **Valid values:** String of length 64 with valid characters ‘a’-‘z’, ’A’-‘Z’, ’0’-‘9’, ’-‘, ’_’and ‘.‘ **Default value:** null
gwy ip-address	This specifies the default gateway IP address **Type:** Optional **Valid values:** Any valid class A/B/C IP address **Default value:** *0.0.0.0*
pop3 ip-address	This specifies the IP address of the POP3 Server **Type:** Optional **Valid values:** Any valid class A/B/C IP address **Default value:** *0.0.0.0*
nntp ip-address	This specifies the IP address of the NNTP Server **Type:** Optional **Valid values:** Any valid class A/B/C IP address **Default value:** *0.0.0.0*

Name	Description
web ip-address	This specifies the IP address of the WWW Server **Type:** Optional **Valid values:** Any valid class A/B/C IP address **Default value:** *0.0.0.0*
irc ip-address	This specifies the IP address of the IRC Server **Type:** Optional **Valid values:** Any valid class A/B/C IP address **Default value:** *0.0.0.0*
wins ip-address	This specifies the IP address of the primary WIN Server **Type:** Optional **Valid values:** Any valid class A/B/C IP address **Default value:** *0.0.0.0*
swins ip-address	This specifies the IP address of the secondary WIN Server **Type:** Optional **Valid values:** Any valid class A/B/C IP address **Default value:** *0.0.0.0*
dns ip-address	This specifies the IP address of the primary Domain Name Server **Type:** Optional **Valid values:** Any valid class A/B/C IP address **Default value:** *0.0.0.0*
sdns ip-address	This specifies the IP address of the secondary Domain Name Server **Type:** Optional **Valid values:** Any valid class A/B/C IP address **Default value:** *0.0.0.0*
smtp ip-address	This specifies the IP address of the SMTP Server **Type:** Optional **Valid values:** Any valid class A/B/C IP address **Default value:** *0.0.0.0*
dlease default-lease-time	This specifies the lease period for which the server assigns an IP address to a client in case the client does not request for a specific lease period itself. **Type:** Optional **Valid values:** *0 -mlease* **Default value:** *2592000 seconds (this equals 30 days)*
mlease max-lease-time	This specifies the maximum period for which the DHCP server can lease out an IP address to a DHCP client. **Type:** Optional **Valid values:** *0 – 4294967295* **Default value:** *31536000 seconds (this equals 1 year)*

Name	Description
enable*|*disable	The state the pool is to be set in. **Type:** Optional **Valid values:** *enable, disable* **Default value:** *enable*
lthres low-threshold	Specifies the lowest threshold value on the number of available IP addresses for a particular shared network. If the number of free IP addresses fall below this value, then a trap is raised. This value has to be less than the pool size specified using the start and end ip addresses. **Type:** Optional **Valid values:** *0 – 255* **Default value:** *0*

Mode Super-User

Example ***$ create dhcp server pool start-ip*** **192.168.1.1** ***end-ip*** **192.168.1.200** ***mask*** **255.255.255.0**

Output Verbose Mode On:

```
Entry Created

Pool Id          : 0                 Status           : Disable
Start Ip         : 192.168.1.1       End Ip           : 192.168.1.200
Def Lease(sec)   : 2592000           Max Lease(sec)   : 31536000
Range Inuse      : 0                 Outstd Offers    : 0
Low Thres        : 0                 Subnet Mask      : 255.255.255.0
Domain Name      :
Gateway Ip       : 0.0.0.0           Smtp Ip          : 0.0.0.0
Dns Ip           : 0.0.0.0           Sec. Dns Ip      : 0.0.0.0
Pop3 Ip          : 0.0.0.0           Nntp Ip          : 0.0.0.0
Www Ip           : 0.0.0.0           Irc Ip           : 0.0.0.0
Wins Ip         : 0.0.0.0           Sec. Wins Ip    : 0.0.0.0
```

Verbose Mode Off:

```
Entry Created
```

Output field description

Field	Description
Pool Id	This is the pool identifier.
Status	This defines the Admin status of the entry. It may be: *Enable, Disable*
Start Ip	The IP address of the first address in the range.
End Ip	The IP address of the last address in the range
Def Lease	This specifies the lease period for which the server assigns an IP address to a client in case the client does not request for a specific lease period itself.
Max Lease	This specifies the maximum period for which the DHCP server can lease out an IP address to a DHCP client.

Field	Description
Range Inuse	The number of addresses in this range that are currently in use. This number includes those addresses whose lease has not expired and addresses which have been reserved
Outstd Offers	The number of outstanding DHCPOFFER messages for this range is reported with this value. An offer is outstanding if the server has sent a DHCPOFFER message to a client, but has not yet received a DHCPREQUEST message from the client nor has the server-specific timeout, within which a client can respond to the offer message, for the offer message expired
Low Thres	This specifies the lowest threshold value on the number of available/ free IP addresses for a particular shared network
Subnet Mask	The subnet mask provided to any client offered an address from this range
Domain Name	Domain name used per subnet.
Gateway Ip	This specifies the default gateway IP address
Smtp Ip	This specifies the IP address of the NNTP Server
Dns Ip	This specifies the IP address of the primary Domain Name Server
Sec.Dns Ip	This specifies the IP address of the secondary Domain Name Server
Pop3 Ip	This specifies the IP address of the POP3 Server
Nntp Ip	This specifies the IP address of the SMTP Server
Www Ip	This specifies the IP address of the WWW Serve
Irc Ip	This specifies the IP address of the IRC Server
Wins Ip	This specifies the IP address of the primary WIN Server
Sec.Wins Ip	This specifies the IP address of the secondary WIN Server

Caution No two pools can overlap i.e. an IP Address cannot belong to more than 1 pool.

References

- *get dhcp server pool* command
- *delete dhcp server pool* related commands
- *modify dhcp server pool* related commands
- *dhcp server cfg* related commands
- *dhcp server exclude* related commands
- *dhcp server address* related commands.

3.19 create dns servaddr

Description Use this command to create DNS server addresses.

Command Syntax ***create dns servaddr*** <ip-address>

Parameters :

Name	Description
ip-address	This parameter specifies the IP address for configuring the DNS server address. **Type:** Mandatory **Valid values:** Valid IP address.

Mode Super-User.

Example : ***$ create dns servaddr*** *182.25.2.1*

Output Verbose mode on:

```
Entry Created

DNS Server IP Address
---------------------
182.25.2.1
```

Verbose mode off:

```
Entry Created
```

Output Field description:

Field	Description
DNS Server IP Address	This specifies the IP address of the DNS server.

Caution None

References:

- get dns servaddr
- delete dns servaddr
- modify dns relay cfg
- get dns relay cfg
- get dns relay stats
- reset dns relay stats

3.20 create eoa intf

Description Use this command to create an eoa interface.

Command Syntax

create eoa intf ifname interface-name ***[ip*** ip-address***] [mask*** net-mask***] lowif*** low-interface-name ***[inside|outside|none] [usedhcp true|false] [droute true|false] [ifsectype public|private|dmz] [gwy*** <ddd.ddd.ddd.ddd>***][mtu <decvalue>]***

Parameters

Name	Description
ifname interface-name	This parameter specifies the name assigned to this interface. **Type:** Mandatory **Valid values:** *eoa-0 - **
ip ip-address	The IP address to be assigned to the eoa interface. **Type:** Optional **Valid values:** Any valid class A/B/C IP address **Default value:** *0.0.0.0*
mask net-mask	This parameter specifies the subnet mask to be applied to the IP address. **Type:** Optional **Valid values:** *128.0.0.0 – 255.255.255.254* **Default value:** *0.0.0.0*
lowif low-interface-name	This parameter specifies the lower interface of an eoa interface. **Type:** Mandatory **Valid values:** *aal5-0 - **
inside|outside|none	This specifies the NAT direction for the interface. **Type:** Optional **Valid values:** *inside, outside, none* **Default value:** *none*
usedhcp true|false	This specifies whether a DHCP client is to be triggered to obtain an IP address for this interface from a DHCP server. **Type:** Optional **Valid values:** *true or false* **Default value:** *false*
droute true|false	This specifies the default route **Type:** Optional **Valid values:** *true or false* **Default value:** *false*
ifsectype public|private|dmz	Type of interface security. **Type:** Optional **Valid values :** public, private or dmz **Default Value :** public

Name	Description
gwy <ddd.ddd.ddd.ddd>	This specifies the gateway IP address **Type:** Optional **Valid values:** Any valid class A/B/C IP address **Default value:** *0.0.0.0*
mtu <decvalue>	This specifies the MTU Size configured for EOA interface **Type:** Optional **Valid values :** 120 ..65535 **Default Values:** 65535

Mode Super-User

Example

```
$ create eoa intf ifname eoa-0 ip 192.168.1.1 mask
255.255.255.0 lowif aal5-0 none ifsectype public mtu 300
```

Output Verbose Mode On:

```
IfName               : eoa-0          Interface Sec Type : Public
Configured IP Address: 0.0.0.0        Mask               : 0.0.0.0
Low IfName           : aal5-0         NAT Direction      : OUT
Gateway              : 0.0.0.0       DRoute             : False
Oper Status          : Down           Admin Status       : Up
UseDHCP              : False
Configured MTU       : 500           Actual MTU         : 300
```

Verbose Mode Off:

```
Entry Created
```

Output field description

Field	Description
IfName	The name of the interface which has been created.
Configured IpAddress	IP address assigned to the eoa interface.
Mask	Network mask to be applied to the IP Address.
LowIfName	Specifies the lower interface.
Nat Direction	This specifies the NAT direction which may be: *inside, outside or none*.
Oper Status	The actual/current state of the interface. It can be either *Up* or *Down*
Admin Status	The desired state of the interface. It may be either *Up* or *Down*
UseDhcp	Whether or not a DHCP client is used to obtain the IP address for this interface from a DHCP server
Interface Sec Type	Interface Security Type.
Droute	Default route
Gateway address	Gateway IP address

Field	Description
Configured MTU	This specifies the MTU value configured by the user for the EOA interface.
Actual MTU	This specifies the MTU value actually operational for the EOA interface.

Caution None.

References

- *get eoa intf* command
- *delete eoa intf* command
- *modify eoa intf* command
- *eoa stats* related commands
- *interface stats* related commands
- *atm vc intf* related commands

3.21 create ethernet intf

Description

Use this command to create a physical or a virtual Ethernet interface. The type of interface to be created is identified by the name of the interface.

Command Syntax

create ethernet intf ifname interface-name ***[ip*** ip-address***]*** ***[mask*** net-mask***]*** ***[phyif*** low-interface-name***]*** ***[inside|outside|none]*** ***[usedhcp local|remote|false]*** ***[ifsectype public|private|dmz]*** ***[mtu <decvalue>]***

Parameters

Name	Description
ifname interface-name	This parameter specifies the name which will be used to refer to the interface in future. The interface type, i.e., whether it is physical or virtual is implicit in the name. *eth* (e.g., *eth-0*) specifies a physical interface and *veth* (eg *veth-0*, *veth-1* etc.) specifies a virtual interface. **Type**: Mandatory **Valid values:** *eth-0, veth-0 - **
ip ip-address	The IP address to be assigned to the Ethernet interface. **Type:** Mandatory only when virtual interface is specified, i.e., it is not eth-0 **Valid values:** Any valid class A/B/C IP address. *0.0.0.0* is invalid for a virtual ethernet interface. **Default value:** *0.0.0.0*
Mask net-mask	This parameter specifies the subnet mask to be applied to the IP address. Mask not allowed when usedhcp true, along with ip 0.0.0.0 **Type:** This field is not allowed when a physical interface is specified and ip is *0.0.0.0*. In all other cases the field is mandatory. **Valid values:** *255.0.0.0 – 255.255.255.255* **Default value:** *255.0.0.0*
phyif low-interface-name	When a virtual interface is being created, this specifies the lower interface name to be specified. This can be the interface name of a physical ethernet interface only. **Type:** Optional for virtual (*veth*) interfaces. Not allowed for physical (*eth*) interfaces. **Valid values:** *eth-0* **Default value:** *eth-0*
inside|outside|none	This specifies the NAT direction for the interface. **Type:** Optional **Valid values:** *inside, outside, none* **Default value:** *none*

Name	Description
usedhcp local|remote|false	Local: IP address for this interface is obtained from a local DHCP server Remote: DHCP client is used to obtain the IP address for this interface from a remote DHCP server False: DHCP client is not used. **Type:** Optional **Valid value**: *local, remote, false* **Default value:** *false*
ifsectype public|private|dmz	IP Filter Interface type **Type:** Optional **Valid values :** public, private or dmz **Default Value :** private
mtu <decvalue>	This specifies the MTU Size configured on ethernet interface. **Type:** Optional **Valid values :** 120 ..1500 **Default Value :** 1500

Mode Super-User

Example ***$ create ethernet intf ifname eth-0 ip 192.168.1.1 mask 255.255.0.0 ifsectype private inside mtu 300***

Output Verbose Mode On:

```
Entry Created

Interface          : veth-0         MTU                   : 300
IP Filter Type     : Public         Configured IP Address : 192.168.1.1
Mask               : 255.255.255.0  UseDhcp               : False
Physical Interface : eth-0          Nat Direction         : None
Configured Duplex  : half           Duplex                : half
Configured Speed   : auto           Speed                 : 10BT
Operational Status : Up             Admin Status          : Up
```

Verbose Mode Off:

```
Entry Created
```

Output field description

Field	Description
Interface	The name of the interface which has been created.
Configured Ip Address	IP address assigned to the Ethernet port.
Mask	Network mask to be applied to the IP Address.
UseDhcp	Local: IP address for this interface is obtained from a local DHCP server Remote: DHCP client is used to obtain the IP address for this interface from a remote DHCP server False: DHCP client is not used.

Field	Description
Physical Interface	Valid only in case of virtual interfaces i.e. the Type is not *eth*. It can only be *eth-0*
Nat Direction	This specifies the NAT direction which may be: *inside, outside or none*.
Operational Status	The actual/current state of the interface. It can be either *up* or d*own*
Admin Status	The desired state of the interface. It may be either *up* or *down*
Configured Duplex	The duplex mode to be used by the interface as configured by the user
Duplex	The duplex mode used by the interface
Configured Speed	Line speed to be used by Ethernet interface as configured by the user
Speed	Line speed used by Ethernet interface
IP Filter Type	IP Filter interface type.
MTU	This specifies the MTU Size configured on the Ethernet interface.

Caution A virtual interface (*veth-0, veth-1* etc.) cannot be created unless a physical interface (i.e. *eth-0*) exists.

References

- *get ethernet intf* command
- *delete ethernet intf* command
- *modify ethernet intf* related commands
- *ethernet stats* related commands
- *interface stats* related commands.

3.22 create igmp intf

Description Use this command to start IGMP over a given IP interface.

Command Syntax ***create igmp intf ifname*** <interface-name> ***[qinterval*** <query-interval>***] [robust*** <robustness-variable>***] [host|router] [version igmpv1|igmpv2] [qmaxresponsetime < qmaxresponsetime >] [lmqinterval < lmqinterval >]***

Parameters

Name	Description
ifname <interface-name>	This identifies the interface on which IGMP is enabled. **Type:** Mandatory **Valid values:** *eth-0*, veth-0 - *, ppp-0 - *, eoa-0 - *, usb-0, ipoa-0-* **Default value:** *None*.
qinterval <query-interval>	This specifies the periodic interval in seconds at which host-query messages (queries) are transmitted on this interface. **Type:** Optional **Valid values:** 1-*4294967295* **Default value:** 125 seconds
robust <robustness-variable>	The Robustness Variable allows tuning for the expected packet loss on a subnet. If a subnet is expected to be lossy, the Robustness Variable may be increased. IGMP is robust to (Robustness Variable-1) packet losses. **Type:** Optional. **Valid values:** 1-255 **Default value:** *2*
host|router	This tells whether the interface is configured as IGMP Host Interface or IGMP Router Interface **Type:** Optional. **Valid values:** host or router **Default value:** router
Version igmpv1|igmpv2	This identifies the version of IGMP. **Type:** Optional **Valid values:** igmpv1 and igmpv2 **Default value:** igmpv2
qmaxresponsetime < qmaxresponsetime>	This identifies the query max response time (in secs) **Type:** Optional **Valid Values:** Any decimal value. **Default value:** 10
lmqinterval < lmqinterval >	This identifies the Last Member Query Interval (in secs) **Type :** Optional **Valid Values:** Any decimal value. **Default value**: 1

Mode Super-User.

Example

```
$ create igmp intf ifname eth-0 qinterval 150 robust 10
version igmpv1 lmqinterval 2 qmaxresponsetime 10
```

Output Verbose Mode On

```
Entry Created

IfName                   : eth-0         Type                        : Host
Version                  : igmpv1        Query Interval(sec)         : 150
Query Max Resp Time(sec) : 10            Last Memb QueryIntvl(sec)   : 2
Robustness               : 10            Join Requests               : 10
Current Groups           : 8
```

Verbose Mode Off

```
Entry Created
```

Output field description

Field	Description
Query Interval(sec)	This is the periodic interval at which host-query messages (queries) are transmitted on this interface
Version	This field specifies the version of IGMP.
Query Max ResponseTime(sec)	This field specifies the query max response time (in secs)
Last Memb QueryIntvl(sec)	This is the periodic interval at which host-query messages (queries) are transmitted on this interface.
Join Requests	This is the number of times a group membership has been added to this interface
Current Groups	This is the current number of entries for this interface in the IGMP Group Table.

Caution None.

References

- *create igmp intf* command
- *get igmp intf* command
- *get igmp groups* command

3.23 create ilmi intf

Description This command is used for configuring ILMI based auto configuration parameters on an ATM interface.

Command Syntax ***create ilmi intf ifname*** interface-name ***[enable|disable] [vpi*** vpi-number***] [vci*** vci-number***] [timeout*** time-out***] [keepalive*** keep-alive***] [maxretry*** max-retry***]***

Parameters

Name	Description
ifname interface-name	It specifies the ATM port on which ILMI based auto configuration is to be configured. **Type:** Mandatory **Valid values:** *atm-0.*
enable|disable	Whether ILMI based auto configuration is enabled or not on this interface **Type:** Optional **Valid values:** *enable, disable* **Default value:** *disable*
vpi vpi-number	VPI to be used for ILMI SNMP message exchanges **Type:** Optional **Valid values:** *0 - 255* **Default value:** *0*
vci vci-number	VCI to be used for ILMI SNMP message exchanges **Type:** Optional **Valid values:** *0-65535* **Default value:** *16*
timeout time-out	Timeout value in seconds, for SNMP Get/Set messages exchanged between peer Interface Management Entities (IMEs). **Type:** Optional **Valid values:** *1-65535* **Default value:** *1*
keepalive keep-alive	The time-interval in seconds, ILMI should use to poll for peer ILMI's availability. **Type:** Optional **Valid values:** *1-65535* **Default value:** *5*
maxretry max-retry	Number of times ILMI should retry before declaring ILMI connectivity as lost. **Type:** Optional **Valid values:** 0-65535 **Default value:** 4

Mode Super-User

Example ***$ create ilmi intf ifname atm-0 enable vpi*** 10 ***vci*** 5 ***timeout*** 3 ***keepalive*** 5 ***maxretry*** 11

Output

Verbose Mode On:

```
Entry Created

Interface:    : atm-0          Status            : Enable
VPI           : 10             VCI               : 5
Timeout(sec) : 3               Keep Alive (sec)  : 5
Max Retries   : 11             Version           : 4.0
```

Verbose Mode Off:

```
Entry Created
```

Output field description

Field	Description
Interface	It specifies the ATM port on which ILMI based auto configuration is to be configured.
Status	Whether ILMI based auto configuration is enabled or not on this interface.
VPI	VPI to be used for ILMI SNMP message exchanges
VCI	VCI to be used for ILMI SNMP message exchanges.
Timeout	Timeout value for SNMP Get/ Set messages exchanged between peer IMEs.
Keep Alive	The time-interval, ILMI should use to poll for peer ILMI's availability.
Max Retries	Number of times ILMI should retry before declaring ILMI connectivity as lost.
Version	The version of ILMI

Caution

Enabling the ILMI interface only marks the state of the interface as enabled. The actual procedure begins only after the *trigger ilmi* command is given, or after the modem is rebooted. On the other hand, to disable the procedure, it is sufficient set the ILMI interface state as disabled.

References

- *get ilmi intf* command
- *modify ilmi intf* command
- *modify ilmi trigger* command
- *trigger ilmi* command
- *get ilmi access protocol* command

3.24 create ip route

Description Use this command to create a routing table entry.

Command Syntax ***create ip route ip*** dest-ip-address ***gwyip*** gwy-ip-address ***mask*** net-mask

Parameters

Name	Description
ip dest-ip-address	Destination IP address of this route. **Type:** Mandatory **Valid values:** Any valid class A/B/C address
gwyip gwy-ip-address	The IP address of the next hop for this route. **Type:** Mandatory **Valid values:** Any valid class A/B/C address
mask net-mask	The Mask of the destination IP Address. **Type:** Mandatory **Valid values:** *128.0.0.0 – 255.255.255.254*

Mode Super-User

Example ***$ create ip route ip 192.168.2.40 gwyip 192.168.1.1 mask 55.255.255.0***

Output Verbose Mode On:

```
Entry Created

Destination     Mask           Gateway      If-name   Route  Route  Age(sec)
                                                        Type   Orig
-------------------------------------------------------------------------------
192.168.2.40    255.255.255.0  192.168.1.1  veth-0    IND    LCL    0
```

Verbose Mode Off:

```
Entry Created
```

Output field description

Field	Description
Destination	Destination IP address of this route
Mask	The Mask of the destination IP Address
Gateway	The IP address of the next hop for this route
If-Name	The local interface through which the next hop of this route will be reached
Route Type	The type of route. It may be: *dir* (for Direct), *ind* (for Indirect), or inv (for invalid route)

Field	Description
Route Orig	The routing mechanism through which this route was learned. It may be: *NET* (for Network Management), *LCL* (for Local), *RIP*, *ICMP*,*DYI* (Dynamic through Interface creation)
Age	The number of seconds since this route was last updated or otherwise determined to be correct

Caution None.

References

- *get ip route* command
- *delete ip route* command
- *ip stats* related commands
- *ip cfg* related commands
- *ip address* related commands
- *arp* related commands

3.25 create ipf rule entry

Description This command is used for creating an IP filter rule.

Command Syntax

```
create ipf rule entry
ruleid rule-id
[ifname interface-name|public|private|dmz|all]
[dir in|out]
[inifname interface-name|public|private|dmz|all]
[act accept|deny]
[log enable|disable]
[enable|disable]
[srcaddr {lt|lteq|gt|gteq|eq|neq
<ddd.ddd.ddd.ddd>}|{{range|erange} <ddd.ddd.ddd.ddd>
<ddd.ddd.ddd.ddd>}|any|self]
[destaddr {lt|lteq|gt|gteq|eq|neq
<ddd.ddd.ddd.ddd>}|{{range|erange} <ddd.ddd.ddd.ddd>
<ddd.ddd.ddd.ddd>}|any|bcast|self]
[srcport {lt|lteq|gt|gteq|eq|neq {num
<decvalue>}|echo|discard|chargen|ftp|telnet|smtp|dns|boot|tf
tp|http|pop3|snmp >}|{{range|erange} <decValue>
<decValue>}|any]
[destport {lt|lteq|gt|gteq|eq|neq {num
<decvalue>}|echo|discard|chargen|ftp|telnet|smtp|dns|boot|tf
tp|http|pop3|snmp >}|{{range|erange} <decValue>
<decValue>}|any]
[icmpcode {eq|neq <decValue>}|any]
[icmptype {eq|neq  echoreq|unreach|redir|echorep|{num
<decValue>}}|any]
[transprot {eq|neq TCP|UDP|ICMP|{num <decValue>}}|any]
[tcpflag syn|nosyn|any]
[storestate enable|disable]
[seclevel {high|medium|low}+] [blistprotect enable|disable]
[logtag "log-tag"] [isfrag yes|no|ignore] [isipopt
yes|no|ignore]
[pktsize {lt|lteq|gt|gteq|eq|neq <decvalue>}|any]
[todfrom <hh:mm:ss>] [todto <hh:mm:ss>] [todstatus
enable|disable]
```

Parameters

Name	Description
ruleid rule-id	The index given by the caller to identify the rule entry. **Type**: Mandatory **Valid values:** *1-4294967295*
ifname interface-name|public|private|dmz|all	This specifies the IP enabled physical interface to be associated to this Rule. 'ALL' indicates that Rule is to be associated to all interfaces. Public, Private or DMZ indicates that rule is to be associated with public, private or DMZ type of interfaces recpectively. **Type**: Optional **Valid values** : eth-0,veth, eoa,ppp,usb or public/private/dmz interfaces. **Default value** : all

Name	Description
Dir in|out	Specifies the direction of data flow on which filtering is to be applied. **Type:** Optional **Valid values:** *in, out* **Default value:** *out*
Act accept|deny	Specifies the action to be taken when a packet matches a rule. **Type**: Optional **Valid values:** *accept, deny* **Default value:** *deny*
[log enable|disable]	This flag controls the logging of matched packets. Each log will contain IP header and TCP/UDP header or ICMP fields, if available. **Type**: Optional **Valid values:** *enable|disable* **Default value:** *disable*
Srcaddr {lt|lteq|gt|gteq|eq|neq <ddd.ddd.ddd.ddd>***}|{{range|erange}*** <ddd.ddd.ddd.ddd> <ddd.ddd.ddd.ddd>***}|any***	Specifies the matching criteria for source IP address. **Type**: Optional **Valid values:** *lt* (less than), *lteq* (less than or equal to), *gt* (greater than), *gteq* (greater than or equal to), *eq* (equal to), *neq* (not equal to), *range* (in the range), *erange* (out of the range) and *any*. *Any* is used when no comparison has to be done. For *range* and *erange*, both the specified IP addresses are inclusive. **Default value:** *any*
Destaddr {lt|lteq|gt|gteq|eq|neq <ddd.ddd.ddd.ddd>***}|{{range|erange}*** <ddd.ddd.ddd.ddd> <ddd.ddd.ddd.ddd>***}|any***	Specifies the matching criteria for destination IP address. **Type**: Optional **Valid values:** *lt* (less than), *lteq* (less than or equal to), *gt* (greater than), *gteq* (greater than or equal to), *eq* (equal to), *neq* (not equal to), *range* (in the range), *erange* (out of the range) and *any*. *Any* is used when no comparison has to be done. For *range* and *erange*, both the specified IP addresses are inclusive. **Default value:** *any*
Srcport {lt|lteq|gt|gteq|eq|neq {num <decvalue>}|echo|discard|chargen|ftp|telnet|smtp|dns|boot|tftp|http|pop3|snmp>}|{{range|erange} <decValue> <decValue>}|any]	Specifies the matching criteria for source port **Type:** Optional **Valid values:** *lt* (less than), *lteq* (less than or equal to), *gt* (greater than), *gteq* (greater than or equal to), *eq* (equal to), *neq* (not equal to), *range* (in the range), *erange* (out of the range) and *any*. *Any* is used when no comparison has to be done. For *range* and *erange*, both the specified values are inclusive. This field can have valid values of echo, discard, chargen, ftp, telnet, smtp, dns, boot, tftp, http, pop3, snmp and any decimal value. **Default value:** *any*

Name	Description
Destport {lt|lteq|gt|gteq|eq|neq {num <decvalue>}|echo|discard|chargen|ftp|telnet|smtp|dns|boot|tftp|http|pop3|snmp>}|{{range|erange} <decValue> <decValue>}|any|self	Specifies the matching criteria for destination Port. **Type:** Optional **Valid values:** *lt* (less than), *lteq* (less than or equal to), *gt* (greater than), *gteq* (greater than or equal to), eq (equal to), *neq* (not equal to), *range* (in the range), *erange* (out of the range) and *any*. *Any* is used when no comparison has to be done. For *range* and *erange*, both the specified values are inclusive. This field can have valid values of echo, discard, chargen, ftp, telnet, smtp, dns, boot, tftp, http, pop3, snmp and any decimal value. **Default value:** *any*
Icmpcode {eq|neq <decValue>}|any	Specifies the matching criteria for ICMP code value. **Type:** Optional **Valid values:** Decimal value(0-255) which is specified in case of ICMP packets need filtering based on code field in ICMP header. Any is used when no comparison has to be done. **Default value:** *any*
Icmptype {eq|neq echoreq|unreach|redir|echorep|{num <decValue>}|any	Specifies the matching criteria for ICMP Type **Type**. Optional **Valid values**: Decimal value (0-255) which is specified in case of ICMP packets need filtering based on type field in ICMP header. It can also take values echoreq, unreach, redir, echorep. Any is used when no comparison has to be done. **Default value**: any
transprot {eq|neq TCP|UDP|ICMP| <decValue>}|any	Specifies the matching criteria for transport protocol field. **Type:** Optional **Valid values:** *TCP, UDP*, *ICMP*, <decValue> **Default value:** *any*
inifname interface-name|public|private|dmz|all	This field specifies the input interface id which may be used to dictate the rules like accept/deny all traffic from a specific interface or a spefic type of interface namely Public, Private , or DMZ. So, this field can be specified only if direction is out. **Type** : Optional **Valid values** : eth-0,veth, eoa,ppp,usb or all interfaces. **Default value** : all
enable|disable	This specifies administrative status of Rule entry. **Type:** Optional **Valid values:** *enable* or *disable* **Default value:** *disable*
tcpflag syn|nosyn|any	Specifies filtering criteria for TCP packet types. **Type:** Optional **Valid values:** *syn* or *nosyn* or *any* **Default value:** *any*

Name	Description
storestate enable|disable	If this flag is enabled then stateful filtering is done and the rule action is also applied in the other direction on the given interface. **Type:** Optional **Valid values:** *enable* or *disable* **Default value:** *disable*
seclevel high,medium,low	It specifies at which security level(s) this rule is applicable. A rule can be applicable at multiple security levels. **Type** : Optional **Valid values** : high,medium and low **Default Value** : low
blistprotect enable|disable	This specifies whether source of the packet should be blacklisted if it matches with the rule. It will be applicable to deny kind of rules. **Type** : Optional **Valid values** : enable or disable **Default Value** : enable
logtag "log-tag"	This specifies the Filter logging tag, which will be added to all the logs generated due to the rule **Type** : Optional **Valid values** : Display string of 16 char in quotes **Default Value** : NULL
isfrag yes|no|ignore	yes: Rule is applicable to fragmented packets only.no: Rule is applicable to non-fragmented packets only.ignore: Applicable irrespective of whether the packet is a fragment or not. **Type** : Optional **Valid values** : yes, no or ignore **Default Value** : ignore
isipopt yes|no|ignore	yes: Rule is applicable to IP packets with IP options only.no: Rule is applicable to IP packets without IP options only.ignore: Rule is applicable irrespective of whether the packet contains IP options or not. **Type** : Optional **Valid values** : yes, no or ignore **Default Value** : ignore
pktsize {lt|lteq|gt|gteq|eq|neq <decvalue>}|any	pktsize {lt|lteq|gt|gteq|eq|neq <decvalue>}|any *Rule* is applicable if packet size value in IP header conforms to this criterion. *Any* implies that packet size value is to be ignored. **Type** : Optional **Valid values** : 0- 65535 **Default Value** : any
Todfrom <hh:mm:ss>	This field specifies the wall time for starting a Time of Day based rule **Type** : Optional **Valid values** : *00:00:00 to23:59:59* **Default Value** : *00:00:00*

Name	Description
Todto <hh:mm:ss>	This field specifies the wall time for stopping a Time of Day based rule. **Type** : Optional **Valid values** : *00:00:00 to23:59:59* **Default Value** : *23:59:59*
todstatus enable|disable	This field specifies whether a Time of Day based rule should be applied for duration specified using start time and stop time. Active indicate that the TOD based rule should be applied from Start time to Stop time, while Inactive indicates that rule is not applicable from Start Time to stop time but it is applicable for remaining time of the day. **Type** : Optional **Valid values** : enable or disable **Default Value** : enable

Mode Super-User.

Example

```
$ create ipf rule entry ruleid 1 ifname eth-0 dir out inifname
all act accept log enable enable srcaddr lt 172.25.8.76
destaddr range 172.25.8.70 172.25.8.90 srcport erange 10 20
destport neq 3 icmpcode neq 10 icmptype eq unreach
transprot eq TCP tcpflag syn storestate enable
seclevel high blistprotect enable isfrag yes isipopt no
pktsize lt 10 todfrom 01:02:30 todto 02:01:30 todstatus enable
```

Output Verbose Mode On

```
Entry Created


Rule id           : 1Interface         : eth-0
Rule Admin status : EnableRule Oper Status  : Enable
In interface      : ALLDirection         : Out
Security Level    : HighBlacklist Status          : Enable
Logging           : EnableAction            : Accept
Log Tag           : -
IP Frag Pkt       : Yes         IP Opt Pkt        : No
TCP Flag          : SynStore State       : Enable
Src Addr    : Equal           172.25.8.76
Dest Addr   : Range           172.25.8.70          172.25.8.90
Src Port    : Out Of Range    10                   20
Dest Port   : Not Equal       3
ICMP Code   : Not Equal       10
ICMP Type   : Equal           unreach
TransProt   : Equal           TCP
IP Pkt Size : Less Than       10
TOD Rule    : Enable Between  01:02:30              02:01:30
```

Verbose Mode Off

```
Entry Created
```

Output field description

Field	Description
ruleid	The index given by the caller to identify the rule entry.
Rule Admin Status	This specifies administrative status of Rule entry.
Interface	This specifies the ip enabled physical interface to be associated to this Rule. 'ALL' indicates that Rule is to be associated to all interfaces
In *Interface*	This field specifies the input interface id which may be used to dictate the rules like deny/accept all traffic from a specific interface. So, this field can be specified only if direction is out.
Direction	This specifies the direction of Data flow on which filtering is to be applied.
Action	This specifies the action to be taken when a packet matches a rule .
Logging	This specifies the criteria for the logging of packets. Each log will contain IP Header and TCP/UDP header or ICMP fields, if available.
Log Tag	This specifies the Filter logging tag, which will be added to all the logs generated due to the rule

Field	Description
Scr Addr	This field specifies the matching criteria for source IP Address along with the source IPAddress value and the destination IPAddress value. The source or destination or both are shown depending on whether the matching criteria is relational, range, erange, any or self.
Dest Addr	This field specifies the matching criteria for destination IP Address along with the start destination IPAddress value and end destination IPAddress value. The start or end or both are shown depending on whether the matching criteria is relational, range, erange, any or self.
Src Port	This field specifies the matching criteria for source port along with the start of src port and the end of src port. The start or end or both are shown depending on whether the matching criteria is relational, range, erange, any or bcast.
Dest Port	This field specifies the matching criteria for destination Port along with the start dest port and the end dest port. The start or end or both are shown depending on whether the matching criteria is relational, range, erange, any or bcast.
ICMP Code	This field specifies the matching criteria for ICMP code value along with the code field in ICMP header in case of ICMP packets.
ICMP Type	This field specifies the matching criteria for ICMP Type along with the type field in ICMP header in case of ICMP packets.
TransProt	This field specifies the matching criteria for transport protcol field along with the transport layer protocol number as per IANA.
TCP Flag	This specifies filtering criteria for TCP packet types.
Store State	This specifies whether stateful filtering is done or not
Security Level	This specifies the association of rule with system wide service protection level.
Blacklist Status	This specifies whether source of the packet should be put in blacklist if it matches with the rule. It will be applicable to deny kind of rules
IP Frag Pkt	This specifies whether the rule is applicable to fragmented packets, non fragmented packets or in both cases.
IP Opt Pkt	This specifies whether the rule is applicable to IP packet with or without IP options or in both cases.

Field	Description
IP Pkt Size	This field specifies the matching criteria for IP Pkt Size along with IP packet filtering attribute . It should be compared against the packet size value in IP header.
TOD Rule	This field specifies whether the rule should be applied for the duration specified."Enable Between" indicates that the rule is applied between the specified time duration."Disable Between" indicates that rule is not applicable between the specified duration, but it is applicable for remaining time of the day.
Rule Oper Stat	A rule will be operationally enabled if and only if it is administratively enabled, its Time of Day status as per current time is Enable, and if the rule's security level matches the global security level as shown by get ipf global.

Caution Some standard port numbers, as mentioned in the list below, are used for the following service names, irrespective of the transport protocol selected.

- Echo 7
- Discard 9
- CHARGEN 19
- FTP 21
- TELNET 23
- SMTP 25
- DNS 53
- BOOTP 67
- TFTP 69
- HTTP 80
- POP3 110
- SNMP 161

References

- *modify ipf rule entry* command
- *get ipf rule entry* command
- *delete ipf rule entry* command

3.26 create ipoa intf

Description This command is used for creating an IPoA (IP over ATM) interface.

Command Syntax ***create ipoa intf ifname*** *interface-name* ***ip*** *ip-address* ***mask*** *net-mask* ***[type 1577|non1577] [inside|outside|none] [ifsectype public|private|dmz] [gwy <ddd.ddd.ddd.ddd>] [droute true|false] [usedhcp true|false][mtu <decvalue]***

Parameters

Name	Description
Ifname interface-name	This parameter uniquely identifies the name of the IPoA interface. **Type:** Mandatory **Valid values:** *ipoa-0-*,ipoa-1 etc.*
ip ip-address	The IP address to be assigned to the interface. **Type:** Mandatory **Valid values:** *Valid IP Address.*
mask net-mask	This parameter specifies the subnet mask to be applied to the IP address. **Type:** Mandatory **Valid values:** *255.0.0.0 – 255.255.255.255*
type 1577|non1577	This parameter specifies the type of IPoA interface. **Type:** Optional **Valid Values** : 1577 or non1577 **Default Value:** non1577
inside|outside|none	This specifies the NAT direction. **Type:** Optional **Valid values:** *inside, outside, none* **Default value:** *outside*
ifsectype public|private|dmz	Interface security type. **Type:** Optional **Valid values :** public, private or dmz **Default Value :** public
[gwy <ddd.ddd.ddd.ddd>]	Gateway IP address **Type:** Optional **Valid values :** any valid IP address **Default Value :** 0.0.0.0
droute true|false]	Default Route **Type:** Optional **Valid values :** true or false **Default Value :** False
mtu <decvalue>	This specifies the MTU Size configured for IPOA interface **Type:** Optional **Valid values :** 120 ..65535 **Default Value:** 65535

Mode Super-User.

Example

```
$ create ipoa intf ifname ipoa-0 ip 192.168.1.1 mask
255.255.255.0 type 1577 inside ifsectype public gwy 0.0.0.0
droute false mtu 300
```

Output

Verbose Mode On

```
Entry Created
  IfName               : ipoa-0          UseDHCP           : true
  Type                 : non1577         Interface Sec Type: Public
  Configured IP Address: 172.25.12.74    Mask              : 255.255.0.0
  DRoute               : False           Gateway           : 0.0.0.0
  NAT Direction        : OUT             Oper Status       : Down
  Configured MTU       : 300Actual       MTU               : 200
```

Verbose Mode Off

```
  Entry Created
```

Output field description

Field	Description
If-Name	The name of the IPoA interface which has been created.
UseDHCP	This specifies whether a DHCP client is used to obtain the IP address for this interface from a DHCP server, or not.
Type	This specifies the type of IPoA interface.
Interface Sec Type	Interface security type
Configured IP Address	IP address assigned to the IPoA interface.
Mask	Network mask to be applied to the IP Address.
Droute	Default Route
Gateway	Gateway IP Address.
Nat Direction	This specifies the NAT direction, which may be: inside, outside or none.
Oper Status	The actual/current state of the interface. It can be either Up or Down
Configured MTU	This specifies the MTU value configured by the user for IPOA interface.
Actual MTU	This specifies the MTU value actually operational for IPOA interface.

Caution

IPoA interface will come up only when ipoa map is created fr that interface.

References

- *get ipoa intf* command
- *delete ipoa intf command*
- *create ipoa map* command
- *delete ipoa map* command

3.27 create ipoa map

Description Use this command to associate an IP over ATM (IPoA) interface with an AAL5 interface.

Command Syntax ***create ipoa map ifname*** *interface-name* ***lowif*** low-interface-name

Parameters

Name	Description
Ifname interface-name	This parameter uniquely identifies the name of the IPoA interface. **Type:** Mandatory **Valid values:** ipoa-0,ipoa-1 etc.,.
Lowif low-interface-name	This parameter specifies the lower interface (ATM VC interface) to be associated with IPoA interface. **Type**: Mandatory **Valid Values:** aal5-0, aal5-1 etc.,.

Mode Super-User.

Example ***$ create ipoa map ifname*** *ipoa-0* ***lowif*** *aal5-0*

Output Verbose mode on:

```
Entry Created

IfName   LowIfName   Peer IP Address
-----------------------------------
ipoa-0   aal5-0      172.25.1.130
```

Verbose mode off:

```
Entry Created
```

Output Field description:

Field	Description
IfName	The name of the IPoA interface.
LowIfName	Specifies the lower (ATM VC) interface.
Peer IP Address	IP address of peer.

Caution None

References

- create ipoa map
- delete ipoa map
- get ipoa map
- get ipoa intf
- delete ipoa intf
- modify ipoa intf

3.28 create l2tp tunnel config

Description Use this command to create an L2TP tunnel.

Command Syntax

```
create l2tp tunnel config
ifname interface-name
localip local-ip-address
localhostname local-host-name
remoteip remote-ip-address
remotehostname remote-host-name
[start|stop]
[authtype simple|challenge|none]
[secret tunnel-secret]
[hellointerval hello-interval]
[idletimeout {infinite|{num <decValue>}}]
[crws contol-recv-windowsize]
[maxretx max-retransmission]
[maxretxtimeout max-retransmission-timeout]
[payloadseq never|always}]
[transport udpip]
[initiator local|remote]
```

Parameters

Name	Description
ifname interface-name	Identifies the interface name for L2TP layer. **Type**: Mandatory **Valid values:** l2t-0-l2t-*.
localip local-ip-address	This field specifies the address of the local endpoint of the tunnel, or 0.0.0.0 if the device is free to choose any of its addresses at tunnel establishment time. **Type:** Mandatory **Valid values:** Valid IP address.
localhostname host-name	Name of the local End-point of the tunnel. **Type:** mandatory **Valid values:** Display string of 255 characters
remoteip remote-ip-address	This field specifies the address of the remote end-point of the tunnel to which the tunnel is to be established. **Type:** mandatory **Valid values:** Valid IP address. **Default Value:** 0.0.0.0
remotehostname remote-host-name	Name of the remote End-point of the tunnel **Type:** Mandatory **Valid values:** Display string of 255 characters.
start|**stop**	This attribute specifies the action to be taken for the tunnel. True establishes the Tunnel. False tears the tunnel down. **Type:** Optional **Valid values:** Start

Name	Description
authtype simple*|*challenge*|*none	This object describes how L2TP tunnel peers are to be authenticated **Type:** optional **Valid values:** simple, challenge, none **Default Value:** none
secret tunnel-secret	This object is used to configure the shared secret used during the tunnel authentication phase of tunnel establishment if authtype is challenge. **Type:** optional **Valid values:** Hex Value - maximum of 64 octet length.
Hellointerval hello-interval	This object defines the interval (in sec) in which Hello packets are to be sent to the tunnel peer. A value '0' indicates that Hello packets will not be sent to tunnel peer. **Type:** optional **Valid values:** 0..3600(sec) **Default Value:** 60
idletimeout idle-timeout	This object defines the period of time (in seconds) that an established tunnel with no sessions will wait before disconnecting the tunnel.A value of '0' indicates that the tunnel will disconnect immediately after the last session disconnects. "infinite" leaves the tunnel up indefinitely. **Type:** optional **Valid values:** 0.86400(sec), infinite **Default Value:** 0
crws contol-recv-windowsize	This object defines the control channel receive window size. It specifies the maximum number of packets the tunnel peer can send without waiting for an acknowledgement from this peer **Type:** optional **Valid values:** 1..10 **Default Value:** 4
maxretx max-retransmission	This object defines the number of retransmissions, which the tunnel will attempt before assuming that the peer is no longer responding.A value of '0' indicates that this peer will not attempt to retransmit an unacknowledged control packet. **Type:** optional **Valid values:** 0..32 **Default Value:**5
maxretxtimeout max-retransmission-timeout	This object defines the maximum retransmission timeout interval that the tunnel will wait before retransmitting a control packet that has not been acknowledged. **Type:** optional **Valid values:** 1..32 **Default Value:** 1

Name	Description
payloadseq never|always	This object determines whether or not session payload packets will be requested to be sent with sequence numbers from tunnel peer's. **Type:** optional **Valid values:** never, always **Default Value:** never
transport udpip	This object defines the underlying transport media that is in use for this tunnel entry. **Type:** optional **Valid values:** udpip **Default Value:**udpip
initiator local|remote	This object indicates whether the tunnel will be initiated locally or not. **Type:** optional **Valid values:** local, remote **Default Value:** local

Mode Super-User.

Example

```
$ create l2tp tunnel config ifname l2t-0 localip 178.10.10.10
remoteip 178.10.11.10 start authtype  simple secret passwd
hellointerval 300 idletimeout num 100 crws 5 maxretx 10
maxretxtimeout 10 payloadseq  always transport udpip
initiator local  localhostname titanium remotehostname
columbia
```

Output Verbose mode on:

```
Entry Created

If Name             : l2t-0
Status              : Start             Oper Status       : Up
Local IP-address    : 178.10.10.10    Remote IP-address : 178.10.11.10
Hello Interval      : 300             Idle Timeout      : 100
Max Retx Attempt    : 10              Max Retx Timeout  : 10
Initiator           : local           Payload Sequencing: always
Authentication Type : simple          Transport         : udpip
Control RWS         : 5
Shared Secret       : passwd
Local Host name     : titanium
Remote Host name    : columbia
```

Verbose mode off:

```
Entry Created
```

Output Field description:

Field	Description
If-name	Identifies the interface name for L2TP layer.
Local IP-address	This field specifies the address of the local endpoint of the tunnel
Local Host name	This field specifies the address of the local endpoint of the tunnel
Remote IP-address	This field specifies the address of the remote endpoint of the tunnel to which the tunnel is to be established.
Status	This field specifies the status of the of the l2tp interface.
Oper Status	This field specifies the Operstatus of the of the l2tp interface.
Remote Host name	This field specifies the hostname of the remote endpoint of the tunnel to which the tunnel is to be established.
Hello Interval	Defines the interval (in sec) in which Hello packets are to be sent to the tunnel peer
Idle Timeout	Defines the period of time (in seconds) that an established tunnel with no sessions will wait before disconnecting the tunnel.
Control RWS	Defines the control channel receive window size
Max Retx Timeout	Defines the maximum retransmission timeout interval that the tunnel will wait before retransmitting a control packet that has not been acknowledged.
Initiator	This indicates whether the tunnel will be initiated locally or not.
Payload Sequencing	This object determines whether or not session payload packets will be requested to be sent with sequence numbers from tunnel peer's. The value never(2) indicates that L2TP will never initiate sequencing but will do sequencing if asked. The value always(3) indicates that L2TP will send the sequencing Required AVP during session establishment
Authentication Type	Describes how L2TP tunnel peers are to be authenticated
Transport	Defines the underlying transport media that is in use for this tunnel entry.

Field	Description
Shared Secret	Shared secret is used during the tunnel authentication phase of tunnel establishment if authtype is challenge
Max Retx Attempt	Defines the number of retransmissions, which the tunnel will attempt before assuming that the peer is no longer responding.

Caution None.

References

- delete l2tp tunnel config ifname
- get l2tp tunnel config

3.29 create mctl iplist

Description Use this command to create Management Control - Allowed IP addresses list

Command Syntax ***create mctl iplist ipaddress*** ipaddress

Parameter

Name	Description
ipaddress ipaddress	IP address **Type:** Mandatory

Mode Super-User

Example ***$ create mctl iplist ipaddress*** 172.25.12.13

Output Verbose Mode On

```
Entry Created

Mgmt Ctrl Ip Address
--------------------------------------------------------------------------------
172.25.12.13
```

Verbose Mode Off:

```
Entry Created
```

Output field description

Field	Description
Ip Address	IP address

Caution None

References

- *get mctl iplist* command
- *delete mctl iplist* command

3.30 create nat rule entry

Description Use this command to create a NAT rule.

Command Syntax

```
create nat rule entry ruleid rule-id
{basic|filter|napt|bimap|rdr|pass} [prot {any|tcp|udp|
icmp|num prot-number}] [ifname interface –name] [lcladdrfrom
local-address-from] [lcladdrto local-address-to]
[destaddrfrom dest-address-from] [destaddrto dest-address-
to] [destportfrom {num
<decvalue>}|echo|discard|chargen|ftp|telnet|smtp|dns|boot|
tftp|http|pop3|snmp
] [destportto {num
<decvalue>}|echo|discard|chargen|ftp|telnet|smtp|dns|boot|tf
tp|http|pop3|snmp] [glbaddrfrom global-address-from]
[glbaddrto global-address-to] [lclport {num
<decvalue>}|echo|discard|
chargen|ftp|telnet|smtp|dns|boot|tftp|http|pop3|snmp
]
```

Parameters

Name	Description
ruleid rule-id	This identifies the NAT rule which is being created **Type:** Mandatory **Valid values:** *0 – 4294967295*
basic|**filter**|**napt**|**bimap**|**rdr**|**pass**	This specifies the type of rule. The rule type is also referred to as the rule flavor. **Type:** Mandatory **Valid values:** *basic, filter, napt, bimap, rdr, pass*
ifname interface-name	This specifies the Interface or the outgoing device on which this Nat Rule would apply. **Type:** Optional **Valid values:** *eth-0, veth-0 - *, eoa-0 - *, ppp-0 - ** **Default value:** The rule applies on all outgoing interfaces
prot any|**tcp**|**udp**|**icmp num** <prot-number>	This specifies the protocol type for which the rule is meant. **Type:** Optional **Valid values:** *any, tcp, udp, icmp* or 0-255 (Valid IANA specified protocol) **Default value:** Rule is valid for all Protocols (*any*)

Name	Description
lcladdrfrom local-address-from	This is the starting address when a range of IP addresses are mapped. In case of *bimap*, the user can only specify a valid Host Address. In case of *rdr*, this is the translated local network address; if *lcladdrto* is different from this, redirection will be working in Load-Sharing mode. **Type:** Optional. **Valid values:** *0.0.0.0 – 255.255.255.255* **Default value:** *0.0.0.0*
lcladdrto local-address-to	This is the last IP address of the range of IP addresses mapped by this rule. In case of *bimap*, this can only be same as *lcladdrfrom*. **Type:** Optional. **Valid values:** *0.0.0.0 – 255.255.255.255* **Default value:** *255.255.255.255*
destaddrfrom dest-ddress-from	This specifies the start of the range of destination IP addresses to be matched. **Type:** Optional. This field is valid only when the rule type is *filter.* **Valid values:** *0.0.0.0 – 255.255.255.255* **Default value:** *0.0.0.0*
destaddrto dest-ddress-to	This specifies the end of the range of the destination IP addresses to be matched. **Type:** Optional. This field is valid only when the rule type is *filter.* **Valid values:** *0.0.0.0 – 255.255.255.255* **Default value:** *255.255.255.255*
destportfrom {num <decvalue>}|echo|discard|chargen|ftp|telnet|smtp|dns|boot|tftp|http|pop3|snmp	This specifies the start of the range of the destination port numbers to be matched. **Type:** Optional. This field is valid only when the rule type is *filter* or *rdr* **Valid values:** echo, discard, chargen, ftp, telnet, smtp, dns, boot, tftp, http, pop3, snmp and any decimal value. **Default value:** *65535*
destportto {num <decvalue>}|echo|discard|chargen|ftp|telnet|smtp|dns|boot|tftp|http|pop3|snmp	This specifies the end of the range of destination port numbers to be matched. **Type:** Optional. This field is valid only when the rule type is *filter* or *rdr* **Valid values:** echo, discard, chargen, ftp, telnet, smtp, dns, boot, tftp, http, pop3, snmp and any decimal value. **Default value:** *65535*
glbaddrfrom global-address-from	This specifies the first globally unique IP address of the range of IP addresses being mapped. In case of *bimap*, this has to be to equal to *glbaddrto.* This is not valid in case of *pass* and will be ignored. **Type:** Optional. **Valid values:** *0.0.0.0 – 255.255.255.255* **Default value:** *0.0.0.0*

Name	Description
glbaddrto global-address-to	This specifies the last globally unique IP address of the range of IP addresses used in the mapping. In case of *bimap*, this has to be same as *glbaddrto*. This is not valid in case of *pass* and so will be ignored. In case of *rdr*, IP addresses in range of *glbaddrfrom* and *glbaddrto* will be redirected. If both of these parameters are set to 0.0.0.0, all the incoming packets will redirected. In case of *map*, *napt*, *filter*, if *glbaddrfrom* and *glbaddrto* both are equal and set to 0.0.0.0, then packet will take the interface address. **Type:** Optional **Valid values:** *0.0.0.0 – 255.255.255.255.* **Default value:** *0.0.0.0*
lclport {num <decvalue>} | ***echo*** | ***discard*** | ***chargen*** | ***ftp*** | ***telnet*** | ***smtp*** | ***dns*** | ***boot*** | ***tftp*** | ***http*** | ***pop3*** | ***snmp***	This is the translated port number to be used in case of *rdr*. In the other NAT flavors, this will be ignored. **Type:** Optional only when the rule type is *rdr*.In all other cases it will be ignored. **Valid values:** echo, discard, chargen, ftp, telnet, smtp, dns, boot, tftp, http, pop3, snmp and any decimal value. **Default value:** *0*

Mode Super-User

Example ***$ create nat rule entry ruleid 1 napt***

Output Verbose Mode On:

```
Entry Created

Rule Id          : 1                  Flavor           : NAPT
Interface        : ALL                Protocol         : ANY
Local Addr From  : 0.0.0.0            Local Addr To    : 0.0.0.0
Dest Addr From   : 0.0.0.0            Dest Addr to     : 0.0.0.0
Global Addr From : 0.0.0.0            Global Addr To   : 255.255.255.255
Dest Port From   : 0                  Dest Port To     : 0
Local Port       : 0
```

Verbose Mode Off:

```
Entry Created
```

Output field description

Field	Description
Rule Id	This identifies the NAT rule, information pertaining to which is being displayed.
Flavor	This specifies the type of rule. It may be: *BASIC, FILTER, NAPT, BIMAP,REDIRECTION* (for RDR) and *PASS.*
Interface	This specifies the Interface or the outgoing device on which this Nat Rule would apply. It may be: *eth-0, ppp-0*, *ppp-1…*

Field	Description
Protocol	This specifies the protocol type for which the rule is meant. It may be: *Any, TCP, UDP, ICMP* or IANA-specified protocol between 0 to 255.
Local Addr From	This is the starting address when a range of private IP addresses are mapped
Local Addr To	This is the last IP address of the range of private IP addresses mapped by this rule.
Dest Addr From	This specifies the start of the range of destination IP address of the packet to matched.
Dest Addr To	This specifies the end of the range of destination IP address to be matched
Dest Port From	This specifies the start of the range of destination port numbers to be matched.
Dest Port To	This specifies the end of the range of destination port numbers to be matched.
Global Addr From	This specifies the first globally unique IP address of the range of IP addresses being mapped.
Global Addr To	This specifies the last globally unique IP address of the range of IP addresses used in the mapping.
Local Port	This is the translated port number to be used .

Caution None.

References

- *delete nat rule entry* command
- *get nat rule entry* command
- *nat global info* related commands
- *nat rule statistics* related commands
- *nat rule status* related commands.

3.31 create pfraw rule entry

Description Use this command to create a rule for filtering.

Command Syntax ***create pfraw rule entry ruleid*** rule-id ***[ifname*** interface-name|***all|public|private|dmz] [dir in|out] [inifname*** incoming-if-name|***all|public|private|dmz] [enable|disable] [log disable|match|nomatch|all] [act accept|deny|callmgmt] [ssb ssb] [ssbmask ssbmask] [priority priority] [outifname out-ifname]***

Parameters

Name	Description
ruleid rule-id	This identifies the rule index with which a rule should be created. **Type:** Mandatory **Valid values:** *0 - 65535*
ifname interface-name|***all***	This specifies the interface name for the rule. **Type:** Optional **Valid values:** *eth-0, veth-0, veth-1, veth-2, veth-3, eoa-0 - *, ppp-0 - *,* or *all.* **Default value:** *all*
inifname incoming-if-name	In case of a rule for an outgoing interface, this specifies the incoming interface. Only packets which are received on the *inifname* and which are going out via the *ifname* will be matched against this rule. **Type:** Optional **Valid values:** *eth-0, veth-0, veth-1, veth-2, veth-3, eoa-0 - *, ppp-0 - *, all.* This can be specified only when the direction is out. **Default value:** *all*
dir **in|out**	This specifies the filtering direction to which this rule is applied. **Type:** Optional **Valid values:** *in* or *out* **Default value:** *out*
enable|disable	This specifies whether this rule should be enabled or disabled. **Type:** Optional **Valid values:** *enable* or *disable* **Default value:** *disable*
Log disable|match|nomatch|all	This specifies the log option of this rule. **Type:** Optional **Valid values:** *disable* or *match* or *nomatch* or *all.* *disable* - No packets are logged. *match* - All matching packets are logged. *nomatch* - All packets which do not match this rule are logged. *all* – All packets are logged, whether they match the rule or not. **Default value:** *disable*

Name	Description
Act accept|deny|callmgmt	This specifies the action to be taken when a packet matches this rule. **Type:** Optional **Valid values:** *accept* or *deny* or *callmgmt.* *accept* – Packets matching this rule are accepted. *deny* – Packets matching this rule are dropped. *callmgmt* - If a packet matches this rule, it is passed on to management function **Default value:** *accept*
ssb ssb	Service Specification Byte value to be set in the packet **Type:** Optional **Valid values:** any hexadecimal pattern beginning with 0x and of length 2.
ssbmask ssbmask	Service Specification Byte value mask **Type:** Optional **Valid values:** any hexadecimal pattern beginning with 0x and of length 2.
priority priority	Priority value to be attached to the packet. 0 is highest priority. 2 is lowest priority. **Type :** Optional **Valid values :** 0-2
outifname outIfName	In case of a rule for an incoming interface, this specifies the outgoing interface. Only packets which are received on the outifname and which are coming in via the ifname will be matched against this rule. **Type:** Optional **Valid values:** eth-0, veth-0, veth-1, veth-2, veth-3, eoa-0 - *, ppp-0 - *, all. This can be specified only when the direction is **in**. **Default value:** all

Mode Super-User.

Example ***$ create pfraw rule entry ruleid 2 ifname eth-0 enable ssb 0x34 ssbmask 0xff priority 1***

Output Verbose Mode On:

```
Entry Created

Rule id        : 2        Rule status      : Enable
Interface      : eth-0    In interface     : All
Direction      : Out      SSB              : 0x34
SSB Mask       : 0xff     Priority         : 1
Action         : Accept
Logging        : Disable
Out interface  : ALL
```

Verbose Mode Off:

```
Entry Created
```

Output field description

Field	Description
Rule id	This identifies the rule index of the rule.
Rule Status	This specifies whether this rule is enabled or disabled.
Interface	This specifies the interface name for a rule.
In Interface	In case of a rule for an outgoing interface, this specifies the incoming interface. Only packets which are received on the *inifname* and which are going out via the *ifname* are matched against this rule.
Direction	This specifies the filtering direction to which this rule is applied.
SSB	Service Specification Byte value to be set in the packet.
SSB Mask	Service Specification Byte value mask.
Priority	Priority value to be attached to the packet.
Action	This specifies the action taken when a packet matches this rule
Logging	This specifies the log option of this rule
Out interface	This specifies the outgoing interface. Only packets which are received on the outifname and which are coming in via the ifname will be matched against this rule.

Caution Raw filter rules should be configured with care since configuring incorrect rules may render the system unusable.

References

- *pfraw* commands.

3.32 create pfraw subrule entry

Description Use this command to create a sub-rule for an already existing rule.

Command Syntax ***create pfraw subrule entry ruleid*** rule-id ***subruleid*** sub-rule-id ***mask*** mask-value ***[start linkh|iph|tcph|tcpd|udph|udpd|icmph|icmpd] offset*** offset ***[enable|disable] cmpt {eq|neq|lt|lteq|gt|gteq*** val***}|{range*** low-val high-val***}|{any}***

Parameters

Name	Description
ruleid rule-id	This identifies the rule index of the rule for which the sub-rule has to be added. **Type:** Mandatory **Valid values:** *0 - 65535* Only existing rule ids accepted as input.
subruleid sub-rule-id	This specifies the sub-rule index with which a sub-rule should be created. **Type:** Mandatory **Valid values:** *0 - 254*
mask mask-value	This specifies the mask with which the data in the packet is to be masked before using it for comparison with the values specified in *cmpt*. The mask is not used if *cmpt* is *any*. **Type:** Mandatory **Valid values:** any hexadecimal pattern beginning with 0x.
start linkh|iph|tcph|tcpd|udph|udpd|icmph|icmpd	This specifies the beginning position in the packet for an offset. The start position can be the beginning of the header or data portions of various protocols as listed below. **Type:** Optional **Valid values:** *linkh|iph|tcph|tcpd|udph|udpd|icmph|icmpd* **Default value:** *linkh*
offset offset	This specifies the offset with in the header or data part of the packet, calculated from the *start*. **Type:** Mandatory **Valid values:** *0—4294967295* **Default value:** *0*

Name	Description
enable*|*disable	This specifies whether this subrule should be enabled or disabled. **Type:** Optional **Valid values:** *enable* or *disable* **Default value:** *disable*
Cmpt ***{eq|neq|lt|lteq|gt|gteq*** val**}**| **{range** low-val high-val**}**|***{any}***	This specifies the type of comparison that can be done on the extracted data and the comparison value(s). **Type:** Mandatory **Valid values:** *val*, *low-val* and *high-val* are hexadecimal patterns to be used for comparison. *low-val* and *high-val* are used when range related comparison is to be done else *val* is used. The value(s) should start with 0x. If no comparison has to be done then *any* is given on the command line

Mode Super-User.

Example

```
$ create pfraw subrule entry ruleid 2 subruleid 1 start linkh
offset 6 mask 0x00000000ffff0000 cmpt range
0x00000000ff000000 0x00000000ffcd0000 enable
```

Output Verbose Mode On:

```
Entry Created

Sub Rule id      : 1          Rule id          : 2
Sub Rule status  : Enable     Offset from      : Linkh
Offset           : 6
Comp operation   : Range
Low value        : 0x00000000ff000000
High value       : 0x00000000ffcd0000
Mask             : 0x00000000ffff0000
```

Verbose Mode Off:

```
Entry Created
```

Output field description

Field	Description
Sub Rule id	This identifies the sub-rule index of the sub-rule.
Rule id	This specifies the rule index of the rule of which this is the subrule
Sub Rule status	This specifies whether this subrule is enabled or disabled.
Offset from	This specifies the start position in the packet for an offset. The start position can be the beginning of the header or data portions of various protocols.
Offset	This specifies the offset with in the header or data part of the packet.

Field	Description
Comp Operation	This specifies the type of comparison that is done on the extracted data and the comparison value(s)
Low Value	This is hexadecimal pattern to be used for comparison when comparison type is Range.
High Value	This is hexadecimal pattern to be used for comparison when comparison type is Range.
Value	This is hexadecimal pattern to be used for comparison when comparison type is Relational.
Mask	This is hexadecimal pattern which specifies the mask with which the data in the packet is masked before using it for comparison.

Caution Raw filter rules should be configured with care since configuring incorrect rules may render the system unusable.

References

- *create pfraw rule* command

3.33 create ppe pconf

Description Use this command to create an entry in the policy table for serv-to-ac policy

Command Syntax ***create ppe pconf acname*** AC-name ***[srvname*** service-name***]***

Parameters

Name	Description
acname AC-name	This specifies the Access Concentrator name. **Type:** Mandatory **Valid values:** String of up to 63 Chars. ('A'- 'Z', 'a'- 'z', '0'-'9','-','_')
srvname service-name	This specifies the service name **Type:** Optional **Valid values:** String of up to 63 Chars. ('A'- 'Z', 'a'- 'z', '0'-'9','-','_')

Mode Super-User.

Example ***$ create ppe pconf acname*** **AC1** ***srvname*** **Srv1**

Output Verbose Mode On:

```
Entry Created

Ac Name:        AC1
Service Name:   Srv1
```

Verbose Mode Off:

```
Entry Created
```

Output field description

Field	Description
ACName	This specifies the Access Concentrator name.
ServiceName	This specifies the service name

Caution The specified AC name and service should be supported by the system.

References

- *delete ppe pconf* command
- *get ppe pconf* command
- *ppe cfg* related commands
- *get ppe stats global* command
- *get ppe stats session* command.

3.34 create ppp intf

Description Use this command to create a PPP interface and a L2TP session.

Command Syntax

```
create ppp intf ifname interface-name lowif low-interface-
name {PPOE|PPOA|L2TP} [ip ip-address] [usedhcp {true|false}]
[inside|outside|none] [mru max-rx-unit] [magic {true|false}]
[droute {true|false}] [sname service-name]
[start|stop|startondata] [usedns true|false] [ifsectype
public|private|dmz] [l2tpcalltype outlns|outlac|inlns|inlac]
[usegwy local|remote][gwyip <ddd.ddd.ddd.ddd>]
[numif <name>][mtu <decvalue>]
```

Parameters

Name	Description
ifname interface-name	The PPP interface for the PPP Links. **Type:** Mandatory **Valid values:** *ppp-0, ppp-1,…*
usedhcp {true|false}	This specifies whether DHCP is to be used to obtain additional configuration information. Note that DHCP is NOT used to get the IP address, gateway address and DNS server addresses for the PPP link since this information is always negotiated using IPCP. **Type:** Optional **Default value:** true
usedns true|false	This specifies whether DNS server addresses are to be obtained using IPCP or not.
ip ip-address	If specified, it is used as the proposed IP address during address negotiation using IPCP. The address assigned after the negotiation may be different from the user specified value. **Type:** Optional **Valid values:** Any valid class A/B/C IP address **Default value:** *0.0.0.0*
lowif low-interface-name	Name of the lower interface on which PPP will run **Type:** Mandatory **Valid values:** *aal5-0, aal5-1…*
Mru max-rx-unit	The initial Maximum Receive Unit (MRU) that the local PPP entity will advertise to the remote entity. If the value of this variable is 0 then the local PPP entity will not advertise any MRU to the remote entity and the default MRU will be assumed. **Type:** Optional **Valid values:** *0* or between *1492* and Aal5 Rx Size as determined by `Get atm vc intf` **Default value:** 1492 or aal5 rx size whichever is less

Name	Description
magic {true|false}	If set to true, the local node will attempt to perform Magic Number negotiation with the remote node. If set to false, then this negotiation is not performed. **Type:** Optional **Default value:** *False*
PPOE|PPOA|L2TP	This specifies the lower layer protocol used below this PPP Link **Type:** Mandatory
l2tpcalltype outlns|outlac|inlns|inlac	This object indicates the l2tp call type. **Type**: optional **Values**: outlac, outlns, inlac, inlns
sname service-name	This specifies the service name used for PPPoE This field gives the criteria on the basis of which AC respond. (typically it will be ISP name) **Type:** Optional **Valid values:** string of max. length 63 ('A'- 'Z', 'a'-'z', '0'-'9','-','_')
start|stop|startondata	Setting of this object results in start and stop of the PPP session on this interface. If the session is already started then only stop value can be set. startondata will cause the PPP link to start only after there is some data activity. **Type:** Optional **Default value:** start
inside|outside|none	This variable specifies whether this interface's NAT direction is inside or outside. **Type:** Optional **Default value:** *out*
droute {true|false}	If set to true, then the default route is chosen through this interface **Type:** Optional **Default value:** *false*
ifsectype public|private|dmz	Type of interface security. **Type:** Optional **Valid values :** public, private or dmz **Default Value :** public
[usegwy local|remote]	This specifies whether local or remote gateway is to be used. **Type:** Optional **Valid values:** local, remote **Default Value:** remote
gwyip <ddd.ddd.ddd.ddd>	This specifies the IP Address for the Gateway. **Type:** Optional **Valid values:** Any valid class A/B/C IP address **Default value:** 0.0.0.0

Name	Description
numif <name>	This specifies the interface name of the associated numbered interface. **Type:** Optional **Valid values:** eth-0, eth-1, …. **Default value:** If not specified, it implies that ppp interface is not associated with any numbered interface.
mtu <decvalue>	This specifies the MTU Size configured for PPP interface **Type:** Optional **Valid values:** 120 ..65535 **Default Value:** 1500

Mode Super-User

Example ***$ create ppp intf ifname ppp-0 lowif aal5-0 ppoa ifsectype public numif eth-0 gwyip 202.1.1.2 mtu 300***

Output Verbose Mode On:

```
Entry Created

If-Name               : ppp-0          L2TP Call type        : inlac
Interface Sec Type    : Public         Phy Interface         : aal5-0
Configured IP Address : 0.0.0.0        NAT Direction         : OUT
Init MRU              : 1500           Magic                 : False
Encapsulation         : PPPOA          Service Name          : -
UseDhcp               : False          UseDns                : False
DRoute                : False          Status                : Start
Gateway IP Address    : 202.1.1.2      Associated Num If-Name : eth-0
Use Gateway           : remote
Configured MTU        : 300          Actual MTU            : 200
```

Verbose Mode Off:

```
Entry Created
```

Output field description

Field	Description
If-Name	This specifies the PPP interface for the PPP Links: It may be: *ppp-0, ppp-1…*
L2TP Call Type	This field specifies the l2tp call type.
Interface Sec Type	Interface security type.
Phy Interface	This specifies Name of the lower interface on which PPP is running. It may be: *aal5-0, aal5-1…*
Configured IP Address	This specifies the IP Address for the PPP Link.
NAT Direction	This variable specifies whether this interface's address is inside or outside. It may be: *inside, outside, none*
Init MRU	The initial Maximum Receive Unit (MRU) that the local PPP entity will advertise to the remote entity

Field	Description
Magic	This specifies whether the local node will attempt to perform Magic Number negotiation with the remote node. It may be: *True, False*
Encapsulation	This specifies the lower layer protocol used below this PPP Link. It may be: *PPPOA, PPPOE*
Service Name	This specifies the service name used for PPPoE. It is generally the name of the ISP.
UseDhcp	This specifies whether DHCP is to be used for address negotiation. It may be either True or False
UseDns	This specifies whether DNS server addresses are to be obtained using IPCP or not.
Droute	Default Route
Status	This shows whether PPP session on this interface is active. It may be: *Start, Stop, StartOnData.*
Gateway IP Address	This specifies the IP Address of the Gateway.
Associated Num If-Name	This specifies the interface name of the associated numbered interface. A "-" indicates that this ppp interface is not associated with any numbered interface.
Use Gateway	This specifies whether local or remote gateway is to be used.
Configured MTU	This specifies the MTU value configured by the user for PPP interface.
Actual MTU	This specifies the MTU value actually operational for PPP interface.

Caution An ATM VC should pre-exist. Please refer to *create atm vc intf* command. PPP security should be properly created for successful creation of ppp intf.

References

- *delete ppp intf* command
- *get ppp intf* command
- *modify ppp intf* command
- *create atm vc intf* command
- *ppp lstatus* related commands
- *ppp security* related commands.

3.35 create ppp security

Description Use this command to create a PPP security secrets entry for a PPP interface. The login and password given here are used to authenticate the PPP session for the given interface.

Command Syntax ***create ppp security ifname*** interface-name ***[pap|chap] login*** login-name ***passwd*** password

Parameters

Name	Description
ifname interface-name	This specifies the PPP interface for which the security entry is to be created **Type:** Mandatory **Valid values:** *ppp-0, ppp-1…, default*. The *default* entry gets used in case there is no specific entry for that interface.
pap|chap	This is the protocol used for authentication **Type:** Optional **Default value:** pap
login login-name	This is the login name **Type:** Mandatory **Valid values:** String of up to 128 characters ('A'- 'Z', 'a'-'z', '0'-' 9','-','_') and any combination of printable characters excluding ";"
passwd password	This is the password used to authenticate the user **Type:** Mandatory **Valid values:** String of up to 128 characters ('A'- 'Z', 'a'-'z', '0'-' 9','-','_') and any combination of printable characters excluding ";"

Mode Super-User

Example ***$ create ppp security ifname*** **ppp-0** ***login*** **abc** ***passwd*** **abc** ***pap***

Output Verbose Mode On:

```
Entry Created
IfName   : ppp-0     Protocol : PAP
Login    : abc
```

Verbose Mode Off:

```
Entry Created
```

Output field description

Field	Description
IfName	This specifies the PPP interface for which the security entry has been created It may be: *ppp-0, ppp-1…, default.* The *default* entry gets used in case there is no specific entry for that interface.
Protocol	This is the protocol used for authentication It may be: *PAP, CHAP*
Login	This is the login name

Caution None.

References

- *delete ppp security* command
- *get ppp security* command
- *modify ppp security* command
- *ppp lstatus* related commands
- *ppp intf* related commands.

3.36 create radius acctserv config

Description Use this command to create Radius Accounting Server Configuration

Command Syntax ***create radius acctserv config index*** index ***ip*** ip ***port*** port ***[retries*** retries ***] [starttimeout*** starttimeout ***] [ontimeout*** ontimeout ***] secret*** secret

Parameter

Name	Description
index index	A number uniquely identifying each RADIUS Accounting server with which this client communicates **Type:** Mandatory **Valid values:** 1 - 2147483647
ip ip	The IP address of the RADIUS server referred to in this table entry. **Type:** Mandatory
port port	The server port to which the client sends accounting requests **Type:** Mandatory **Valid values:** 1 - 65535
retries retries	The number of times the request packet shall be retransmitted to the server on getting timedout. **Type:** Optional **Valid values:** 0 - GS_CFG_RADC_MAX_SRV_RETRIES **Default value:** GS_CFG_RADC_DEF_SRV_RETRIES
starttimeout starttimeout	The time in seconds for which the client needs to wait before retransmitting the Accounting START request packet to the server. **Type:** Optional **Valid values:** 0 - GS_CFG_RADC_MAX_SRV_RETRNS_TOUT **Default value:** GS_CFG_RADC_DEF_SRV_RETRNS_TOUT
ontimeout ontimeout	The time in seconds for which the client needs to wait before retransmitting the Accounting ON request packet to the server. **Type:** Optional **Valid values:** 0 - GS_CFG_RADC_MAX_SRV_RETRNS_TOUT **Default value:** GS_CFG_RADC_DEF_SRV_RETRNS_TOUT
secret secret	The secret shared between this server and the client. String of up to GS_CFG_RADC_MAX_SRV_SHRDSCRT_LEN characters (All printable characters excluding ";") **Type:** Mandatory

Mode Super-User

Example

```
$ create radius acctserv config index 1 ip 192.166.56.67 port
1700 retries 5 starttimeout 60 ontimeout 60 secret 0x1090
```

Output Verbose Mode On

```
Entry Created

Server Index       : 1          IP address      : 192.166.56.67
Port               : 1700       Retries         : 5
Start timeout(sec) : 60         On timeout(sec) : 60
Current State      : Start
```

Verbose Mode Off:

```
Entry Created
```

Output field description

Field	Description
Server Index	A number uniquely identifying each RADIUS Accounting server with which this client communicates
IP address	The IP address of the RADIUS server referred to in this table entry.
Port	The server port to which the client sends accounting requests
Retries	The number of times the request packet shall be retransmitted to the server on getting timedout.
Start timeout(sec)	The time in seconds for which the client needs to wait before retransmitting the Accounting START request packet to the server.
On timeout(sec)	The time in seconds for which the client needs to wait before retransmitting the Accounting ON request packet to the server.
Current State	The current state of the accounting server.

Caution None

References

- *get radius acctserv config* command
- *delete radius acctserv config* command
- *modify radius acctserv config* command

3.37 create radius authserv config

Description Use this command to create Radius Authentication Server Configuration

Command Syntax ***create radius authserv config index*** index ***ip*** ip ***port*** port ***[retries*** retries ***] [retxtimeout*** retxtimeout ***] secret*** secret

Parameter

Name	Description
index index	A number uniquely identifying each RADIUS Authentication server with which this client communicates **Type:** Mandatory **Valid values:** 1 - 2147483647
ip ip	The IP address of the RADIUS server referred to in this table entry. **Type:** Mandatory
port port	The server port to which the client sends authentication requests **Type:** Mandatory **Valid values:** 1 - 65535
retries retries	The number of times the request packet shall be transmitted to the server on getting timedout. **Type:** Optional **Valid values:** 0 - GS_CFG_RADC_MAX_SRV_RETRIES **Default value:** GS_CFG_RADC_DEF_SRV_RETRIES
retxtimeout retxtimeout	The time, in seconds, for which the client needs to wait before retransmitting the request packet to the server. **Type:** Optional **Valid values:** 0 - GS_CFG_RADC_MAX_SRV_RETRNS_TOUT **Default value:** GS_CFG_RADC_DEF_SRV_RETRNS_TOUT
secret secret	The secret shared between this server and the client. String of up to GS_CFG_RADC_MAX_SRV_SHRDSCRT_LEN characters (All printable characters excluding ";") **Type:** Mandatory

Mode Super-User

Example ***$ create radius authserv config index*** 1 ***ip*** 192.166.56.67 ***port*** 1800 ***retries*** 5 ***retxtimeout*** 60 ***secret*** 0x1090

Output Verbose Mode On

```
Entry Created
```

```
Server Index : 1
IP address   : 192.166.56.67    Port                          : 1800
Retries      : 5                Retransmission timeout(sec) : 60
```

Verbose Mode Off:

```
Entry Created
```

Output field description

Field	Description
Server Index	A number uniquely identifying each RADIUS Authentication server with which this client communicates.
IP address	The IP address of the RADIUS server referred to in this table entry.
Port	The server port to which the client sends authentication requests.
Retries	The number of times the request packet shall be transmitted to the server on getting timed out.
Retransmission timeout(sec)	The time, in seconds, for which the client needs to wait before retransmitting the request packet to the server.

Caution None

References

- *get radius authserv config* command
- *delete radius authserv config* command
- *modify radius authserv config* command

3.38 create rip intf

Description This command allows user to start RIP protocol on the specified IP Interface.

Command Syntax

```
create rip intf ifname interface-name [metric metric-value]
[send {rip1|rip2|rip1compat|none}] [senddefroute
{enable|disable}] [receive {rip1|rip2|both|none}]
[recvdefroute {enable|disable}] [auth {none|text password}]
```

Parameters

Name	Description
Ifname interface-name	Specifies the IP Interface name on which RIP is to be started. **Type:** Mandatory **Valid values:** *eth-0*, *veth-0 - **, *ppp-0 - **, *eoa-0 - *, ipoa-0-**
Metric metric-value	This tells the metric value attached to the interface. The metric is used by RIP in deciding which among alternate routes is the most optimal. **Type:** Optional **Valid values:** *1-15* **Default value:** *1*
send {rip1|rip2|rip1compat|none}	This specifies the RIP version to be used for sending RIP updates and requests **Type:** Optional **Valid values:** *rip1, rip2, rip1compat, none* **Default value:** *rip1*
senddefroute {enable|disable}	If Default route is to be included in the updates sent on the interface, or not. **Type:** Optional **Valid values:** *enable* or *disable* **Default value:** *enable*
receive {rip1|rip2|both|none}	This specifies the RIP version to be accepted while receiving RIP updates and requests and responses **Type:** Optional **Valid values:** *rip1, rip2, both, none* **Default value:** *rip1*

Name	Description
Recvdefroute {enable|disable}	If Default route is to be processed in the updates received on the interface or not. **Type:** Optional **Valid values:** *enable* or *disable* **Default value:** *enable*
***auth* none|*auth text* password**	Authentication to be used with RIPv2 (authentication is not supported in RIPv1). If *auth* is *text*, then the password must be given. The specified password is used to authenticate RIP updates received on the interface. The same password is also used while sending message out on this interface. **Type:** Optional **Valid values:** *none* or if *text* then *password* of length up to 16 characters. **Default value:** *none*

Mode Super-User

Example ***create rip intf ifname ppp-0 metric 1 send rip1 senddefroute enable receive rip1 recvdefroute disable***

Output Verbose Mode On:

```
Entry Created

IP Interface Name    : ppp-0       RIP Interface Metric  : 1
RIP Send Mode        : rip1        RIP Receive Mode      : rip1
RIP Send Def Route   : Enable      RIP Recv Def Route    : Disable
RIP packet auth       : None
```

Verbose Mode Off:

```
Entry Created
```

Output field description

Field	Description
IP Interface Name	This tells the IP Interface name on which RIP is to be started.
RIP Interface Metric	This tells the metric value attached to the interface. The metric is used by RIP in deciding which among alternate routes is the most optimal.
RIP Send Mode	This tells the packet format used for sending RIP updates and requests
RIP Receive Mode	This tells the packet format accepted while receiving RIP updates and requests and responses
RIP Send Def Route	This tells whether default route is to be included in the updates sent on the interface, or not.

Field	Description
RIP Recv Def Route	This tells whether default route is to be processed in the updates received on the interface or not.
RIP packet auth	This tells whether RIP authentication is enabled or not

Caution None.

References

- *modify rip global* command

3.39 create snmp comm

Description Use this command to create an SNMP community on the SNMP agent.

Command Syntax ***create snmp comm community*** comm-name ***[ro|rw]***

Parameters

Name	Description
community comm-name	This specifies the Community name **Type:** Mandatory **Valid values:** String of max. 50 characters ('A'- 'Z', 'a'-'z', '0'-'9','_', '-')
ro|rw	This specifies the access permissions given to managers with this community name. *ro* implies Read Only permissions and *rw* implies Read-Write permissions. **Type:** Optional **Default value:** *ro*

Mode Super-User.

Example ***$ create snmp comm community*** **public** ***ro***

Output Verbose Mode On:

```
Entry Created

Access          Community
------------------------
RO             public
```

Verbose Mode Off:

```
Entry Created
```

Output field description

Field	Description
Community	This specifies the Community name
Access	This specifies the access permissions given to managers with this community name. It may be: *RO* (Read Only), *RW* (Read-Write)

Caution None.

References

- *get snmp comm* command
- *delete snmp comm* command
- *snmp host* related commands

3.40 create snmp host

Description This command is used for creating an SNMP host entry.

Command Syntax ***create snmp host {ip ip-addr|hdlc|ilmi community comm-name***

Parameters

Name	Description
community comm-name	This specifies the Community name. This must be a valid community in the snmp community table. **Type:** Mandatory **Valid values:** String of max. 50 characters('A'- 'Z', 'a'-'z', '0'-'9','-','_')
{ip ip-addr}|hdlc|ilmi	This specifies the IP address of the manager (snmp over udp interface) that has access permissions for the modem. A value of 'hdlc' specifies SNMP over HDLC interface. A value of 'ilmi' specifies SNMP over ILMI interface. **Type:** Mandatory **Valid values:** Any valid class A/B/C IP address, hdlc, ilmi.

Mode Super-User.

Example ***$ create snmp host community*** **public** ***ip*** **192.168.1.3**

Output Verbose Mode On:

```
Entry Created

Host Address              Community
-----------------------------------
192.168.1.3          Public
```

Verbose Mode Off:

```
Entry Created
```

Output field description

Field	Description
Host Address	This specifies the IP address of the manager that has access permissions for the modem.
Community	This specifies the Community name.

Caution The SNMP Community used in the command should exist.

References

- *get snmp host* command
- *delete snmp host* command
- *snmp trap* related commands
- *snmp host* related commands

3.41 create sntp servaddr

Description Use this command to configure the SNTP server address

Command Syntax ***create sntp servaddr*** <ip-address>|***dname*** <domain-name>

Parameters

Name	Description
<ip-address>|dname <domain-name>	This parameter specifies the IP address or fully qualified domain name for configuring the SNTP server address. **Type**: Mandatory **Valid values**: Valid IP address or fully qualified domain name.

Mode Super-User.

Example ***$ create sntp servaddr*** *192.168.1.1*

Output Verbose Mode On:

```
Entry Created

Server Addr : 192.168.1.1 Status : Standby
Domain Name : abc.com
```

Verbose Mode Off:

```
Entry Created
```

Output field description

Field	Description
Server Addr	IP address of the SNTP server.
Status	Operational Status of the SNTP server address entry.
Domain Name	The fully qualified domain name of the SNTP server.

Caution The SNMP Community used in the command should exist.

References

- *delete sntp servaddr* command
- *get sntp servaddr* command
- *modify sntp cfg* command
- *get sntp cfg* command
- *get sntp stats* command.
- *reset sntp stats* command

3.42 create usb intf

Description Use this command to create a USB interface

Command Syntax **create usb intf ifname** interface – name ***[ip*** ip-address***] [mask*** net–mask***] [inside|outside|none] [ifsectype public|private|dmz]][mtu <decvalue]***

Parameters

Name	Description
ifname interface-name	This parameter specifies the name assigned to this interface. **Type:** Mandatory **Valid values:** *usb-0 - **
ip ip-address	The IP address to be assigned to interface. **Type:** Optional **Valid values:** Any valid class A/B/C IP address **Default value:** *0.0.0.0*
mask net-mask	This parameter specifies the subnet mask to be applied to the IP address. **Type:** Optional **Valid values:** *128.0.0.0 – 255.255.255.254* **Default value:** *0.0.0.0*
inside|outside|none	This specifies the NAT direction for the interface. **Type:** Optional **Valid values:** *inside, outside, none* **Default value:** Inside if the IP address is valid and non-zero otherwise *none*
ifsectype public|private|dmz	Interface security type. **Type:** Optional **Valid values :** public, private or dmz **Default Value :** private
mtu <decvalue>	This specifies the MTU Size configured for Ethernet over USB interface. **Type:** Optional **Valid values :** 120 ..1500 **Default Value :** 1500

Mode Super-User.

Example ***$ create usb intf ifname*** usb-0 ***ip*** 192.168.1.1 ***mask*** 255.255.255.0 ***ifsectype*** public **mtu 300**

Output Verbose Mode On

```
Entry Created

IfName   If Sec Type   Ip Address     Mask           Nat Dir      Oper   MTU
-------------------------------------------------------------------------------
usb-0     Public      192.168.1.1    255.255.255.0  Inside       Down    300
```

Verbose Mode Off

```
Entry Created
```

Output field description

Field	Description
IfName	The name of the interface, which has been created.
Ip Address	IP address assigned to the USB interface.
Mask	Network mask to be applied to the IP Address
Nat Dir	This specifies the NAT direction, which may be: *inside, outside or none*.
Oper	The actual/current state of the interface. It can be either *Up* or *Down*
If SecType	Interface Security Type.
MTU	This specifies the MTU Size configured for Ethernet over USB interface.

Caution None.

References

- *get usb intf* command
- *delete usb intf* command
- *modify usb intf* command
- *get usb stats* command.

3.43 create user

Description Use this command to create a user account. At maximum four accounts can exist.

Command Syntax

```
create user name user-name passwd password
[root|user|intermediate] useserial
```

Parameters

Name	Description
name user-name	This specifies the User Name to be created. **Type:** Mandatory **Valid values:** String of up to 128 characters ('A'- 'Z', 'a'-'z', '0'-'9','-','_') and any combination of printable characters excluding ";"
passwd password	This specifies the password required by this user to login to IAD. **Type:** Mandatory. Is valid when user does not specify "useserial" parameter **Valid values:** String of up to 128 characters ('A'- 'Z', 'a'-'z', '0'-'9','-','_') and any combination of printable characters excluding ";"..
root|**user**|**intermediate**	This indicates the privilege level of the user. **Type:** Optional **Default value:** *user*
Useserial	This specifies that the password required by this user to login to IAD is the "Serial Number" of the modem the user is using. **Type:** Mandatory - Is valid when user does not specify "passwd" parameter

Mode Super-User

Example

```
$ create user name user1 passwd temp1 user
```

Output Verbose Mode On:

```
Entry Created

User Name : user1
Privilege : user
```

Verbose Mode Off:

```
Entry Created
```

Output field description

Field	Description
UserName	This shows the new user login which has been created.
Privilege	This represents the privilege level associated with the user name shown. It may be: *user, intermediate, root.* In CLI, intermediate privilege has the same previliges as the user. In HTTP, the intermediate privilege has ALL the privileges as the "user" except that he can also modify the ATM VPI and VCI values and the PPP username and password.

Caution User can specify either **Passwd** or **Useserial,** not both.

References

- *delete user* command
- *get user* command
- *passwd* related commands.

3.44 create wlan intf

Description Use this command to create 802.11 Interface

Command Syntax

create wlan intf ifname ifname ***[encrtype*** disable | 64bit | 128bit ***] [deftxkeyid*** deftxkeyid ***] [defchannel*** defchannel ***] [rtsthreshold*** rtsthreshold ***] [fragthreshold*** fragthreshold ***] [essid "essid"] [micwaverobust*** enable | disable ***] [intrabssrelay*** enable | disable ***] [ip*** ip ***] [mask*** mask ***] [natdir*** none | inside | outside ***] [usedhcp*** false | remote | local ***] [ifsectype*** public | private | dmz ***] [mtu*** mtu ***]***

Parameter

Name	Description
ifname ifname	Name of the wireless interface. **Valid Values:** wlan-0 - wlan-* **Type:** Mandatory
encrtype disable | 64bit | 128bit	WEP Encryption Type.Disabled for no encryption.64bit for 40bit encryption.128bit for 128bit encryption. **Type:** Optional **Default value:** disable
deftxkeyid deftxkeyid	Combined with WepEncryption attribute, determines which encryption key (between 0-3) to use by default. The actual key is picked up from the 802.11 WEP Keys MO. **Type:** Optional **Valid values:** 0 - 3 **Default value:** 0
defchannel defchannel	Default Channel **Type:** Optional **Valid values:** 0 - 2147483647 **Default value:** 0
rtsthreshold rtsthreshold	Maximum packet size to use RTS/CTS With **Type:** Optional **Valid values:** 0 - 2147483647 **Default value:** 2347
fragthreshold fragthreshold	Minimum packet size to use fragmentation with **Type:** Optional **Valid values:** 0 - 2147483647 **Default value:** 2346
essid essid	Service set identifier of upto 32 characters which each 802.11b station uses. **Type:** Optional **Default value:** "Viking"
micwaverobust enable | disable	Enable/Disable Microwave robustness **Type:** Optional **Default value:** enable

Name	Description
intrabssrelay enable | disable	Relay packets between BSS (AP) **Type:** Optional **Default value:** disable
ip ip	This specifies the IP address configured for the interface. **Type:** Optional **Default value:** 0
mask mask	This specifies the network mask configured for the interface. **Type:** Optional **Default value:** 0
natdir none | inside | outside	This variable specifies whether this interface's address is inside or outside. This is used by NAT. **Type:** Optional **Default value:** inside
usedhcp false | remote | local	DHCPclient will do/not do link address negotiation locally/remotely depending on the UseDHCP values of local/remote or false **Type:** Optional **Default value:** false
ifsectype public | private | dmz	This specifies the interface type from firewall point of view. **Type:** Optional **Default value:** private
mtu mtu	This specifies the maximum transmission unit for interface. **Type:** Optional **Valid values:** 120 - 1500 **Default value:** 1500

Mode Super-User

Example

```
$ create wlan intf  ifname wlan-0 encrtype 64bit deftxkeyid 1
defchannel 1 rtsthreshold 1 fragthreshold 1 essid "Viking"
micwaverobust enable intrabssrelay enable ip 192.168.3.4 mask
255.255.255.0 natdir inside usedhcp false ifsectype public
mtu 1500
```

Output Verbose Mode On

```
Entry Created

Interface                : wlan-0
Encryption Type          : 64bit            Default Tx Key Id      : 1
Default Channel          : 1                Rts Threshold          : 1
Fragmentation Threshold  : 1                Service set identifier : Viking
Relay packets between BSS : enable          IP address             : 192.168.3.4
Mask                     : 255.255.255.0    Nat Dir                : inside
Use DHCP                 : false            Security Type          : public
Microwave robustness     : enable
Maximum Transmission Unit : 1500
```

Verbose Mode Off:

```
Entry Created
```

Output field description

Field	Description
Interface	Name of the wireless interface.
Encryption Type	WEP Encryption Type.Disabled for no encryption.64bit for 40bit encryption.128bit for 128bit encryption.
Default Tx Key Id	Combined with WepEncryption attribute, determines which encryption key (between 0-3) to use by default. The actual key is picked up from the 802.11 WEP Keys MO.
Default Channel	Default Channel
Rts Threshold	Maximum packet size to use RTS/CTS With
Fragmentation Threshold	Minimum packet size to use fragmentation with
Service set identifier	Service set identifier of upto 32 characters which each 802.11b station uses.
Relay packets between BSS	Relay packets between BSS (AP)
IP address	This specifies the IP address configured for the interface.
Mask	This specifies the network mask configured for the interface.
Nat Dir	This variable specifies whether this interface's address is inside or outside. This is used by NAT.
Use DHCP	DHCPclient will do/not do link address negotiation locally/remotely depending on the UseDHCP values of local/remote or false
Security Type	This specifies the interface type from firewall point of view.
Microwave robustness	Enable/Disable Microwave robustness
Maximum Transmission Unit	This specifies the maximum transmission unit for interface.

Caution None.

References

- *get wlan intf* command
- *delete wlan intf* command
- *modify wlan intf* command

3.45 create wlan key

Description Use this command to create 802.11 Wired Equivalent Privacy Keys

Command Syntax ***create wlan key ifname*** ifname ***encrtype*** 64bit | 128bit ***keyid*** keyid ***keyval*** keyval

Parameter

Name	Description
ifname ifname	Name of the wireless interface. **Valid Values:** wlan-0 - wlan-* **Type:** Mandatory
encrtype 64bit | 128bit	Encryption type with which this key is to be used(64 bit or 128 bit). **Type:** Mandatory
keyid keyid	Key index. Used to identify which key to use as the default key on the interface. **Type:** Mandatory **Valid values:** 0 - 3
keyval keyval	64 or 128 bit Encryption key.Value to be given in Hex **Type:** Mandatory

Mode Super-User

Example ***$ create wlan key ifname*** wlan-0 ***encrtype*** 64bit ***keyid*** 1 ***keyval*** 0x3455678902345678

Output Verbose Mode On

```
Entry Created

Interface       : wlan-0
Encryption Type : 64bit
Key Id          : 1
```

Verbose Mode Off:

```
Entry Created
```

Output field description

Field	Description
Interface	Name of the wireless interface.
Encryption Type	Encryption type with which this key is to be used(64 bit or 128 bit).
Key Id	Key index. Used to identify which key to use as the default key on the interface.

Caution None.

References

- *get wlan key* command
- *delete wlan key* command
- *modify wlan key* command

3.46 create 8021x intf

Description Use this command to create Dot1x Interface Configuration

Command Syntax

```
create 8021x intf  ifname ifname [ enable | disable  ] [
admindir both | in ] [ portcontrol ForceUnAuth | Auto |
ForceAuth ] [ assoc one_to_one | many_to_one ] [ qperiod
qperiod ] [ txperiod txperiod ] [ supptimeout supptimeout ] [
servtimeout servtimeout ] [ maxreq maxreq ] [ reauthenabled
true|false ] [ reauthperiod reauthperiod ] [ reauthmax
reauthmax ] [ keytxenabled true|false ] [ dynamicsuppallow
true|false ] [ rekeytimeout rekeytimeout ]
```

Parameter

Name	Description
ifname ifname	Interface index **Type:** Mandatory **Valid values:** 1 - 4294967295
enable | ***disable***	Feature 802.1x status on this Interface **Type:** Optional **Default value:** enable
admindir both | in	This specifies the controlled directions for the port. If set to **both**, then the port needs to be authenticated for traffic to flow either to or from it. If set to **in**, then traffic going out via this port does not require it to be authenticated. **Type:** Optional **Default value:** both
portcontrol ForceUnAuth | Auto | ForceAuth	This allows administrative control over the Port's authorization status. If set to ForceUnAuth, the port is never authorized. If set to ForceAuth, the port is autorized unconditionally. If set to Auto, the port's authorization status is determined by outcome of the authentication exchanges between Supplicant PAE, Authenticator PAE, and the Authentication Server. **Type:** Optional **Default value:** Auto
assoc one_to_one | many_to_one	This specifies whether there will be one supplicant or many supplicants per port . **Type:** Optional **Default value:** one_to_one
qperiod qperiod	The Authenticator state machine uses a timer to define periods of time during which it will not attempt to acquire a Supplicant. The initial value of this timer is quietPeriod. **Type:** Optional **Valid values:** 0 - 65535 **Default value:** 60

Name	Description
txperiod txperiod	The Authenticator state machine uses a timer to determine when an EAPOL PDU is to be transmitted. The initial value of this timer is txPeriod. **Type:** Optional **Valid values:** 1 - 65535 **Default value:** 30
supptimeout supptimeout	The initialization value used for timing out the supplicant. Its default value is 30 s; however, if the type of challenge involved in the current exchange demands a different value of timeout (for example, if the challenge requires an action on the part of the user), then the timeout value is adjusted accordingly. **Type:** Optional **Valid values:** 1 - 65535 **Default value:** 30
servtimeout servtimeout	The initialization value used for timing out the Authentication Server. Its default value is 30 s; however, the timeout value may be adjusted to take account of the communication medium being used to communicate with the Authentication Sever. **Type:** Optional **Valid values:** 1 - 65535 **Default value:** 30
maxreq maxreq	The maximum number of times that the state machine will retransmit an EAP Request packet to the Supplicant before it times out the authentication session. **Type:** Optional **Valid values:** 1 - 10 **Default value:** 2
reauthenabled true|false	A constant that defines whether regular reauthentication will take place on this Port. **Type:** Optional **Valid values:** False, True **Default value:** GS_TRUE
reauthperiod reauthperiod	A constant that defines a nonzero number of seconds between periodic reauthentication of the Supplicant **Type:** Optional **Valid values:** 1 - 65535 **Default value:** 3600
reauthmax reauthmax	The number of reauthentication attempts that are permitted before the Port becomes Unauthorized. **Type:** Optional **Valid values:** 1 - 65535 **Default value:** 2

Name	Description
txperiod txperiod	The Authenticator state machine uses a timer to determine when an EAPOL PDU is to be transmitted. The initial value of this timer is txPeriod. **Type:** Optional **Valid values:** 1 - 65535 **Default value:** 30
supptimeout supptimeout	The initialization value used for timing out the supplicant. Its default value is 30 s; however, if the type of challenge involved in the current exchange demands a different value of timeout (for example, if the challenge requires an action on the part of the user), then the timeout value is adjusted accordingly. **Type:** Optional **Valid values:** 1 - 65535 **Default value:** 30
servtimeout servtimeout	The initialization value used for timing out the Authentication Server. Its default value is 30 s; however, the timeout value may be adjusted to take account of the communication medium being used to communicate with the Authentication Sever. **Type:** Optional **Valid values:** 1 - 65535 **Default value:** 30
maxreq maxreq	The maximum number of times that the state machine will retransmit an EAP Request packet to the Supplicant before it times out the authentication session. **Type:** Optional **Valid values:** 1 - 10 **Default value:** 2
reauthenabled true|false	A constant that defines whether regular reauthentication will take place on this Port. **Type:** Optional **Valid values:** False, True **Default value:** GS_TRUE
reauthperiod reauthperiod	A constant that defines a nonzero number of seconds between periodic reauthentication of the Supplicant **Type:** Optional **Valid values:** 1 - 65535 **Default value:** 3600
reauthmax reauthmax	The number of reauthentication attempts that are permitted before the Port becomes Unauthorized. **Type:** Optional **Valid values:** 1 - 65535 **Default value:** 2

Name	Description
keytxenabled true|false	Controls transmission of key information after the port has been authorized. **Type:** Optional **Valid values:** False, True **Default value:** GS_FALSE
dynamicsuppallow true|false	This controls whether only management-created Supplicants or both management-created and Dynamically-learnt Supplicants are allowed. **Type:** Optional **Valid values:** False, True **Default value:** GS_TRUE
rekeytimeout rekeytimeout	Timer period after which keys will be transmitted to all the supplicants in the port. **Type:** Optional **Valid values:** 20 - 3600 **Default value:** 600

Mode Super-User

Example

```
$ create 8021x intf  ifname wan-0  enable admindir both
portcontrol Auto assoc many_to_one qperiod 60 txperiod 30
supptimeout 30 servtimeout 30 maxreq 2 reauthenabled true
reauthperiod 3600 reauthmax 2 keytxenabled true
dynamicsuppallow true rekeytimeout 600
```

Output Verbose Mode On

```
Entry Created

If Index                : wan-0
802.1x status           : enable      Admin dir            : both
Port Control            : Auto        Association          : many_to_one
Quiet Period(secs)      : 60          Tx Period(secs)      : 30
Supplicant Timeout(secs) : 30         Server Timeout(secs) : 30
Max Request             : 2           ReAuth Enabled       : true
ReAuth Period(secs)     : 3600        ReAuth Max requests  : 2
Key Tx Enabled          : true        Dynamic Supp Allowed : true
ReKey timeout(secs)     : 600
```

Verbose Mode Off:

```
Entry Created
```

Output field description

Field	Description
If Index	Interface index
802.1x status	Feature 802.1x status on this Interface
Admin dir	This specifies the controlled directions for the port. If set to both, then the port needs to be authenticated for traffic to flow either to or from it. If set to in, then traffic going out via this port does not require it to be authenticated.

Field	Description
Port Control	This allows administrative control over the Port's authorization status. If set to ForceUnAuth, the port is never authorized. If set to ForceAuth, the port is autorized unconditionally. If set to Auto, the port's authorization status is determined by outcome of the authentication exchanges between Supplicant PAE, Authenticator PAE, and the Authentication Server.
Association	This specifies whether there will be one supplicant or many supplicants per port .
Quiet Period(secs)	The Authenticator state machine uses a timer to define periods of time during which it will not attempt to acquire a Supplicant. The initial value of this timer is quietPeriod.
Tx Period(secs)	The Authenticator state machine uses a timer to determine when an EAPOL PDU is to be transmitted. The initial value of this timer is txPeriod.
Supplicant Timeout(secs)	The initialization value used for timing out the supplicant. Its default value is 30 s; however, if the type of challenge involved in the current exchange demands a different value of timeout (for example, if the challenge requires an action on the part of the user), then the timeout value is adjusted accordingly.
Server Timeout(secs)	The initialization value used for timing out the Authentication Server. Its default value is 30 s; however, the timeout value may be adjusted to take account of the communication medium being used to communicate with the Authentication Sever.
Max Request	The maximum number of times that the state machine will retransmit an EAP Request packet to the Supplicant before it times out the authentication session.
ReAuth Enabled	A constant that defines whether regular reauthentication will take place on this Port.
ReAuth Period(secs)	A constant that defines a nonzero number of seconds between periodic reauthentication of the Supplicant
ReAuth Max requests	The number of reauthentication attempts that are permitted before the Port becomes Unauthorized.
Key Tx Enabled	Controls transmission of key information after the port has been authorized.
Dynamic Supp Allowed	This controls whether only management-created Supplicants or both management-created and Dynamically-learnt Supplicants are allowed.
ReKey timeout(secs)	Timer period after which keys will be transmitted to all the supplicants in the port.

Cautions None.

References

- *get 8021x intf* command
- *delete 8021x intf* command
- *modify 8021x intf* command

3.47 create 8021x supp

Description Use this command to create a dot1x supplicant.

Command Syntax

```
create 8021x supp ifname <ifname> macaddr <macaddr> [reauth yes|no] [authcontrol forceauth|forceunauth|auto] [qperiod <decvalue>] [authtxperiod <decvalue>] [authtimeout <decvalue>] [authservtimeout <decvalue>] [authmaxreq <decvalue>] [reauthmax <decvalue>] [reauthperiod <decvalue>] [authkeytx enable|disable] [reauthenabled true|false]
```

Parameter

Name	Description
ifname <ifname>	This specifies the Interface Index of a port. **Type:** Mandatory **Valid Values :**
macaddr <macaddr>	This specifies the MAC aaddress of a supplicant for which individual authenticator state machines are running. **Type:** Mandatory **Valid Values :** A Valid mac address
reauth yes|no	This specifies the re-authentication control for this port. **Type :** Optional **Valid Values :** yes, no **Default Value:** no
authcontrol forceauth|forceunauth|auto	This specifies the Current value of auth contro parameter. **Type :** Optional **Valid Values :** forceauth, forceunauth, auto **Default Value:** auto
qperiod <decvalue>	This specifies the Value in seconds of Quiet Period constant used by authenticator PAE state machine. **Type :** Optional **Valid Values :** 0 - 65535 **Default Value:** 60
authtxperiod <decvalue>	This specifies the value in seconds of TxPeriod constant used by authenticator PAE state machine. **Type :** Optional **Valid Values :** 0 - 65535 **Default Value:** 30
authtimeout <decvalue>	This specifies the value in seconds of SuppTimeout constant used by backend authenticator state machine. **Type :** Optional **Valid Values :** 0 - 65535 **Default Value:** 30

Name	Description
authservtimeout <decvalue>	This specifies the Value in seconds of ServerTime-out constant used by Backend authenticator state machine. **Type** : Optional **Valid Values** : 0 - 65535 **Default Value:** 30
authmaxreq <decvalue>	This specifies the value of MaxReq constant used by backend authenticator state machine. **Type** : Optional **Valid Values** : 1-10 **Default Value:** 2
reauthmax <decvalue>	This specifies the value of ReAuthMax constant used by Authenticator PAE state machine. **Type** : Optional **Valid Values** : *1*-65535 **Default Value:** 2
reauthperiod <decvalue>	This specifies the value in seconds of re-authenti-cate period constant used by re-authenticate state machine. **Type** : Optional **Valid Values** : *1*-65535 **Default Value:** 3600
authkeytx enable|disable	This specifies the whether auth key Transmission is enabled or disabled. **Type** : Optional **Valid Values** : enable, disable **Default Value:** disable
reauthenabled true|false	This specifies whether re-authentication is enabled or disabled. **Type** : Optional **Valid Values** : true, false **Default Value:** true

Mode Super-User

Example ***$ create 8021x supp ifname wlan-0 macaddr 0x0085a00004***

Output Verbose Mode On

```
If Index                : wlan-0        Mac address              :  0x0085a00004
Virtual port Number     : 3000          Owner                    : 802.1x
Protocol Version        : 2.0.1.1       Port capability          : Auth
Re- authenticate        : no            Auth Pae State           : forceauth
Auth backend state      : request       Auth Key Transmission    :  disable
Auth Admin dir          : both          Auth Oper dir            : both
Auth Control status     : authorized    Auth control value       : forceauth
Auth Q period(secs)     : 1000          Auth Tx Period(secs)     : 200
Auth Supp Timeout(sec)  : 30            Auth Server timeout(secs) :30
Auth Max req            : 2             Auth Re-auth max         : 2
Auth reauth Period(secs): 3600          Auth reauth enabled      : true
```

Verbose Mode Off:

```
Entry Created
```

Output field description

Field	Description
If Index	This specifies the Interface Index of a port.
Mac address	This specifies the MAC aaddress of a supplicant for which individual authenticator state machines are running.
Virtual port Number	This specifies the virtual Port Number to be used for an authenticator PAE associated with a Supplicant.
Owner	This specifies of the owner of the entry.
Protocol Version	This specifies the EAPOL Protocol Version associated with this supplicant.
Port capability	This specifies the PAE functionality (authenticator or supplicant) supported by this port.
Re- authenticate	This specifies the Re-authentication control for this port (it will always be returned false while reading)
Auth Pae State	This specifies the Current State of Authenticator PAE state machine.
Auth backend state	This specifies the Current State of Backend Authentication state machine.
Auth Key Transmission	This specifies the Key Transmission enable/disable control parameter.
Auth Admin dir	This specifies the Administrative Controlled Direction Parameter.
Auth Oper dir	This specifies the Operational Controlled Direction Parameter.
Auth Control status	This specifies the Supplicant's Current Authentication Status.
Auth control value	This specifies the Current value of AuthControl Parameter.
Auth Q period(secs)	This specifies the Value in seconds of QuietPeriod constant used by authenticator PAE state machine.
Auth Tx Period(secs)	This specifies the Value in seconds of TxPeriod constant used by authenticator PAE state machine.
Auth Supp Timeout(sec)	This specifies the Value in seconds of SuppTimeout constant used by Backend authenticator state machine.
Auth Server timeout(secs)	This specifies the Value in seconds of ServerTimeout constant used by Backend authenticator state machine.
Auth Max req	This specifies the Value of MaxReq constant used by Backend authenticator state machine.

Field	Description
Auth Re-auth max	This specifies the Value of ReAuthMax constant used by Authenticator PAE state machine.
Auth reauth Period(secs)	This specifies the Value in seconds of ReauthPeriod constant used by Re-authenticate state machine.
Auth reauth enabled	This specifies the Re-authentication enable/disable control parameter.

Caution None.

References

- *get 8021x supp* command
- *delete 8021x supp* command
- *modify 8021x supp* command

3.48 delete alg port

Description Use this command to delete an ALG port entry.

Command Syntax ***delete alg port portno*** port-no ***[prot {any|tcp|udp|num*** <prot-number***>}]***

Parameters

Name	Description
portno port-no	The Port number on which the ALG is running. The port here is the destination port of the untranslated packet **Type:** Mandatory **Valid values:** *0 – 65535*
prot any|tcp|udp|num <prot-number>	This specifies the protocol type for which the ALG is running. **Type:** Optional. **Valid values:** *any, tcp, udp* or *0-255* (Valid IANA specified protocol).

Mode Super-User.

Example ***$ delete alg port portno 21 prot tcp***

Output Verbose Mode On:

```
Port Num                Protocol                ALG Type
-------------------------------------------------------------
21                      Tcp                     FTP

Entry Deleted
```

Verbose Mode Off:

```
Entry Deleted
```

Output field description

Field	Description
Port Num	The Port number on which the ALG was running. The port here is the destination port of the untranslated packet.
Protocol	The protocol for which the was running.
Port Type	This specifies the ALG with has to be applied to this port. It may be: FTP, SNMP, REAL AUDIO, REMOTE CMD, L2TP,MIRC,ICQ, CUSEEME,H323_Q931,H323_RAS

Caution None.

References

- *create alg port* command
- *get alg port* command
- *get alg type* command.

3.49 delete arp

Description Use this command to delete an entry from the ARP table.

Command Syntax ***delete arp ip*** ip-address

Parameters

Name	Description
ip ip-address	IP Address corresponding to the media-dependent "physical" address, whose entry is to be deleted. **Type:** Mandatory **Valid values:** Any valid class A/B/C IP address

Mode Super-User

Example ***$ delete arp ip 192.168.1.1***

Output Verbose Mode On:

```
If Name    Type         Mac Address              Ip Address
-------------------------------------------------------------
veth-0     Static      11:11:11:11:11:11         192.168.1.1

Entry Deleted
```

Verbose Mode Off:

```
Entry Deleted
```

Output field description

Field	Description
If Name	This specifies the physical Interface for the media. It may be: *eth-0* or *veth-0 to veth-4*
Type	This defines the type of mapping in use. The value *Invalid* has the effect that this entry is not used. It may be: *Static, Dynamic, Other, Invalid*
Mac Address	The media-dependent `physical' address
Ip Address	IP Address corresponding to the media-dependent `physical' address

Caution None.

References

- *create arp* command
- *get arp* command
- *ip stats* related commands
- *ip route* related commands
- *ip address* related commands
- *ip cfg* related commands

3.50 delete atm port

Description This command is used to delete a virtual atm port.

Command Syntax ***delete atm port ifname*** interface-name

Parameters

Name	Description
Ifname interface-name	This specifies the ATM port to be deleted **Type:** Mandatory **Valid values:** *atm-0*

Mode Super-User.

Example ***$ delete atm port ifname*** **atm-0**

Output Verbose Mode On:

```
If-Name          : atm-0            MaxVccs          : 4
CBRPriority      : 5                UBRPriority      : 1
RTVBRPriority    : 4                NRTVBRPriority   : 3
GFRPriority      : 2                Latency          : fast
MaxConfVccs      : 0
OAMSrc           : 0xffffffffffffffffffffffffffffffff
Oper Status      : Up                Admin Status    : Up

Entry Deleted
```

Verbose Mode Off:

```
Entry Deleted
```

Output field description

Field	Description
If Name	This specifies the name of the ATM port which has been deleted. It can be: *atm-0.*
MaxVccs	This specifies the maximum number of VCCs (PVCCs and SVCCs) supported at this ATM interface. It may be: *0-64.*
CBRPriority	Priority of the CBR Class. A value of *1* means lowest priority and higher the value higher the priority. It may be *1-5*.
UBRPriority	Priority of the best effort traffic. A value *0* means no traffic of this class is supported. The higher the value, the higher the priority. It may be: *1-5.*
RTVBRPriority	Priority of the RT-VBR service category. The higher the value, the higher the priority. It may be *1-5*.
NRTVBRPriority	Priority of the NRTVBR service category. The higher the value, the higher the priority. It may be: *1-5.*
GFRPriority	This specifies the priority of GFR class. A value of *0* means no traffic of this class is supported. Higher the value higher the priority. It may be: *1-5.*

Field	Description
Latency	Type of DSL channel in use on the underlying DSL port. It may be: *fast, interleaved*
MaxConfVccs	This specifies the current number of VCCs configured on this port. It may be:*0* - Value defined in MaxVccs
OAMSrc	Loop back source id assigned to the ATM port. The ATM port will respond to all loopback cells which carry this OAM id.
Oper Status	The actual/current state of the interface. It can be either *Up* or *Down*
Admin Status	The desired state of the interface. It may be either *Up* or *Down*

Caution All VCs created on the ATM port must be deleted before deleting the port itself.

References

- *atm trfdesc* commands
- *atm vc* related commands
- *oam lpbk* command
- Other *atm port* commands
- *atm statistics* related commands.

3.51 delete atm svccfg

Description Use this command to delete a configured SVC.

Command Syntax ***delete atm svccfg ifname*** interface-name

Parameters

Name	Description
Ifname interface-name	Interface name of the SVC to be deleted. **Type:** Mandatory **Valid values:** *aal5-0, aal5-1…*

Mode Super-User, User.

Example ***$ delete atm svccfg ifname aal5-0***

Output Verbose Mode On

```
VC IfName        : aal5-0          AAL5 Encap       : VC Mux
VPI              : 5               VCI              : 10
Numbering Plan   : atmes
Dest Atm Address : 0x47000580ffde000000000001050000000000000000
Trf Descr Index  : 1               Access Protocol  : PPPoA
Aal5 Tx Size     : 200             Aal5 Rx Size     : 200

Entry Deleted
```

Verbose Mode Off

```
Entry Deleted
```

Output field description

Name	Description
VC Ifname	Interface name of the deleted SVC.
AAL5 Encap	The type of Protocol Multiplexing used over 1483
VPI	The VPI of the ATM VC found towards the specified ATM Destination
VCI	The VCI of the ATM VC found towards the specified ATM Destination
Numbering Plan	The Address Plan to which the specified ATM Destination Address (for SVC to be opened) belongs.
Dest Atm Address	The ATM address of the destination with which the connection is established.
Trf Descr Index	The index of the Traffic Descriptor Table entry whose traffic parameters are for the SVC to be opened.
Access Protocol	This specifies the protocol that runs on the VC
Aal5 Tx Size	This specifies the transmit CPCS SDU size.
Aal5 Rx Size	This specifies the receive CPCS SDU size.

Caution None.

References

- *create atm* svccfg command
- *Get atm svccfg* command

3.52 delete atm trfdesc

Description Use this command to delete a traffic descriptor.

Command Syntax ***delete atm trfdesc trfindex*** traffic-descriptor-index

Parameters

Name	Description
trfindex traffic-descriptor-index	This identifies the traffic descriptor entry to be deleted. **Type:** Mandatory **Valid values:** *0* - *

Mode Super-User

Example

```
$ delete atm trfdesc trfindex 2
```

Output Verbose Mode On:

```
Traffic Descr Id     : 2              Type                : NOCLP_NOSCR
Service Category     : UBR            Frame Discard       : Enabled
PCR                  : 0              MCR                 : 0

Entry Deleted
```

Verbose Mode Off:

```
Entry Deleted
```

Output field description

Field	Description
Traffic Descr Id	This identifies the traffic descriptor entry which has been deleted.
Type	This defines the type of traffic used. It may be: *NOCLP_NOSCR*, *CLP_NOTAG_MCR*, or *NOCLP_SCR*.
Service Category	This specifies the service category to be used. It may be: *UBR, GFR, CBR, RTVBR, NRTVBR*.
Frame Discard	It is always *Enabled.* It indicates that the network is requested to treat data for this connection, in the given direction, as frames (e.g. AAL5 CPCS_PDU's) rather than as individual cells. This treatment may for example involve discarding entire frames during congestion, rather than a few cells from many frames.
PCR	Peak Cell Rate for ATM Traffic
MCR	Minimum Cell Rate for ATM Traffic

Caution The traffic descriptor should not be in use before deletion.

References

- Other *atm trfdesc* commands
- *atm vc* related commands
- Other *atm port* commands
- *atm statistics* related commands

3.53 delete atm uni

Description Use this command to delete UNI configuration.

Command Syntax ***delete atm uni ifname*** interface-name

Parameters

Name	Description
Ifname interface-name	Interface Index of the ATM VC over which UNI signaling is run. **Type:** Mandatory **Valid values:** *aal5-0, aal5-1…*

Mode Super-User.

Example ***$ delete atm uni ifname aal5-0***

Output Verbose Mode On

```
IfName          : aal5-0          ATM Numb Plan : atmes
Status          : Up              Version       : UNI40
Self ATM Address: 0x39000760ff8900000000000119000000000000000

Entry Deleted
```

Verbose Mode Off

```
Entry Deleted
```

Output field description

Name	Description
Ifname	Interface name of VC over which UNI signaling is running. It can be: *aal5-0, aal5-1…*
ATM NumbPlan	The Address Plan to which the specified ATM Source Address belongs.
Status	This specifies the status of the Signaling ATM Adaptation Layer (SAAL) layer. The purpose of SAAL is to provide reliable transfer of signaling message between peer UNI entities.
Version	This specifies the version of the UNI used. UNI31 and UNI40 mean UNI3.1 and UNI4.1 respectively.
SelfAtmAddress	The source ATM address.

Caution None.

References

- *create atm uni* command
- *get atm uni* command

3.54 delete atm vc intf

Description Use this command to delete an existing ATM Virtual Circuit.

Command Syntax ***delete atm vc intf ifname*** interface-name

Parameters

Name	Description
ifname interface-name	Interface Name of the VC which is to be deleted **Type:** Mandatory **Valid values:** *aal5-0, aal5-1…*

Mode Super-User

Example ***$ delete atm vc intf ifname*** **aal5-0**

Output Verbose Mode On:

```
LowIf              : atm-0     VPI              : 10         VCI    : 10
VC IfName          : aal5-0    VC Type          : PVC
Admin Status       : Up        Oper Status      : Up
Aal5 Tx Size       : 9200      Aal5 Rx Size     : 9200
AAL Type           : AAL5      AAL5 Encap       : LLC Mux
Max Aal5 Proto     : 3         Trf Descr Index  : 2
VC Weight          : 40
Entry Deleted
```

Verbose Mode Off:

```
Entry Deleted
```

Output field description

Field	Description
Lowif	Lower interface index. It is always: *atm-0*
VPI	It is the Virtual Path Identifier.
VCI	It is the Virtual Circuit Identifier.
VC If-Name	Interface name of the VC which has been deleted. It can be: *aal5-0, aal5-1…*
VC Type	This field specifies whether VC type is PVC or SVC
Oper Status	The actual/current state of the interface. It can be either *Up* or *Down*
Admin Status	The desired state of the interface. It may be either *Up*, *Down or Loopback. Loopback* has a special significance. A Loopback VC will loop back whatever cells it receives.
Aal5 Tx Size	This specifies the transmit CPCS SDU size to be used
Aal5 Rx Size	This specifies the receive CPCS SDU size to be used
AAL Type	AAL type in use for the VC

Field	Description
AAL5 Encap	This specifies the data multiplexing method to be used over the AAL5 SSCS layer.
Max Aal5 Proto	This specifies the maximum number of protocols that are supported over the VC
Trf Descr Index	This identifies the transmit traffic parameters in use. It corresponds to a valid entry in the traffic descriptor table
VC Weight	This specifies the priority of the VC. Higher value means higher priority

Caution Do not create anything using the VC you are deleting.

References

- Other *atm vc intf* commands
- *atm trfdesc* related commands
- *oam lpbk* command
- *atm port* commands
- *atm statistics* commands

3.55 delete bridge port intf

Description This command is used to delete an existing bridge port.

Command Syntax ***delete bridge port intf ifname*** interface-name

Parameters

Name	Description
ifname interface-name	This specifies the bridge port interface to be deleted. **Type:** Mandatory **Valid values:** *eoa-0 - *, eth-0, usb-0*

Mode Super-User

Example ***$ delete bridge port intf ifname*** **eth-0**

Output Verbose Mode On:

```
Port     If-Name   Delay-Exceed-Discards    MTU-Exceed-Discards
-------------------------------------------------------------
1        eth-0     0                        0

Entry Deleted
```

Verbose Mode Off:

```
Entry Deleted
```

Output field description

Field	Description
Port	The port number of the interface which is being deleted.
If-Name	This specifies the Interface name corresponding to the above port. It can be: *eoa-0 - *, eth-0, usb-0*
Delay-Exceed-Discards	The number of frames discarded by this port due to excessive transit delay through the bridge
MTU-Exceed-Discards	The number of frames discarded by this port due to the frame size being greater than the MTU of the interface

Caution None.

References

- *get bridge port intf* command
- *create usb intf* command
- *create bridge port intf* command
- *bridge mode* related commands
- *bridge port stats* related commands
- *bridge static* related commands
- *bridge forwarding* related commands

3.56 delete bridge static

Description Use this command to delete an existing bridge static entry for a given MAC address.

Command Syntax ***delete bridge static macaddr*** mac-address ***inifname*** interface-name|all

Parameters

Name	Description
macaddr mac-address	The destination MAC address for the bridge static entry which is to be deleted. **Type:** Mandatory **Valid values:** *0:0:0:0:0:0 to FF:FF:FF:FF:FF:FF*
inifname interface-name	Interface from which a frame must be received in order for this entry's filtering information to apply. A value of all indicates that this entry applies on all interfaces of the bridge for which there is no other applicable entry. **Type:** Mandatory **Valid values:** *eth-0, eoa-0 - *, usb-0*

Mode Super-User

Example ***delete bridge static macaddr 1:1:1:1:1:1 inifname veth-0***

Output Verbose Mode On:

```
MAC Address        : 01:01:01:01:01:01      Incoming Interface : veth-0
Interfaces         : eth-0 eoa-1

Entry Deleted
```

Verbose Mode Off:

```
Entry Deleted
```

Output field description

Field	Description
MAC Address	The destination MAC address for the bridge static entry which is being deleted.
Incoming Interface	Interface from which a frame must be received in order for this entry's filtering information to apply. A value of *all* indicates that this entry applies on all interfaces of the bridge for which there is no other applicable entry.
Interfaces	The interfaces to which frames destined for a specific MAC address are allowed to be forwarded. They may be: *eoa-0 - *, eth-0*

Caution None.

References

- *create bridge static* command
- *get bridge static* command
- *modify bridge static* command
- *bridge mode* related commands
- *bridge static* related commands
- *bridge forwarding* related commands
- *bridge port stats* related commands

3.57 delete ddns hostname

Description Use this command to delete Dynamic DNS Host Name Table

Command Syntax ***delete ddns hostname ifname*** ifname ***name*** name

Parameter

Name	Description
ifname ifname	Interface name of the public interface for which this entry defines the Dynamic DNS Host Name. **Valid Values :** ppp-0 - ppp-*, ipoa-0 - ipoa-*, eoa-0 - eoa-*, eth-0 - eth-*, usb-0, wlan-0 **Type:** Mandatory
name name	Hostname registered at service provider. **Type:** Mandatory

Mode Super-User

Example ***$ delete ddns hostname ifname*** ppp-0 ***name*** www.xyz.com

Output Verbose Mode On:

```
Interface  HostName
--------------------------------------------------------------------------------
ppp-0      www.xyz.com

Entry Deleted
```

Verbose Mode Off:

```
Entry Deleted
```

Output field description

Field	Description
Interface	Interface name of the public interface for which this entry defines the Dynamic DNS Host Name. Valid Values : ppp-0 - ppp-*, ipoa-0 - ipoa-*, eoa-0 - eoa-*, eth-0 - eth-*, usb-0, wlan-0
HostName	Hostname registered at service provider.

Cautions None.

References

- *get ddns hostname* command
- *create ddns hostname* command

3.58 delete ddns intf

Description Use this command to delete Dynamic DNS Service Configuration

Command Syntax ***delete ddns intf ifname*** ifname

Parameter

Name	Description
ifname ifname	Interface name of the public interface for which this entry defines the Dynamic DNS profile. **Valid Values :** ppp-0 - ppp-*, ipoa-0 - ipoa-*, eoa-0 - eoa-*, eth-0 - eth-*, usb-0, wlan-0 **Type:** Mandatory

Mode Super-User

Example ***$ delete ddns intf ifname*** ppp-0

Output Verbose Mode On:

```
Interface        : ppp-0
Service Provider : dyndns
User Name        : "Viking"
Type of system   : dynamic WildCard        : enable
Mail Exchanger   : www.IAD1.com
Mail Backup      : enable  Offline Support : enable

Entry Deleted
```

Verbose Mode Off:

```
Entry Deleted
```

Output field description

Field	Description
Interface	Interface name of the public interface for which this entry defines the Dynamic DNS profile. Valid Values : ppp-0 - ppp-*, ipoa-0 - ipoa-*, eoa-0 - eoa-*, eth-0 - eth-*, usb-0, wlan-0
Service Provider	This is the name of the Dynamic DNS service provider where the user has registered and has an account.Some examples are www.tzo.com, www.dyndns.org
User Name	Username registered at service provider. The value is to be given in double quotes.

Field	Description
Type of system	This parameter is valid only when SrvcName is DYNDNS.www.dyndns.org provides 3 kinds of services - Dynamic DNS, Custom DNS and Static DNS. The user can create different domains in these systems.Custom DNS service is a full DNS solution for newly purchased domains or domains you already own. A web-based interface provides complete control over resource records and your entire domain including support for dynamic IPs and automated updates.Static DNS service points a DNS hostname in some domain owned by dyndns.org to the user's ISP-assigned static or pseudo-static (meaning which do not change too frequently) IP address.DynDNS service points a fixed hostname in some domain owned by dyndns.org to the user's ISP-assigned dynamic IP address. This allows more frequent updation of IP addresses than Static DNS.
WildCard	This parameter is valid only if SrvcName is DYNDNS.It specifies whether Wildcard CNAME are to be resolved or not. If enabled, addresses *.yourhost.ourdomain.ext are aliased to the same address as yourhost.ourdomain.ext.
Mail Exchanger	This parameter is valid only if SrvcName is DYNDNS. It specifies a Mail Exchanger (MX) for use with the hostname being modified. The specified MX must resolve to an IP address,or it will be ignored.Providing no MX setting (or an MX that doesn't resolve properly to an A record) will cause the hostname's MX record(s) to be removed.
Mail Backup	This parameter is valid only if SrvcName is DYNDNS.It specifies whehter mails are to be backed up by the service provider.
Offline Support	This parameter is valid only if SrvcName is DYNDNS.If enabled, the service provider redirects browsers to its own site if the registered host is currently offline.

Cautions None.

References

- *get ddns intf* command
- *create ddns intf* command

3.59 delete dhcp relay intf

Description Use this command to disable DHCP relaying on the specified interface.

Command Syntax ***delete dhcp relay intf ifname*** interface-name

Parameters

Name	Description
Ifname interface-name	This specifies the Interface for which DHCP Relaying is to be disabled **Type:** Mandatory **Valid values:** *eth-0, ppp-0, ppp-1, ipoa -0-*, usb-0*

Mode Super-User

Example ***$ delete dhcp relay intf ifname*** **eth-0**

Output Verbose Mode On:

```
If-name
-------
eth-0

Entry Deleted
```

Verbose Mode Off:

```
Entry Deleted
```

Output field description

Field	Description
If-Name	This specifies an interface which is enabled for DHCP Relay. It can be: *eth-0, ppp-0, ppp-1…*

Caution None.

References

- *get dhcp relay intf* command
- *create dhcp relay intf* command
- *dhcp relay cfg* related commands
- *dhcp relay stats* related commands

3.60 delete dhcp server exclude

Description Use this command to delete an entry in the address exclusion table. The entry thus deleted, is now available for allocation to a client.

Command Syntax ***delete dhcp server exclude ip*** ip-address

Parameters

Name	Description
ip ip-address	The IP address that has to be deleted from the exclusion list. The IP Address must belong to a pool. **Type:** Mandatory **Valid values:** Any valid class A/B/C IP address

Mode Super-User

Example ***$ delete dhcp server exclude ip*** **192.168.1.5**

Output Verbose Mode On:

```
Ip Address
----------
192.168.1.5

Entry Deleted
```

Verbose Mode Off:

```
Entry Deleted
```

Output field description

Field	Description
Ip Address	This is the IP Address that has been excluded.

Caution None.

References

- *get dhcp server exclude* command
- *create dhcp server exclude* command
- *dhcp server pool* related commands

3.61 delete dhcp server host

Description Use this command to delete the specified static DHCP host entry.

Command Syntax ***delete dhcp server host ip*** ip-address

Parameters

Name	Description
ip ip-address	This specifies the IP address of the host the entry pertaining to which is to be deleted. **Type:** Mandatory **Valid values:** Any valid class A/B/C IP address

Mode Super-User

Example ***$ delete dhcp server host ip*** **192.168.1.7**

Output Verbose Mode On:

```
Host Ip          : 192.168.1.7        Hardware Addr    : 12:34:45:56:03:02
Def Lease(sec)   : 2592000            Max Lease(sec)   : 31536000
Domain Name      :
Subnet Mask      : 255.255.255.0
Gateway Ip       : 0.0.0.0            Smtp Ip          : 0.0.0.0
Dns Ip           : 0.0.0.0            Sec. Dns Ip      : 0.0.0.0
Pop3 Ip          : 0.0.0.0            Nntp Ip          : 0.0.0.0
Www Ip           : 0.0.0.0            Irc Ip           : 0.0.0.0
Wins Ip          : 0.0.0.0            Sec. Wins Ip     : 0.0.0.0

Entry Deleted
```

Verbose Mode Off:

```
Entry Deleted
```

Output field description

Field	Description
Host Ip	This specifies the IP address provided to this host
Hardware Addr	This specifies the hardware address of the client
Def Lease	This specifies the lease period for which the server assigns an IP address to a client in case the client does not request for a specific lease period itself.
Max Lease	This specifies the maximum period for which the DHCP server can lease out an IP address to a DHCP client.
Domain Name	Specifies the domain name configured for this host
Subnet Mask	This specifies the subnet mask to be provided to the host
Gateway Ip	This specifies the default gateway IP address
Smtp Ip	This specifies the IP address of the NNTP Server

Field	Description
Dns Ip	This specifies the IP address of the primary Domain Name Server
Sec. Dns Ip	This specifies the IP address of the secondary Domain Name Server
Pop3 Ip	This specifies the IP address of the POP3 Server
Nntp Ip	This specifies the IP address of the SMTP Server
Www Ip	This specifies the IP address of the WWW Server
Irc Ip	This specifies the IP address of the IRC Server
Wins Ip	This specifies the IP address of the primary WIN Server
Sec. Wins Ip	This specifies the IP address of the secondary WIN Server

Caution None.

References

- *get dhcp server host* command
- *create dhcp server host* command
- *modify dhcp server host* command
- *dhcp server* related commands.

3.62 delete dhcp server pool

Description Use this command to delete an existing DHCP server pool.

Command Syntax ***delete dhcp server pool pool-id*** pool-id

Parameters

Name	Description
pool-id pool-id	This identifies the pool for which is to be deleted. **Type:** Mandatory **Valid values:** *0 - 255*

Mode Super-User

Example ***$ delete dhcp server pool-id poolid*** 0

Output Verbose Mode On:

```
Pool Id          : 0                  Status           : Disable
Start Ip         : 192.168.1.1        End Ip           : 192.168.1.200
Def Lease(sec)   : 2592000            Max Lease(sec)   : 31536000
Range Inuse      : 0                  Outstd Offers    : 0
Low Thres        : 0                  Subnet Mask      : 255.255.255.0
Domain Name      :
Gateway Ip       : 0.0.0.0            Smtp Ip          : 0.0.0.0
Dns Ip           : 0.0.0.0            Sec. Dns Ip      : 0.0.0.0
Pop3 Ip          : 0.0.0.0            Nntp Ip          : 0.0.0.0
Www Ip           : 0.0.0.0            Irc Ip           : 0.0.0.0
Wins Ip          : 0.0.0.0            Sec. Wins Ip     : 0.0.0.0

Entry Deleted
```

Verbose Mode Off:

```
Entry Deleted
```

Output field description

Field	Description
Pool Id	This is the pool identifier.
Status	This defines the Admin status of the entry. It may be either *Enable* or *Disable*
Start Ip	The IP address of the first address in the range.
End Ip	The IP address of the last address in the range
Def Lease	This specifies the lease period for which the server assigns an IP address to a client in case the client does not request for a specific lease period itself.
Max Lease	This specifies the maximum period for which the DHCP server can lease out an IP address to a DHCP client.
Range Inuse	The number of addresses in this range that are currently in use. This number includes those addresses whose lease has not expired and addresses which have been reserved

Field	Description
Outstd Offers	The number of outstanding DHCPOFFER messages for this range is reported with this value. An offer is outstanding if the server has sent a DHCPOFFER message to a client, but has not yet received a DHCPREQUEST message from the client nor has the server-specific timeout, within which a client can respond to the offer message, for the offer message expired
Low Thres	This specifies the lowest threshold value on the number of available/free IP addresses for a particular shared network
Subnet Mask	The subnet mask provided to any client offered an address from this range
Domain Name	Domain name used per subnet.
Gateway Ip	This specifies the default gateway IP address
Smtp Ip	This specifies the IP address of the NNTP Server
Dns Ip	This specifies the IP address of the primary Domain Name Server
Sec. Dns Ip	This specifies the IP address of the secondary Domain Name Server
Pop3 Ip	This specifies the IP address of the POP3 Server
Nntp Ip	This specifies the IP address of the SMTP Server
Www Ip	This specifies the IP address of the WWW Server
Irc Ip	This specifies the IP address of the IRC Server
Wins Ip	This specifies the IP address of the primary WIN Server
Sec. Wins Ip	This specifies the IP address of the secondary WIN Server

Caution None.

References

- *create dhcp server pool* command
- *create dhcp server pool* command
- *get dhcp server pool* command
- *dhcp server cfg* related commands
- *dhcp server exclude* related commands
- *dhcp server address* related commands

3.63 delete dns servaddr

Description Use this command to delete DNS server addresses.

Command Syntax ***delete dns servaddr*** <ip-address>

Parameters :

Name	Description
<ip-address>	This parameter specifies the IP address for configuring the DNS server address.Type: Mandatory-Valid values: Valid IP address.

Mode Super-User.

Example ***$ delete dns servaddr*** *182.25.2.1*

Output Verbose mode on:

```
DNS Server IP Address
---------------------
182.25.2.1

Entry Deleted
```

Verbose mode off:

```
Entry Deleted
```

Output Field description:

Field	Description
DNS Server IP Address	This specifies the IP address of the DNS server.

Caution None

References:

- create dns servaddr
- get dns servaddr
- modify dns relay cfg
- get dns relay cfg
- get dns relay stats
- reset dns relay stats

3.64 delete eoa intf

Description Use this command to delete an eoa interface.

Command Syntax ***delete eoa intf ifname*** interface-name

Parameters

Name	Description
ifname interface-name	This parameter specifies the eoa interface which has to be deleted. **Type:** Mandatory. **Valid values:** *eoa-0* - *

Mode Super-User

Example ***$ delete eoa intf ifname eoa-0***

Output Verbose Mode On:

```
IfName               : eoa-0          Interface Sec Type : Public
Configured IP Address: 0.0.0.0        Mask               : 0.0.0.0
Low IfName           : aal5-0         NAT Direction      : OUT
Gateway              : 0.0.0.0       DRoute             : False
Oper Status          : Down           Admin Status       : Up
UseDHCP              : False

Entry Deleted
```

Verbose Mode Off:

```
Entry Deleted
```

Output field description

Field	Description
IfName	The name of the interface which has been created.
Configured IpAddress	IP address assigned to the eoa interface.
Mask	Network mask to be applied to the IP Address.
LowIfName	Specifies the lower interface.
Nat Direction	This specifies the NAT direction which may be: *inside, outside or none*.
Oper Status	The actual/current state of the interface. It can be either *Up* or *Down*
Admin Status	The desired state of the interface. It may be either *Up* or *Down*
UseDhcp	Whether or not a DHCP client is used to obtain the IP address for this interface from a DHCP server
Interface Sec Type	Interface Security Type.

Field	Description
Droute	Default route
Gateway address	Gateway IP address

Caution No bridge port can be created on the eoa interface.

References

- *create eoa intf* command
- *get eoa intf* command
- *modify eoa intf* command
- *eoa stats* related commands
- *interface stats* related commands
- *atm vc intf* related commands

3.65 delete ethernet intf

Description Use this command to delete a virtual ethernet interface

Command Syntax ***delete ethernet intf ifname*** interface-name

Parameters

Name	Description
ifname interface-name	This parameter specifies the interface to be deleted. **Type:** Mandatory **Valid values:** *veth-0* - *

Mode Super-User

Example ***$ delete ethernet intf ifname*** **eth-0**

Output Verbose Mode Off:

```
Entry Deleted

Interface          : veth-0
Interface Sec Type : Public                Configured IP Address : 192.168.1.1
Mask               : 255.255.255.0         UseDhcp               : False
Physical Interface : eth-0                 Nat Direction         : None
Configured Duplex  : auto                   Configured Speed      : auto
Duplex             : half                  Speed                 : 10BT
Operational Status : Up                    Admin Status          : Up
```

Verbose Mode Off:

```
Entry Deleted
```

Output field description

Field	Description
Interface	The name of the interface which has been created.
Interface Sec Type	Interface security type.
Configured Ip Address	IP address assigned to the Ethernet port.
Mask	Network mask to be applied to the IP Address.
UseDhcp	Local: IP address for this interface is obtained from a local DHCP server Remote: DHCP client is used to obtain the IP address for this interface from a remote DHCP server False: DHCP client is not used.
Physical Interface	Valid only in case of virtual interfaces i.e. the Type is not *eth*. It can only be *eth-0*
Nat Direction	This specifies the NAT direction which may be: *inside, outside or none*.

Field	Description
Configured Duplex	The duplex modeto be used by theinterface as configured by the user
Configured Speed	Line speed to be used by Ethernet interface as configured by the user
Duplex	The duplex mode used by the interface.
Speed	Line speed used by Ethernet interface
Operational Status	The actual/current state of the interface. It can be either *up* or d*own*
Admin Status	The desired state of the interface. It may be either *up* or *down*

Caution None.

References

- *get ethernet intf* command
- *create ethernet intf* command
- *modify ethernet intf* command
- *ethernet stats* related commands
- *interface stats* related commands

3.66 delete fwl blacklist

Description Use this command to delete a blacklisted host.

Command Syntax ***delete fwl blacklist ip*** ddd.ddd.ddd.ddd

Parameters

Name	Description
ip <ddd.ddd.ddd.ddd>	This specifies the IP address of the blacklisted host that is to be deleted. **Type**: Mandatory **Valid values** : 0.0.0.0 - 255.255.255.255

Mode Super-User

Example ***$ delete fwl blacklist ip*** *172.25.7.8*

Output Verbose Mode On:

```
IP Address      Blacklist Reason    RuleId     Time Left(sec)
-------------------------------------------------------------
172.25.7.8      Ping of Death         1 20

Entry Deleted
```

Verbose Mode Off:

```
Entry Deleted
```

Output field description

Field	Description
IP Address	This specifies the IP address of the blacklisted host
Blacklist Reason	This specifies the reason for blacklisting the host.
RuleId	This specifies the firewall rule id which caused the black-listing.
Time Left(sec)	This specifies time duration in seconds after which the IP address entry will be removed from this table.

Caution None.

References

- *get fwl blacklist* command

3.67 delete igmp intf

Description Use this command to delete an IGMP interface over a given interface.

Command Syntax ***delete igmp intf ifname*** interface-name

Parameters

Name	Description
ifname interface-name	This identifies the interface on which IGMP has to be deleted. **Type:** Mandatory **Valid values:** *eth-0*, *veth-0 - **, *ppp-0 - **, *eoa-0 - **, *usb-0, ipoa -0-** **Default value:** *none*.

Mode Super-User.

Example ***$ delete igmp intf ifname veth-0***

Output Verbose Mode Off

```
IfName                  : eth-0   Type                    : Host
Version                 : igmpv1  Query Interval(sec)     : 150
Query Max Resp Time(sec): 10Last  Memb QueryIntvl(sec)     : 2
Robustness              : 10      Join Requests           : 10
Current Groups          : 8

Entry Deleted
```

Verbose Mode Off

```
Entry Deleted
```

Output field description

Field	Description
Query Interval(sec)	This is the periodic interval at which host-query messages (queries) are transmitted on this interface
Version	This field specifies the version of IGMP.
Query Max ResponseTime(sec)	This field specifies the query max response time (in secs)
Last Memb QueryIntvl(sec)	This field specifies the Last Member Query Interval (in secs)
Join Requests	This is the number of times a group membership has been added to this interface
Current Groups	This is the current number of entries for this interface in the IGMP Group Table.

Caution None.

References

- *get igmp intf* command
- *create igmp intf* command
- *get igmp groups* command

3.68 delete ilmi intf

Description Use this command to delete an ILMI interface.

Command Syntax ***delete ilmi intf ifname*** interface-name

Parameters

Name	Description
ifname interface-name	Its value is same as ifIndex for the ATM type of interface in the ifTable. **Type:** Mandatory. **Valid Values :** atm-0, atm-1, etc.

Mode Super-user.

Example ***$ delete ilmi intf ifname*** atm-0

Output Verbose Mode On

```
Interface Name    : atm-0      Status       : Disable
VPI               : 12         VCI          : 50
Timeout(sec)      : 1          Keep Alive Time(sec) : 3
Maximum Retries   : 11         Version  : 4.0

Entry Deleted
```

Verbose Mode Off

```
Entry Deleted
```

Output field description

Field	Description
Interface Name	The name of the interface which has been created.
Status	Whether ilmi is enabled or not on this interface.
VPI	VPI to be used for ILMI message exchanges between peer ILMIs
VCI	VCI to be used for ILMI message exchanges between peer ILMIs.
Timeout	Timeout value in seconds, for SNMP Get/ Set messages exchanged between peer ILMIs.
Keep Alive Time	The time-interval in seconds, ILMI should use to poll for peer ILMI's availability.
Maximum Retries	Number of times ILMI should retry.
Version	The version of ILMI

Caution None

References

- *create ilmi intf* command
- *get ilmi intf* command
- *modify ilmi intf* command
- *modify ilmi trigger* command

3.69 delete ip route

Description Use this command to delete an existing routing table entry.

Command Syntax ***delete ip route ip*** dest-ip-address ***mask*** net-mask

Parameters

Name	Description
ip dest-ip-address	Destination IP address of the route which is to be deleted. **Type:** Mandatory **Valid values:** Any valid class A/B/C IP address
mask net-mask	The Mask of the destination IP Address. **Type:** Mandatory **Valid values:** *128.0.0.0 – 255.255.255.254*

Mode Super-User

Example ***$ delete ip route ip 192.168.2.40 mask 255.255.255.0***

Output Verbose Mode On:

```
Destination   Net Mask       Gateway     If-name    Route  Route  Age(sec)
                                                     Type   Orig
-------------------------------------------------------------------------------
192.168.2.40  255.255.255.0  192.168.1.1  veth-0    IND    LCL    0

Entry Deleted
```

Verbose Mode Off:

```
Entry Deleted
```

Output field description

Field	Description
Destination	Destination IP address of this route
Mask	The Mask of the destination IP Address
Gateway	The IP address of the next hop for this route
If-Name	The local interface through which the next hop of this route will be reached
Route Type	The type of route. It may be: *Dir* (for Direct), *Ind* (for Indirect), or *inv* (for invalid route)
Route Orig	The routing mechanism through which this route was learned. It may be: *NET* (for Network Management), *LCL* (for Local), *RIP*, *ICMP*,*DYI* (Dynamic through Interface creation)
Age	The number of seconds since this route was last updated or otherwise determined to be correct

Caution None.

References

- *get ip route* command
- *create ip route* command
- *ip stats* related commands
- *ip cfg* related commands
- *ip address* related commands
- *arp* related commands

3.70 delete ipf rule entry

Description This command is used for deleting an IP filter rule.

Command Syntax ***delete ipf rule entry ruleid*** rule-id

Parameters

Name	Description
ruleid rule-id	The index given by the caller to identify the rule entry. **Type**: Mandatory **Valid values:** *1-4294967295*

Mode Super-User.

Example ***$ delete ipf rule entry ruleid 1***

Output Verbose Mode On

```
Rule id           : 1Interface         : eth-0
Rule Admin status : DisableRule Oper Status  : Disable
In interface      : ALLDirection         : Out
Security Level    : HighBlacklist Status        : Enable
Logging           : DisableAction            : Accept
Log Tag           : -
IP Frag Pkt       : Yes         IP Opt Pkt        : No
TCP Flag          : SynStore State       : Enable
Src Addr    : Equal          172.25.8.76
Dest Addr   : Range          172.25.8.70          172.25.8.90
Src Port    : Out Of Range   10                   20
Dest Port   : Not Equal      3
ICMP Code   : Not Equal      10
ICMP Type   : Equal          unreach
TransProt   : Equal          TCP
IP Pkt Size : Less Than      10
TOD Rule    : Enable Between  01:02:30              02:01:30


Entry Deleted
```

Verbose Mode Off

```
Entry Deleted
```

Output field description

Field	Description
Rule id	The index given by the caller to identify the rule entry.
Rule Admin Status	Specifies the administrative status of the rule entry.
Interface	Specifies the IP-enabled physical interface to be associated to this rule. *All* indicates that rule is to be associated to all interfaces.

Field	Description
In Interface	Specifies the input interface ID which may be used to dictate the rules like deny/accept all traffic from a specific interface. So, this field can be specified only if direction is *out*.
Direction	Specifies the direction of Data flow on which filtering is to be applied.
Action	Specifies the action to be taken when a packet matches a rule.
Logging	This flag controls the logging of matched packets. Each log will contain IP Header and TCP/UDP header or ICMP fields, if available.
Log Tag	This specifies the Filter logging tag, which will be added to all the logs generated due to the rule
Src Addr	This field specifies the matching criteria for source IP Address along with the source IPAddress value and the destination IPAddress value. The source or destination or both are shown depending on whether the matching criteria is relational, range, erange, any or self.
Dest Addr	This field specifies the matching criteria for destination IP Address along with the start destination IPAddress value and end destination IPAddress value. The start or end or both are shown depending on whether the matching criteria is relational, range, erange, any or self.
Src Port	This field specifies the matching criteria for source port along with the start of src port and the end of src port. The start or end or both are shown depending on whether the matching criteria is relational, range, erange, any or bcast.
Dest Port	This field specifies the matching criteria for destination Port along with the start dest port and the end dest port. The start or end or both are shown depending on whether the matching criteria is relational, range, erange, any or bcast.
ICMP Code	This field specifies the matching criteria for ICMP code value along with the code field in ICMP header in case of ICMP packets.
ICMP Type	This field specifies the matching criteria for ICMP Type along with the type field in ICMP header in case of ICMP packets.
TransProt	This field specifies the matching criteria for transport protcol field along with the transport layer protocol number as per IANA.
TCP Flag	This specifies filtering criteria for TCP packet types.
Store State	This specifies whether stateful filtering is done or not

Field	Description
Security Level	This specifies the association of rule with system wide service protection level.
Blacklist Status	This specifies whether source of the packet should be put in blacklist if it matches with the rule. It will be applicable to deny kind of rules
IP Frag Pkt	This specifies whether the rule is applicable to fragmented packets, non fragmented packets or in both cases.
IP Opt Pkt	This specifies whether the rule is applicable to IP packet with or without IP options or in both cases.
IP Pkt Size	This field specifies the matching criteria for IP Pkt Size along with IP packet filtering attribute . It should be compared against the packet size value in IP header.
ToD Rule	This field specifies whether the rule should be applied for the duration specified."Enable Between" indicates that the rule is applied between the specified time duration."Disable Between" indicates that rule is not applicable between the specified duration, but it is applicable for remaining time of the day.
Rule Oper Status	A rule will be operationally enabled if and only if it is administratively enabled, its Time of Day status as per current time is Enable, and if the rule's security level matches the global security level as shown by get ipf global.

Caution None.

References

- *create ip rule entry* command
- *get ip rule entry* command
- *modify ip rule entry* command

3.71 delete ipf session

Description Use this command to delete IP Filter session information.

Command Syntax ***delete ipf session sessid*** decvalue

Parameters

Name	Description
sessid decvalue	This is index of a session, which needs to be deleted. **Type**: Mandatory **Valid values** : *1-4294967295*

Mode Super-User.

Example ***$ delete ipf session sessid 1***

Output Verbose Mode On

```
Session Index          : 1
Time To Expire (sec)   : 200            Protocol               : TCP
IfName-1               : eth-0          IfName-2               : ppp-0
IP Address-1        : 172.25.8.9        IP Address-2        : 202.1.1.10
Port-1                 : 1245           Port-2                 : 23
IN RuleID on IfName-1  : 10             IN RuleID on IfName-2  : 20
IN Action on IfName-1  : accept         IN Action on IfName-2  : accept
OUT RuleID on IfName-1 : 30             OUT RuleID on IfName-2 : 40
OUT Action on IfName-1 : accept         OUT Action on IfName-2 : accept

Entry Deleted
```

Verbose Mode Off

```
Entry Deleted
```

Output field description

Field	Description
Session Index	This is index for display of session information This specifies the action defined in OUT RuleID on If-Name-2.
Time To Expire (sec)	Time remaining before the session is deleted.
Protocol	This field specifies the protocol type for which session is created.
IfName-1	This specifies the first physical interface associated with this session. This is the interface due to which session creation is initiated.

Field	Description
IfName-2	This specifies the second physical interface associated with this session. This interface is the one on which packet is routed.
IP Address-1	This specifies the IP address associated with ifName-1. If the packet originates from ifName-1, then this will be the source IP address and if the packet is arriving at ifName-1, then this will be the destination address.
IP Address-2	This specifies the IP address associated with ifName-2. If the packet originates from ifName-2, then this will be the source IP address and if the packet is arriving at ifName-2, then this will be the destination address.
Port-1	This specifies port associated with IP Address-1. If the packet originates from ifName-1, then this will be the source port and if the packet is arriving at ifName-1, then this will be the destination port.
Port-2	This specifies port associated with IP Address-2. If the packet originates from ifName-2, then this will be the source port and if the packet is arriving at ifName-2, then this will be the destination port.
IN RuleID on IfName-1	This specifies the matching rule id (i.e. the first rule that matches the packet selectors) on IfName-1 for incoming direction.
IN RuleID on IfName-2	This specifies the matching rule id on interface IfName-2 for incoming direction.
IN Action on IfName-1	This specifies the action defined in IN RuleID on IfName-1.
IN Action on IfName-2	This specifies the action defined in IN RuleID on IfName-2.
OUT RuleID on IfName-1	This specifies the matching rule id on interface IfName-1 for outgoing direction.
OUT RuleID on IfName-2	This specifies the matching rule id on interface IfName-2 for outgoing direction.
OUT Action on IfName-1	This specifies the action defined in OUT RuleID on IfName-1.
OUT Action on IfName-2	This specifies the action defined in OUT RuleID on IfName-2.

Caution None.

References

- *get ipf session* command
- *reset ipf session* command

3.72 delete ipf session

Description Use this command to delete an IP Filter session information.

Command Syntax ***delete ipf session sessid*** decvalue

Parameters :

Name	Description
sessid decvalue	This is index of a session, which needs to be deleted. **Type:** Mandatory **Valid values :** *1-4294967295*

Mode Super-User.

Example ***$ delete ipf session sessid 1***

Output Verbose mode on:

```
Session Index          : 1
Time To Expire (sec)   : 200    Protocol   : TCP
IfName-1               : eth-0  IfName-2   : ppp-0
IP Address-1    : 172.25.8.9        IP Address-2    : 202.1.1.10
Port-1                 : 1245   Port-2     : 23
IN RuleID on IfName-1  : 10     IN RuleID on IfName-2  : 20
IN Action on IfName-1  : accept IN Action on IfName-2  : accept
OUT RuleID on IfName-1 : 30     OUT RuleID on IfName-2 : 40
OUT Action on IfName-1 : accept OUT Action on IfName-2 : accept

Entry Deleted
```

Verbose mode off:

```
Entry Deleted
```

Output Field description:

Field	Description
Session Index	This is index for display of session information
Time To Expire (sec)	Time remaining before the session is deleted.
Protocol	This field specifies the protocol type for which session is created.

Field	Description
IfName-1	This specifies the first physical interface associated with this session. This is the interface due to which session creation is initiated.
IfName-2	This specifies the second physical interface associated with this session. This interface is the one on which packet is routed.
IP Address-1	This specifies the IP address associated with ifName-1. If the packet originates from ifName-1, then this will be the source IP address and if the packet is arriving at ifName-1, then this will be the destination address.
IP Address-2	This specifies the IP address associated with ifName-2. If the packet originates from ifName-2, then this will be the source IP address and if the packet is arriving at ifName-2, then this will be the destination address.
Port-1	This specifies port associated with IP Address-1. If the packet originates from ifName-1, then this will be the source port and if the packet is arriving at ifName-1, then this will be the destination port.
Port-2	This specifies port associated with IP Address-2. If the packet originates from ifName-2, then this will be the source port and if the packet is arriving at ifName-2, then this will be the destination port.
IN RuleID on IfName-1	This specifies the matching rule id (i.e. the first rule that matches the packet selectors) on IfName-1 for incoming direction.
IN RuleID on IfName-2	This specifies the matching rule id on interface IfName-2 for incoming direction.
IN Action on IfName-1	This specifies the action defined in IN RuleID on IfName- 1.
IN Action on IfName-2	This specifies the action defined in IN RuleID on IfName-2.
OUT RuleID on IfName-1	This specifies the matching rule id on interface IfName-1 for outgoing direction.
OUT RuleID on IfName-2	This specifies the matching rule id on interface IfName-2 for outgoing direction.
OUT Action on IfName-1	This specifies the action defined in OUT RuleID on IfName-1.
OUT Action on IfName-2	This specifies the action defined in OUT RuleID on IfName-2.

Caution None

References:

- get ipf session
- reset ipf session
- modify ipf global
- create ipf rule entry

3.73 delete ipoa intf

Description This command is used for deleting an IPoA interface.

Command Syntax ***delete ipoa intf ifname*** interface-name

Parameters

Name	Description
ifname interface-name	This parameter specifies the IPoA interface, which has to be deleted. **Type:** Mandatory. **Valid values:** *ipoa-0, ipoa-1, etc.*

Mode Super-User.

Example ***$ delete ipoa intf ifname ipoa-0***

Output Verbose Mode On

```
IfName                : ipoa-0          UseDHCP            : True
Type                  : non1577         Interface Sec Type: Public
Configured IP Address: 0.0.0.0          Mask               : 0.0.0.0
DRoute                : False           Gateway            : 0.0.0.0
NAT Direction         : OUT             Oper Status        : Down

Entry Deleted
```

Verbose Mode Off

```
Entry Deleted
```

Output field description

Field	Description
If-Name	The name of the IPoA interface which has been created.
UseDHCP	This specifies whether a DHCP client is used to obtain the IP address for this interface from a DHCP server, or not.
Type	This specifies the type of IPoA interface.
Interface Sec Type	Interface security type
Configured IP Address	IP address assigned to the IPoA interface.
Mask	Network mask to be applied to the IP Address.

Field	Description
Droute	Default Route
Gateway	Gateway IP Address.
Nat Direction	This specifies the NAT direction, which may be: inside, outside or none.
Oper Status	The actual/current state of the interface. It can be either Up or Down

Caution None.

References

- *create ipoa intf* command
- *get ipoa intf* command
- create ipoa map command
- delete ipoa map command
- get ipoa map command

3.74 delete ipoa map

Description Use this command to delete an IPoA interface association with AAL5 interface.

Command Syntax ***delete ipoa map ifname*** interface-name ***lowif*** low-interface-name

Parameters

Name	Description
ifname interface-name	The name of the IPoA interface for which the association with lower interface has to be deleted. **Type:** Mandatory **Valid values:** ipoa-0,ipoa-1 etc.,.
lowif low-interface-name	This parameter specifies the lower interface (ATM VC interface) of the IPoA interface. **Type**: Mandatory **Valid Values:** aal5-0, aal5-1 etc.,.

Mode Super-User.

Example ***$ delete ipoa map ifname*** *ipoa-0* ***lowif*** *aal5-0*

Output Verbose mode on:

```
IfName    LowIfName    Peer IP Address
-----------------------------------
ipoa-0    aal5-0       172.25.1.130

Entry Deleted
```

Verbose mode off:

```
Entry Deleted
```

Output Field description

Field	Description
IfName	The name of the IPoA interface for which the association with the lower interface has been deleted.
LowIfName	Specifies the lower (ATM VC) interface.
Peer IP Address	IP address of peer.

Caution None

References

- create ipoa map
- delete ipoa map
- get ipoa map
- get ipoa intf
- delete ipoa intf
- modify ipoa intf

3.75 delete l2tp tunnel config ifname l2t-0

Description Use this command to delete an L2TP tunnel.

Command Syntax ***delete l2tp tunnel config ifname*** interface-name

Parameters

Name	Description
ifname interface-name	Identifies the interface name for L2TP layer. **Type**: Mandatory **Valid values:** l2t-0-l2t-*..

Output Verbose mode on:

```
If Name             : l2t-0
Status              : Start        Oper Status         : Up
Local IP-address    : 178.10.10.10 Remote IP-address   : 178.10.11.10
Hello Interval      : 300          Idle Timeout        : 100
Max Retx Attempt    : 10           Max Retx Timeout    : 10
Initiator           :  local       Payload Sequencing  : always
Authentication Type : simple       Transport           : udpip
Control RWS         : 5
Shared Secret       : passwd
Local Host name     : titanium
Remote Host name    : Columbia

Entry Deleted
```

Verbose mode off:

```
Entry Deleted
```

Output Field description:

Field	Description
If-name	Identifies the interface name for L2TP layer.
Local IP-address	This field specifies the address of the local endpoint of the tunnel
Local Host name	This field specifies the address of the local endpoint of the tunnel
Remote IP-address	This field specifies the address of the remote end-point of the tunnel to which the tunnel is to be estab-lished.
Status	This field specifies the status of the of the l2tp inter-face.
Oper Status	This field specifies the Operstatus of the of the l2tp interface.

Field	Description
Remote Host name	This field specifies the hostname of the remote end-point of the tunnel to which the tunnel is to be established.
Hello Interval	Defines the interval (in sec) in which Hello packets are to be sent to the tunnel peer
Idle Timeout	Defines the period of time (in seconds) that an established tunnel with no sessions will wait before disconnecting the tunnel.
Control RWS	Defines the control channel receive window size
Max Retx Timeout	Defines the maximum retransmission timeout interval that the tunnel will wait before retransmitting a control packet that has not been acknowledged.
Initiator	This indicates whether the tunnel will be initiated locally or not.
Payload Sequencing	This object determines whether or not session payload packets will be requested to be sent with sequence numbers from tunnel peer's. The value never(2) indicates that L2TP will never initiate sequencing but will do sequencing if asked. The value always(3) indicates that L2TP will send the sequencing Required AVP during session establishment
Authentication Type	Describes how L2TP tunnel peers are to be authenticated
Transport	Defines the underlying transport media that is in use for this tunnel entry.
Shared Secret	Shared secret is used during the tunnel authentication phase of tunnel establishment if authtype is challenge
Max Retx Attempt	Defines the number of retransmissions, which the tunnel will attempt before assuming that the peer is no longer responding.

Caution This command will fail if sessions are present on tunnel.

References

- create l2tp tunnel config ifname interface-name

3.76 delete mctl iplist

Description Use this command to delete Management Control - Allowed IP addresses list

Command Syntax ***delete mctl iplist ipaddress*** ipaddress

Parameter

Name	Description
ipaddress ipaddress	IP address **Type:** Mandatory

Mode Super-User

Example ***$ delete mctl iplist ipaddress*** 172.25.12.13

Output Verbose Mode On:

```
Ip Address
--------------------------------------------------------------------------------
172.25.12.13

Entry Deleted
```

Verbose Mode Off:

```
Entry Deleted
```

Output field description

Field	Description
Ip Address	IP address

Caution None

References

- *get mctl iplist* command
- *create mctl iplist* command

3.77 delete nat rule entry

Description Use this command to delete an existing NAT rule table entry.

Command Syntax ***delete nat rule entry ruleid*** rule-id

Parameters

Name	Description
ruleid rule-id	This identifies the NAT rule which is to be deleted. **Type:** Mandatory **Valid values:** *1-4294967295*

Mode Super-User

Example ***$ delete nat rule entry ruleid*** **1**

Output Verbose Mode On:

```
Rule Id          : 1                  Flavor           : NAPT
Interface        : ALL                Protocol         : ANY
Local Addr From  : 0.0.0.0            Local Addr To    : 0.0.0.0
Dest Addr From   : 0.0.0.0            Dest Addr to     : 0.0.0.0
Global Addr From : 0.0.0.0            Global Addr To   : 255.255.255.255
Dest Port From   : 0                  Dest Port To     : 0
Local Port       : 0

Entry Deleted
```

Verbose Mode Off:

```
Entry Deleted
```

Output field description

Field	Description
Rule Id	This identifies the NAT rule, information pertaining to which is being displayed.
Flavor	This specifies the type of rule. It may be: *BASIC, FILTER, NAPT, BIMAP,REDIRECTION* (for RDR) and *PASS.*
Interface	This specifies the Interface or the outgoing device on which this Nat Rule would apply. It may be: *eth-0, veth-0 - *, eoa-0 - *, ppp-0, ppp-1…*
Protocol	This specifies the protocol type for which the rule is meant. It may be: *Any, TCP, UDP, ICMP* or IANA specified protocol between 0 to 255.
Local Addr From	This is the starting address when a range of private IP addresses are mapped
Local Addr To	This is the last IP address of the range of private IP addresses mapped by this rule.
Dest Addr From	This specifies the start of the range of destination IP address of the packet to be matched.

Field	Description
Dest Addr To	This specifies the end of the range of destination IP address to be matched
Dest Port From	This specifies the start of the range of the destination port number to be matched.
Dest Port To	This specifies the end of the range of destination port numbers to be matched.
Global Addr From	Specifies the first globally unique IP address of the range of IP addresses being mapped.
Global Addr To	Specifies the last globally unique IP address of the range of IP addresses used in the mapping.
Local Port	This is the translated port number to be used .

Caution None.

References

- *create nat rule entry* command
- *get nat rule entry* command
- *nat global info* related commands
- *nat rule statistics* related commands
- *nat rule status* related commands.

3.78 delete pfraw rule entry

Description Use this command to delete a rule.

Command Syntax ***delete pfraw rule entry ruleid*** rule-id

Parameters

Name	Description
ruleid rule-id	This identifies the rule index of the rule which has to be deleted. **Type:** Mandatory **Valid values:** *0 - 65535* Only existing rule ids accepted as input.

Mode Super-User

Example ***$ delete pfraw rule entry ruleid 2***

Output Verbose Mode On:

```
Rule id : 2                    Rule status : Enable
Interface : eth-0              In interface : All
Direction : Out                SSB          : 0x34
SSB Mask : 0xff                Priority     : 1
Action   : Accept              Logging      : Match
Out interface : ALL

Entry Deleted
```

Verbose Mode Off:

```
Entry Deleted
```

Output field description

Field	Description
Rule id	This identifies the rule index of the rule.
Rule Status	This specifies whether this rule is enabled or disabled.
Interface	This specifies the interface name for a rule.
In Interface	In case of a rule for an outgoing interface, this specifies the incoming interface. Only packets, which are received on the inifname, and which are going out via the ifname, are matched against this rule..
Direction	This specifies the filtering direction to which this rule is applied.
SSB	Service Specification Byte value to be set in the packet.
SSB Mask	Service Specification Byte value mask
Priority	Priority value to be attached to the packet

Field	Description
Action	This specifies the action taken when a packet matches this rule.
Logging	This specifies the log option of this rule.
Out interface	This specifies the outgoing interface. Only packets which are received on the outifname and which are coming in via the ifname will be matched against this rule.

Caution pfraw rule cannot be deleted until all the subrule entries created on this rule are deleted.

References

- *delete pfraw subrule* command

3.79 delete pfraw subrule entry

Description Use this command to delete a specific sub-rule of an already existing rule.

Command Syntax ***delete pfraw subrule entry ruleid*** rule-id ***subruleid*** sub-rule-id

Parameters

Name	Description
ruleid rule-id	This identifies the rule index of the rule for which the sub-rule has to be deleted. **Type:** Mandatory **Valid values:** *0 - 65535* Only existing rule ids accepted as input.
subruleid sub-rule-id	This specifies the sub-rule index of the sub-rule which has to be deleted. **Type:** Mandatory **Valid values:** *0 - 254*

Mode Super-User

Example ***$ delete pfraw subrule entry ruleid 2 subruleid 1***

Output Verbose Mode On:

```
Sub Rule id     : 1       Rule id     : 2
Sub Rule status : Enable  Offset from : Linkh
Offset          : 6
Comp operation  : Range
Low value       : 0x00000000ff000000
High value      : 0x00000000ffcd0000
Mask            : 0x00000000ffff0000

Entry Deleted
```

Verbose Mode Off:

```
Entry Deleted
```

Output field description

Name	Description
Sub Rule id	This identifies the sub-rule index of the sub-rule.
Rule id	This specifies the rule index of the rule of which this is the subrule
Sub Rule status	This specifies whether this subrule is enabled or disabled.
Offset from	This specifies the start position in the packet for an offset. The start position can be the beginning of the header or data portions of various protocols.
Offset	This specifies the offset with in the header or data part of the packet.

Name	Description
Comp Operation	This specifies the type of comparison that is done on the extracted data and the comparison value(s)
Low Value	This is hexadecimal pattern to be used for comparison when comparison type is Range.
High Value	This is hexadecimal pattern to be used for comparison when comparison type is Range.
Value	This is hexadecimal pattern to be used for comparison when comparison type is Relational.
Mask	This is hexadecimal pattern which specifies the mask

Caution None.

References None.

3.80 delete ppe pconf

Description Use this command to delete a PPPoE AC-name to Service-name entry.

Command Syntax ***delete ppe pconf acname*** AC-name ***srvname*** service-name

Parameters

Name	Description
acname AC-name	This specifies the Access Concentrator name. **Type:** Mandatory **Valid values:** String of up to 63 chars. ('A'- 'Z', 'a'- 'z', '0'-'9','-','_')
srvname service-name	This specifies the service name **Type:** Optional **Valid values:** String of up to 63 chars. ('A'- 'Z', 'a'- 'z', '0'-'9','-','_')

Mode Super-User

Example ***$ delete ppe pconf acname*** **AC1** ***srvname*** **Srv1**

Output Verbose Mode On:

```
Ac Name        : AC1
Service Name   : Srv1

Entry Deleted
```

Verbose Mode Off:

```
Entry Deleted
```

Output field description

Field	Description
ACName	This specifies the Access Concentrator name
ServiceName	This specifies the service name

Caution None.

References

- *create ppe pconf* command
- *get ppe pconf* command
- *ppe cfg* command
- *get ppe stats global* command
- *get ppe stats session* command

3.81 delete ppp intf

Description Use this command to delete the specified ppp interface.

Command Syntax ***delete ppp intf ifname*** interface-name

Parameters

Name	Description
ifname interface-name	This specifies the Interface for PPP Links, which is to deleted. **Type:** Mandatory **Valid values:** *ppp-0, ppp-1…*

Mode Super-User

Example ***$ delete ppp intf ifname*** **ppp-0**

Output Verbose Mode On:

```
If-Name               : ppp-0          L2TP Call type        : inlac
Interface Sec Type    : Public         Phy Interface         : aal5-0
Configured IP Address : 0.0.0.0        NAT Direction         : OUT
Init MRU              : 1500           Magic                 : False
Encapsulation         : PPPOA          Service Name          : -
UseDhcp               : False          UseDns                : False
DRoute                : False          Status                : Start
Gateway IP Address    : 202.1.1.2    Associated Num If-Name : eth-0
Use Gateway           : remote

Entry Deleted
```

Verbose Mode Off:

```
Entry Deleted
```

Output field description

Field	Description
If-Name	This specifies the PPP interface for the PPP Links: It may be: *ppp-0, ppp-1…*
L2TP Call Type	This field specifies the l2tp call type.
Interface Sec Type	Interface security type.
Phy Interface	This specifies Name of the lower interface on which PPP is running. It may be: *aal5-0, aal5-1…*
Configured IP Address	This specifies the IP Address for the PPP Link.
NAT Direction	This variable specifies whether this interface's address is inside or outside. It may be: *inside, outside, none*
Init MRU	The initial Maximum Receive Unit (MRU) that the local PPP entity will advertise to the remote entity

Field	Description
Magic	This specifies whether the local node will attempt to perform Magic Number negotiation with the remote node. It may be: *True, False*
Encapsulation	This specifies the lower layer protocol used below this PPP Link. It may be: *PPPOA, PPPOE*
Service Name	This specifies the service name used for PPPoE. It is generally the name of the ISP.
UseDhcp	This specifies whether DHCP is to be used for address negotiation. It may be either True or False
UseDns	This specifies whether DNS server addresses are to be obtained using IPCP or not.
Droute	Default Route
Status	This shows whether PPP session on this interface is active. It may be: *Start, Stop, StartOnData.*
Gateway IP Address	This specifies the IP Address of the Gateway.
Associated Num If-Name	This specifies the interface name of the associated numbered interface. A "-" indicates that this ppp interface is not associated with any numbered interface.
Use Gateway	This specifies whether local or remote gateway is to be used.

Caution None.

References

- *get ppp intf* command
- *create ppp intf* command
- *modify ppp intf* command
- *ppp lstatus* related commands
- *ppp security* related commands.

3.82 delete ppp security

Description Use this command to delete a PPP security secrets entry.

Command Syntax ***delete ppp security ifname*** interface-name

Parameters

Name	Description
ifname interface-name	This specifies the PPP interface for which the security secrets entry is to be deleted. **Type:** Mandatory **Valid values:** *ppp-0 - *, default.*

Mode Super-User

Example ***$ delete ppp security ifname*** **ppp-0**

Output Verbose Mode On:

```
IfName    : ppp-0       Protocol : PAP
Login     : abc
```

Verbose Mode Off:

```
Entry Deleted
```

Output field description

Field	Description
IfName	This specifies the PPP interface for which the security entry has been deleted. It may be: *ppp-0 - * or default.* The *default* entry gets used in case there is no specific entry for that interface.
Protocol	This is the protocol used for authentication It may be: *PAP, CHAP*
Login	This is the login name

Caution Do not delete ppp security when ppp interface is using it.

References

- *create ppp security* command
- *get ppp security* command
- *modify ppp security* command
- *ppp lstatus* related commands
- *ppp intf* related commands

3.83 delete radius acctserv config

Description Use this command to delete Radius Accounting Server Configuration

Command Syntax ***delete radius acctserv config index*** index

Parameter

Name	Description
index index	A number uniquely identifying each RADIUS Accounting server with which this client communicates **Type:** Mandatory **Valid values:** 1 - 2147483647

Mode Super-User

Example ***$ delete radius acctserv config index*** 1

Output Verbose Mode On:

```
Server Index       : 1          IP address      : 192.166.56.67
Port               : 1700       Retries         : 5
Start timeout(sec) : 60         On timeout(sec) : 60
Current State      : Start

Entry Deleted
```

Verbose Mode Off:

```
Entry Deleted
```

Output field description

Field	Description
Server Index	A number uniquely identifying each RADIUS Accounting server with which this client communicates.
IP address	The IP address of the RADIUS server referred to in this table entry.
Port	The server port to which the client sends accounting requests.
Retries	The number of times the request packet shall be retransmitted to the server on getting timed out.
Start timeout(sec)	The time in seconds for which the client needs to wait before retransmitting the Accounting START request packet to the server.
On timeout(sec)	The time in seconds for which the client needs to wait before retransmitting the Accounting ON request packet to the server.
Current State	The current state of the accounting server.

Caution None

References

- *get radius acctserv config* command
- *create radius acctserv config* command
- *modify radius acctserv config* command

3.84 delete radius authserv config

Description Use this command to delete Radius Authentication Server Configuration

Command Syntax ***delete radius authserv config index*** index

Parameter

Name	Description
index index	A number uniquely identifying each RADIUS Authentication server with which this client communicates **Type:** Mandatory **Valid values:** 1 - 2147483647

Mode Super-User

Example ***$ delete radius authserv config index*** 1

Output Verbose Mode On:

```
Server Index : 1
IP address   : 192.166.56.67    Port                          : 1800
Retries      : 5                Retransmission timeout(sec) : 60

Entry Deleted
```

Verbose Mode Off:

```
Entry Deleted
```

Output field description

Field	Description
Server Index	A number uniquely identifying each RADIUS Authentication server with which this client communicates.
IP address	The IP address of the RADIUS server referred to in this table entry..
Port	The server port to which the client sends authentication requests.
Retries	The number of times the request packet shall be transmitted to the server on getting timed out.
Retransmission timeout(sec)	The time, in seconds, for which the client needs to wait before retransmitting the request packet to the server.

Caution None

References

- *get radius authserv config* command
- *create radius authserv config* command
- *modify radius authserv config* command

3.85 delete rip intf

Description Use this command to stop RIP protocol on the specified IP Interface.

Command Syntax ***delete rip intf ifname*** interface-name

Parameters

Name	Description
ifname interface-name	Specifies the IP Interface name on which RIP is to be stopped. **Type:** Mandatory **Valid values:** eth-0, veth-0 - *, ppp-0 - *, eoa-0 - *, ipoa-0-*, usb-0

Mode Super-User

Example ***delete rip intf ifname ppp-0***

Output Verbose Mode On:

```
IP Interface Name    : ppp-0      RIP Interface Metric : 1
RIP Send Mode        : rip1       RIP Receive Mode     : rip1
RIP Send Def Route   : Enable     RIP Recv Def Route   : Disable
RIP packet auth      : None

Entry Deleted
```

Verbose Mode Off:

```
Entry Deleted
```

Output field description

Field	Description
IP Interface Name	This tells the IP Interface name on which RIP is to be stopped.
RIP Interface Metric	This tells the metric value attached to the interface. The metric is used by RIP in deciding which among alternate routes is the most optimal.
RIP Send Mode	This tells the packet format used for sending RIP updates and requests
RIP Receive Mode	This tells the packet format accepted while receiving RIP updates and requests and responses
RIP Send Def Route	This tells whether default route is to be included in the updates sent on the interface, or not.
RIP Recv Def Route	This tells whether default route is to be processed in the updates received on the interface or not.
RIP packet auth	This tells whether RIP authentication is enabled or not

Caution None.

References

- *modify rip global* command.

3.86 delete snmp comm

Description Use this command to delete the specified community from the community table.

Command Syntax ***delete snmp comm community*** comm-name

Parameters

Name	Description
community comm-name	This specifies the Community name which is to be deleted. **Type:** Mandatory **Valid values:** String of Max. 50 Characters('A'- 'Z', 'a'-'z', '0'-'9','-','_')

Mode Super-User

Example ***$ delete snmp comm community*** **public**

Output Verbose Mode On:

```
Access          Community
------------------------
RO              public

Entry Deleted
```

Verbose Mode Off:

```
Entry Deleted
```

Output field description

Field	Description
Community	This specifies the Community name
Access	This specifies the access permissions given to managers with this community name. It may be: *RO* (Read Only), *RW* (Read-Write)

Caution A community cannot be deleted if there are some SNMP hosts created for the community.

References

- *get snmp comm* command
- *create snmp comm* command
- *snmp trap* related commands
- *snmp host* related commands
- *snmp stats* related commands

3.87 delete snmp host

Description Use this command to delete the specified host from the SNMP host table.

Command Syntax ***delete snmp host {ip ip-addr}|hdlc|ilmi community comm-name***

Parameters

Name	Description
{ip ip-addr}|hdlc|ilmi	This specifies the IP address of the manager (snmp over udp interface) that has access permissions for the modem. A value of 'hdlc' specifies SNMP over HDLC interface. A value of 'ilmi' specifies SNMP over ILMI interface. **Type:** Mandatory **Valid values:** Any valid class A/B/C IP address, hdlc, ilmi
community comm-name	This specifies the Community name. This together with the ip determines which entry is to be deleted. **Type:** Mandatory **Valid values:** String of Max. 50 Characters ('A'- 'Z', 'a'-'z', '0'-'9','-','_')

Mode Super-User

Example ***$ delete snmp host community*** **public** ***ip*** **192.168.1.3**

Output Verbose Mode On:

```
Host Address              Community
-----------------------------------
192.168.1.3               public

Entry Deleted
```

Verbose Mode Off:

```
Entry Deleted
```

Output field description

Field	Description
Host Address	This specifies the IP address of the manager (snmp over udp interface) that has access permissions for the modem. A value of 'hdlc' specifies SNMP over HDLC interface. A value of 'ilmi' specifies SNMP over ILMI interface.
Community	This specifies the Community name.

Caution None.

References

- *get snmp host* command
- *create snmp host* command

- *snmp trap related* commands
- *snmp comm* related commands
- *snmp stats* related commands

3.88 delete sntp servaddr

Description Use this command to delete the SNTP server address.

Command Syntax ***delete sntp servaddr*** <ip-address|***dname*** domain-name>

Parameters

Name	Description
<ip-address>|dname <domain-name>	This parameter specifies the IP address or fully qualified domain name of SNTP server address to be deleted.Type: MandatoryValid values: Valid IP address or fully qualified domain name.

Mode Super-User

Example

```
$ delete sntp servaddr 192.168.1.1
```

Output Verbose Mode On:

```
Server Addr : 192.168.1.1 Status : Active
Domain Name : abc.com

Entry Deleted
```

Verbose Mode Off:

```
Entry Deleted
```

Output field description

Field	Description
Server Addr	IP address of the SNTP server
Status	Operational Status of the SNTP server address entry.
Domain Name	The fully qualified domain name of the SNTP server.

Caution None.

References

- *create sntp servaddr* command
- *get sntp servaddr* command
- *modify sntp cfg* command
- *get sntp cfg* command
- *get sntp stats* command
- *reset sntp stats* command

3.89 delete tcp conn

Description Use this command to forcibly delete a TCP connection entry.

Command Syntax ***delete tcp conn lclip*** local-ip-address ***lclport*** local-port ***rmtip*** remote-ip-address ***rmtport*** remote-port

Parameters

Name	Description
lclip local-ip-address	The local IP address for the TCP connection, which is to be deleted. **Type:** Mandatory **Valid values:** Any valid class A/B/C IP address
lclport local-port	The local port number for the TCP connection to be deleted. **Type:** Mandatory **Valid values:** *0-65535*
rmtip remote-ip-address	The remote IP address for the TCP connection which is to be deleted **Type:** Mandatory **Valid values:** Any valid class A/B/C IP address
rmtport remote-port	The remote port number for the TCP connection to be deleted. **Type:** Mandatory **Valid values:** *0-65535*

Mode Super-User

Example ***$ delete tcp conn lclip*** **192.168.1.11** ***lclport*** **80** ***rmtip*** **202.34.4.5** ***rmtport*** **80**

Output Verbose Mode On:

```
Local Addr       Local Port       Remote Addr        Remote Port
-------------------------------------------------------------------------
192.168.1.11        80            202.34.4.5           80

Entry Deleted
```

Verbose Mode Off:

```
Entry Deleted
```

Output field description

Field	Description
Local Addr	The local IP address for the TCP connection.
Local Port	The local port number for the TCP connection.
Remote Addr	The remote IP address for the TCP connection
Remote Port	The remote port number for the TCP connection.

Caution None.

References

- *get tcp conn* command
- *get tcp stats* command

3.90 delete usb intf

Description Use this command to delete a USB interface.

Command Syntax ***delete usb intf ifname*** interface-name

Parameters

Name	Description
ifname interface-name	This parameter specifies the USB interface, which has to be deleted. **Type:** Mandatory. **Valid values:** *usb-0*.

Mode Super-User.

Example ***$ delete usb intf ifname usb-0***

Output Verbose Mode On

```
IfName   If SecType   Ip Address     Mask           Nat Dir      Oper
------------------------------------------------------------------------------
usb-0    Public       192.168.1.1    255.255.255.0    Inside      Down

Set Done
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
IfName	The name of the interface, which has been created.
Ip Address	IP address assigned to the usb-0 interface.
Mask	Network mask to be applied to the IP Address.
Nat Dir	This specifies the NAT direction, which may be: *inside, outside* or *none*.
Oper	The actual/current state of the interface. It can be either *Up* or *Down*
If SecType	Interface security type.

Caution None.

References

- *create usb intf* command
- *get usb intf* command
- *modify usb intf* command
- *get usb stats* command

3.91 delete user

Description Use this command to delete a user login.

Command Syntax ***delete user name*** user-name

Parameters

Name	Description
Name user-name	This specifies the User Name to be deleted. **Type:** Mandatory **Valid values:** String of up to 128 characters ('A'- 'Z', 'a'-'z', '0'-'9','-','_')

Mode Super-User

Example ***$ delete user name user1***

Output Verbose Mode On:

```
User Name : user1
Privilege : user

Entry Deleted
```

Verbose Mode Off:

```
Entry Deleted
```

Output field description

Field	Description
UserName	This represents the user login which is being deleted.
Privilege	This represents the privilege level associated with the user being deleted. It may be: *user, intermediate, root.* In CLI, intermediate privilege has the same previliges as the user. In HTTP, the intermediate privilege has ALL the privileges as the "user" except that he can also modify the ATM VPI and VCI values and the PPP username and password.

Caution If there is only one user login with root privileges then that entry cannot be deleted.

References

- *create user* command
- *get user* command
- *passwd* command

3.92 delete wlan intf

Description Use this command to delete 802.11 Interface

Command Syntax ***delete wlan intf ifname*** ifname

Parameter

Name	Description
ifname ifname	Name of the wireless interface. **Valid Values :** wlan-0 - wlan-* **Type:** Mandatory

Mode Super-User

Example ***$ delete wlan intf ifname*** wlan-0

Output Verbose Mode On:

```
Interface                : wlan-0
Encryption Type          : 64bit          Default Tx Key Id      : 1
Default Channel          : 1              Rts Threshold          : 1
Fragmentation Threshold  : 1              Service set identifier : Viking
Relay packets between BSS : enable        IP address             : 192.168.3.4
Mask                     : 255.255.255.0  Nat Dir                : inside
Use DHCP                 : false          Security Type          : public
Microwave robustness     : enable
Maximum Transmission Unit : 1500

Entry Deleted
```

Verbose Mode Off:

```
Entry Deleted
```

Output field description

Field	Description
Interface	Name of the wireless interface.
Encryption Type	WEP Encryption Type.Disabled for no encryption.64bit for 40bit encryption.128bit for 128bit encryption.
Default Tx Key Id	Combined with WepEncryption attribute, determines which encryption key (between 0-3) to use by default. The actual key is picked up from the 802.11 WEP Keys MO.
Default Channel	Default Channel
Rts Threshold	Maximum packet size to use RTS/CTS With
Fragmentation Threshold	Minimum packet size to use fragmentation with
Service set identifier	Service set identifier of upto 32 characters which each 802.11b station uses.
Relay packets between BSS	Relay packets between BSS (AP)

Field	Description
IP address	This specifies the IP address configured for the interface.
Mask	This specifies the network mask configured for the interface.
Nat Dir	This variable specifies whether this interface's address is inside or outside. This is used by NAT.
Use DHCP	DHCPclient will do/not do link address negotiation locally/remotely depending on the UseDHCP values of local/remote or false.
Security Type	This specifies the interface type from firewall point of view.
Microwave robustness	Enable/Disable Microwave robustness
Maximum Transmission Unit	This specifies the maximum transmission unit for interface.

Cautions None.

References

- *get wlan intf* command
- *create wlan intf* command
- *modify wlan intf* command

3.93 delete wlan key

Description Use this command to delete 802.11 Wired Equivalent Privacy Keys

Command Syntax ***delete wlan key ifname*** ifname ***encrtype*** 64bit | 128bit ***keyid*** keyid

Parameter

Name	Description
ifname ifname	Name of the wireless interface. **Valid Values :** wlan-0 - wlan-* **Type:** Mandatory
encrtype 64bit | 128bit	Encryption type with which this key is to be used(64 bit or 128 bit). **Type:** Mandatory
keyid keyid	Key index. Used to identify which key to use as the default key on the interface. **Type:** Mandatory **Valid values:** 0 - 3

Mode Super-User

Example ***$ delete wlan key ifname*** wlan-0 ***encrtype*** 64bit ***keyid*** 1

Output Verbose Mode On:

```
Interface       : wlan-0
Encryption Type : 64bit
Key Id          : 1

Entry Deleted
```

Verbose Mode Off:

```
Entry Deleted
```

Output field description

Field	Description
Interface	Name of the wireless interface.
Encryption Type	Encryption type with which this key is to be used (64 bit or 128 bit).
Key Id	Key index. Used to identify which key to use as the default key on the interface.

Caution None.

References

- *get wlan key* command
- *create wlan key* command
- *modify wlan key* command

3.94 delete 8021x intf

Description Use this command to delete Dot1x Interface Configuration

Command Syntax ***delete 8021x intf ifname*** ifname

Parameter

Name	Description
ifname ifname	Interface index **Type:** Mandatory **Valid values:** 1 - 4294967295

Mode Super-User

Example ***$ delete 8021x intf ifname*** wan-0

Output Verbose Mode On:

```
If Index                : wan-0
802.1x status           : enable      Admin dir            : both
Port Control            : Auto        Association          : many_to_one
Quiet Period(secs)      : 60          Tx Period(secs)      : 30
Supplicant Timeout(secs) : 30         Server Timeout(secs) : 30
Max Request             : 2           ReAuth Enabled       : true
ReAuth Period(secs)     : 3600        ReAuth Max requests  : 2
Key Tx Enabled          : true        Dynamic Supp Allowed : true
ReKey timeout(secs)     : 600

Entry Deleted
```

Verbose Mode Off:

```
Entry Deleted
```

Output field description

Field	Description
If Index	Interface index
802.1x status	Feature 802.1x status on this Interface
Admin dir	This specifies the controlled directions for the port. If set to **both**, then the port needs to be authenticated for traffic to flow either to or from it. If set to **in**, then traffic going out via this port does not require it to be authenticated.
Port Control	This allows administrative control over the Port's authorization status. If set to ForceUnAuth, the port is never authorized. If set to ForceAuth, the port is autorized unconditionally. If set to Auto, the port's authorization status is determined by outcome of the authentication exchanges between Supplicant PAE, Authenticator PAE, and the Authentication Server.
Association	This specifies whether there will be one supplicant or many supplicants per port .

Field	Description
Quiet Period(secs)	The Authenticator state machine uses a timer to define periods of time during which it will not attempt to acquire a Supplicant. The initial value of this timer is quietPeriod.
Tx Period(secs)	The Authenticator state machine uses a timer to determine when an EAPOL PDU is to be transmitted. The initial value of this timer is txPeriod.
Supplicant Timeout(secs)	The initialization value used for timing out the supplicant. Its default value is 30 s; however, if the type of challenge involved in the current exchange demands a different value of timeout (for example, if the challenge requires an action on the part of the user), then the timeout value is adjusted accordingly.
Server Timeout(secs)	The initialization value used for timing out the Authentication Server. Its default value is 30 s; however, the timeout value may be adjusted to take account of the communication medium being used to communicate with the Authentication Sever.
Max Request	The maximum number of times that the state machine will retransmit an EAP Request packet to the Supplicant before it times out the authentication session.
ReAuth Enabled	A constant that defines whether regular reauthentication will take place on this Port.
ReAuth Period(secs)	A constant that defines a nonzero number of seconds between periodic reauthentication of the Supplicant
ReAuth Max requests	The number of reauthentication attempts that are permitted before the Port becomes Unauthorized.
Key Tx Enabled	Controls transmission of key information after the port has been authorized.
Dynamic Supp Allowed	This controls whether only management-created Supplicants or both management-created and Dynamically-learnt Supplicants are allowed.
ReKey timeout(secs)	Timer period after which keys will be transmitted to all the supplicants in the port.

Caution None.

References

- *get 8021x intf* command
- *create 8021x intf* command
- *modify 8021x intf* command

3.95 delete 8021x supp

Description This command is used to delete a 8021x supp entry.

Command Syntax ***delete 8021x supp ifname interface-name macaddr mac-address***

Parameters

Name	Description
ifname <ifname>	This specifies the Interface Index of a port. **Type:** Mandatory **Valid values:**
macaddr <macaddr>	This specifies the MAC address of a supplicant for which individual authenticator state **Type : Mandatory** **Valid values:** A valid mac address

Output Verbose Mode On

```
If Index                : wlan-0          Mac address              :  0x0085a00004
Virtual port Number     : 3000            Owner                    : 802.1x
Protocol Version        : 2.0.1.1         Port capability          : Auth
Re- authenticate        : no              Auth Pae State           : forceauth
Auth backend state      : request         Auth Key Transmission    :  disable
Auth Admin dir          : both            Auth Oper dir            : both
Auth Control status     : authorized      Auth control value       : forceauth
Auth Q period(secs)     : 1000            Auth Tx Period(secs)     : 200
Auth Supp Timeout(sec)  : 30              Auth Server timeout(secs):30
Auth Max req            : 2               Auth Re-auth max         : 2
Auth reauth Period(secs): 3600            Auth reauth enabled      : true

Entry deleted.
```

Verbose Mode Off

```
Entry deleted.
```

Output field description

Field	Description
If Index	This specifies the Interface Index of a port.
Mac address	This specifies the MAC aaddress of a supplicant for which individual authenticator state machines are running.
Virtual port Number	This specifies the virtual Port Number to be used for an authenticator PAE associated with a Supplicant.
Owner	This specifies of the owner of the entry.
Protocol Version	This specifies the EAPOL Protocol Version associated with this supplicant

Field	Description
Port capability	This specifies the PAE functionality (authenticator or supplicant) supported by this port.
Re- authenticate	This specifies the Re-authentication control for this port (it will always be returned false while reading)
Auth Pae State	This specifies the Current State of Authenticator PAE state machine.
Auth backend state	This specifies the Current State of Backend Authentication state machine
Auth Key Transmission	This specifies the Key Transmission enable/ disable control parameter.
Auth Admin dir	This specifies the Administrative Controlled Direction Parameter.
Auth Oper dir	This specifies the Operational Controlled Direction Parameter.
Auth Control status	This specifies the Supplicant's Current Authentication Status.
Auth control value	This specifies the Current value of AuthControl Parameter.
Auth Q period(secs)	This specifies the Value in seconds of QuietPeriod constant used by authenticator PAE state machine
Auth Tx Period(secs)	This specifies the Value in seconds of TxPeriod constant used by authenticator PAE state machine.
Auth Supp Timeout(sec)	This specifies the Value in seconds of SuppTimeout constant used by Backend authenticator state machine.
Auth Server timeout(secs)	This specifies the Value in seconds of ServerTimeout constant used by Backend authenticator state machine
Auth Max req	This specifies the Value of MaxReq constant used by Backend authenticator state machine.
Auth Re-auth max	This specifies the Value of ReAuthMax constant used by Authenticator PAE state machine.

Field	Description
Auth reauth Period(secs)	This specifies the Value in seconds of ReauthPeriod constant used by Re-authenticate state machine.
Auth reauth enabled	This specifies the Re-authentication enable/ disable control parameter.

Caution None

References

- *create 8021x supp* command
- *get 8021x supp* command
- *modify 8021x supp* command

3.96 do getserialize

Description Use this command to view the Viking unit's MAC address and serial number, and to view the serial number assigned to the USB host PC, if any.

Command Syntax ***do getserialize***

Parameters None.

Example ***$do getserialize***

Output Verbose Mode On/Off:

```
Serial Number: 123456789abcdx
Ethernet Mac Address: 00-85-A0-01-01-00
Usb Host Mac Address: 00-85-A0-01-01-04
```

Output field description

Name	Description
Serial Number	The serial number assigned to the Viking unit
Ethernet MAC Address	The MAC address assigned to all LAN interfaces (i.e., eth-0 and usb-0) on the Viking unit
Usb Host Mac Addrses	The MAC address assigned to the USB host PC, if any.

Caution None.

References

- *do serialize rule entry* command

3.97 do getver

Description Use this command to get details about the current software and hardware versions.

Command Syntax `do getver`

Parameters None

Example `$ do getver`

Output Verbose Mode On/Off:

```
SW Version: VIK-1.37.020618j
FW Version: T93.3.19
```

Output field description

Field	Description
SW Version	Current Software version
HW Version	Current hardware version

Caution None.

References None.

3.98 do serialize

Command Syntax ***do serialize*** **<**Ethernet-MAC-Address**>** [Serial-Number] [USB-MAC Address]

Parameters

Name	Description
Ethernet-Mac-Address	Specifies the MAC address to assign to the Ethernet and USB ports on the Viking unit. **Type:** Mandatory **Valid values:** *6 hexadecimal pairs, with or without dashes*
Serial-Number	Specifies the serial number to assign to the Viking unit. **Type:** Optional **Valid values:** any alphanumeric characters, up to 24
USB-MAC-Address	Specifies the MAC address to assign to the USB host PC (*not* the USB interface on the Viking unit) **Type:** Optional **Valid values:** 6 hexadecimal pairs, with or without dashes

Example ***$do serialize a1-00-0b-00-00-26 8a723v842d79477499797adf a1-00-b0-00-78-26***

Output Verbose Mode On/Off:

```
REBOOT REQ: Awaiting Flash Access To Finish

Serialization done. Rebooting the board...
```

(system reboots)

Output field description None.

Caution None.

References

- *do getserialize* command
- *get interface stats* command

3.99 download

Description Use this command to download a configuration or binary file from another host on to the modem.

Command Syntax ***download fname*** file-name ***ip*** ip-address

Parameters

Name	Description
fname file-name	This specifies the name of the binary or configuration file to be downloaded. The filename contains the complete path on the host. The filename extension must be either *.cfg* or *.bin*. A *.cfg* file can contain only valid CLI commands, with the last line being the string “end” (without the quotes). A *.bin* file must be a valid image file for the modem. **Type:** Mandatory **Valid values:** String of up to 128 characters (all characters except ‘;’, ‘ ‘, ‘?’)
ip ip-address	This specifies the address of the host from which the file is to be downloaded. **Type:** Mandatory **Valid values:** Any valid class A/B/C IP address

Mode Super-User.

Example ***$ download fname*** myconfig.cfg ***ip*** 192.168.1.10

Output Verbose Mode On:

```
Downloading The Code File. . .

Download Completed
```

Verbose Mode Off:

```
Downloading The Code File. . .
Download Completed
```

Output field description None.

Caution If the *autoupdate* flag is set to *True*, the downloaded file is applied immediately. In case of a *.cfg* file the commands in it are executed; in case of a *.bin* file the code in it is programmed into the flash (removing the earlier code) and the modem reboots with the new code. Ensure that the tftp server is running on the specified host.

References

- *modify autoupdate* command
- *set autoupdate* command
- *remove* command.
- *list* command.
- *apply* command.

3.100 get alg port

Description Use this command to get one or all alg port entries, which satisfy a particular filtering criteria. The port number and protocol together uniquely identify an entry.

Command Syntax ***get alg port [portno*** *port-no]*

Parameters

Name	Description
portno port-no	The Port number for which ALG entries are to be retrieved.The port here is the destination port of the untranslated packet If none is specified then ALG entries for all ports are displayed. **Type**: Optional **Valid values** *: 0 - 65535*

Mode Super-User, User

Example ***$ get alg port***

Output

```
Port Num                Protocol                ALG Type
-------------------------------------------------------------
21                      Tcp                     FTP
```

Output field description

Field	Description
Port Num	The Port number on which the ALG is running.The port here is the destination port of the untranslated packet.
Protocol	The protocol for which this ALG is running.
Port Type	This specifies the ALG with has to be applied to this port. It may be: FTP, SNMP, REAL AUDIO, REMOTE CMD, L2TP,MIRC, CU-SEEME,H323_Q931,H323_RAS,PPTP,RTSP, TIM-BUKTU, LDAP, SGICOMPCORE, MSN MSGR, IKE, ESP

Caution None.

References

- *delete alg port* command
- *create alg port* command
- *get alg type* command

3.101 get alg type

Description Use this command to display all the ALGs that are supported in the system.

Command Syntax ***get alg type***

Parameters None

Mode Super-User, User

Example ***$ get alg type***

Output

```
Alg Type
--------
FTP
SNMP
REAL AUDIO
REMOTE CMD
L2TP
MIRC
CUSEEME
H323_Q931
H323_RAS
PPTP
RTSP
TIMBUKTU
LDAP
T120
SGICompCore
MSN MSGR
IKE
ESP
```

Output field description

Field	Description
Alg Type	This is an ALG Type supported by the system. It may be:FTP, SNMP, REAL AUDIO, REMOTE CMD,L2TP,MIRC,CU-SEEME,H323_Q931,H323_RAS,PPTP,RTSP,TIM-BUKTU, LDAP, T120, SGICompCore, MSN MSGR, IKE, ESP.

Caution None.

References

- *get alg port* command

3.102 get arp

Description Use this command to display either the full ARP table or a single entry.

Command Syntax ***get arp [ip*** *ip-address]*

Parameters

Name	Description
ip ip-address	IP Address corresponding to the media-dependent `physical' address for which information is to be displayed. If none is specified then information for all valid IPs in ARP Table is displayed. **Type**: Optional **Valid Values** : Any valid class A/B/C IP address

Mode Super-User, User

Example ***$ get arp***

Output

```
If Name    Type         Mac Address              Ip Address
-------------------------------------------------------------
eth-0     Static       00:00:00:00:00:00         127.0.0.1
```

Output field description

Field	Description
If-Name	This specifies the physical Interface for the media. It may be :eth-0 or veth-0 to veth-4
Type	This defines the type of mapping in use.The value Invalid has the effect that this entry is not used. It may be: Static, Dynamic, Other
Mac Address	The media-dependent `physical' address
IP Address	IP Address corresponding to the media-dependent `physical' address

Caution None.

References

- *atm trfdesc* related commands
- *delete arp* command
- *create arp* command
- *ip stats* related commands
- *ip route* related commands
- *ip address* related commands
- *ip cfg related* commands.

3.103 get atm 1483 stats

Description Use this command to retrieve Global Statistics related to RFC1483 encapsulation.

Command Syntax ***get atm 1483 stats***

Parameters None

Mode Super-User, User

Example ***$ get atm 1483 stats***

Output

```
Invalid SAP count                : 2          Invalid Ctl count      : 0
Invalid OUI count                : 0          Invalid PID count      : 3
Unregistered Mea5 Protocol count  : 0
```

Output field description

Field	Description
Invalid SAP	The number of frames received with invalid SAP in LLC header.
Invalid Ctl	The number of frames received with invalid Ctl in LLC header.
Invalid OUI	The number of frames received with invalid OUI in SNAP header.
Invalid PID	The number of frames received with invalid PID in SNAP header.
Unregistered Mea5 Protocol	The number of valid frames received but dropped since no upper layer was configured for the encapsulation type

Caution None.

References Other atm commands.

3.104 get atm aal5 stats

Description Use this command to get AAL5 VC statistics.

Command Syntax ***get atm aal5 stats [ifname interface-name]***

Parameters

Name	Description
ifname interface-name	This parameter specifies the interface for which information is desired. In case the field is not specified, then the information for all valid aal5 interfaces should be displayed. **Type**: Optional **Valid values :** *aal5-0 - **

Mode Super-User, User

Example ***$ get atm aal5 stats ifname aal5-0***

Output

```
LowIf                  : atm-0     VPI                     : 0
VCI                    : 1         VC IfName               : aal5-0
Tx Frames count        : 100        Rx Frames count         : 85
Tx Bytes count         : 1535       Rx Bytes count          : 1200
Large Pkts Rx count    : 4          CIS Rx count            : 2
CRC Errors count       : 0          Invalid CPI SDU count   : 0
Invalid PAD count      : 0          Invalid Length SDU count: 0
RAS Timer Expired count : 1
```

Output field description

Field	Description
LowIf	This specifies the ATM port name: It can be : atm-0
VPI	This is the Virtual Port Identifier
VCI	This is the Virtual Circuit Identifier
VC IfName	The name of the aal5 (aal5-0 etc)interface whose statistics are to be retrieved.
Tx Frames	This specifies the total number of frames sent on this AAL5 VC
Rx Frames	This specifies the total number of frames received on this AAL5 VC
Tx Bytes	This specifies the total number of octets sent on this AAL5 VC
Rx Bytes	This specifies the total number of octets received on this AAL5 VC
Large Pkts Rx	This specifies the number of AAL5 packets whose length is greater than the AAL5 CPCS receive SDU size
CIS Rx	This specifies the number of congestion Indication received from the lower layers

Field	Description
CRC Errors	This specifies the number of CRC errors encountered.
Invalid CPI SDU	This specifies the number of SDU received with invalid CPI
Invalid PAD	This specifies the number of SDU received with invalid PAD length
Invalid Length SDU	This specifies the number of SDU received with invalid length
RAS Timer Expired	This specifies the number of times reassembly timer expired

Caution None.

References

- *atm trfdesc* related commands
- *atm vc* related commands
- *oam lpbk* command
- *atm port* and *statistics* related commands.

3.105 get atm port

Description Use this command to get information about a specific or all atm ports.

Command Syntax ***get atm port [ifname interface-name]***

Parameters

Name	Description
ifname interface-name	This specifies the ATM port for which information is to be displayed. If this is not specified then information for all ATM ports is displayed. **Type**: Optional **Valid values :** atm-0

Mode Super-User, User

Example ***$ get atm port ifname atm-0***

Output

```
If-Name     : atm-0                              MaxVccs          : 4
UBRPriority : 1                                  GFRPriority      : 2
Latency     : fast                               MaxConfVccs      : 0
OAMSrc      : 0xffffffffffffffffffffffffffffffff
Oper Status : Up                                 Admin Status     : Up
```

Output field description

Field	Description
If-Name	This specifies the name of the ATM port. It can be : atm-0
MaxVccs	This specifies The maximum number of VCCs (PVCCs and SVCCs) supported at this ATM interface. It may be: 0-64
UBRPriority	Priority of the best effort traffic. A value 0 means no traffic of this class is supported. Higher the value, higher the priority. It may be : 0-2
GFRPriority	This specifies the priority of GFR class. A value 0 means no traffic of this class is supported. Higher the value, higher the priority. It may be: 0-2
Latency	Type of DSL channel in use on the underlying DSL port. It may be: fast, interleaved
MaxConfVccs	This specifies the current number of VCCs configured on this port. It may be :0 - Value defined in MaxVccs
OAMSrc	Loop back source id assigned to the ATM port. The ATM port will respond to all loopback cells which carry this OAM id.
Oper Status	The actual/current state of the interface. It can be either Up or Down
Admin Status	The desired state of the interface. It may be either Up or Down

Caution None.

References

- *atm trfdesc* related commands
- *atm vc* related commands
- *oam lpbk* command
- *atm port* and *statistics* related commands.

3.106 get atm stats

Description Use this command to get the ATM virtual port statistics for a specific port or for all ports.

Command Syntax ***get atm stats [ifname*** interface-name***]***

Parameters

Name	Description
ifname interface-name	This specifies the ATM port. If this is not specified then information for all interfaces is displayed. **Type:** Optional **Valid values:** *atm-0*

Mode Super-User, User

Example ***$ get atm stats ifname*** **atm-0**

Output

```
If-Name : atm-0
Rx User Cells count       : 200     Tx User Cells count    : 250
Rx OAM Cells count        : 10      Tx OAM Cells count     : 9
Rx CLPI count             : 20       Tx CLPI count         : 15
Rx Bytes count            : 5000     Tx Bytes count        : 4900
Rx OAM Seg Cells count    : 2        Tx OAM Seg Cells count : 4
Rx OAM End Cells count    : 8        Tx OAM End Cells count : 5
Rx  CC Cells count        :10        Tx CC Cells count      : 20
Rx CC AD Cells count      : 10       Tx CC AD Cells count   :  20
Dropped Cells count       : 2        Invalid Cells count    : 3
Out Of Rx Buffer count    : 0       Out of Rx Descr count   : 0
Rejected Tx Pkts count    : 0       CRC Errors count        : 0
```

Output field description

Field	Description
If-Name	*The ATM port name: It can be: atm-00*
Rx User Cells	The number of user cells received on this interface
Tx User Cells	The number of user cells transmitted on this interface
Rx OAM Cells	The number of OAM cells received on this interface
Tx OAM Cells	The number of OAM cells transmitted on this interface
Rx CLPI	The number of cells received with Cell Loss Priority =1
Tx CLPI	The number of user cells transmitted with Cell Loss Priority =1
Rx Bytes	The number of bytes received (including ATM cell header)
Tx Bytes	The number of bytes transmitted (including ATM cell header)
Rx OAM Seg Cells	The number of OAM cells received for segment loopback
Tx OAM Seg Cells	The number of OAM cells transmitted for segment loopback

Field	Description
Rx OAM End Cells	The number of OAM cells received for end-to-end loopback
Tx OAM End Cells	The number of OAM cells transmitted for end-to-end loopback
Rx CC Cells count	This specifies the number of CC Cells (Cell used for Continuity Check) received on the ATM Port
Tx CC Cells count	This specifies the number of CC Cells (Cell used for Continuity Check) transmitted on the ATM Port
Rx CC AD Cells count	This specifies the number of CC Activation/DeactivationCells (Cell used for activating Continuity Check) received on the ATM Port
Tx CC AD Cells count	This specifies the number of CC Activation/DeactivationCells (Cell used for activating Continuity Check) transmitted on the ATM Port
Dropped Cells	The number of received cells discarded due to some error
Invalid Cells	The number of invalid received cells
Out Of Rx Buffer	The number of times receive buffer overflow was encountered
Out of Rx Descr	The number of time receive buffer descriptor overflow was encountered
Rejected Tx Pkts	The number of packets rejected because of resource crunch
CRC Errors	The number of packets rejected because of CRC errors

Caution None.

References

- *reset atm stats* command
- *atm trfdesc* related commands
- *atm vc* related commands
- *oam lpbk* command
- *atm port* related commands.

3.107 get atm svccfg

Description Use this command to get information on a particular SVC or all SVCs.

Command Syntax ***get atm svccfg [ifname*** interface-name***]***

Parameters

Name	Description
ifname interface-name	Interface name of the configured SVC. **Type:** Optional **Valid values:** *aal5-0, aal5-1…*

Mode Super-User, User.

Example ***$ get atm svccfg ifname aal5-0***

Output

```
VC IfName        : aal5-0    AAL5 Encap       : VC Mux
VPI              : 5         VCI              : 10
Numbering Plan   : atmes
Dest Atm Address : 0x47000580ffde000000000001050000000000000000
Trf Descr Index  : 1          Access Protocol  : PPPoA
Aal5 Tx Size     : 200        Aal5 Rx Size     : 200
```

Output field description

Field	Description
VC Ifname	Interface name of the configured SVC.
AAL5 Encap	The type of Protocol Multiplexing used over 1483
VPI	The VPI of the ATM VC found towards the specified ATM Destination
VCI	The VCI of the ATM VC found towards the specified ATM Destination
Numbering Plan	The Address Plan to which the specified ATM Destination Address (for SVC to be opened) belongs.
Dest Atm Address	The ATM address of the destination with which the connection is established.
Trf Descr Index	The index of the Traffic Descriptor Table entry whose traffic parameters are for the SVC to be opened.
Access Protocol	This specifies the protocol that runs on the VC
Aal5 Tx Size	This specifies the transmit CPCS SDU size.
Aal5 Rx Size	This specifies the receive CPCS SDU size.

Caution None.

References

- *create atm svccfg* command
- *delete atm svccfg* command

3.108 get atm trfdesc

Description Use this command to get information for a specific traffic descriptor or all traffic descriptors.

Command Syntax ***get atm trfdesc trfindex [***traffic-descriptor-index***]***

Parameters

Name	Description
trfindex traffic-descriptor-index	This identifies the traffic descriptor entry which is to be retrieved. **Type:** Optional **Valid values:** *0* - *

Mode Super-User, User

Example ***$ get atm trfdesc trfindex*** 0

Output

```
Traffic Descr Id     : 0              Type                 : NOCLP_NOSCR
Service Category     : UBR            Frame Discard        : Enabled
PCR                  : 0              MCR                  : 0
```

Output field description

Field	Description
Traffic Descr Id	This identifies the traffic descriptor.
Type	This defines the type of traffic used. It may be: *NOCLP_NOSCR*, *CLP_NOTAG_MCR*, *NOCLP_SCR.*
Service Category	This specifies the service category to be used. It may be: *UBR, GFR, CBR, RTVBR, NRTVBR.*
Frame Discard	It is always *Enabled.* It indicates that the network is requested to treat data for this connection, in the given direction, as frames (e.g. AAL5 CPCS_PDUs) rather than as individual cells. This treatment may, for example, involve discarding entire frames during congestion, rather than a few cells from many frames.
PCR	Peak Cell Rate for ATM Traffic.
MCR	Minimum Cell Rate for ATM Traffic.

Caution None.

References

- Other *atm trfdesc* commands
- *atm vc* related commands
- *atm port* and *statistics* related commands.

3.109 get atm uni

Description Use this command to get ATM UNI configuration information.

Command Syntax ***get atm uni [ifname*** interface-name***]***

Parameters

Name	Description
ifname interface-name	Interface Index of the ATM VC over which UNI signaling is run. **Type:** Optional **Valid values:** *aal5-0, aal5-1…*

Mode Super-User.

Example ***$ get atm*** **uni** ***ifname aal5-0***

Output

```
IfName          : aal5-0           ATM Numb Plan : atmes
Status          : Up               Version       : UNI40
Self ATM Address: 0x39000760ff8900000000000119000000000000000
```

Output field description

Name	Description
Ifname	Interface name of VC over which UNI signaling is running. It can be: *aal5-0, aal5-1…*
ATM NumbPlan	The Address Plan to which the specified ATM Source Address belongs.
Status	This specifies the status of the Signaling ATM Adaptation Layer (SAAL) layer. The purpose of SAAL is to provide reliable transfer of signaling message between peer UNI entities.
Version	This specifies the version of the UNI used. UNI31 and UNI40 mean UNI3.1 and UNI4.1 respectively.
SelfAtmAddress	The source ATM address.

Caution None.

References None.

3.110 get atm vc intf

Description Use this command to display information corresponding to a single VC or for all VCs.

Command Syntax ***get atm vc intf [ifname*** interface-name***]***

Parameters

Name	Description
ifname interface-name	Interface name of the VC which is to be displayed. If not specified then all VCs are displayed. **Type:** Optional **Valid values:** *aal5-0 - **

Mode Super-User, User

Example ***$ get atm vc intf ifname*** **aal5-0**

Output

```
LowIf               : atm-0       VPI              : 10          VCI  : 10
VC IfName           : aal5-0      VC Type          :PVC
Admin Status        : Up          Oper Status      : Up
Aal5 Tx Size        : 9200        Aal5 Rx Size     : 9200
AAL Type            : AAL5        AAL5 Encap       : LLC Mux
Max Aal5 Proto      : 3           Trf Descr Index  : 2
VC Weight           : 10          Creator          : nonilmi
```

Output field description

Field	Description
If-Name	Interface name of the VC being displayed. It can be: *aal5-0, aal5-1…*
Lowif	Interface index of the underlying ATM port. It is always: *atm-0*
VPI	It is the Virtual Path Identifier.
VCI	It is the Virtual Circuit Identifier.
VC IfNmae	This specifies the VC interface name
VC Type	This specifies the VC Type
Oper Status	The actual/current state of the interface. It can be either *Up* or *Down*
Admin Status	The desired state of the interface. It may be either *Up*, *Down or Loopback. Loopback* has a special significance. A Loopback VC will loop back whatever cells it receives.
Aal5 Tx Size	This specifies the transmit CPCS SDU size to be used
Aal5 Rx Size	This specifies the receive CPCS SDU size to be used
AAL Type	AAL type in use for the VC
AAL5 Encap	This specifies the data multiplexing method to be used over the AAL5 SSCS layer.

Field	Description
Max Aal5 Proto	This specifies the maximum number of protocols that are supported over the VC
Trf Descr Index	This identifies the transmit traffic parameters in use. It corresponds to a valid entry in the traffic descriptor table
VC Weight	This specifies the priority of the VC. Higher value means higher priority
Creator	This specifies the VC creator.

Caution None.

References

- Other *atm vc intf* commands
- *atm trfdesc* related commands
- *oam lpbk* command
- *atm port* related commands
- *atm statistics* related commands.

3.111 get atm vc stats

Description Use this command to get statistical information about a specific or all atm virtual circuits.

Command Syntax ***get atm vc stats [ifname*** interface-name***]***

Parameters

Name	Description
Ifname interface-name	This specifies the Virtual Circuit. If this is not specified then information for all VCs is displayed. **Type:** Optional **Valid values:** *aal5-0* - *

Mode User, Super-User

Example ***$ get atm vc stats ifname*** **aal5-0**

Output

```
LowIf                    : atm-0                VPI          : 1
VCI                      : 1
VC IfName                : aal5-0
User Tx Cells count      : 250                  User Rx Cells count : 200
OAM Tx Cells count       : 3                    OAM Rx Cells count : 2
OAM LB Seg Tx Cells count : 3                   OAM LB Seg Rx Cells count : 2
OAM LB End Tx Cells count : 0                   OAM LB End Rx Cells count : 0
OAM CC Tx Cells count    : 20                   OAM CC Rx Cells count : 10
OAM CC Tx AD Cells count  : 20                  OAM CC Rx AD Cells count: 10
CLPI 1 Tx Cells count     : 10                  CLPI 1 Rx Cells count : 9
Bytes Transmitted count   : 5000                Bytes Received count : 4900
Rx BD Overflow count      : 0                   Rx Buff Overflow count : 0
Tx Pkts Rejected count    : 0                   Last Reset Time(sec) : 5000
```

Output field description

Field	Description
LowIf	This specifies the ATM port name: It can be: atm-0
VPI	The Virtual Port Identifier.
VCI	The Virtual Circuit Identifier.
VC Ifname	The name of the aal5 (aal5-0) interfaces whose statistics are to be retrieved
User Tx Cells	This specifies number of user cells transmitted on this interface
User Rx Cells	This specifies number of user cells received on this interface
OAM Tx Cells	This specifies the number of OAM cells transmitted on this interface
OAM Rx Cells	This specifies the number of OAM cells received on this interface

Field	Description
OAM LB Seg Tx Cells	This specifies the number of OAM cells transmitted for segment loopback
OAM LB Seg Rx Cells	This specifies the number of OAM cells received for segment loopback
OAM LB End Tx Cell	This specifies the number of OAM cells transmitted for end-to-end loopback
OAM LB End Rx Cells	This specifies the number of OAM cells received for end-to-end loopback
OAM CC Tx Cells count	This specifies the number of CC Cells (Cell used for Continuity Check) transmitted on the ATM Port
OAM CC Rx Cells count	This specifies the number of CC Cells (Cell used for Continuity Check) received on the ATM Port
OAM CC Tx AD Cells count	This specifies the number of CC Activation/DeactivationCells (Cell used for activating Continuity Check) transmitted on the ATM Port
OAM CC Rx AD Cells count	This specifies the number of CC Activation/DeactivationCells (Cell used for activating Continuity Check) received on the ATM Port
CLPI 1 Tx Cells	This specifies the number of user cells transmitted with CLP=1
CLPI 1 Rx Cells	This specifies the number of cells received with CLP=1
Bytes Received	This specifies the number of bytes received (including ATM cell header)
Rx Buff Descr Overflow	This specifies the number of time receive buffer descriptor overflow was encountered
Rx Buff Overflow	This specifies the number of times receive buffer overflow was encountered
Tx Pkts Rejected	This specifies the number of packets rejected because of resource crunch
Last Reset Time (sec)	This specifies the time elapsed in seconds since the last reset for statistics for this interface.

Caution None.

References

- *atm trfdesc* related commands
- Other *atm vc* related commands
- *oam lpbk* command
- *atm port* related commands
- *atm statistics* related commands.

3.112 get autodetect cfg

Description Use this command to get the status of automatic detect mode.

Command Syntax ***get autodetect cfg***

Parameters None

Mode User, Super-User

Example ***$ get autodetect cfg***

Output

```
Auto Detect Mode : Enable       Mode        : Bridge

Detect PPP       : PADI LCP     VC Range    : From file
```

Output field description

Field	Description
Auto Detect Mode	Status of the Automatic Detect Mode.
Mode	This specifies whether modem is configured for bridging or routing mode.
Detect PPP	This specifies the auto detection procedure.
VC Range	This specifies the range of VC values for which auto detection procedure will be followed.

Caution None

References

- *modify autodetect cfg*

3.113 get autodetect status

Description Use this command to get the status of automatic detect mode.

Command Syntax ***get autodetect status***

Parameters None

Mode User, Super-User

Example ***$ get autodetect status***

Output

```
VPI      : 9                    VCI            : 102

Port     : atm-0

Protocol :  DHCP IPOA1577
```

Output field description

Field	Description
VPI	This specifies the VPI detected.
VCI	This specifies the VCI detected.
Port	This specifies the port on which VPI and VCI have been detected.
Protocol	This specifies the range of protocols, which have been detected.

Caution None

References

- *modify autodetect status*

3.114 get autoupdate

Description Use this command to see the autoupdate flag

Command Syntax ***get autoupdate***

Parameters None.

Mode User, Super-User.

Example ***$ get autoupdate***

Output

```
Auto Update: False
```

Output field description

Field	Description
Auto Update	This specifies the current value of the autoupdate flag. If it is *True* then any file downloaded using the *download command* is applied immediately after being downloaded (in case of a *.cfg* file its commands would be immediately executed; in case of a *.bin* file the code in it will get programmed into the flash and the modem will reboot with the new code). If the flag is *False* then the file is simply downloaded and not executed.

Caution None.

References

- *apply* command
- *modify autoupdate* command
- *remove* command.
- *download* command.
- *list* command.

3.115 get bras cfg

Description Use this command to get BRAS Configuration.

Command Syntax ***get bras cfg***

Parameters None

Mode Super-User, User

Example ***$ get bras cfg***

Output

```
Status : Enable
```

Output field description

Field	Description
Status	This field specifes whether Bridge Router Auto Sense (BRAS) feature is enabled or disabled. If enabled, the modem's PPoE client is disabled when a PPoE client is detected on the LAN.

Caution None.

References

- *modify bras cfg* command.

3.116 get bridge forwarding

Description Use this command to display the forwarding information available with the bridge for the specified address or for all the addresses.

Command Syntax ***get bridge forwarding [macaddr*** mac-address***]***

Parameters

Name	Description
macaddr mac-address	A MAC address for which the bridge has forwarding and/or filtering information. If it is not specified then information for all MAC addresses is displayed. **Type:** Optional **Valid values:** *0:0:0:0:0:0 to FF:FF:FF:FF:FF:FE*

Mode Super-User, User

Example ***$ get bridge forwarding macaddr*** **1:1:1:1:1:1**

Output

```
MAC Addr           If-Name    Status
-----------------------------------------
01:01:01:01:01:01   eth-0      Learned
```

Output field description

Field	Description
MAC Addr	A unicast MAC address for which the bridge has forwarding and/or filtering information
If-Name	It identifies the interface on which at least one frame corresponding to the MAC address above, has been seen. A value of *0* indicates that the forwarding information has not been learned dynamically but is available (e.g. by using *create bridge static* command).
Status	The status of this entry. The value *Learned* indicates that the value is known and currently being used. It may be: *Learned*

Caution None.

References

- *bridge port* related commands.
- *bridge port stats* command
- *bridge static* related commands
- *bridge mode* related commands

3.117 get bridge tbg info

Description Use this command to get bridging related global information.

Command Syntax ***get bridge tbg info***

Parameters None.

Mode Super-User, User

Example ***$ get bridge tbg info***

Output

```
Learned Entry Discards : 0
Aging Timeout(sec)     : 300
MacAddress             : 00:00:00:00:00:00
No. of Ports           : 5
Base Type              : Transparent
```

Output field description

Field	Description
Learned Entry Discards	The total number of Forwarding Database entries, which have been or would have been learnt, but have been discarded due to a lack of space to store them in the Forwarding Database. If this counter is increasing, it indicates that the Forwarding Database is regularly becoming full (a condition which has unpleasant performance effects on the subnetwork). If this counter has a significant value but is not presently increasing, it indicates that the problem has been occurring but is not persistent.
Aging TimeOut(sec)	The timeout period in seconds for aging out dynamically learned forwarding information.
MacAddress	The MAC address used by this bridge when it must be referred to in a unique fashion. It is the address of the ethernet port.
No. of Ports	The maximum number of ports that can be controlled by this bridge.
Base Type	Indicates what type of bridging this bridge can perform. It is always *Transparent.*

Caution None.

References

- *modify bridge tbg info* command
- *bridge* related commands
- *bridge port stats* related command
- *bridge static* command
- *bridge forwarding* command.

3.118 get bridge mode

Description Use this command to get the current bridging mode of modem.

Command Syntax ***get bridge mode***

Parameters None.

Mode Super-User, User

Example ***$ get bridge mode***

Output

```
Bridging     Wan to Wan Bridging
-----------------------------------------
enable       disable
```

Output field description

Field	Description
Bridging	This specifies whether bridging mode is enabled or disabled.
Wan to Wan Bridging	This specifies whether WAN-to-WAN bridging mode is enabled or disabled..

Caution None.

References

- *modify bridge mode* command
- *bridge port* command
- *bridge port stats* command
- *bridge static* command
- *bridge forwarding* command.

3.119 get bridge port intf

Description Use this command to get the information about a specific bridge port or for all the ports.

Command Syntax ***get bridge port intf [ifname*** interface-name***]***

Parameters

Name	Description
ifname interface-name	This specifies the bridge Interface. If this is not specified then information for all interfaces is displayed. **Type:** Optional **Valid values:** *eoa-0 - * eth-0, usb-0*

Mode Super-User, User

Example ***$ get bridge port intf ifname*** **eth-0**

Output

```
Port     If-Name   Delay-Exceed-Discards    MTU-Exceed-Discards
-------------------------------------------------------------
1        eth-0     0                        0
```

Output field description

Field	Description
Port	The port number of the interface for which information is being displayed.
If-Name	This specifies the Interface name corresponding to the above port. It can be: *eoa-0 - *, , eth-0, usb-0*
Delay-Exceed-Discards	The number of frames discarded by this port due to excessive transit delay through the bridge
MTU-Exceed-Discards	The number of frames discarded by this port due to the frame size being greater than the MTU of the interface

Caution None.

References

- *delete bridge port intf* command
- *create bridge port intf* command
- *bridge mode* commands
- *bridge port stats* command
- *bridge static* commands
- *bridge forwarding* commands

3.120 get bridge port stats

Description Use this command to get the statistics of a single port or all the ports.

Command Syntax ***get bridge port stats [ifname*** interface-name***]***

Parameters

Name	Description
ifname interface-name	This specifies the bridge Interface. If this is not specified then information for all interfaces is displayed. **Type:** Optional **Valid values:** *eoa-0 - *, eth-0, usb-0*

Mode Super-User, User

Example ***$ get bridge port stats ifname*** **eth-0**

Output

```
If-Name           : eth-0
Delay Exceeded    : 0              MTU Exceeded    : 0
Max Info Size     : 0              Out Frames      : 138
In Frames         : 129            In Discards     : 3
```

Output field description

Field	Description
If-Name	This specifies the Interface name corresponding to which the statistics are being displayed. It can be: *eoa-0 - *, eth-0, usb-0*
Delay Exceeded	The number of frames discarded by this port due to excessive transit delay
MTU Exceeded	The number of frames discarded by this port due to an excessive size.
Max Info Size	The maximum size of the INFO (non-MAC) field that this port will receive or transmit
Out Frames	The number of frames that have been transmitted by this port to its segment.
In Frames	The number of frames that have been received by this port from its segment.
In Discards	Count of valid frames received which were discarded (i.e., filtered) by the Forwarding Process

Caution None.

References

- *bridge mode* related commands
- *bridge port intf* command
- *bridge static* related commands
- *bridge forwarding* related commands.

3.121 get bridge static

Description Use this command to get information about a specific or all bridge static entries.

Command Syntax ***get bridge static [macaddr mac-address][inifname interface-name|all]***

Parameters

Name	Description
macaddr mac-address	This identifies the entry for which the information is to be displayed. It is the destination MAC address in a frame to which this entry's filtering information applies. If not specified then information for all entries is displayed. **Type:** Optional **Valid values:** *0:0:0:0:0:1 to FF:FF:FF:FF:FF:FE*

Mode Super-User, User

Example ***$ get bridge static macaddr 1:1:1:1:1:1***

Output

```
MAC Address : 01:01:01:01:01:01        Incoming Interface : veth-0
Interfaces : eth-0 eoa-1
```

Output field description

Field	Description
MAC Address	The destination MAC address in a frame to which this entry's filtering information applies
Interfaces	The interfaces to which frames received from a specific port and destined for the given MAC address, are allowed to be forwarded. They may be: *eth-0, eoa-0 - * , usb-0*

Caution None.

References

- *delete bridge static* command
- *create bridge static* command
- *modify bridge static* command
- *bridge mode* related commands
- *bridge port stats* related commands
- *bridge static* related commands
- *bridge forwarding* related commands

3.122 get ddns hostname

Description Use this command to get Dynamic DNS Host Name Table

Command Syntax ***get ddns hostname*** ***[ifname*** ifname ***] [name*** name ***]***

Parameter

Name	Description
ifname ifname	Interface name of the public interface for which this entry defines the Dynamic DNS Host Name. **Valid Values :** ppp-0 - ppp-*, ipoa-0 - ipoa-*, eoa-0 - eoa-*, eth-0 - eth-*, usb-0, wlan-0 **Type:** Optional
name name	Hostname registered at service provider. **Type:** Optional

Mode Super-User, User

Example ***$ get ddns hostname ifname*** ppp-0 ***name*** www.xyz.com

Output

```
Interface  HostName
-------------------------------------------------------------------------------
ppp-0      www.xyz.com
```

Output field description

Field	Description
Interface	Interface name of the public interface for which this entry defines the Dynamic DNS Host Name. Valid Values : ppp-0 - ppp-*, ipoa-0 - ipoa-*, eoa-0 - eoa-*, eth-0 - eth-*, usb-0, wlan-0
HostName	Hostname registered at service provider.

Cautions None.

References

- *create ddns hostname* command
- *delete ddns hostname* command

3.123 get ddns intf

Description Use this command to get Dynamic DNS Service Configuration

Command Syntax ***get ddns intf [ifname*** ifname ***]***

Parameter

Name	Description
ifname ifname	Interface name of the public interface for which this entry defines the Dynamic DNS profile. **Valid Values :** ppp-0 - ppp-*, ipoa-0 - ipoa-*, eoa-0 - eoa-*, eth-0 - eth-*, usb-0, wlan-0 **Type:** Optional

Mode Super-User, User

Example ***$ get ddns intf ifname*** ppp-0

Output

```
Interface        : ppp-0
Service Provider : dyndns
User Name        : "Viking"
Type of system   : dynamic            WildCard        : enable
Mail Exchanger   : www.IAD1.com
Mail Backup      : enable             Offline Support : enable
```

Output field description

Field	Description
Interface	Interface name of the public interface for which this entry defines the Dynamic DNS profile. Valid Values : ppp-0 - ppp-*, ipoa-0 - ipoa-*, eoa-0 - eoa-*, eth-0 - eth-*, usb-0, wlan-0
Service Provider	This is the name of the Dynamic DNS service provider where the user has registered and has an account.Some examples are www.tzo.com, www.dyndns.org
User Name	Username registered at service provider. The value is to be given in double quotes.

Field	Description
Type of system	This parameter is valid only when SrvcName is DYNDNS. www.dyndns.org provides three kinds of services - Dynamic DNS, Custom DNS and Static DNS. The user can create different domains in these systems. Custom DNS service is a full DNS solution for newly purchased domains or domains you already own. A web-based interface provides complete control over resource records and your entire domain including support for dynamic IPs and automated updates. Static DNS service points a DNS hostname in some domain owned by dyndns.org to the user's ISP-assigned static or pseudo-static (meaning which do not change too frequently) IP address. DynDNS service points a fixed hostname in some domain owned by dyndns.org to the user's ISP-assigned dynamic IP address. This allows more frequent updation of IP addresses than Static DNS.
WildCard	This parameter is valid only if SrvcName is DYNDNS. It specifies whether Wildcard CNAME are to be resolved or not. If enabled, addresses *.yourhost.ourdomain.ext are aliased to the same address as yourhost.ourdomain.ext.
Mail Exchanger	This parameter is valid only if SrvcName is DYNDNS. It specifies a Mail Exchanger (MX) for use with the hostname being modified. The specified MX must resolve to an IP address, or it will be ignored. Providing no MX setting (or an MX that doesn't resolve properly to an A record) will cause the hostname's MX record(s) to be removed.
Mail Backup	This parameter is valid only if SrvcName is DYNDNS.It specifies whehter mails are to be backed up by the service provider.
Offline Support	This parameter is valid only if SrvcName is DYNDNS. If enabled, the service provider redirects browsers to its own site if the registered host is currently offline.

Cautions None.

References

- *create ddns intf* command
- *delete ddns intf* command

3.124 get datauserslist

Description Use this command to get DHCP client information, for clients on the specified interface or for all the interfaces.

Command Syntax ***get datauserslist***

Parameters None

Mode Super-User, User

Example ***$ get datauserslist***

Output Verbose mode on/off

```
User Name: james
IP Address: 172.25.2.12
```

Output field description

Field	Description
User Name	This specifies the login name of the data user.
IP Address	This specifies the IP Address of host from which the data user is currently logged in.

Caution None.

References

- *reset datauserslist* command
- *get usagectrl* command
- *modify usagectrl* command.

3.125 get dhcp client info

Description Use this command to get DHCP client information, for clients on the specified interface or for all the interfaces.

Command Syntax ***get dhcp client info [ifname*** interface-name***]***

Parameters

Name	Description
ifname interface-name	This specifies the interface name on which DHCP is running. If this is not specified then information for clients on all such interfaces will be displayed. **Type:** Optional **Valid values:** *eth-0, eoa-0 - **

Mode Super-User, User

Example ***$ get dhcp client info ifname*** **eth-0**

Output

```
If-name    Server         Status      Lease Start Date     Lease Time (sec)
-----------------------------------------------------------------
eth-0      1.1.1.1        Bound        Thu Jan 01 00:00:38 1970  500
```

Output field description

Field	Description
If-Name	This is an interface on which DHCP is running. It can be: *eth-0-*, etc.*
Server	This specifies the address of the DHCP server with whom the client has obtained the IP address and other configurations
Status	This specifies the current state of the client. It may be: *Init*, *Selecting*, *Bound*, *Requesting*, *Renew* or *Bind*.
Lease Start Date	This signifies the date on which the DHCP server leased out the IP address to the client.
Lease Time	This specifies the time period (in seconds) for which an IP address was leased out by the server. The client is expected to renew the lease before the expiry of this timer or release the IP Address

Caution None.

References

- *dhcp client stats* related commands
- *dhcp server* related commands.

3.126 get dhcp client stats

Description Use this command to get dhcp client statistics on an interface on which the dhcp client is running, or on all such interfaces. .

Command Syntax ***get dhcp client stats [ifname*** interface-name***]***

Parameters

Name	Description
ifname interface-name	This specifies the interface name on which DHCP is running. If this is not specified then information for clients on all such interfaces will be displayed. **Type:** Optional **Valid values:** *eth-0, eoa-0 - **

Mode Super-User, User

Example ***$ get dhcp client stats ifname*** **eth-0**

Output

```
If-name              : eth-0
Msgs Sent            : 4                 Msgs Rcvd          : 0
Decline Sent         : 0                 Offer Msgs Rcvd    : 0
Discover Msgs Sent   : 4
Req Sent             : 0                 Acks Rcvd          : 0
Rel Sent             : 0                 Nacks Rcvd         : 0
Inform Sent          : 0                 Invalid Rcvd       : 0
```

Output field description

Field	Description
If-Name	This is an interface on which DHCP is running: It can be: *eth-0*
Msgs Sent	This specifies number of dhcp messages sent on this interface
Msgs Rcvd	This specifies number of dhcp messages received on this interface
Decline Sent	This specifies number of dhcp decline messages sent on this interface
Offer Msgs Rcvd	This specifies number of dhcp offer messages received on this interface
Discover Msgs Sent	This specifies number of dhcp discover messages sent on this interface
Req Sent	This specifies number of dhcp request messages sent on this interface
Acks Rcvd	This specifies number of dhcp acks received on this interface
Rel Sent	This specifies number of dhcp release messages sent on this interface

Field	Description
Nacks Rcvd	This specifies number of dhcp nacks received on this interface
Inform Sent	This specifies number of dhcp inform messages sent on this interface.
Invalid Rcvd	This specifies number of invalid dhcp messages received on this interface

Caution None.

References

- *dhcp client info* related commands
- *dhcp server* related commands

3.127 get dhcp relay cfg

Description Use this command display DHCP relay global configuration.

Command Syntax ***get dhcp relay cfg***

Parameters None.

Mode Super-User, User

Example ***$ get dhcp relay cfg***

Output

```
Status     : Disable
Server IP  : 202.64.23.4
```

Output field description

Field	Description
Status	This specifies the Admin Status of the DHCP Relay. It may be: *Enable, Disable*
Server IP	This specifies the IP Address where the DHCP Server is running.

Caution None.

References

- *modify dhcp relay cfg* command
- *fdhcp relay stats* related commands.

3.128 get dhcp relay intf

Description Use this command to display a list of all interfaces on which DHCP relaying is enabled.

Command Syntax ***get dhcp relay intf [ifname*** `interface-name`***]***

Parameters

Name	Description
ifname `interface-name`	This specifies the physical Interface. If this is not specified then information for all interfaces on which DHCP Relaying is enabled is displayed. **Type:** Optional **Valid values:** *eth-0, ppp-0 - *,...*

Mode Super-User, User

Example ***$ get dhcp relay intf***

Output

```
If-name
-------
eth-0
```

Output field description

Field	Description
If-Name	This specifies an interface which is enabled for DHCP Relay. It can be: *eth-0, ppp-0 - *, ...*

Caution None.

References

- *`delete dhcp relay intf`* command
- *`create dhcp relay intf`* command
- *`dhcp relay cfg`* related commands
- *`dhcp relay stats`* related commands

3.129 get dhcp relay stats

Description Use this command to display the global DHCP relay statistics.

Command Syntax ***get dhcp relay stats***

Parameters None.

Mode Super-User, User

Example ***$ get dhcp relay stats***

Output

```
Msgs Rcvd              : 10          Msgs Rlyd               : 10
Requests Rcvd          : 5           Requests Rlyd           : 5
Replies Rcvd           : 5           Replies Rlyd            : 5
Requests Drop          : 0           Replies Drop            : 0
Req Drop Invld Hops    : 0           Reply Drop NotConn Dir  : 0
Req Drop Intf Disabld  : 0           Msgs Drop Relay Disabld : 0
```

Output field description

Field	Description
Msgs Rcvd	Total no of msgs received
Msgs Rlyd	Total no of messages relayed
Requests Rcvd	Total no of BOOTREQUEST messages received
Requests Rlyd	Total no of BOOTREQUEST messages relayed
Replies Rcvd	Total no of BOOTREPLY messages received
Replies Rlyd	Total no of BOOTREPLY messages relayed.
Requests Drop	Total no of BOOTREQUEST messages dropped
Replies Drop	Total no of BOOTREPLY messages dropped.
Req Drop Hops	Total no of messages dropped because ‘hops’ value is greater than 16.
Replies Drop NotConn	Total no of BOOTREPLY messages dropped because client to which it is to be relayed is not connected directly.
Req Drop Intf	Total no of BOOTPREQUEST messages dropped because relaying is disabled for the interface on which the message was received.
Msgs Drop Relay	Total no of messages dropped because relaying is disabled in the global configuration

Caution None.

References

- *create dhcp* command
- *reset dhcp* command
- *relay stats* command
- *dhcp relay cfg* related commands
- *dhcp relay intf* related commands

3.130 get dhcp server address

Description This command is used for getting information about specific client or information of all the clients (when ip-addr is not specified) from the DHCP Server Address Table. The client be a static client, created by executing a *create dhcp server host* command or a dynamic client.

Command Syntax ***get dhcp server address [ip*** ip-address***]***

Parameters

Name	Description
ip ip-address	The IP address of client. If this is not specified then information for all entries in the address table is displayed. **Type:** Optional **Valid values:** Any valid class A/B/C IP address

Mode Super-User, User

Example ***$ get dhcp server address***

Output

```
Client-Ip        : 192.168.1.200      Subnet Mask     : 255.255.0.0
Rem Lease(sec)   : 0                  H/W Addr        : AA:AA:BC:1A:44:45
Start Ip         : 0.0.0.0            Type            : Static
Domain Name      : abc
```

Output field description

Field	Description
Client-Ip	The IP address of the Client whose information is being displayed.
Subnet Mask	The subnet mask provided to the client offered this address
Rem Lease	The number of seconds until the lease expires. A value of 4294967295 is used for BOOTP leases and for leases that have an 'infinite' lease time.
H/W Addr	The hardware address of the client that has been assigned this lease.
Start Ip	The starting IP address of the range (in DHCP Server Pool Table) to which this address belongs. If the address does not fall into one of the configured ranges the value displayed will be 0.0.0.0
Type	The type of this address. The valid values are: Static, Dynamic, Config-Reserved, Server-Reserved.
Domain Name	The domain name assigned to the client

Caution None.

References

- *dhcp server* related commands
- *dhcp client* related commands
- *dhcp server pool* related commands
- *dhcp server host* related commands

3.131 get dhcp server cfg

Description Use this command to display the current status of the DHCP server.

Command Syntax ***get dhcp server cfg***

Parameters None.

Mode Super-User, User

Example ***$ get dhcp server cfg***

Output

```
Status             : Enable          Backup Interval(mins): 10
Def Pri DNS Server : 172.25.8.9      Def Sec DNS Server   : 172.25.7.67
```

Output field description

Field	Description
Status	The state of the DHCP Server. It may be either *Enable* or *Disable*
Backup Interval(mins)	This specifies the backup interval(mins) of the dhcp server. A value of "immediate" will indicate that flash backup is to be done whenever the configuration gets updated. A value of "disable" will indicate that backup is never done by DHCP
Def Pri DNS Server	The default primary DNS server assigned by the DHCP server when user does not specify a primary DNS server in the DHCP pool configuration
Def Sec DNS Server	The default secondary DNS server assigned by the DHCP server when user does not specify a secondary DNS server in the DHCP pool configuration

Caution None.

References

- *modify dhcp server cfg* command
- *dhcp client* related commands
- *dhcp server pool* related commands
- *dhcp server host* related commands

3.132 get dhcp server exclude

Description Use this command for a listing of all the IP addresses that have been excluded globally.

Command Syntax ***get dhcp server exclude***

Parameters None.

Mode Super-User, User

Example ***$ get dhcp server exclude***

Output

```
Entry Created

Ip Address
-----------
192.168.1.5
```

Output field description

Field	Description
Ip Address	This is the IP address that has been excluded.

Caution None.

References

- *delete dhcp server exclude* command
- *create dhcp server exclude* command
- *dhcp server pool* related commands

3.133 get dhcp server host

Description Use this command to get information pertaining to a specific static DHCP host or for all static hosts.

Command Syntax ***get dhcp server host [ip*** ip-address***]***

Parameters

Name	Description
ip ip-address	This specifies the IP address of the host whose information is to be displayed. If no IP address is specified then information for all static hosts is displayed. **Type:** Optional **Valid values:** Any valid class A/B/C IP address

Mode Super-User, User

Example ***$ get dhcp server host ip*** **192.168.1.7**

Output

```
Host Ip          : 192.168.1.7        Hardware Addr    : 12 34 45 56 03 02
Def Lease(sec)   : 2592000            Max Lease(sec)   : 31536000
Domain Name      :
Subnet Mask      : 255.255.255.0
Gateway Ip       : 0.0.0.0            Smtp Ip          : 0.0.0.0
Dns Ip           : 0.0.0.0            Sec. Dns Ip      : 0.0.0.0
Pop3 Ip          : 0.0.0.0            Nntp Ip          : 0.0.0.0
Www Ip           : 0.0.0.0            Irc Ip           : 0.0.0.0
Wins Ip          : 0.0.0.0            Sec. Wins Ip     : 0.0.0.0
```

Output field description

Field	Description
Host Ip	This specifies the IP address to be provided to this host
Hardware Addr	This specifies the hardware address of the client
Def Lease	This specifies the lease period for which the server assigns an IP address to a client in case the client does not request for a specific lease period itself.
Max Lease	This specifies the maximum period for which the DHCP server can lease out an IP address to a DHCP client.
Domain Name	Specifies the domain name configured for this host
Subnet Mask	This specifies the subnet mask to be provided to the host
Gateway Ip	This specifies the default gateway IP address
Smtp Ip	This specifies the IP address of the NNTP Server
Dns Ip	This specifies the IP address of the primary Domain Name Server
Sec. Dns Ip	This specifies the IP address of the secondary Domain Name Server
Pop3 Ip	This specifies the IP address of the POP3 Server

Field	Description
Nntp Ip	This specifies the IP address of the SMTP Server
Www Ip	This specifies the IP address of the WWW Serve
Irc Ip	This specifies the IP address of the IRC Server
Wins Ip	This specifies the IP address of the primary WIN Server
Sec. Wins Ip	This specifies the IP address of the secondary WIN Server

Caution None.

References

- *create dhcp server host* command
- *delete dhcp server host* command
- *modify dhcp server host* command
- *dhcp server* related commands.

3.134 get dhcp server pool

Description This command is used to get information about a specific or all configured DHCP pools.

Command Syntax ***get dhcp server pool [*pool-id** pool-id***]***

Parameters

Name	Description
pool-id ***pool-id***	This identifies the pool for which information is to be retrieved. If no pool ID is specified then information for all pools is displayed. **Type:** Optional **Valid values:** 0-* , where * dependes upon the iad.conf value.

Mode Super-User, User

Example ***$ get dhcp server poolid*** 0

Output

```
Entry Created

Pool Id          : 0                  Status           : Disable
Start Ip         : 192.168.1.1        End Ip           : 192.168.1.200
Def Lease(sec)   : 2592000            Max Lease(sec)   : 31536000
Range Inuse      : 0                  Outstd Offers    : 0
Low Thres        : 0                  Subnet Mask      : 255.255.255.0
Domain Name      :
Gateway Ip       : 0.0.0.0            Smtp Ip          : 0.0.0.0
Dns Ip           : 0.0.0.0            Sec. Dns Ip      : 0.0.0.0
Pop3 Ip          : 0.0.0.0            Nntp Ip          : 0.0.0.0
Www Ip           : 0.0.0.0            Irc Ip           : 0.0.0.0
Wins Ip          : 0.0.0.0            Sec. Wins Ip     : 0.0.0.0
```

Output field description

Field	Description
Pool Id	This is the pool identifier.
Status	This defines the Admin status of the entry. It may be either *Enable* or *Disable*
Start Ip	The IP address of the first address in the range.
End Ip	The IP address of the last address in the range
Def Lease	This specifies the lease period for which the server assigns an IP address to a client in case the client does not request for a specific lease period itself.
Max Lease	This specifies the maximum period for which the DHCP server can lease out an IP address to a DHCP client.
Range Inuse	The number of addresses in this range that are currently in use. This number includes those addresses whose lease has not expired and addresses which have been reserved

Field	Description
Outstd Offers	The number of outstanding DHCPOFFER messages for this range is reported with this value. An offer is outstanding if the server has sent a DHCPOFFER message to a client, but has not yet received a DHCPREQUEST message from the client nor has the server-specific timeout, within which a client can respond to the offer message, for the offer message expired
Low Thres	This specifies the lowest threshold value on the number of available/ free IP addresses for a particular shared network
Subnet Mask	The subnet mask provided to any client offered an address from this range
Domain Name	Domain name used per subnet.
Gateway Ip	This specifies the default gateway IP address
Smtp Ip	This specifies the IP address of the NNTP Server
Dns Ip	This specifies the IP address of the primary Domain Name Server
Sec.Dns Ip	This specifies the IP address of the secondary Domain Name Server
Pop3 Ip	This specifies the IP address of the POP3 Server
Nntp Ip	This specifies the IP address of the SMTP Server
Www Ip	This specifies the IP address of the WWW Serve
Irc Ip	This specifies the IP address of the IRC Server
Wins Ip	This specifies the IP address of the primary WIN Server
Sec. Wins Ip	This specifies the IP address of the secondary WIN Server

Caution None.

References

- *modify dhcp server pool* command
- *create dhcp server pool* command
- *get dhcp server pool* command
- *dhcp server cfg* related commands
- *dhcp server exclude* related commands
- *dhcp server address* related commands

3.135 get dhcp server stats

Description Use this command to get the global statistics for DHCP Server.

Command Syntax ***get dhcp server stats***

Parameters None.

Mode Super-User, User

Example ***$ get dhcp server stats***

Output

```
Msgs Sent           : 0          Msgs Rcvd           : 0
Offers Sent         : 0          Discover Rcvd       : 0
Acks Sent           : 0          Rel Rcvd            : 0
Nacks Sent          : 0          Inform Rcvd         : 0
Drop Invld Client   : 0          Decline Rcvd        : 0
Drop Invld Subnet   : 0          Req Rcvd            : 0
Active Pools        : 0          Invalid Rcvd        : 0
IP Inactive Pools : 0
IP Curr Leased      : 0          IP Curr Free        : 0
IP Curr Unavailable: 0           IP Curr Forced Renew: 0
```

Output field description

Field	Description
Msgs Sent	This defines number of DHCP messages sent by the server
Msgs Rcvd	This defines number of DHCP messages received by the server
Offers Sent	This defines number of DHCP Offer messages sent by the server
Discover Rcvd	This defines number of DHCP Discover messages received by the server
Acks Sent	This defines number of ack messages sent by the server
Rel Rcvd	This defines number of DHCP release messages received by the server
Nacks Sent	This defines number of Nack messages sent by the server
Inform Rcvd	This defines number of DHCP inform messages received by the server
Drop Invld Client	The number of DHCP packets dropped because the client referred
Decline Rcvd	This defines number of DHCP decline messages received by the server
Drop Invld Subnet	The number of DHCP packets dropped due to the server not serving addresses on the subnet from which this message was received
Req Rcvd	This defines number of DHCP request messages received by the Server

Field	Description
Active Pools	This specifies number of active pools
Invalid Rcvd	This defines number of invalid messages received by the server
IP Inactive Pools	This specifies number of IP addresses in the inactive pools
IP Curr Leased	This specifies the number of addresses currently leased out
IP Curr Free	This specifies the number of addresses available for the lease
IP Curr Unavailable	This specifies number of IP addresses currently unavailable
IP Curr Forced Renew	This specifies the number of IP addresses currently in forced re-new state

Caution None.

References

- *reset dhcp server stats* command
- *dhcp server cfg* related commands
- *dhcp server exclude* related commands
- *dhcp server address* related commands
- *dhcp server pool* related commands

3.136 get dns relay cfg

Description Use this command to get DNS relay configuration information.

Command Syntax ***get dns relay cfg***

Parameters None

Output Verbose Mode On

```
Status     : Disable
Poll Status :  enable          Poll interval: 2
```

Verbose Mode off

```
Status     : Disable
Poll Status :  enable          Poll interval: 2
```

Output field description

Field	Description
Status	This specifies whether DNS relay is enabled or disabled.
Poll Status	If enabled, the DNS servers are probed periodically to see if they can be reached.
Poll interval	The periodic interval after which DNS servers are probed (if polling is enabled).

Mode User

Example ***$ get dns relay cfg***

Caution None

References

- *modify dns relay cfg* command

3.137 get dns relay stats

Description Use this command to get DNS relay stats values.

Command Syntax: ***get dns relay stats***

Mode: User

Example: ***$ get dns relay stats***

Output: Verbose mode on

```
DNS Server in Use          : 172.24.89.100
Requests Received Count    : 20
Requests Forwarded Count   : 20
Responses Received Count   : 20
Responses Forwarded Count  : 20
Table Full Count           : 0
No Server Configured Count : 0
No Valid Entry Count       : 0
```

Verbose mode off

```
DNS Server in Use          : 172.24.89.100
Requests Received Count    : 20
Requests Forwarded Count   : 20
Responses Received Count   : 20
Responses Forwarded Count  : 20
Table Full Count           : 0
No Server Configured Count : 0
No Valid Entry Count       : 0
```

Output Field description:

Field	Description
DNS Server in Use	This parameter specifies the current DNS server in use by DNS relay.
Requests Received count	This parameter specifies the number of DNS requests received by DNS Relay
Requests Forwarded Count	This parameter specifies the number of DNS requests forwarded by DNS relay.
Responses Received Count	This parameter specifies the number of DNS responses received by DNS relay from DNS server.
Responses Forwarded Count	This parameter specifies the number of DNS responses forwarded by DNS relay to the hosts.
Table Full Count	This parameter specifies the number of DNS requests dumped because the DNS relay session table is full.

Field	Description
No Server Configured Count	This parameter specifies the number of DNS requests dumped by DNS Relay because no valid DNS server was configured at DNS Relay.
No Valid Entry Count	This parameter specifies the number of DNS responses dumped because no valid DNS Relay session entry exists for it.

Caution: None

References :

- modify dns relay cfg
- reset dns relay stats
- get dns relay cfg
- create dns servaddr
- get dns servaddr
- delete dns servaddr

3.138 get dns servaddr

Description Use this command to get DNS server addresses.

Command Syntax ***get dns servaddr***

Parameters None

Mode User, Super-User.

Example ***$ get dns servaddr***

Output Verbose mode on:

```
DNS Server IP Address
---------------------
172.24.32.100
192.168.2.48
```

Verbose mode off:

```
DNS Server IP Address
---------------------
172.40.30.150
192.168.2.48
```

Output Field description:

Field	Description
DNS Server IP Address	This specifies the IP address of the DNS server.

Caution None

References:

- create dns servaddr
- delete dns servaddr
- modify dns relay cfg
- get dns relay cfg
- get dns relay stats
- reset dns relay stats

3.139 get dsl config

Description Use this command to get the global statistics for DHCP Server.

Command Syntax ***get dsl config***

Parameters None

Mode Super-User.

Example ***$ get dsl config***

Output

```
Whip              : Disable       Annex Type            : Annex A
Standard          : G.dmt         Trellis coding        : Enable
ExpExchSeq        : Expanded      Framing structure     : Framing-3
TxAttenuation(dB) : 0             Coding Gain           : Auto
TxBinAdjust       : Enable        RxBinAdjust           : Disable
TxStartBin        : 6             TxEndBin              : 31
RxStartBin        : 32            RxEndBin              : 255
Fast Retrain      : Disable       Esc Fast Retrain      : Disable
MaxBits/bin On Rx : 14            Bit Swap              : Disable
Dual Latency      : Enable        Pmode                 : Enable
Pilot Request     : Enable        Last Failed Status    : 0x19
OperStatus       : Shakeup       Startup Progress      : 0xa0
AC Mode item      : fbm           AC Ttr R Offset       : 0
AC Pilot Request  : Disable       EC Fdm Mode           : ec
Max Down Rate     : 0xff
```

Output field description

Field	Description
Whip	Enable or disable Windows Based Host Interface Program
Standard	This specifies the standard to be supported for the DSL line.
Trellis coding	This is used to enable or disable Trellis coding on the interface.
ExpExchSeq	Expanded Exchange Sequence (EES) enable/disable, only valid for T1.413. This is largely for compatibility testing.
Framing structure	Full overhead to reduced overhead (0x00-03). This value is ignored for G.lite (G992.2).
TxAttenuation (dB)	This specifies the value of transmit power attenuation. Its range is from 0dB to 12dB.
Coding Gain	Coding gain is the gain due to trellis/RS coding. Its value ranges from 0 to 7dB.
TxBinAdjust	Enable or disable automatic bin adjustment for transmit signal.
RxBinAdjust	Enable or disable automatic bin adjustment for receive signal.
TxStartBin	Lowest bin number allowed for transmit signal
TxEndBin	Highest bin number allowed for transmit signal.
RxStartBin	Lowest bin number allowed for receive signal

Field	Description
RxEndBin	Highest bin number allowed for receive signal.
Fast Retrain	Enable or disable fast retrain capability.
Esc Fast Retrain	Enable or disable escape to fast retrain capability.
MaxBits/bin On Rx	Maximum number of receive bits per bin.
Bit Swap	Enable or disable bit swapping,
Dual Latency	Enable or disable dependant upon support of dual latency. Valid only for T1.413 and G.DMT.
Pmode	If enable, use the upstream pilot for data if the CO is Conexant.
Pilot Request	Enable or disable request for pilot tone during training.
Last Failed Status	This value is reset to 0 each time a startup is attempted. If there is a failure, it indicates the reason for the failure.
Oper Status	Operational status of the transceiver. Values include *Idle, Showtime/Data, Bootup Load, Startup HShake, Startup Trning, Framer Sync, Lcl Anlg Lpbk, Lcl Dig Lpbk, Spectrum Test*.
Startup Progress	Detailed startup information to be used for debugging.
AC Mode item	This specifies the Annex C mode item
AC Ttr R Offset	This specifies the Annex C Ttr R Offset
AC Pilot Request	This specifies the Annex C Pilot Request.
EC Fdm Mode	This specifies the Echo Cancellation Fdm mode.
Max Down Rate	This specifies the Maximum Down Rate.

Caution None.

See Also

- *modify dsl config*
- *get dsl params*

3.140 get dsl params

Description Use this command to get DSL parameters

Command Syntax ***get dsl params***

Parameters None.

Mode Super-User.

Example ***$ get dsl params***

Output

```
Vendor ID              : 00B5GSPN
Revision Number        : R67.3.3
Serial number          : 123456789abcdx
Self Test             : Passed           Framing Structure   : Framing-0
Standard               : T1.413           Trellis Coding      : Disable
Local Tx. Power(dB)    :  0.0             Remote Tx. Power(dB): 0.0
Local Line Atten(dB)   :  0.5             Remote Line Atten(dB): 0.5
Local SNR Margin(dB)   : 0.0              Remote SNR Margin(dB): 0.0
Up SValue              : 0                Down SValue          : 0
Up DValue              :  0               Down DValue          : 0

                    UpIntrlvd   UpFast   DownIntrlvd  DownFast
AS0(kbps):             -          -         128          96
AS1(kbps):             -          -         192         160
LS0(kbps):           576        544          -           -
LS1(kbps):           640        608          -           -
RValue    :            0          0          0           0
```

Output field description

Field	Description
Vendor ID	Vendor ID
Revision Number	OEM's product revision number
Self Test	Indicates whether DSL line has passed self-test. Can be passed or failed.
Serial Number	Serial number of unit
Local Line Atten	Local Line Attenuation - Indicates line attenuation where the attenuation is the difference in dB between the power received at the near-end and that transmitted from the far-end. Received signal power in dBm is the sum of all data carrying (i.e. b i >0) DMT subcarrier powers averaged over a one second period. The attenuation ranges from 0 to 63.5 dB in 0.5 dB increments.

Field	Description
Local SNR Margin	Local Signal to Noise Ration (SNR) Margin which represents the amount of increased received noise (in dB) relative to the noise power that the system is designed to tolerate and still meet the target BET of 10 -7 , accounting for all coding gains included in the design. The SNR ranges from -64.0 dB to +63.5dB in 0.5 dB increments.
NearSEF	Count of near-end severely errored frame defects
NearLOS	Count of near-end loss of signal defects
FarSEF	Count of far-end severely errored frame defects
FarLOS	Count of far-end loss of signal defects
NearFECInterleave	Count of near-end Reed-Solomon forward error corrections for the interleaved data stream
NearFECFast	Count of near-end Reed-Solomon forward error corrections for the fast data stream
FarFECInterleave	Count of far-end Reed-Solomon forward error corrections for the interleaved data stream
FarFECFast	Count of far-end Reed-Solomon forward error corrections for the fast data stream
NearCRCInterleave	Count of CRC near-end (cyclic redundancy check) anomalies for the interleaved data stream
NearCRCFast	Count of near-end CRC (cyclic redundancy check) anomalies for the fast data stream
FarCRCInterleave	Count of CRC far-end (cyclic redundancy check) anomalies for the interleaved data stream
FarCRCFast	Count of far-end CRC (cyclic redundancy check) anomalies for the fast data stream
NearNCDInterleave	Count of near-end no cell delineation for the interleaved data stream. Counts until in synch for the first time.
NearNCDFast	Count of near-end no cell delineation for the fast data stream. Counts until in synch for the first time.
FarNCDInterleave	Count of far-end no cell delineation for the interleaved data stream. Counts until in synch for the first time.
FarNCDFast	Count of far-end no cell delineation for the fast data stream. Counts until in synch for the first time.
NearHECInterleave	Near-end header error check counter for the interleaved data stream
NearHECFast	Near-end header error check counter for the fast data stream
FarHECInterleave	Far-end header error check counter for the interleaved data stream
FarHECFast	Far-end header error check counter for the fast data stream

Field	Description
Local SNR Margin	Local Signal to Noise Ration (SNR) Margin which represents the amount of increased received noise (in dB) relative to the noise power that the system is designed to tolerate and still meet the target BET of 10 -7 , accounting for all coding gains included in the design. The SNR ranges from -64.0 dB to +63.5dB in 0.5 dB increments.
NearSEF	Count of near-end severely errored frame defects
NearLOS	Count of near-end loss of signal defects
FarSEF	Count of far-end severely errored frame defects
FarLOS	Count of far-end loss of signal defects
NearFECInterleave	Count of near-end Reed-Solomon forward error corrections for the interleaved data stream
NearFECFast	Count of near-end Reed-Solomon forward error corrections for the fast data stream
FarFECInterleave	Count of far-end Reed-Solomon forward error corrections for the interleaved data stream
FarFECFast	Count of far-end Reed-Solomon forward error corrections for the fast data stream
NearCRCInterleave	Count of CRC near-end (cyclic redundancy check) anomalies for the interleaved data stream
NearCRCFast	Count of near-end CRC (cyclic redundancy check) anomalies for the fast data stream
FarCRCInterleave	Count of CRC far-end (cyclic redundancy check) anomalies for the interleaved data stream
FarCRCFast	Count of far-end CRC (cyclic redundancy check) anomalies for the fast data stream
NearNCDInterleave	Count of near-end no cell delineation for the interleaved data stream. Counts until in synch for the first time.
NearNCDFast	Count of near-end no cell delineation for the fast data stream. Counts until in synch for the first time.
FarNCDInterleave	Count of far-end no cell delineation for the interleaved data stream. Counts until in synch for the first time.
FarNCDFast	Count of far-end no cell delineation for the fast data stream. Counts until in synch for the first time.
NearHECInterleave	Near-end header error check counter for the interleaved data stream
NearHECFast	Near-end header error check counter for the fast data stream
FarHECInterleave	Far-end header error check counter for the interleaved data stream
FarHECFast	Far-end header error check counter for the fast data stream

Field	Description
NearOCDInterleave	Count of near-end out of cell delineation for the interleaved data stream. Counts if has been in synch, then becomes out of synch.
NearOCDFast	Count of near-end out of cell delineation for the fast data stream. Counts if has been in synch, then becomes out of synch.
Remote Line Atten	Remote Line Attenuation - Indicates remote line attenuation where the attenuation is the difference in dB between the power received at the near-end and that transmitted from the far-end. Received signal power in dBm is the sum of all data carrying (i.e. b i >0) DMT subcarrier powers averaged over a one second period. The attenuation ranges from 0 to 63.5 dB in 0.5 dB increments.
Remote SNR Margin	Remote Signal to Noise Ration (SNR) Margin which represents the amount of increased received noise (in dB) relative to the noise power that the system is designed to tolerate and still meet the target BET of 10 -7 , accounting for all coding gains included in the design. The SNR ranges from -64.0 dB to +63.5dB in 0.5 dB increments.
Standard	Actual standard of the DSL line.
Trellis Coding	Actual Trellis Coding
Local Tx Power(dB)	Local Transmit Power.
Framing Structure	Actual framing structure.
Rvalue UpIntrlvd	Number of redundant bytes per ReedSolomon code word for the interleaved buffer in the upstream direction.
Rvalue UpFast	Number of redundant bytes per ReedSolomon code word for the fast buffer in the upstream direction.
Rvalue DownIntrlvd	Number of redundant bytes per ReedSolomon code word for the interleaved buffer in the downstream direction.
Rvalue DownFast	Number of redundant bytes per ReedSolomon code word for the fast buffer in the downstream direction.

Caution None.

References

- *modify dsl config* command
- *get dsl config* command

3.141 get dsl stats cntrs

Description Get DSL statistics error counters.

Command Syntax ***get dsl stats cntrs***

Parameters None.

Mode User and Super-User.

Example ***$ get dsl stats cntrs***

Output Verbose Mode On

```
Near SEF             : 0             Near LOS          : 0
Far SEF              : 0             Far LOS           : 0
Near FEC Interleave  : 0             Near FEC Fast     : 0
Far FEC Interleave   : 0             Far FEC Fast      : 0
Near CRC Interleave  : 0             Near CRC Fast     : 0
Far CRC Interleave   : 1             Far CRC Fast      : 0
Near NCD Interleave  : 0             Near NCD Fast     : 0
Far NCD Interleave   : 0             Far NCD Fast      : 0
Near HEC Interleave  : 0             Near HEC Fast     : 0
Far HEC Interleave   : 0             Far HEC Fast      : 0
Near OCD Interleave  : 0             Near OCD Fast     : 0
```

Verbose Mode Off

```
Near SEF             : 0             Near LOS          : 0
Far SEF              : 0             Far LOS           : 0
Near FEC Interleave  : 0             Near FEC Fast     : 0
Far FEC Interleave   : 0             Far FEC Fast      : 0
Near CRC Interleave  : 0             Near CRC Fast     : 0
Far CRC Interleave   : 1             Far CRC Fast      : 0
Near NCD Interleave  : 0             Near NCD Fast     : 0
Far NCD Interleave   : 0             Far NCD Fast      : 0
Near HEC Interleave  : 0             Near HEC Fast     : 0
Far HEC Interleave   : 0             Far HEC Fast      : 0
Near OCD Interleave  : 0             Near OCD Fast     : 0
```

Output field description

Field	Description
NearSEF	Count of near-end severely errored frame defects.
NearLOS	Count of near-end loss of signal defects.
FarSEF	Count of far-end severely errored frame defects.
FarLOS	Count of far-end loss of signal defect.
NearFECInterleave	Count of near-end Reed-Solomon forward error corrections for the interleaved data stream.
NearFECFast	Count of near-end Reed-Solomon forward error corrections for the fast data stream.
FarFECInterleave	Count of far-end Reed-Solomon forward error corrections for the interleaved datastream.
FarFECFast	Count of far-end Reed-Solomon forward error corrections for the fast data stream.
NearCRCInterleave	Count of CRC near-end (cyclic redundancy check) anomalies for the interleaved datastream.

Field	Description
NearCRCFast	Count of near-end CRC (cyclic redundancy check) anomalies for the fast data stream.
FarCRCInterleave	Count of CRC far-end (cyclic redundancy check) anomalies for the interleaved datastream.
FarCRCFast	Count of far-end CRC (cyclic redundancy check) anomalies for the fast data stream.
NearNCDInterleave	Count of near-end no cell delineation for the interleaved data stream.
NearNCDFast	Count of near-end no cell delineation for the fast data stream.
FarNCDInterleave	Count of far-end no cell delineation for the interleaved data stream.
FarNCDFast	Count of far-end no cell delineation for the fast data stream.
NearHECInterleave	Near-end header error check counter for the interleaved data stream.
NearHECFast	Near-end header error check counter for the fast data stream.
FarHECInterleave	Far-end header error check counter for the interleaved data stream.
FarHECFast	Far-end header error check counter for the fast data stream.
NearOCDInterleave	Count of near-end out of cell delineation for the interleaved data stream.
NearOCDFast	Count of near-end out of cell delineation for the fast data stream.

Caution None.

References

- *reset dsl stats cntrs* command

3.142 get dsl stats curr

Description Get DSL current performance data.

Command Syntax ***get dsl stats curr***

Parameters None.

Mode User

Example ***$ get dsl stats curr***

Output Verbose mode on

```
No. of 15 Min. Valid Data Intervals    : 5
No. of 15 Min. Invalid Data Intervals  : 1
Current 15 Min. Elapsed Time (MM:SS)   : 5:10
Current 15 Min. Errored Seconds        : 0
Current 15 Min. Sev Errored Seconds    : 0
Current 15 Min. Unavailable Seconds    : 0
Current Day Elapsed Time (HH:MM:SS)    : 0:80:10
Current Day Errored Seconds            : 0
Current Day Sev Errored Seconds        : 0
Current Day Unavailable Seconds        : 0
Previous Day Monitored Time (HH:MM:SS) : 0:0:0
 Previous Day Errored Seconds            : 0
Previous Day Sev Errored Seconds       : 0

Previous Day Unavailable Seconds       : 0
```

Verbose Off

```
No. of 15 Min. Valid Data Intervals    : 5
No. of 15 Min. Invalid Data Intervals  : 0
Current 15 Min. Elapsed Time (MM:SS)   : 5:10
Current 15 Min. Errored Seconds        : 0
Current 15 Min. Unavailable Seconds    : 0
Current Day Elapsed Time (HH:MM:SS)    : 0:80:10
Current Day Errored Seconds            : 0
Current Day Unavailable Seconds        : 0
Previous Day Monitored Time (HH:MM:SS) : 0:0:0
Previous Day Errored Seconds           : 0
Previous Day Unavailable Seconds       : 0
```

Output Field Description

Field	Description
No.of 15 Min. Valid Data Intervals	The number of previous 15-minute intervals for which data was collected.
No. of 15 Min Invalid Data Interval	The number of intervals in the range from 0 to the value of "No. of 15 Min. Valid Data Intervals" for which no data is available. This value will typically be zero except in cases where the data for some intervals are not available
Current 15 Min. Elapsed Time (MM:SS)	Total elapsed time in this interval.

Field	Description
Current 15 Min. Errored Seconds	Count of errored seconds in the current 15-minute interval.
Current 15 Min. Unavailable Seconds	Count of unavailable seconds in the current 15-minute interval.
Current Day Elapsed Time (HH:MM:SS)	Time elapsed since the beginning of the current 1-day interval.
Current Day Errored Seconds	Count of errored seconds in the current 1-day interval.
Current Day Unavailable Seconds	Count of unavailable seconds in the current 1-day interval.
Previous Day Monitored Time (HH:MM:SS)	The amount of time in the previous 1-day interval over which the performance monitoring information is actually counted.
Previous Day Errored Seconds	Count of errored seconds in the previous 1-day interval.
Previous Day Unavailable Seconds	Count of unavailable seconds in the previous 1-day interval.
Current 15 Min. Sev Errored Seconds	Count of severely errored seconds in the current 15-minute interval.
Current Day Sev Errored Seconds	Count of severely errored seconds in the current 1-day interval
Previous Day Sev Errored Seconds	Count of severely errored seconds in the previous 1-day interval

Caution None.

References

- *get dsl stats hist* command

3.143 get dsl stats flrs

Description Use this command to get DSL statistics failures.

Command Syntax ***get dsl stats flrs***

Parameters None.

Mode Super User, User

Example ***$ get dsl stats flrs***

Output Verbose mode on/off

```
Local LOS Fail : 10         Remote LOS Fail : 30
Local SEF Fail : 20         Remote SEF Fail : 50
Local NCD Fail : 5          Remote NCD Fail : 10
Local LCD Fail : 15         Remote LCD Fail : 30
```

Output Field Description

Field	Description
Local LOS Fail	The count of near-end loss of signal. A DSL failure will occur if this counter surpasses 127.
Remote LOS Fail	The count of far-end, loss of signal. A DSL failure will occur if this counter surpasses 127.
Local SEF Fail	The count of near-end severely errored frames. A DSL failure will occur if this counter surpasses 127
Remote SEF Fail	The count of far-end, severely errored frames. A DSL failure will occur if this counter surpasses 127.
Local NCD Fail	The count of near-end, no cell delineation for data stream. Counts until in sync for the first time .A DSL failure will occur if this counter surpasses 127
Remote NCD Fail	The count of far-end, no cell delineation for data stream. Counts until in sync for the first time. A DSL failure will occur if this counter surpasses 127
Local LCD Fail	The count of near-end, loss of cell delineation for data stream. Counts loss of cell delineation after being in sync. A DSL failure will occur if this counter surpasses 127
Remote LCD Fail	The count of far-end, loss of cell delineation for data stream. Counts loss of cell delineation after being in sync. A DSL failure will occur if this counter surpasses 127

Caution None.

References

- *reset dsl stats flrs* command

3.144 get dsl stats hist

Description Get DSL history (previous intervals) performance data

Command Syntax ***get dsl stats hist [sintrvl*** start-interval-number***] [nintrvl*** num-of-intervals***]***

Parameters

Name	Description
Sintvl start-interval-number	First interval number from which data is to be displayed. **Type:** Optional **Valid values:** *1* to *96* **Default value:** *1*
nintvl num-of-intervals	Number of intervals for which data is to be displayed. **Type:** Optional **Valid values:** *1* to *96* **Default value:** *12*

Mode User

Example ***$ get dsl stats hist sintrvl 10 nintrvl 3***

Output Verbose mode on

```
IntrvlNo    ErroredSecs    SevErroredSecs    UnavailSecs   Valid Data
-----------------------------------------------------------------
10          2              1                 0             Valid
11          0              0                 0             Valid

12          0              0                 0             Invalid
```

Verbose Off

```
IntrvlNo    ErroredSecs    SevErroredSecs    UnavailSecs   Valid Data
-----------------------------------------------------------------
10          2              1                 0             Valid
11          0              0                 0             Valid

12          0              0                 0             Invalid
```

Output Field Description

Field	Description
Intrvl No	Performance history data interval number. Interval number 1 is the most recent previous interval. Interval number 96 is 24 hours ago.
Errored Secs	Count of errored seconds in this interval.
Sev Errored Secs	Count of severely errored seconds in this interval.
Unavail Secs	Count of unavailable seconds in this interval.
Valid Data	Indicates if the data for this interval is valid or invalid.

Caution None.

References

- *get dsl stats curr* command

3.145 get eoa intf

Description Use this command to get information on a particular eoa interface or on all the eoa interfaces.

Command Syntax ***get eoa intf [ifname*** interface-name***]***

Parameters

Name	Description
ifname interface-name	This parameter specifies the interface for which information is desired. In case the field is not specified, then the information for all valid eoa interfaces is displayed. **Type:** Optional **Valid values:** *eoa-0 - *, etc.*

Mode Super-User, User

Example ***$ get eoa intf ifname eoa-0***

Output

```
IfName                : eoa-0              Interface Sec Type: public
Configured IP Address : 192.168.1.1        Mask              : 255.255.255.0
Low IfName            : aal5-0             NAT Direction     : None
Gateway               : 172.25.12.1        Droute            : True
Oper Status           : Down               Admin Status      : Up
UseDHCP               : true
Configured MTU        : 500                Actual MTU        : 300
```

Output field description

Field	Description
IfName	The name of the interface for which information is being displayed.
Configured IpAddress	IP address assigned to the EoA interface.
Mask	Network mask to be applied to the IP Address.
LowIfName	Specifies the lower interface.
NatDir	This specifies the NAT direction which may be: *inside, outside* or *none*.
OperStatus	The actual/current state of the interface. It can be either *Up* or *Down*
AdminStatus	The desired state of the interface. It may be either *Up* or *Down*
UseDhcp	Whether or not a DHCP client is used to obtain the IP address for this interface from a DHCP server
Droute	Default Route
Interface Sec Type	Interface security type.

Field	Description
Configured MTU	This specifies the MTU value configured by the user for the EOA interface.
Actual MTU	This specifies the MTU value actually operational for the EOA interface.

Caution None.

References

- *create eoa intf* command
- *delete eoa intf* command
- *modify eoa intf* command
- *eoa stats* related commands
- *interface stats* related commands.

3.146 get ethernet intf

Description Use this command to get information on a particular Ethernet interface or on all the interfaces.

Command Syntax ***get ethernet intf [ifname*** interface-name***]***

Parameters

Name	Description
ifname interface-name	This parameter specifies the interface for which information is desired. In case the field is not specified, then the information for all valid ethernet interfaces is displayed. **Type:** Optional **Valid values:** *eth-0*, *veth-0 - **, *veth-2*, *veth-3*

Mode Super-User, User

Example ***$ get ethernet intf ifname*** **veth-0**

Output

```
Interface          : veth-0              MTU                  : 300
Interface Sec Type : Public              Configured IP Address : 192.168.1.1
Mask               : 255.255.255.0       UseDhcp              : False
Physical Interface : eth-0               Nat Direction        : None
Duplex             : half                Speed                : 10BT
Operational Status : Up                  Admin Status         : Up
```

Output field description

Field	Description
Interface	The name of the interface which has been created.
Interface Sec Type	Interface security type.
Configured Ip Address	IP address assigned to the Ethernet port.
Mask	Network mask to be applied to the IP Address.
UseDhcp	Local: IP address for this interface is obtained from a local DHCP server Remote: DHCP client is used to obtain the IP address for this interface from a remote DHCP server False: DHCP client is not used.
Physical Interface	Valid only in case of virtual interfaces i.e. the Type is not *eth*. It can only be *eth-0*
Nat Direction	This specifies the NAT direction which may be: *inside, outside or none*.
Duplex	The duplex mode used by the interface.
Speed	Line speed used by Ethernet interface

Field	Description
Operational Status	The actual/current state of the interface. It can be either *up* or d*own*
Admin Status	The desired state of the interface. It may be either *up* or *down*
MTU	This specifies the MTU Size configured on ethernet interface

Caution None.

References

- *create ethernet intf* command
- *delete ethernet intf* command
- *modify ethernet intf* command
- *ethernet stats* related commands
- *interface stats* related commands

3.147 get ethernet stats

Description Use this command to get statistics on a particular Ethernet interface or on all the Ethernet interfaces.

Command Syntax ***get ethernet stats [ifname*** interface-name***]***

Parameters

Name	Description
ifname interface-name	This parameter specifies the interface for which information is desired. In case the field is not specified, then the information for all valid ethernet interfaces should be displayed. **Type:** Optional **Valid values:** *eth-0, veth-0 - **

Mode Super-User, User

Example ***$ get ethernet stats ifname eth-0***

Output

```
If Name                       : eth-0
Align Error count             : 0      FCS Error count             : 0
Single Collisn Frame count    : 0      Two Collisn Frame Count     : 30
SQE Test Errors count         : 2      Deferred Transaction count  : 0
Late Collisn count            : 0      Excess Collisn count        : 0
Internal MAC Rx Errs count    : 5      Internal MAC Tx Errs count  : 0
Carrier Sense Errs count      : 0      Frame Too Long count        : 0
Tx count                      : 0      Rx count                    : 0
Control Pause count           : 0      Total Collisn count         : 0
```

Output field description

Field	Description
If Name	The interface name
Align Error count	This is a count of frames received on the interface that are not an integral number of octets in length and do not pass the FCS (Frame Check Sequence) check.
FCS Error count	This is a count of frames received on the interface that are an integral number of octets in length but do not pass the FCS check.
Single Collision Frame count	This is a count of successfully transmitted frames on the interface for which transmission is inhibited by exactly one collision.
Two Collisn Frame Count	This is a count of successfully transmitted frames on the interface for which transmission is inhibited by two collisions.

Field	Description
SQE Test Errors count	This is a count of times that the SQE TEST ERROR message is generated by the PLS sublayer for the interface. The SQE TEST ERROR message is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985 and its generation is described in section 7.2.4.6 of the same document. Ref. ANSI/IEEE Std 802.3-1985 Carrier Sense Multiple Access with Collision Detection Access Method and Physical Layer Specifications
Deferred Transactions count	This is a count of frames for which the first transmission attempt on the interface is delayed because the medium is busy
Late Collisions count	This is the number of times that a collision is detected on the interface later than 512 bit-times into the transmission of a packet
Excess Collisions count	This is a count of frames for which transmission on the interface fails due to excessive collisions
Internal MAC Rx Errors count	This is a count of frames for which reception on the interface fails due to an internal MAC sublayer receive error
Internal MAC Tx Errors count	This is a count of frames for which transmission on the interface fails due to an internal MAC sublayer transmit error
Carrier Sense Errors count	This is the number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on the interface
Frame Too Long	This is a count of frames received on the interface that exceed the maximum permitted frame size
Tx count	Count of Ethernet packets transmitted.
Rx count	Count of Ethernet packets received.
Control Paus count	TBD
Total Collision count	This is a count of frame collisions.

Caution None.

References

- *ethernet intf* related commands
- *interface stats* command

3.148 get fwl blacklist

Description Use this command to get information on a blacklisted host

Command Syntax ***get fwl blacklist [ip <ddd.ddd.ddd.ddd>]***

Parameters

Name	Description
ip <ddd.ddd.ddd.ddd>	This specifies the IP address of the blacklisted host. ***Type****: Optional* ***Valid values*** *: 0.0.0.0 - 255.255.255.255*

Mode User

Example ***$ get fwl blacklist***

Output Verbose Mode on:

```
IP Address      Blacklist Reason    RuleId     Time Left(sec)
-------------------------------------------------------------
172.25.7.8      Ping of Death        1             20
172.25.45.7     Ping of Death        2             10
```

Verbose Mode off:

```
IP Address      Blacklist Reason    RuleId     Time Left(sec)
-------------------------------------------------------------
172.25.7.8      Ping of Death        1             20
172.25.45.7     Ping of Death        2             10
```

Output field description

Field	Description
IP Address	This specifies the IP address of the blacklisted host.
Blacklist Reason	This specifies the reason for blacklisting the host.
RuleId	This specifies the firewall rule id which caused the blacklisting.
Time Left(sec)	This is a count of successfully transmitted frames on the interface for which transmission is inhibited by exactly one collision.

Caution None.

References

- *delete fwl blacklist* command.

3.149 get fwl global

Description Use this command to get global information of IP Firewall

Command Syntax ***get fwl global]***

Parameters None

Mode User

Example ***$ get fwl global***

Output Verbose Mode on:

```
Attack Protection     : Disable       Max Half Open TCP Conn (%)  : 25
DOS Protection         : Disable      Max ICMP Conn (%)       : 25
Blacklist Status       : Enable        Max Single Host Conn(%): 100
Blacklist Period (min): 10             Min Log Time(min)       :10
Log Destination        : Email
E-Mail 1               : xyz@hotmail.com
E-Mail 2               : pqr@excite.com
E-Mail 3               : abc@hotmail.com
```

Verbose Mode off:

```
Attack Protection     : Disable       Max Half Open TCP Conn (%)  : 25
DOS Protection         : Disable       Max ICMP Conn (%)        : 25
Blacklist Status       : Enable        Max Single Host Conn(%): 100
Blacklist Period (min): 10             Min Log Time(min)       :10
Log Destination        : Email
E-Mail 1               : xyz@hotmail.com
E-Mail 2               : pqr@excite.com
E-Mail 3               : abc@hotmail.com
```

Output field description

Field	Description
Attack Protection	This specifies the status of attack protection in firewall.
DOS Protection	This specifies the status of DOS protection in firewall.
Blacklist Status	This specifies the status of Blacklist protection in firewall.
Blacklist Period (min)	It specifies the duration to blacklist an attacking host.
Min Log Time (min)	It specifies the minimum time between logging of an individual attack.
Max Half Open TCP Conn (%)	It specifies the % of total connections that can be in a TCP half open state.
Max ICMP Conn (%)	It specifies the % of total connections that can be ICMP connections.

Field	Description
Max Single Host Conn (%)	It specifies % of connections from a single host.
Log Destination	This specifies the destination type for firewall logs.
E-Mail 1	This field specifies the email address of the firewall administrator1
E-Mail 2	This field specifies the email address of the firewall administrator2
E-Mail 3	This field specifies the email address of the firewall administrator3

Caution None.

References

- *modify fwl global* command.

3.150 get fwl stats

Description Use this command to get firewall statistics.

Command Syntax ***get fwl stats***

Parameters None

Mode User, Super-User

Example ***$ get fwl stats***

Output Verbose Mode on/off

```
Sessions Used : 13 ICMP Sessions : 3
Half Open TCP Sessions: 10

Attack type    Time Stamp at last log          After Log        Total
              (Day Mon date HH:MM:SS YYYY)     (count)          (count)
-------------------------------------------------------------------------
Tear Drop          Tue Jan 01 01:00:06 2002        10            12
Ping of death      Wed Jan 02 02:04:06 2002        10            12
IP Spoof           Thu Jan 03 03:04:06 2002        12            15
Land Attack        Fri Jan 04 02:00:06 2002        13            14
TCP SYN DOS        Fri Jan 04 03:04:06 2002        15            19
ICMP DOS           Sat Jan 06 02:04:06 2002         2             4
Sngl host DOS      Sun Jan 07 01:01:06 2002         6             8
Smurf Attack       Mon Jan 08 02:03:07 2002         6             9
Frag ScanTue       Jan 01 01:00:06 2002            10            12
TCP Sess Scan      Wed Jan 02 02:04:06 2002        10            12
TCP SYN ACK Scan   Thu Jan 03 03:04:06 2002        12            15
TCP ACK Scan       Fri Jan 04 02:00:06 2002        13            14
TCP FIN Scan       Fri Jan 04 03:04:06 2002        15            19
TCP RST Scan       Sat Jan 06 02:04:06 2002         2             4
TCP NULL Scan      Sun Jan 07 01:01:06 2002         6             8
TCP XMAS Scan      Mon Jan 08 02:03:07 2002         4             9
UDP Scan           Sun Jan 07 01:01:06 2002         7             8
ICMP Scan          Mon Jan 08 02:03:07 2002         6             9
```

Output field description

Field	Description
Sessions Used	This specifies the number of sessions currently used.
ICMP Sessions	This specifies the number of ICMP sessions currently created
Half Open TCP Sessions	This specifies the number of Half open TCP sessions currently created
Attack type	This specifies the type of attack.
Time Stamp at last log	This is the time stamp taken when last time logging was done.

Field	Description
After Log	This specifies the total number of attacks since last time logging was done.
Total	This specifies the total number of attacks of this type.

Caution None.

References

- *reset fwl stats* command.

3.151 get hdlceoc cfg

Description Use this command to get HDLC Global Configuration

Command Syntax ***get hdlceoc cfg***

Parameter None

Mode Super-User, User

Example ***$ get hdlceoc cfg***

Output

```
HDLC Status           SAR Status
-----------------------------------------
disable               disable
```

Output field description

Field	Description
HDLC over DSL Status	This provides Administrative control to enable/disable the HDLC over DSL channel on the modem.
SAR Status	This provides control to enable/disable SAR(Segmentation & reassembly) of HDLC frames.

Caution None

References

- *modify hdlceoc cfg* command

3.152 get hdlceoc stats

Description Use this command to get HDLC Statistics

Command Syntax ***get hdlceoc stats***

Parameter None

Mode Super-User, User

Example ***$ get hdlceoc stats***

Output

```
Successfully Tx Frames : 100        Dropped Tx Frames : 1
Successfully Tx Bytes  : 1024       Dropped Tx Bytes  : 10
Successfully Rx Frames : 100        Dropped Rx Frames : 3
Successfully Rx Bytes  : 2048       Dropped Rx Bytes  : 100
```

Output field description

Field	Description
Successfully Tx Frames	Frames successfully transmitted.
Dropped Tx Frames	Frames dropped in transmit direction.
Successfully Tx Bytes	Bytes successfully transmitted.
Dropped Tx Bytes	Bytes dropped in transmit direction(due to dropped frames).
Successfully Rx Frames	Frames successfully received.
Dropped Rx Frames	Frames dropped in the receive direction.
Successfully Rx Bytes	Bytes successfully received.
Dropped Rx Bytes	Bytes dropped in receive direction(due to dropped frames).

Caution None

References

- *reset hdlceoc stats* command.

3.153 get host info

Description Use this command to get information about various IP sessions on the host

Command Syntax ***get host info [ip <ipaddress>]***

Parameters

Name	Description
ip <ipaddress>	This parameter specifies the ip address of the host. **Type:** Optional **Valid Values:** valid ip address..

Mode User, Super-User.

Example ***$ get host info ip 102.11.11.11***

Output Verbose Mode on:

```
ipaddress                    Session Used
-----------------------------------------
102.11.11.11                  13
```

Output field description

Field	Description
ipaddress	This specifies the IP Address of host.
Session Used	This specifies the number of sessions currently used for this host.

Caution None.

References None.

3.154 get icmp stats

Description Use this command to display ICMP statistics.

Command Syntax ***get icmp stats***

Parameters None.

Mode Super-User, User

Example ***$ get icmp stats***

Output

```
In Msgs                 : 0          Out Msgs                : 0
In Errors               : 0          Out Errors              : 0
Dest Unreach Msgs Rcvd  : 0          Dest Unreach Msgs Sent  : 0
Time Exceeded Msgs Rcvd : 0          Time Exceeded Msgs Sent : 0
Param Problem Msgs Rcvd : 0          Param Problem Msgs Sent : 0
Source Quench Msgs Rcvd : 0          Source Quench Msgs Sent : 0
Redirect Msgs Rcvd      : 0          Redirect Msgs Sent      : 0
Echo Msgs Rcvd          : 0          Echo Msgs Sent          : 0
Echo Reply Msgs Rcvd    : 0          Echo Reply Msgs Sent    : 0
Timestamp Msgs Rcvd     : 0          Timestamp Msgs Sent     : 0
Timestamp Rep Msgs Rcvd : 0          Timestamp Rep Msgs Sent : 0
Addr Mask Req Msgs Rcvd : 0          Addr Mask Req Msgs Sent : 0
Addr Mask Rep Msgs Rcvd : 0          Addr Mask Rep Msgs Sent : 0
```

Output field description

Field	Description
In Msgs	The total number of ICMP messages which the entity received
Out Msgs	The total number of ICMP messages which this entity attempted to send
In Errors	The number of ICMP messages which the entity received but determined as having ICMP-specific errors
Out Errors	The number of ICMP messages which this entity did not send due to problems discovered within ICMP such as a lack of buffers
Dest Unreach Msgs Rcvd	The number of ICMP Destination Unreachable messages received
Dest Unreach Msgs Sent	The number of ICMP Destination Unreachable messages sent
Time Exceeded Msgs Rcvd	The number of ICMP Time Exceeded messages received
Time Exceeded Msgs Sent	The number of ICMP Time Exceeded messages sent
Param Problem Msgs Rcvd	The number of ICMP Parameter Problem messages received.
Param Problem Msgs Sent	The number of ICMP Parameter Problem messages sent.

Field	Description
Source Quench Msgs Rcvd	The number of ICMP Source Quench messages received.
Source Quench Msgs Sent	The number of ICMP Source Quench messages sent
Redirect Msgs Rcvd	The number of ICMP Redirect messages received
Redirect Msgs Sent	The number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects
Echo Msgs Rcvd	The number of ICMP Echo (request) messages received
Echo Msgs Sent	The number of ICMP Echo (request) messages sent
Echo Reply Msgs Rcvd	The number of ICMP Echo Reply messages received.
Echo Reply Msgs Sent	The number of ICMP Echo Reply messages sent
Timestamp Msgs Rcvd	The number of ICMP Timestamp (request) messages received
Timestamp Msgs Sent	The number of ICMP Timestamp (request) messages sent
Timestamp Rep Msgs Rcvd	The number of ICMP Timestamp (reply) messages received
Timestamp Rep Msgs Sent	The number of ICMP Timestamp Reply messages sent
Addr Mask Req Msgs Rcvd	The number of ICMP Address Mask Request messages received
Addr Mask Req Msgs Sent	The number of ICMP Address mask Request messages sent
Addr Mask Rep Msgs Rcvd	The number of ICMP Address Mask Reply messages received
Addr Mask Rep Msgs Sent	The number of ICMP Address Mask Reply messages sent

Caution None.

References

- *TCP* and *UDP* commands
- *get ip stats* command

3.155 get igmp intf

Description Use this command to get information on an IGMP interface for a given interface or for all interfaces.

Command Syntax ***get igmp intf [ifname*** <interface-name>***]***

Parameters

Name	Description
ifname <interface-name>	This identifies the interface on which IGMP related information is required. **Type:** Optional **Valid values:** *eth-0*, *veth-0 - **, *ppp-0 - * …*, *eoa-0 - **, *usb-0, ipoa-0-** **Default value:** *none*

Mode Super-User, User

Example ***$ get igmp intf ifname eth-0***

Output Verbose Mode On

```
IfName                  : eth-0              Type                      : Host
Version                 : igmpv1             Query Interval(sec)       : 150
Query Max Resp Time(sec): 10                 Last Memb QueryIntvl(sec) : 2
Robustness              : 10                 Join Requests             : 10
Current Groups          : 8
```

Verbose Mode Off

```
IfName                  : eth-0              Type                      : Host
Version                 : igmpv1             Query Interval(sec)       : 150
Query Max Resp Time(sec): 10                 Last Memb QueryIntvl(sec) : 2
Robustness              : 10                 Join Requests             : 10
Current Groups          : 8
```

Output field description

Field	Description
Query Interval(sec)	This is the periodic interval at which host-query messages (queries) are transmitted on this interface
Version	This field specifies the version of IGMP.
Query Max ResponseTime(sec)	This field specifies the query max response time (in secs)
Last Memb QueryIntvl(sec)	This field specifies the Last Member Query Interval (in secs).
Join Requests	This is the number of times a group membership has been added to this interface
Current Groups	This is the current number of entries for this interface in the IGMP Group Table.

Caution None.

References

- *delete igmp intf* command
- *get igmp groups* command
- *create igmp intf* command

3.156 get igmp groups

Description Use this command to list information on all IP multicast groups.

Command Syntax

```
get igmp groups [grpaddr <ddd.ddd.ddd.ddd>]
[ifname <interface-name>]
```

Parameters

Name	Description
Grpaddr <ddd.ddd.ddd.ddd>	This is the IP multicast group address for which information is required. **Type:** Optional
ifname <interface-name>	This identifies the interface for an IP multicast group for which information is required. **Type:** Optional

Mode Super-User, User

Example

```
$ get igmp groups grpaddr 224.25.2.1 ifname eth-0
```

Output Verbose Mode On

```
Group Address   IfName     Expiry Time (sec)
---------------------------------------------
224.25.2.1      eth-0      200
```

Verbose Mode Off

```
Group Address   IfName     Expiry Time (sec)
---------------------------------------------
224.25.2.1      eth-0      200
```

Output field description

Field	Description
Group Address	This is the IP multicast group address for which information is required.
Ifname	This identifies the interface for an IP multicast group for which information is required.
Expiry Time (sec)	The minimum amount of time remaining before this entry will be aged out.

Caution None.

References

- *delete igmp intf* command
- *get igmp intf* command
- *create igmp intf* command.

3.157 get ilmi access protocol

Description Use this command to get the protocol which has been configured by ILMI based auto configuration for a particular ATM VC

Command Syntax ***get ilmi access protocol [ifname*** interface-name***] [vpi*** vpi-num***] [vci*** vci-num***]***

Parameters

Name	Description
ifname interface-name	This specifies the ATM port for the VC(s) for which the access protocol is to be displayed. In case the field is not specified, then the information for all configured VCs is displayed. **Type:** Optional **Valid values:** *atm-0.*
vpi vpi-number	VPI of the VC(s) for which the access protocol is to be displayed. This can be specified only if *ifname* has also been specified. **Type:** Optional **Valid values:** *0-255* **Default value:** *0*
vci vci-number	VCI of the VC for which the access protocol is to be displayed. This can be specified only if *ifname* and *vpi* have also been specified. **Type:** Optional **Valid values:** *0-65535* **Default value:** *16*

Mode Super-User, User

Example ***$ get ilmi access protocol ifname atm-0 vpi 10 vci 5***

Output

```
Interface        : atm-0          VPI             : 10
VCI              : 5            Access Protocol   : PPPoA
```

Output field description

Field	Description
Interface	The ATM port of the VC for which information is being displayed.
VPI	VPI of the VC for which information is being displayed.
VCI	VCI of the VC for which information is being displayed.
Access Protocol	Protocol which has been configured by ILMI based auto configuration for the shown VC.

Caution None

References None.

3.158 get ilmi intf

Description Use this command to get ILMI based auto configuration information on a particular ATM port or on all ATM ports.

Command Syntax ***get ilmi intf [ifname*** interface-name***]***

Parameters

Name	Description
ifname interface-name	It specifies the ATM port for which ILMI based auto configuration information is desired. In case the field is not specified, then the information for all valid ATM ports will be displayed. **Type:** Optional **Valid values:** *atm-0.*

Mode Super-User, User

Example ***$ get ilmi intf ifname atm-0***

Output

```
Interface             : atm-0
Status                : Enable
VPI                   : 10
VCI                   : 5
Timeout(sec)          : 3
Keep Alive (sec)      : 5
Max Retries           : 11
Version               : 4.0
```

Output field description

Field	Description
Interface	It specifies the ATM port for which ILMI based auto configuration information is being shown.
Status	Whether ILMI based auto configuration is enabled or not on this interface.
VPI	VPI to be used for ILMI SNMP message exchanges
VCI	VCI to be used for ILMI SNMP message exchanges
Timeout	Timeout value for SNMP Get/ Set messages exchanged between peer Interface Management Entities (IMEs).
Keep Alive	The time-interval, ILMI should use to poll for peer ILMI's availability.
Max Retries	Number of times ILMI should retry before declaring ILMI connectivity as lost.
Version	The version of ILMI

Caution None.

References

- *create ilmi intf* command
- *modify ilmi intf* command
- *modify ilmi trigger* command
- *trigger ilmi* command
- *get ilmi access protocol* command

3.159 get interface stats

Description Use this command to view statistics for one interface or all the interfaces.

Command Syntax ***get interface stats [ifname*** interface-name***]***

Parameters

Name	Description
ifname interface-name	This uniquely identifies the Interface whose information is to be retrieved. If this is not specified then information for all interfaces is displayed. **Type:** Optional **Valid values:** *aal5-0 - *, eth-0, veth-0 to veth-3, ppp-0 - *, atm-0, eoa-0 - *, dsl, dsli, dslf, usb-0, ipoa-0-* - , l2t-**

Mode Super-User, User

Example ***$ get interface stats ifname*** **eth-0**

Output

```
Interface          : atm-0
Description        : atm-0
Type               : ATM        Mtu                          : 48
Bandwidth          : 1696000    Phy Adddr                    : 00:00:00:00:00:00
Admin Status       : Up         Operational Status           : Up
Last Change(sec)   : 35         Time since Last Change(sec): 3
In Octets          : 0          Out Octets                   : 0
In Discards        : 0          Out Discards                 : 0
In Errors          : 0          Out Errors                   : 0
In Ucast Pkts      : 0          Out Ucast Pkts               : 0
Non-Ucast Pkts     : 0          Out Non-Ucast Pkts           : 0
Out Q Len          : 0          Unknown Prot Pkts            : 0
```

Output field description

Field	Description
Interface	This uniquely identifies the Interface whose information is being displayed. It may be: *aal5-0 - *, eth-0, veth-0 to veth-3, ppp-0 - *, atm-0, dsl, dsli, dslf, usb-0, be l2t-*, ipoa-0-* ,
Description	This is general information about the interface.
Type	The type of interface, distinguished according the physical/link/network protocol immediately below the IP layer. It may be: *ATM, ETHERNET, PPP, AAL5, IPOA, TUNNEL*
Mtu	The size (in bytes) of the largest IP datagram which can be sent/received on this interface
Bandwidth	The current bandwidth of the interface in bps
Phy Addr	Interface's address immediately below the IP layer
Admin Status	This is the Desired state of the interface. It may be: *Up, Down*

Field	Description
Operational Status	This is the current operational state of the interface. It may be: *Up, Down*
Last Change	Value of System UpTime (in seconds) at the time the interface entered its current operational state.
Time since Last Change(sec)	Value of time (in seconds), since last status change of the interface.
In Octets	The total number of octets received on the interface, including the framing characters
Out Octets	The total number of octets transmitted out of the interface including framing characters
In Discards	The number of inbound packets which were discarded though no errors were detected
Out Discards	The number of outbound packets chosen to be discarded even though there were no errors.
In Errors	The number of inbound packets which were not delivered to upper layers because of errors.
Out Errors	The number of outbound packets chosen to be discarded because there were errors
In Ucast Pkts	The number of unicast packets delivered to a higher layer protocol.
Out Ucast Pkts	The total number of packets requested to be sent to unicast addresses, by upper layer protocols.
Non-Ucast Pkts	The total number of packets requested to be sent to non-unicast addresses, by upper layer protocols.
Out Non-Ucast Pkts	The total number of packets requested to be sent to non-unicast addresses, by upper layer protocols
Out Q Len	The length of the output packet Q (in packets.)
Unknown Prot Pkts	The number of packets received via the interface which were discarded because of an unknown or unsupported protocol.

Caution None.

References

- *get ip stats* command

3.160 get ip address

Description Use this command to display either the full IP address table or a single entry in the address table.

Command Syntax ***get ip address [ip*** ip-address***]***

Parameters

Name	Description
ip ip-address	IP Address whose information is to be displayed. If no IP address is specified then all entries in the address table are displayed. **Type:** Optional **Valid values:** *0.0.0.1- 255.255.255.255*

Mode Super-User, User

Example ***$ get ip address***

Output

```
Ip Address     Mask             If Name      BCast Addr        MaxReasm
-------------------------------------------------------------------------------
192.168.1.1    255.255.0.0      eth-0        1                 65535
127.0.0.1      255.0.0.0        lo-0         1                 65535
```

Output field description

Field	Description
Ip Address	The IP address to which this entry's addressing information pertains
Mask	The subnet mask associated with the IP address of this entry
If Name	The interface to which this entry is applicable. It may be: *eth-0*,
BCast Addr	The value of the least significant bit in the IP broadcast address used for sending datagrams on the interface associated with the IP address of this entry
MaxReasm	The size of the largest IP datagram which this entity can re-assemble from incoming IP fragmented datagrams received on this interface

Caution None.

References

- *ip stats* related commands
- *ip route* related commands
- *ip cfg* related commands
- *arp* related commands

3.161 get ip cfg

Description Use this command to get information about IP Stack Configuration Parameters.

Command Syntax ***get ip cfg***

Parameters None.

Mode Super-User, User

Example ***$ get ip cfg***

Output

```
Forwarding             : Disabled
TTL                    : 64
Arp Ageing Timeout(sec):  400
```

Output field description

Field	Description
Forwarding	This indicates whether this entity is acting as an IP gateway in respect to the forwarding of datagrams received by, but not addressed to, this entity. It may be: *Enabled, Disabled*
TTL	The default value inserted into the Time-To-Live field of the IP header of datagrams originated at this entity, whenever this is not supplied by the transport layer protocol. Here it will always be *64.*
Arp Ageing Timeout(sec)	This specifies the duration in seconds, after which an ARP entry is aged out.

Caution None.

References

- *modify ip cfg* command
- *ip stats* related commands
- *ip route* related commands
- *ip address* related commands
- *arp* related commands

3.162 get ipf global

Description Use this command to get IP Filter global configuration.

Command Syntax ***get ipf global***

Parameters None

Mode User.

Example ***get ipf global***

Output Verbose mode on:

```
Security Level        : None       DMZ Default Action    : Deny
Public Default Action : Deny       Private Default Action : Accept
```

Verbose mode off:

```
Security Level        : None       DMZ Default Action    : Deny
Public Default Action : Deny       Private Default Action : Accept
```

Output Field description:

Field	Description
Security Level	This specifies the service protection level applied to the system.
Public Default Action	Specifies the default action when a packet does not match any of the Security rules on a public interface.
Private Default Action	Specifies the default action when a packet does not match any of the Security rules on a private interface.
DMZ Default Action	Specifies the default action when a packet does not match any of the Security rules on a DMZ interface.

Caution None

References

- modify ipf global

3.163 get ipf rule entry

Description This command is used for getting information of an IP filter rule.

Command Syntax ***get ipf rule entry [ruleid*** rule-id***]***

Parameters

Name	Description
ruleid rule-id	An index given by the caller to identify the rule entry. **Type**: Optional **Valid values:** *1-4294967295*

Mode User.

Example ***$ get ipf rule entry ruleid 1***

Output Verbose Mode On

```
Rule id           : 1Interface         : eth-0
Rule Admin status : DisableRule Oper Status  : Disable
In interface      : ALLDirection         : Out
Security Level    : HighBlacklist Status        : Enable
Logging           : DisableAction            : Accept
Log Tag           : -
IP Frag Pkt       : Yes         IP Opt Pkt        : No
TCP Flag          : SynStore State       : Enable
Src Addr    : Equal          172.25.8.76
Dest Addr   : Range          172.25.8.70          172.25.8.90
Src Port    : Out Of Range   10                   20
Dest Port   : Not Equal      3
ICMP Code   : Not Equal      10
ICMP Type   : Equal          unreach
TransProt   : Equal          TCP
IP Pkt Size : Less Than      10
TOD Rule    : Enable Between  01:02:30              02:01:30
```

Verbose Mode Off

```
Rule id           : 1Interface         : eth-0
Rule Admin status : DisableRule Oper Status  : Disable
In interface      : ALLDirection         : Out
Security Level    : HighBlacklist Status        : Enable
Logging           : DisableAction            : Accept
Log Tag           : -
IP Frag Pkt       : Yes         IP Opt Pkt        : No
TCP Flag          : SynStore State       : Enable
Src Addr    : Equal          172.25.8.76
Dest Addr   : Range          172.25.8.70          172.25.8.90
Src Port    : Out Of Range   10                   20
Dest Port   : Not Equal      3
ICMP Code   : Not Equal      10
ICMP Type   : Equal          unreach
TransProt   : Equal          TCP
IP Pkt Size : Less Than      10
TOD Rule    : Enable Between  01:02:30              02:01:30
```

Output field description

Field	Description
Rule id	The index given by the caller to identify the rule entry.
Rule Admin Status	Specifies the administrative status of the rule entry.
Interface	Specifies the IP-enabled physical interface to be associated to this rule. *All* indicates that rule is to be associated to all interfaces.
In Interface	Specifies the input interface ID which may be used to dictate the rules like deny/accept all traffic from a specific interface. So, this field can be specified only if direction is *out*.
Direction	Specifies the direction of Data flow on which filtering is to be applied.
Action	Specifies the action to be taken when a packet matches a rule.
Logging	This flag controls the logging of matched packets. Each log will contain IP Header and TCP/UDP header or ICMP fields, if available.
Log Tag	This specifies the Filter logging tag, which will be added to all the logs generated due to the rule
Src Addr	This field specifies the matching criteria for source IP Address along with the source IPAddress value and the destination IPAddress value. The source or destination or both are shown depending on whether the matching criteria is relational, range, erange, any or self.
Dest Addr	This field specifies the matching criteria for destination IP Address along with the start destination IPAddress value and end destination IPAddress value. The start or end or both are shown depending on whether the matching criteria is relational, range, erange, any or self.
Src Port	This field specifies the matching criteria for source port along with the start of src port and the end of src port. The start or end or both are shown depending on whether the matching criteria is relational, range, erange, any or bcast.
Dest Port	This field specifies the matching criteria for destination Port along with the start dest port and the end dest port. The start or end or both are shown depending on whether the matching criteria is relational, range, erange, any or bcast.
ICMP Code	This field specifies the matching criteria for ICMP code value along with the code field in ICMP header in case of ICMP packets.
ICMP Type	This field specifies the matching criteria for ICMP Type along with the type field in ICMP header in case of ICMP packets.
TransProt	This field specifies the matching criteria for transport protcol field along with the transport layer protocol number as per IANA.

Field	Description
TCP Flag	This specifies filtering criteria for TCP packet types.
Store State	This specifies whether stateful filtering is done or not
Security Level	This specifies the association of rule with system wide service protection level.
Blacklist Status	This specifies whether source of the packet should be put in blacklist if it matches with the rule. It will be applicable to deny kind of rules
IP Frag Pkt	This specifies whether the rule is applicable to fragmented packets, non fragmented packets or in both cases.
IP Opt Pkt	This specifies whether the rule is applicable to IP packet with or without IP options or in both cases.
IP Pkt Size	This field specifies the matching criteria for IP Pkt Size along with IP packet filtering attribute . It should be compared against the packet size value in IP header.
ToD Rule	This field specifies whether the rule should be applied for the duration specified."Enable Between" indicates that the rule is applied between the specified time duration."Disable Between" indicates that rule is not applicable between the specified duration, but it is applicable for remaining time of the day.
Rule Oper Status	A rule will be operationally enabled if and only if it is administratively enabled, its Time of Day status as per current time is Enable, and if the rule's security level matches the global security level as shown by get ipf global.

Caution None.

References

- *create ipf rule entry* command
- *delete ipf rule entry* command
- *modify ipf rule entry* command

3.164 get ipf rule stats

Description This command is used for getting IP filter rule statistics for a rule.

Command Syntax ***get ipf rule stats [ruleid*** rule-id***]***

Parameters

Name	Description
ruleid rule-id	The index given by the caller to identify the rule entry. **Type**: Optional **Valid values:** *1-4294967295*

Mode User.

Example ***$ get ipf rule stats***

Output Verbose Mode On

```
Rule id      Packets count
-------------------------
1            4
```

Verbose Mode Off

```
Rule id      Packets count
-------------------------
1            4
```

Output field description

Field	Description
Rule id	This specifies IP filter rule for which statistics is to be collected.
Packets count	This specifies total number of packets matching the IP filter rule

Caution None.

References

- *reset ipf rule stats* command
- *get ipf stats* command
- *reset ipf stats* command

3.165 get ipf session

Description Use this command to get all IP filter Sessions information.

Command Syntax ***get ipf session***

Parameters None

Mode User

Example ***$ get ipf session***

Output Verbose Mode On and Verbose Mode Off

```
Session Index           : 1
Time To Expire (sec)    : 200               Protocol              : TCP
If-Name-1               : eth-0             If-Name-2             : ppp-0
IP Address-1            : 172.25.8.9        IP Address-2           : 202.1.1.10
Port 1                  : 1245              Port 2                 : 23
IN RuleID on IfName-1   : 10                IN RuleID on IfName-2  : 20
IN Action on IfName-1   : accept            IN Action on IfName-2  :accept
OUT RuleID on IfName-1  : 30                OUT RuleID on IfName-2 : 40
OUT Action on IfName-1  : accept            OUT Action on IfName-2  :accept
```

Output field description

Field	Description
Session Index	This is the index for display of session information
Time To Expire (sec)	Time remaining before the session is deleted.
Protocol	This field specifies the protocol type for which session is created.
IfName-1	This specifies the first physical interface associated with this session. This is the interface due to which session creation is initiated.
IfName-2	This specifies the second physical interface associated with this session. This interface is the one on which packet is routed.
IP Address-1	This specifies the IP address associated with ifName-1. If the packet originates from ifName-1, then this will be the source IP address and if the packet is arriving at ifName-1, then this will be the destination address.
IP Address-2	This specifies the IP address associated with ifName-2. If the packet originates from ifName-2, then this will be the source IP address and if the packet is arriving at ifName-2, then this will be the destination address.
Port-1	This specifies port associated with IP Address-1. If the packet originates from ifName-1, then this will be the source port and if the packet is arriving at ifName-1, then this will be the destination port.

Field	Description
Port-2	This specifies port associated with IP Address-2. If the packet originates from ifName-2, then this will be the source port and if the packet is arriving at ifName-2, then this will be the destination port.
IN RuleID on IfName-1	This specifies the matching rule id (i.e. the first rule that matches the packet selectors) on IfName-1 for incoming direction.
IN RuleID on IfName-2	This specifies the matching rule id on interface IfName-2 for incoming direction.
IN Action on IfName-1	This specifies the action defined in IN RuleID on IfName- 1.
IN Action on IfName-2	This specifies the action defined in IN RuleID on IfName-2.
OUT RuleID on IfName-1	This specifies the matching rule id on interface IfName-1 for outgoing direction.
OUT RuleID on IfName-2	This specifies the matching rule id on interface IfName-2 for outgoing direction.
OUT Action on IfName-1	This specifies the action defined in OUT RuleID on IfName-1.
OUT Action on IfName-2	This specifies the action defined in OUT RuleID on IfName-2.

Caution Session information will be displayed only if IP filter is enabled.

References

- *reset ipf session* command

3.166 get ipf stats

Description Use this command to get global statistics of IP filter.

Command Syntax ***get ipf stats***

Parameters None.

Mode User.

Example ***$ get ipf stats***

Output Verbose Mode On

```
Packets count  : 0
```

Verbose Mode Off

```
Packets count  : 0
```

Output field description

Field	Description
Packets count	This field tells the total packets given to the IP filter.

Caution None.

References

- *reset ipf stats* command
- *get ipf rule stats* command
- *reset ipf rule stats* command

3.167 get ipoa intf

Description This command is used for getting information on a particular IPoA interface or on all the IPoA interfaces.

Command Syntax ***get ipoa intf [ifname*** `interface-name`***]***

Parameters

Name	Description
ifname `interface-name`	This parameter specifies the interface for which information is desired. In case the field is not specified, then the information for all valid IPoA interfaces should be displayed. **Type:** Optional **Valid values:** *ipoa-0-**

Mode Super-User, User.

Example ***$ get ipoa intf ifname ipoa-0***

Output

```
IfName                : ipoa-0          UseDHCP             : true
Type                  : non1577         Interface Sec Type: Public
Configured IP Address: 172.25.12.74     Mask                : 255.255.0.0
DRoute                : False           Gateway             : 0.0.0.0
NAT Direction         : OUT             Oper Status         : Down
Configured MTU        : 300             Actual MTU          : 200
```

Output field description

Field	Description
If-Name	The name of the IPoA interface.
UseDHCP	This specifies whether a DHCP client is used to obtain the IP address for this interface from a DHCP server, or not.
Type	This specifies the type of IPoA interface.
Interface sec Type	Interface security type
Configured Ip Address	IP address assigned to the IPoA interface.
Mask	Network mask to be applied to the IP Address.
Droute	Default Route
Gateway	Gateway IP address
Nat Direction	This specifies the NAT direction, which may be: *inside, outside or none*.

Field	Description
Oper Status	The actual/current state of the interface. It can be either *Up* or *Down*
Configured MTU	This specifies the MTU value configured by the user for IPOA interface.
Actual MTU	This specifies the MTU value actually operational for IPOA interface.

Caution None.

References

- *create ipoa intf* command
- *delete ipoa intf* command
- *create ipoa map* command
- *delete ipoa map* command
- *get ipoa map* command

3.168 get ipoa map

Description Use this command to get the association of IPoA (IP over ATM) interface with lower aal5 interfaces.

Command Syntax ***get ipoa map*** **[*ifname*** interface-name]

Parameters

Name	Description
Ifname interface-name	The name of the IPoA interface for which the association with lower interface has to be deleted. **Type:** Mandatory **Valid values:** ipoa-0,ipoa-1 etc.,.
Lowif low-interface-name	This parameter specifies the lower interface (ATM VC interface) of the IPoA interface. **Type**: Mandatory **Valid Values:** aal5-0, aal5-1 etc.,.

Mode Super-User.

Example *$ get ipoa map ifname ipoa-0 lowif* aal5-0

Output Verbose mode on/off:

```
IfName    LowIfName    Peer IP Address
-------------------------------------
ipoa-0    aal5-0       172.25.1.130
```

Output Field description:

Field	Description
IfName	The name of the IPoA interface for which the association with the lower interface has been deleted.
LowIfName	Specifies the lower (ATM VC) interface.
Peer IP Address	IP address of peer.

Caution None

References:

- create ipoa map
- delete ipoa map
- get ipoa map
- get ipoa intf
- delete ipoa intf
- modify ipoa intf

3.169 get ip route

Description Use this command to get the listing of all routing table entries or for a specific entry.

Command Syntax ***get ip route [ip*** dest-ip-address***] [mask*** net-mask***]***

Parameters

Name	Description
ip dest-ip-address	Destination IP address of the route which is to be displayed. If no IP address is specified then all known routes are displayed. **Type:** Optional **Valid values:** Any valid class A/B/C IP address
mask net-mask	The Mask of the destination IP Address. **Type:** Optional **Valid values:** *0.0.0.1 – 255.255.255.255*

Mode User, Super-User.

Example ***$ get ip route ip 192.168.2.40 mask 255.255.255.0***

Output

```
Destination   Mask       Gateway      If-name   RouteType  RouteOrig   Age(sec)
-------------------------------------------------------------------------------
192.168.2.40  255.255.255.0  192.168.1.1  veth-0    IND     NET          0
```

Output field description

Field	Description
Destination	Destination IP address of this route
Mask	The Mask of the destination IP Address
Gateway	The IP address of the next hop for this route
If-Name	The local interface through which the next hop of this route will be reached
Route Type	The type of route. It may be: *Dir* (for Direct), *Ind* (for Indirect), or *inv* (for invalid route)
Route Orig	The routing mechanism through which this route was learned. It may be: *NET* (for Network Management), *LCL* (for Local), *RIP*, *ICMP*, *DYI* (Dynamic through Interface creation)
Age	The number of seconds since this route was last updated or otherwise determined to be correct

Caution None.

References

- *create ip route* command
- *delete ip route* related commands
- *ip stats* related commands
- *ip cfg* related commands
- *ip address* related commands
- *arp* related commands

3.170 get ip stats

Description Use this command to display the global statistics for the IP Layer.

Command Syntax ***get ip stats***

Parameters None.

Mode Super-User, User

Example ***$ get ip stats***

Output

```
Rx Pkts count                : 10          Rx Hdr Errors count      : 0
Fwd Datagram count           : 0           Unknown Proto count      : 0
Rx Discards count            : 0           Rx Delivered count       : 10
Tx Requests count            : 10          Tx Discards count        : 0
Tx No Routes count           : 0           IP Reasm Reqd count      : 0
IP Reasm OK count            : 0           IP Reasm Failed count    : 0
IP Frag OK count             : 0           IP Frag Failed count     : 0
IP Frag Created count        : 0           Routing Reject count     : 0
In Addr Err count            : 0           Reasm Timeout(sec)       : 60
```

Output field description

Field	Description
Rx Pkts count	This defines number IP packets received
Rx Hdr Errors count	This defines number of IP packets received with header errors
Fwd Datagram count	This defines number of datagrams forwarded by it.
Unknown Proto count	This defines The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol
Rx Discards count	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded. This does not include any datagrams discarded while awaiting reassembly.
Rx Delivered count	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP)
Tx Requests count	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. This counter does not include any datagrams counted in Fwd Datagram.
Tx Discards count	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded. This counter would include datagrams counted in Fwd Datagram if any such packets met this (discretionary) discard criterion
Tx No Routes count	The number of IP datagrams discarded because no route could be found to transmit them to their destination

Field	Description
IP Reasm Reqd count	The number of IP fragments received which needed to be re-assembled at this entity.
IP Reasm OK count	The number of IP datagrams successfully re-assembled
IP Reasm Failed count	The number of failures detected by the IP re-assembly algorithm. This is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
IP Frag OK count	The number of IP datagrams that have been successfully fragmented at this entity.
IP Frag Failed count	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, e.g., because their Don't Fragment flag was set
IP Frag Created count	The number of IP datagram fragments that have been generated as a result of fragmentation at this entity
Routing Reject count	The number of IP datagrams discarded because no route could be found to transmit them to their destination.
In Addr Err count	This defines number of packets received with wrong address information
Reasm Timeout	The maximum number of seconds for which received fragments are held while they are awaiting reassembly at this entity.

Caution None.

References

- *ip address* related commands
- *ip route* related commands
- *ip cfg* related commands
- *arp* related commands

3.171 get l2tp global config

Description Use this command to to get l2tp tunnel global configuration.

Command Syntax ***get l2tp global config***

Mode User, Super-User.

Example ***$ get l2tp global config***

Output

```
Response Timeout (secs)  : 300
```

Output Field description:

Field	Description
Response Timeout(secs)	Defines the period of time (in secs) that a peer will wait for the response. A value of "Infinite" indicates an infinite wait.

Caution None.

References

- modify l2tp global config

3.172 get l2tp global info

Description Use this command to get L2TP global information.

Command Syntax ***get l2tp global info***

Mode User, Super-User.

Example ***$ get l2tp global config***

Output

```
Proto Version: 0X200
Vendor Name  : Conexant
```

Output Field description:

Field	Description
Proto version	First octet identifies the version, second the revision
Vendor name	This field identifies the Vendor name of the L2TP protocol stack.

Caution None.

References None

3.173 get l2tp session stats

Description Use this command to get l2tp session status for a particular PPP/ PPPoE session interface or on all l2tp sessions.

Command Syntax ***get l2tp session stats [pppifname interface-name]***

Parameters

Name	Description
pppifname interface-name	Identifies the PPP interface name from which PPP packets are being tunneled **Type:** Optional **Valid values:** ppp-0, ppp-*
Vendor name	This field identifies the Vendor name of the L2TP protocol stack.

Mode User, Super-User.

Example ***get l2tp session stats pppifname ppp-0***

Output Verbose Mode On/Off

```
PPP If Name          : ppp-0          Tunnel If Name: l2t-0
Session State        : connect        Sess FSM state: established
Local Session Id     : 100            Remote Session Id: 200
Tx Connect Speed     : 10000          Rx Connect Speed: 10000
Bearer Type          : digital        Framing Type: sync
Phy Channel Id       : 12             Sequence State: local
Send Sequence Count: 999              Recv Sequence Count: 1000
Last Result code     : 23             Last Error code: 22
ReAss Timeout Count: 0                Recv Out of Seq: 23
Last Start Time      : 02:03:02       Last Stop time: 03:02:02
Call S. No           : 2
DNIS                 : 4392849
Calling Id           : 2000
SubAddress           : 100001
Pvt Grp Id           : 1000234
Remote User Name     : Conexant
Last Error Msg       : Tunnel is being stopped.
```

Output Field description:

Field	Description
PPP If Name	The ifindex of the interface from which PPP packets are being tunneled.
If Name	This object identifies the session's associated L2TP tunnel ifIndex value.

Field	Description
Call S. No	This object defines the serial number that has been assigned to this session.
Local Session Id	This object contains the local assigned session identifier for this session.
Remote Session Id	This object contains the remote assigned session identifier for this session.
Remote User Name	This object identifies the peer session name on this interface.
Session State	This object contains the current state of the session.
DNIS	This object identifies the Dialed Number Information String that the LAC obtained from the network for the session.
Tx Connect Speed	This object returns the last known transmit baud rate for this session.
Rx Connect Speed	This object returns the last known receive baud rate for this session established.
Bearer Type	This object describes the bearer type of this session.
Framing Type	This object describes the framing type of this session.
Phy Channel Id	This object contains the physical channel identifier for the session.
Sequence State	This object defines which tunnel peers have requested payload sequencing.
Send Sequence count	This object contains the next send sequence number for this session.
Recv Sequence count	This object contains the next receive sequence number expected to be received on this session.
Last Result code	This object contains the last value of the result code as described in the Result Code AVP which caused the Session to disconnect.
Last Error code	This object contains the last value of the error code as described in the Result Code AVP that caused the Session to disconnect.
Sess FSM state	This object contains the current state of the session FSM.
Reassembly Timeout Count	This object returns the number of reassembly timeouts that have occurred for this session.
Last Start Time	This is the time stamp at which the session was started last.

Field	Description
Last Stop time	This is the time stamp at which the session was stopped last.
Calling Id	This object identifies the Calling Line ID that the LAC obtained from the network for the session.
SubAddress	This object identifies the Sub Address that the LAC obtained from the network for the session.
Pvt Grp Id	This object identifies the Private Group Identifier used for this tunneled session.
Last Error Msg	This object contains the last value of the optional message as described in the Result Code AVP which caused the session to disconnect.

Caution None.

References

- *reset l2tp session stats* command

3.174 get l2tp tunnel config

Description Use this command to to get information on a particular l2tp tunnel or on all l2tp tunnels.

Command Syntax ***get l2tp tunnel config*** [ifname interface-name]

Parameters

Name	Description
ifname interface-name	Identifies the interface name for L2TP layer. **Type**: Optional **Valid values:** l2t-0-l2t-*.

Mode User, Super-User.

Example ***$ get l2tp tunnel config ifname*** l2t-0

Output Verbose mode on/off:

```
If Name             : l2t-0
Status              : Start          Oper Status       : Up
Local IP-address    : 178.10.10.10   Remote IP-address : 178.10.11.10
Hello Interval      : 300            Idle Timeout      : 100
Max Retx Attempt    : 10             Max Retx Timeout  : 10
Initiator           : local          Payload Sequencing: always
Authentication Type : simple         Transport         : udpip
Control RWS         : 5
Shared Secret       : passwd
Local Host name     : titanium
Remote Host name    : Columbia
```

Output Field description:

Field	Description
If-name	Identifies the interface name for L2TP layer.
Local IP-address	This field specifies the address of the local endpoint of the tunnel
Local Host name	This field specifies the address of the local endpoint of the tunnel
Remote IP-address	This field specifies the address of the remote end-point of the tunnel to which the tunnel is to be estab-lished.
Status	This field specifies the status of the of the l2tp inter-face.

Field	Description
Oper Status	This field specifies the Operstatus of the of the l2tp interface.
Remote Host name	This field specifies the hostname of the remote end-point of the tunnel to which the tunnel is to be established.
Hello Interval	Defines the interval (in sec) in which Hello packets are to be sent to the tunnel peer
Idle Timeout	Defines the period of time (in seconds) that an established tunnel with no sessions will wait before disconnecting the tunnel.
Control RWS	Defines the control channel receive window size
Max Retx Timeout	Defines the maximum retransmission timeout interval that the tunnel will wait before retransmitting a control packet that has not been acknowledged.
Initiator	This indicates whether the tunnel will be initiated locally or not.
Payload Sequencing	This object determines whether or not session payload packets will be requested to be sent with sequence numbers from tunnel peer's. The value never(2) indicates that L2TP will never initiate sequencing but will do sequencing if asked. The value always(3) indicates that L2TP will send the sequencing Required AVP during session establishment
Authentication Type	Describes how L2TP tunnel peers are to be authenticated
Transport	Defines the underlying transport media that is in use for this tunnel entry.
Shared Secret	Shared secret is used during the tunnel authentication phase of tunnel establishment if authtype is challenge
Max Retx Attempt	Defines the number of retransmissions, which the tunnel will attempt before assuming that the peer is no longer responding.

Caution None.

References
- delete l2tp tunnel config ifname
- create l2tp tunnel config

3.175 get l2tp tunnel stats

Description Use this command to get l2tp tunnel status and statistics for a particular tunnel interface or on all the l2tp tunnels.

Command Syntax ***get l2tp tunnel stats*** [ifname interface-name]

Parameters

Name	Description
ifname interface-name	Identifies the interface name for L2TP layer. **Type**: Optional **Valid values:** l2t-0-l2t-*.

Mode User, Super-User.

Example ***$ get l2tp tunnel stats ifname*** l2t-0

Output Verbose mode on/off:

```
If name               : l2t-0
Tunnel State          : idle      Tunnel FSM State: idle
Local Tunnel Id       : 2         Remote Tunnel Id: 3
Control Pkts Recv     : 10           Remote RWS: 5
Control Recv ZLB      : 10        Remote IntialWindow: 2
Control Out of Seq    : 20        Remote Bearer Cap: none
Control Out of Window : 20        Remote Framing Cap: sync
Control Send Packets  : 20        Remote Proto Ver: 0200
Control Send ZLB      : 20        Number Ack Timeout  : 100
Send Sequence         : 22        Recv Sequence: 26
Send Sequence Ack     : 23        Recv Sequence Ack: 24
Total Sessions        : 100       Total fail session: 2
Active Sessions       : 1000      Remote FirmwareRev: 03
Last Result code      : 23        Last Error code: 25
Last Start Time       : 03:04:02  Last Stop time: 04:05:02
Last Error Msg        : Tunnel is being stopped.
Remote Vendor name    : Conexant
```

Output Field description:

Field	Description
ifname	Identifies the interface name for L2TP layer.
Tunnel State	This field contains the current state of the control tunnel.

Field	Description
Local Tunnel Id	This object contains the local tunnel Identifier.
Remote Tunnel Id	This object contains the remote tunnel Identifier.
Remote FirmwareRev	This object contains the tunnel peer's firmware revision number
Remote RWS	This object contains the current remote peers receive window size.
Remote Intial Window	This object contains the initial remote peers receive window size as indicated by the tunnel peer during the tunnel establishment phase
Remote Bearer Cap	This object describes the Bearer Capabilities of the tunnel peer.
Remote Framing Cap	This object describes the Framing Capabilities of the tunnel peer.
Control Packets Recv	This object contains the number of control packets received on the tunnel.
Control Recv ZLB	This object returns a count of the number of Zero Length Body control packet that were received.
Control Out of Seq	This object returns a count of the number of control packets that were not received in the correct order (as per the sequence number) on this tunnel.
Control Out of Window	This object contains the number of control packets that were received outside of the offered receive window.
Control Send Packets	This object contains the number of control packets that were transmitted to the tunnel peer.
ZLB Sent	This object contains the number of Zero Length Body control packets transmitted to the tunnel peer.
Number Ack Timeout	This object returns a count of the number of control packet timeouts due to the lack of a timely acknowledgement from the tunnel peer.
Remote Proto Ver	This object describes the protocol version and revision of the tunnel peers implementation.
Send Sequence	This object contains the next send sequence number for the control channel.
Send Sequence Ack	This object contains the send sequence number that the tunnel peer has acknowledged for the control channel.
Recv Sequence	This object contains the next receive sequence number expected to be received on this control channel.

Field	Description
Recv Sequence Ack	This object contains the last receive sequence number that was acknowledged back to the tunnel peer for the control channel.
Total Sessions	This object contains the total number of sessions that this tunnel has successfully connected through to its tunnel peer since this tunnel was created.
Total fail session	This object contains the total number of sessions that were initiated but failed to reach the established phase.
Active Sessions	This object contains the total number of sessions in the established state for this tunnel.
Last Result code	This object contains the last value of the result code as described in the Result Code
Last Error code	This object contains the last value of the error code as described in the Result Code AVP which caused the tunnel to disconnect.
Last Start Time	This is the time stamp at which the tunnel was started last.
Last Stop time	This is the time stamp at which the tunnel was stopped last.
Tunnel FSM State	This field contains the current state of the control tunnel FSM.
Last Error Msg	This object contains the last value of the optional message as described in the Result Code AVP which caused the tunnel to disconnect
Remote Vendor name	This object identifies the vendor name of the peer's L2TP implementation.

Caution None.

References

- *reset l2tp tunnel stats* command

3.176 get l2tp udp stats

Description Use this command to get the l2tp udp statistics.

Command Syntax ***get l2tp udp stats [ifname*** interface-name***]***

Parameters

Name	Description
ifname interface-name	Identifies the interface name for L2TP layer. **Type**: Optional **Valid values:** l2t-0-l2t-*.

Mode User, Super-User.

Example ***$ get l2tp udp stats ifname*** *l2t-0*

Output Verbose mode on/off:

```
If name    Peer Port      Local Port
-------------------------------------------
l2t-0      1000           2000
```

Output Field description:

Field	Description
If-name	Identifies the interface name for L2TP layer.
Peer port	This object reflects the peer's UDP port number used for this tunnel.
Local port	This object reflects the local UDP port number that this tunnel is bound to.

Caution None.

References None

3.177 get l2wall cfg

Description Use this command to get L2WALL configuration information.

Command Syntax ***get l2wall cfg***

Parameters None

Mode User, Super-User

Example ***$ get l2wall cfg***

Output

```
Status : on                          Inactive Time(min) : 5
```

Output field description

Field	Description
`Status`	Status of the L2wall configuration.
`Inactive Time(min)`	Time since last recorded activity in minutes.

Caution None

References

- *modify l2wall cfg*

3.178 get mctl access

Description Use this command to get Management Control-Access Configuration

Command Syntax ***get mctl access***

Parameter None

Mode Super-User, User

Example ***$ get mctl access***

Output

```
HTTP Wan Access   : enable  HTTP Lan Access   : enable
Telnet Wan Access : enable  Telnet Lan Access : enable
FTP Wan Access    : enable  FTP Lan Access    : enable
TFTP Wan Access   : enable  TFTP Lan Access   : enable
```

Output field description

Field	Description
HTTP Wan Access	This is used to enable or disable HTTP access to the modem from its WAN interfaces. WAN interfaces are those for which the IP Filter security type is marked as 'public'. The IP addresses allowed are picked up from the Management Control Allowed IP addresses list. If there are no entires in this list, then access is allowed to all addresses.
HTTP Lan Access	This is used to enable or disable HTTP access to the modem from its LAN interfaces. LAN interfaces are those for which the IP Filter security type is marked as 'private' or 'DMZ'. If enabled, HTTP access is allowed to all LAN hosts. LAN access cannot be controlled for specific hosts.
Telnet Wan Access	This is used to enable or disable Telnet access to the modem from its WAN interfaces. WAN interfaces are those for which the IP Filter security type is marked as 'public'. The IP addresses allowed are picked up from the Management Control Allowed IP addresses list. If there are no entires in this list, then access is allowed to all addresses.
Telnet Lan Access	This is used to enable or disable Telnet access to the modem from its LAN interfaces. LAN interfaces are those for which the IP Filter security type is marked as private or DMZ. If enabled, Telnet access is allowed to all LAN hosts. LAN access cannot be controlled for specific hosts.
FTP Wan Access	This is used to enable or disable FTP access to the modem from its WAN interfaces. WAN interfaces are those for which the IP Filter security type is marked as public. The IP addresses allowed are picked up from the Management Control Allowed IP addresses list. If there are no entires in this list, then access is allowed to all addresses.

Field	Description
FTP Lan Access	This is used to enable or disable FTP access to the modem from its LAN interfaces. LAN interfaces are those for which the IP Filter security type is marked as private or DMZ. If enabled, FTP access is allowed to all LAN hosts. LAN access cannot be controlled for specific hosts.
TFTP Wan Access	This is used to enable or disable TFTP access to the modem from its WAN interfaces. WAN interfaces are those for which the IP Filter security type is marked as public. The IP addresses allowed are picked up from the Management Control Allowed IP addresses list. If there are no entires in this list, then access is allowed to all addresses.
TFTP Lan Access	This is used to enable or disable TFTP access to the modem from its LAN interfaces. LAN interfaces are those for which the IP Filter security type is marked as private or DMZ. If enabled, TFTP access is allowed to all LAN hosts. LAN access cannot be controlled for specific hosts.

Caution None

References

- *modify mctl access* command

3.179 get mctl iplist

Description Use this command to get Management Control - Allowed IP addresses list

Command Syntax ***get mctl iplist [ipaddress*** ipaddress ***]***

Parameter

Name	Description
ipaddress ipaddress	Ip address **Type:** Optional

Mode Super-User, User

Example ***$ get mctl iplist ipaddress*** 172.25.12.13

Output

```
Mgmt Ctrl Ip Address
--------------------------------------------------------------------------------
172.25.12.13
```

Output field description

Field	Description
Ip Address	Ip address

Caution None

References

- *create mctl iplist* command
- *delete mctl iplist* command

3.180 get nat global

Description Use this command to get NAT global info.

Command Syntax ***get nat global***

Parameters None.

Mode Super-User, User

Example ***$ get nat global***

Output

```
TCP Idle Timeout(sec): 86400          TCP Close Wait(sec)  : 60
TCP Def Timeout(sec) : 60             UDP Timeout(sec)     : 300
ICMP Timeout(sec)    : 60             GRE Timeout (sec)    : 300
ESP Timeout(sec)     : 300            Default Nat Age(sec) : 240
NAPT Port Start      : 40000          NAPT Port End        : 41023
Admin Status         : Disable
```

Output field description

Field	Description
TCP Idle Timeout	The Time out (in seconds) which is used to expire out Idle TCP Nat Translations
TCP Close Wait	The Wait time (in seconds) after which a TCP connection is closed
TCP Def Timeout	The default timeout (in seconds) in case of errors.
UDP Timeout	The time (in seconds) for UDP timeout
ICMP Timeout	The time (in seconds) for ICMP timeout
GRE Timeout	The time (in seconds) for GRE timeout
ESP Timeout	The time (in seconds) for ESP timeout
Default Nat Age	The default NAT Time Out (in seconds).
NAPT Port Start	The port value from which the port range can start
NAPT Port End	The port value at which the port range ends.
Admin Status	The current NAT Status. It may be: *Enable, Disable*

Caution None.

References

- *modify nat global* command
- *nat rule status* related commands
- *nat rule stats* related commands
- *nat rule entry* related commands

3.181 get nat rule entry

Description Use this command to get the full NAT Rule table or one entry.

Command Syntax ***get nat rule entry [ruleid*** rule-id***]***

Parameters

Name	Description
ruleid rule-id	This identifies the NAT rule, information pertaining to which is to be displayed. If this is not specified then information for all rules is displayed. **Type:** Optional **Valid values:** *1-4294967295*

Mode Super-User, User

Example ***$ get nat rule entry ruleid*** **1**

Output

```
Rule Id          : 1                  Flavor           : NAPT
Interface        : ALL                Protocol         : ANY
Local Addr From  : 0.0.0.0            Local Addr To    : 0.0.0.0
Dest Addr From   : 0.0.0.0            Dest Addr to     : 0.0.0.0
Global Addr From : 0.0.0.0            Global Addr To   : 255.255.255.255
Dest Port From   : 0                  Dest Port To     : 0
Local Port       : 0
```

Output field description

Field	Description
Rule Id	This identifies the NAT rule, information pertaining to which is being displayed.
Flavor	This specifies the type of rule. It may be: *BASIC, FILTER, NAPT, BIMAP,REDIRECTION* (for RDR) and *PASS.*
Interface	This specifies the Interface or the outgoing device on which this Nat Rule would apply. It may be: *eth-0, veth-0 - *, eoa-0 - *, , ppp-0 - *, …*
Protocol	This specifies the protocol type for which the rule is meant. It may be: *Any, TCP, UDP, ICMP* or IANA specified protocol between 0 to 255.
Local Addr From	This is the starting address when a range of private IP addresses are mapped
Local Addr To	This is the last IP address of the range of private IP addresses mapped by this rule.
Dest Addr From	This specifies the start of the range of destination IP address of the packet to matched.
Dest Addr To	This specifies the end of the range of destination IP address to be matched

Field	Description
Dest Port From	This specifies the start of the range of the destination port numbers to be matched.
Dest Port To	This specifies the end of the range of destination port numbers to be matched.
Global Addr From	This specifies the first globally unique IP address of the range of IP addresses being mapped.
Global Addr To	This specifies the last globally unique IP address of the range of IP addresses used in the mapping.
Local Port	This is the translated port number to be used .

Caution None.

References

- *create nat rule entry* command
- *delete nat rule entry* command
- *nat global info* related commands
- *nat rule statistics* related commands
- *nat rule status* related commands

3.182 get nat rule stats

Description Use this command to display statistics for the specified rule or for all the active rules in the system.

Command Syntax ***get nat rule stats [ruleid*** rule-id***]***

Parameters

Name	Description
ruleid rule-id	This identifies the NAT rule, statistics pertaining to which are to be displayed. If this is not specified then statistics for all rules are displayed. **Type:** Optional **Valid values:** *1-4294967295*

Mode Super-User, User

Example ***$ get nat rule stats ruleid*** 1

Output

```
RuleId        Hits          Inbound Packets       Outbound Packets
-------------------------------------------------------------------
1             0             0                     0
```

Output field description

Field	Description
Rule Id	This identifies the NAT rule, statistics pertaining to which is being displayed.
Hits	The number of time this rule was used to create translations

Caution None.

References

- *reset nat rule stats* command
- *nat rule status* related commands
- *nat rule entry* related commands

3.183 get nat rule status

Description This command displays NAT rule status information.

Command Syntax ***get nat rule status [ruleid*** rule-id***]***

Parameters

Name	Description
ruleid rule-id	This identifies the NAT rule, pertaining to which status information is to be displayed. If this is not specified then status for all rules is displayed. **Type:** Optional **Valid values:** *1-4294967295*

Mode Super-User, User

Example ***$ get nat rule status***

Output

```
RuleId         Active Translations
---------------------------------
1              0
```

Output field description

Field	Description
RuleId	This identifies the NAT rule, Status information pertaining to which is being displayed
Active Translations	The current number of active translations using this rule

Caution None.

References

- *reset nat status* command
- *nat stats* related commands

3.184 get nat stats

Description Use this command to display global NAT statistics.

Command Syntax ***get nat stats***

Parameters None.

Mode Super-User, User

Example ***$ get nat stats***

Output

```
Translation Sess     : 10          Translation Misses   : 0
Translated In Pkts   : 412         Translated Out Pkts  : 400
FTP ALG Sess         : 0           SNMP ALG Sess        : 3
RA ALG Sess          : 5           RMCD ALG Sess        : 2
L2TP ALG Sess        : 2           MIRC ALG Sess        : 5
CUSEEME UDP ALG Sess : 2           CUSEEME TCP ALG Sess : 2
H323 Q931 ALG Sess   : 4           H323 RAS ALG Sess    : 5
H323 RTP ALG Sess    : 3           H323 245 ALG Sess    : 4
PPTP ALG Sess        : 3           RTSP ALG Sess        : 5
TIMBUKTU ALG Sess    : 3           T120 ALG Sess        : 4
SGICompCore ALG Sess : 2           Fragments Processed  : 40
LDAP ALG Sess        : 4          MSN MSGR ALG Sess     : 4
IKE ALG Sess         : 20          ESP ALG Sess         : 10
ICQ ALG Sess         : 1           ICQ BUDDY ALG Sess    : 2
SIP ALG Sess         : 10
```

Output field description

Field	Description
Translation Sessions	This gives the total number of translation sessions which have been established so far
Translation Misses	This gives the number of times for a packet a Nat Rule could not be matched i.e that packet went from IN to OUT or OUT to IN without translation
Translated In Pkts	This is the number of inbound packets translated so far.
Translated Out Pkts	This is the number of outbound packets translated so far.
FTP ALG Sessions	The number of translation sessions for FTP ALG.
SNMP ALG Sessions	The number of translation session for SNMP ALG
RA ALG Sessions	The number of translations for Real Audio ALG
RMCD ALG Sessions	The number of translations for Rcmd ALG
L2TP ALG Sessions	Total number of L2TP session that would be running for it.
MIRC ALG Sessions	The number of MIRC Sessions.
CUSEEME UDP ALG Sess	Total number of CUSEEME Udp Sessions
CUSEEME TCP ALG Sess	Total number of CUSEEME Tcp Sessions
H323 Q931 ALG Sess	Total number of H323 Q931 Sessions

Field	Description
H323 RAS ALG Sess	Total number of H323 RAS Sessions
H323 RTP ALG Sess	Total number of H323 RTP Sessions
H323 245 ALG Sess	Total number of H323 245 Sessions
Fragments Processed	The number of fragments processed
TIMBUKTU ALG Sess	Total number of TIMBUKTU Sessions
T120 ALG Sess	Total number of T120 Sessions
LDAP ALG Sess	Total number of LDAP ALG Sessions
SGICompCore ALG Sess	Total number of SGICompCore ALG Sessions
MSN MSGR ALG Sess	Total number of MSN Messenger Sessions
IKE ALG Sess	Total number of IKE ALG sessions
ESP ALG Sess	Total number of ESP ALG sessions
SIP ALG Sess	Total number of SIP ALG sessions
ICQ ALG Sess	Total number of ICQ ALG Sessions
ICQ BUDDY ALG Sess	Total number of ICQ BUDDY ALG Sessions

Caution None.

References

- *reset nat stats* related commands
- *nat status info* related commands

3.185 get nat status

Description Use this command to display NAT status information.

Command Syntax ***get nat status***

Parameters None.

Mode Super-User, User

Example ***$ get nat status***

Output

```
Active Translations  : 47        Active Rules          : 3
FTP ALG Sess         : 4         SNMP ALG Sess         : 2
RA ALG Sess          : 0         RMCD ALG Sess         : 0
L2TP ALG Sess        : 2         MIRC ALG Sess         : 5
CUSEEME UDP ALG Sess : 2         CUSEEME TCP ALG Sess : 2
H323 Q931 ALG Sess   : 4         H323 RAS ALG Sess     : 5
H323 RTP ALG Sess    : 3         H323 245 ALG Sess     : 4
PPTP ALG Sess        : 1         RTSP ALG Sess         : 4
TIMBUKTU ALG Sess    : 3         T120 ALG Sess         : 4
LDAP ALG Sess        : 3         SGICompCore ALG Sess  : 2
MSN MSGR ALG Sess    : 3         IKE ALG Sess          : 2
ESP ALG Sess         : 3         SIP ALG Sess          : 3
ICQ ALG Sess         : 1        ICQ BUDDY ALG Sess     : 2
```

Output field description

Field	Description
Active Translations	The current number of active translation Sessions
Active Rules	The current number of rules which are activated
FTP ALG Sessions	Number of sessions using FTP ALG
SNMP ALG Sessions	Number of sessions using SNMP ALG
RA ALG Sessions	Number of sessions using Real Audio ALG
RMCD Sessions	Number of sessions using Remote Command ALG
L2TP ALG Sessions	Number of sessions using L2TP ALG
MIRC ALG Sessions	Number of sessions using MIRC ALG
CUSEEME UDP ALG Sess	Number of sessions using CUSEEME UDP ALGCurrent number of H323 Sessions.
CUSEEME TCP ALG Sess	Number of sessions using CUSEEME TCP ALG
H323 Q931 ALG Sess	Number of sessions using H323 Q931 ALG
H323 RAS ALG Sess	Number of sessions using H323 RAS ALG
H323 RTP ALG Sess	Number of sessions using H323 RTP ALG
H323 245 ALG Sess	Number of sessions using H323 245 ALG
TIMBUKTU ALG Sess	Number of sessions using TIMBUKTU ALG

Field	Description
T120 ALG Sess	Number of sessions using T120 ALG
LDAP ALG Sess	Total number of LDAP ALG Sessions
SGICompCore ALG Sess	Total number of SGICompCore ALG Sessions
MSN MSGR ALG Sess	Total number of MSN Messenger Sessions
IKE ALG Sess	Total number of IKE ALG sessions.
ESP ALG Sess	Total number of ESP ALG sessions
SIP ALG Sess	Total number of SIP ALG sessions
ICQ ALG Sess	Total number of ICQ ALG Sessions
ICQ BUDDY ALG Sess	Total number of ICQ BUDDY ALG Sessions

Caution None.

References

- *reset nat stats* related commands
- *nat stats* related commands

3.186 get nat translation

Description Use this command to display all the active translations in the system.

Command Syntax ***get nat translation***

Parameters None.

Mode Super-User, User

Example ***$ get nat translation***

Output

```
Interface          : eth-0            Translation index     : 1
Protocol           : TCP              NAT Direction         : OUT
Rule id            : 10               Alg Type              : FTP
Translated In Pkts : 1400             Translated Out Pkts   : 1300
Out Addr           : 202.5.6.1        Out Port              : 21
In Addr            : 192.168.1.3      Translated In Addr    : 202.1.1.1
In Source Port     : 1025             Translated In Port    : 40012
Entry Age(sec)     : 86400
```

Output field description

Field	Description
Interface	The Outside Interface on which the translation is working. It may be: eth-0, veth-0 - *, eoa-0 - *, ppp-0 - *, ...
Translation index	This specifies the index of this active translation.
Protocol	This specifies the protocol for which this translation is working. It may be: *Any, TCP, UDP, GRE, ICMP, or IANA* specified protocol between 0 to 256.
NAT Direction	This tells the translation direction.
Alg Type	This specifies the Alg Type in use. The value 0 means no ALG is in use.
Rule id	Rule identifier of the rule that has created this session entry.
Translated In Pkts	The number of inbound packets translated by this rule.
Translated Out Pkts	The number of Outbound packets translated by this rule.
Out Addr	The IP Address of the remote End.
Out Port	This specifies the remote port.
In Addr	The Inside IP address.
Translated In Addr	The translated Inside IP address.
In Source Port	The inside source port for the translations.
Translated In Port	The translated inside port.

Field	Description
Pkts Translated	The number of packets translated by this rule.
Entry Age	The age of the entry in seconds.

Caution This command can be executed only when NAT Admin Status is enabled. Please refer to the *modify nat global* command.

References

- *nat* related commands

3.187 get nbsize

Description Use this command to see the sizing parameters whose modification takes effect after the next reboot.

Command Syntax ***get nbsize***

Parameters None.

Mode Super-User, User

Example ***$ get nbsize***

Output Verbose Mode On/Off:

```
Max IP Session: 100      HTTP Port : 80
Telnet Port   : 23      FTP Port  : 21
Serial Auth   : Enable
```

Output field description

Field	Description
Max IP Session	This specifies the maximum number of active IP sessions.
HTTP Port	This specifies the HTTP port
Telnet Port	This specifies the telnet port
FTP Port	This specifies the FTP port
Serial Auth	This specifies whether Serial Port Authentication is enabled or disabled.

Caution None.

References

- *modify nbsize* commands

3.188 get oam cc vc

Description Use this command to to get the OAM F5 end to end continuity check configuration and status parameters.

Command Syntax ***get oam cc vc [ifname*** *interface-name]*

Parameters

Name	Description
ifname *interface-name*	This parameter specifies the VC interface for which information is desired. In case the field is not specified, then the information for all valid interfaces is displayed.Type: OptionalValid values: aal5-*

Mode User, Super-User

Example ***$ $ get oam cc vc ifname*** *aal5-0*

Output Verbose Mode On:

```
Ifname   Mode  SourceOperStatus EtherCheck SinkOperStatusInitiator
-------------------------------------------------------------------------
aal5-0  auto  activated        enable      LOC             Peer
```

Verbose Mode Off:

```
Ifname   Mode  SourceOperStatus EtherCheck SinkOperStatusInitiator
-------------------------------------------------------------------------
aal5-0  auto  activated        enable      LOC             Peer
```

Output field description

Field	Description
Ifname	This parameter specifies VC interface.
Mode	This specifies the mode of activation/deactivation of continuity check.
SourceOperStatus	This field specifies the current operational state of source point of the VCC.
EtherCheck	This field specifies whether ethernet device status should be checked before transmitting a CC cell.
SinkOperStatus	This field specifies the current operational state of sink point of the VCC.
Initiator	This field is valid only in auto mode and it specifies the current initiator of CC Activation/Deactivation.

Caution None.

References

- *modify oam cc vc* commands

3.189 get oam lpbk vc

Description Use this command to display result of previous OAM loopback command.

Command Syntax ***get oam lpbk vc ifname*** interface-name

Parameters

Name	Description
ifname interface-name	This parameter specifies the interface for which information is desired. In case the field is not specified, then the information for all valid interfaces should be displayed. **Type:** Mandatory **Valid values:** *aal5-0* - *

Mode Super-User.

Example ***$ get oam lpbk vc ifname*** **aal5-0**

Output

```
If-Name            : aal5-0   VPI           : 1        VCI        : 1
LB Type            : e2e
OAM Location Id    : 0xffffffffffffffffffffffffffffffff
OAM LB Result      : E2e Succeeded
```

Output field description

Field	Description
If-Name	The name of the aal5 (*aal5-0* etc.) interface whose statistics are to be retrieved.
VPI	This is the Virtual Port Identifier
VCI	This is the Virtual Circuit Identifier
LB Type	This specifies the loop back type used. It may be: *e2e* or *seg*
OAM Location Id	This defines the loop back site which was used to loopback the cell.
OAM LB Result	This specifies the result of the loop back test. It may be *Result Unavailable*, *Seg Succeeded*, *Seg Failed*, *E2e Succeeded*, *E2e Failed*, *Test Aborted*, or *Test In Progress*

Caution None.

References

- *atm trfdesc* related commands
- *atm vc* related commands
- *modify oam lpbk* command
- *atm port* and *statistics* related commands

3.190 get pfraw block

Description Use this command to get the pfraw block status for a given protocol.

Command Syntax ***get pfraw block protocol IPV6MCAST|8021Q|ARP|BPDU|IPX|NETBEUI|APPLETALK|RARP|IPMCAST|PPE***

Parameters

Name	Description
protocol IPV6MCAST|8021Q|ARP|BPDU|IPX|NETBEUI|APPLETALK|RARP|IPMCAST|PPE	This object specifies the protocol for which pfraw rule needs to be blocked/unblocked.

Mode Super-User and User

Example ***$ get pfraw block protocol L2WALL***

Output Verbose Mode On:

```
Protocol      : l2wall          Rule status : Enable
```

Verbose Mode Off:

```
Protocol      : l2wall          Rule status : Enable
```

Output field description

Field	Description
Protocol	This field indicates which pfraw protocol is to be blocked.
Rule Status	This field indicates the rule is enabled or disabled.

Caution None.

References *modify pfraw block* command.

3.191 get pfraw global

Description Use this command to get global parameters of raw filter.

Command Syntax ***get pfraw global***

Parameters None.

Mode Super-User and User

Example ***$ get pfraw global***

Output Verbose Mode On:

```
Status         : Disable
Default action : Deny
```

Verbose Mode Off:

```
Status         : Disable
Default action : Deny
```

Output field description

Field	Description
Status	This field indicates whether the raw filter is enabled or disabled.
Default action	This field indicates the default action to be taken if the packet does not match any of the specified rules.

Caution None.

References *modify pfraw global* command..

3.192 get pfraw rule info

Description Use this command to get the attributes of rules and sub-rules based on interface and direction.

Command Syntax ***get pfraw rule info [ifname*** interface-name***] [dir*** **in**|**out***] [ruleid*** rule-id***] [subruleid*** subrule-id***]***

Parameters

Name	Description
ifname interface-name	This specifies the interface name for which the rule info is sought. **Type:** Optional **Valid values:** *eth-0, veth-0, veth-1…, ppp-0 - *, …, eoa-0 - *1, veth-2, veth-3*
dir in**|**out	This specifies the direction for which the applicable rule information is sought. **Type:** Optional **Valid values:** *in* or *out*
ruleid rule-id	This identifies the rule index of the rule for which information is sought. **Type:** Optional **Valid values:** *0 - 65535* Only existing rule ids accepted as input.
subruleid sub-rule-id	This specifies the sub-rule index of the sub-rule for which information is sought. **Type:** Optional **Valid values:** *0 - 254* Only existing rule ids accepted as input.

Mode Super-User and User

Example ***$ get pfraw rule info ifname eth-0 dir in***

Output Verbose Mode On:

```
Rule id        : 2                     Rule status     : Enable
Sub Rule id    : 1                     Sub Rule status : Enable
Interface      : ppp-0                 In interface    : eth-0
Direction      : Out                   Offset from     : Linkh
Offset         : 6
Comp operation : Range
Low value      : 0x00000000FF000000
High value     : 0x00000000FFCD0000
Mask           : 0x00000000FFFF0000    SSB             : 0x34
SSB Mask       : 0xff
Priority       : 1                   Action            : Accept
Logging        : Match
```

Output field description

Field	Description
Rule id	This identifies the rule index of the rule.
Rule Status	This specifies whether this rule is enabled or disabled.
Sub Rule id	This specifies the sub-rule index of the sub-rule.
Sub Rule status	This specifies whether this subrule is enabled or disabled.
Interface	This specifies the interface name for a rule.
In Interface	This specifies the incoming interface for the given outgoing interface.
Direction	This specifies the filtering direction to which this rule is applied.
Offset from	This specifies the start position in the packet for an offset. The start position can be the beginning of the header or data portions of various protocols.
Offset	This specifies the offset with in the header or data part of the packet.
Comp Operation	This specifies the type of comparison that is done on the extracted data and the comparison value(s)
Low Value	This is hexadecimal pattern to be used for comparison when comparison type is Range.
High Value	This is hexadecimal pattern to be used for comparison when comparison type is Range.
Value	This is hexadecimal pattern to be used for comparison when comparison type is Relational.
Mask	This is hexadecimal pattern which specifies the mask
SSB	Service Specification Byte value to be set in the packet
SSB Mask	Service Specification Byte value mask
Priority	Priority value to be attached to the packet
Action	This specifies the action taken when a packet matches this rule
Logging	This specifies the log option of this rule

Caution None.

References *pfraw* related commands.

3.193 get upnp cfg

Description Use this command to get UPNP global configuration.

Command Syntax ***get upnp cfg***

Parameters None

Mode Super-User and User

Example ***$ get upnp cfg***

Output Verbose Mode On/Off:

```
Next Boot Status             : enable
Advertisement Cache Age(sec) : 40
Current Status               : enable
```

Output field description

Field	Description
Next Boot Status	This field specifies the next boot status of UPNP module.
Advertisement Cache Age(sec)	This field specifies the advertisement cache age in seconds of Internet Gateway Device
Current Status	This field specifies the current status of UPNP module.

Caution None.

References

- *modify upnp cfg* command

3.194 get pfraw rule entry

Description Use this command to get a rule for filtering info.

Command Syntax ***get pfraw rule entry [ruleid*** rule-id ***]***

Parameters

Name	Description
ruleid rule-id	This identifies the rule index with which a rule was created. **Type** : Optional **Valid values:** 0 - 65535

Mode Super-User and User

Example ***$ get pfraw rule entry ruleid 36***

Output Verbose Mode On/Off:

```
Rule id : 2                    Rule status : Enable
Interface : eth-0              In interface : All
Direction : Out                SSB          : 0x34
SSB Mask : 0xff                Priority     : 1
Action   : Accept              Logging      : Match
Out interface : ALL
```

Output field description

Field	Description
Rule id	This identifies the rule index of the rule.
Rule Status	This specifies whether this rule is enabled or disabled.
Interface	This specifies the interface name for a rule.
In Interface	In case of a rule for an outgoing interface, this specifies the incoming interface. Only packets, which are received on the inifname, and which are going out via the ifname, are matched against this rule..
Direction	This specifies the filtering direction to which this rule is applied.
SSB	Service Specification Byte value to be set in the packet.
SSB Mask	Service Specification Byte value mask
Priority	Priority value to be attached to the packet
Action	This specifies the action taken when a packet matches this rule.

Field	Description
Logging	This specifies the log option of this rule.
Out interface	This specifies the outgoing interface. Only packets which are received on the outifname and which are coming in via the ifname will be matched against this rule.

Caution None.

References *pfraw* commands

3.195 get pfraw rule stats

Description Use this command to get raw filter stats for a given rule id or for all the rule-ids.

Command Syntax ***get pfraw rule stats [ruleid*** rule-id***]***

Parameters

Field	Description
ruleid rule-id	This identifies the rule index for which the statistics should be shown. **Type:** Optional **Valid values:** *0 - 65535* Only existing rule ids accepted as input.

Mode Super-User and User.

Example ***$ get pfraw rule stats ruleid 1***

Output Verbose Mode On:

```
Rule id Packets count
-------------------------
1           4
```

Verbose Mode Off:

```
Rule id Packets count
-------------------------
1           4
```

Output field description

Field	Description
Rule id	This field indicates whether the raw filter status is enabled or disabled.
Packets count	This field indicates the number of packets matching this rule.

Caution None.

References

- *get pfraw stats* command

3.196 get pfraw stats

Description Use this command to get global statistics of raw filter.

Command Syntax ***get pfraw stats***

Parameters None.

Mode Super-User and User

Example ***$ get pfraw stats***

Output Verbose Mode On:

```
Total rules    : 0
Packets count  : 0
```

Verbose Mode Off:

```
Total rules    : 0
Packets count  : 0
```

Output field description

Field	Description
Packets count	This field tells the total packets given to the raw filter.
Total rules	This field tells the existing number of rules.

Caution None.

References

- *get pfraw rule stats* command

3.197 get pfraw subrule entry

Description Use this command to get a subrule filtering info.

Command Syntax ***get pfraw subrule entry [ruleid rule-id] [subruleid subrule-id]***

Parameters

Name	Description
ruleid rule-id	This identifies the rule index with which a rule was created. **Type** : Optional **Valid values:** 0 - 65535
subruleid subrule-id	This identifies the subrule index with which a subrule was created. **Type** : Optional **Valid values:** 0 - 254.

Mode Super-User and User

Example ***$get pfraw subrule entry ruleid 111 subruleid 2***

Output Verbose Mode On/Off:

```
Sub Rule id     : 2              Rule id       : 111
Sub Rule status : Disable        Offset from   : Linkh
Offset          : 10
Comp operation  : Lower equal
Value           : 0X0123
Mask            : 0X127A
```

Output field description

Field	Description
Sub Rule id	This identifies the sub-rule index of the sub-rule.
Rule id	This specifies the rule index of the rule of which this is the subrule.
Sub Rule status	This specifies whether this subrule is enabled or disabled.
Offset from	This specifies the start position in the packet for an offset. The start position can be the beginning of the header or data portions of various protocols.
Offset	This specifies the offset within the header or data part of the packet.
Comp Operation	This specifies the type of comparison that is done on the extracted data and the comparison value(s).
Low Value	This is the hexadecimal pattern to be used for comparison, when comparison type is Range.

Field	Description
High Value	
Value	This is the hexadecimal pattern to be used for comparison, when comparison type is Relational.
Mask	This is the hexadecimal pattern which specifies the mask with which the data in the packet is masked before using it for comparison.

Caution None.

References

- *pfraw* commands.

3.198 get ppe acserv

Description Use this command to get the Service names supported by the Access Concentrators on the specified interface.

Command Syntax ***get ppe acserv ifname*** interface-name

Parameters

Name	Description
ifname interface-name	This specifies the Interface on which VC on which the AC Name – Service Name query is to be sent. **Type:** Mandatory **Valid values:** *aal5-0 - *, ppp-0 to ppp-63*

Mode Super-User, User

Example ***$ get ppe acserv ifname*** **aal5-0**

Output

```
If-name       : aal5-0
AC Name       : AC1
Service Name  : Srv1
```

Output field description

Field	Description
If-Name	This specifies the VC on which the AC Name – Service Name query was sent.
AC Name	This specifies the Access Concentrator name
Service Name	This specifies the service name supported by the Access Concentrator

Caution None.

References

- *ppe pconf* related commands

3.199 get ppe cfg

Description Use this command to get PPPoE global configuration parameters.

Command Syntax ***get ppe cfg***

Parameters None.

Mode Super-User, User

Example ***$ get ppe cfg***

Output

```
Max PADI Attempts            : 3  Max PADR Attempts          : 3
Max Disc Attempts            : 3  Initial PADI Time Diff(sec)  : 2
Initial PADR Time Diff (sec) : 2  AC Selection Policy        : first-come
PADI per PADT                : 1
```

Output field description

Field	Description
Max PADI Attempts	This specifies the maximum number of PADI attempts that shall be made by PPPoE.
Max PADR Attempts	This specifies the maximum number of PADR attempts that shall be made by PPPoE
Max Disc Attempts	This specifies the maximum number of discovery attempts that shall be made by PPPoE
Initial PADI Time Diff (Secs)	This specifies the initial PADI time difference (in seconds) for retries.
Initial PADR Time Diff (Secs)	This specifies the initial PADR time difference (in seconds) for retries.
AC Selection Policy	This specifies the default AC selection policy used by PPPoE. It may be: *first-come, serv-to-ac*
PADI per PADT	This specifies the number of PADI to be sent before each PADT.

Caution None.

References

- *modify ppe cfg* command
- *ppe pconf* related commands
- *ppe stats global* related commands
- *ppe stats session* related commands

3.200 get ppe pconf

Description This command is used for getting information on all the configured policy table entries.

Command Syntax ***get ppe pconf***

Parameters None.

Mode Super-User, User

Example ***$ get ppe pconf***

Output

```
Ac Name        : AC1
Service Name   : Srv1
```

Output field description

Field	Description
ACName	This specifies the Access Concentrator name
ServiceName	This specifies the service name

Caution None.

References

- *delete ppe pconf* command
- *create ppe pconf* command
- *ppe cfg* related commands
- *get ppe stats global* command
- *get ppe stats session* command

3.201 get ppe stats global

Description Use this command to get global PPPoE statistics.

Command Syntax ***get ppe stats global***

Parameters None.

Mode Super-User, User

Example ***$ get ppe stats global***

Output

```
Session Reqs     : 100              Sessions Term       : 56
Sessions Estd    : 60               Sessions Not Estd   : 40
PADI Msgs Sent   : 100              PADO Msgs Rcvd      : 100
PADR Msgs Sent   : 65               PADS Msgs Rcvd      : 60
PADT Msgs Sent   : 40               PADT Msgs Rcvd      : 16
Data Msgs Sent   : 6000             Data Msgs Rcvd      : 4000
```

Output field description

Field	Description
Session Reqs	This specifies the number of session requests received.
Sessions Estd	This specifies the number of sessions established
Sessions Not Estd	This specifies the number of sessions could not be established
Sessions Term	This specifies the number of sessions terminated
PADI Msgs Sent	This specifies the number of PADI messages sent
PADO Msgs Rcvd	This specifies the number of PADO messages received
PADR Msgs Sent	This specifies the number of PADR messages sent
PADS Msgs Rcvd	This specifies the number of PADS messages received
PADT Msgs Sent	This specifies the number of PADT messages sent
PADT Msgs Rcvd	This specifies the number of PADT messages received
Data Msgs Sent	This specifies the number of session data messages sent
Data Msgs Rcvd	This specifies the number of session data messages received

Caution None.

References

- *ppe pconf* related commands
- *ppe stats session* related commands
- *ppe cfg* related commands

3.202 get ppe stats session

Description Use this command to get PPE statistics per session.

Command Syntax ***get ppe stats session [ifname*** interface-name***]***

Parameters

Name	Description
ifname interface-name	This specifies the Interface on which PPP is running. If this is not specified then information for all interfaces is displayed. **Type:** Optional **Valid values:** *ppp-0 - *, ...*

Mode Super-User, User

Example ***$ get ppe stats session ifname ppp-0***

Output

```
If-Name          : ppp-0
PADI Msgs Sent   : 10              PADO Msgs Rcvd      : 10
PADR Msgs Sent   : 4               PADS Msgs Rcvd      : 3
Data Msgs Sent   : 60              Data Msgs Rcvd      : 40
```

Output field description

Field	Description
If-Name	This specifies the PPPoE interface for which session stats are being shown.
PADI Msgs Sent	This specifies the number of PADI messages sent
PADO Msg Rcvd	This specifies the number of PADO messages received
PADR Msgs Sent	This specifies the number of PADR messages sent
PADS Msgs Rcvd	This specifies the number of PADS messages received

Caution None.

References

- *ppe cfg* related commands
- *ppe stats global* related commands
- *ppe pconf* related commands

3.203 get ppp global

Description Use this command to get PPP global informationl

Command Syntax ***get ppp global***

Parameters None

Mode User

Example ***$ get ppp global***

Output

```
PPP Inactivity Timeout : 0       Ignore WAN to LAN traffic : False
PPP Keep Alive         : enable  Max LCP Echo Requests     : 10
Max Auth Tries         :  4      Auth Retry Delay(sec)     :1
```

Output field description

Field	Description
PPP Inactivity Timeout	This specifies the Inactivity timeout for PPP sessions.
Ignore WAN to LAN traffic	Flag indicating whether to ignore WAN to LAN traffic for PPP Session timeout.
PPP Keep Alive	This specifies whether the PPP Keep alive feature is enabled, disabled or auto.
Max LCP Echo Requests	This specifies the number of unanswered echo requests.
Max Auth Tries	This field specifies Max Number of tries for Authentication.
Auth Retry Delay(sec)	This field specifies the Delay between 2 successive tries for Authentication.

Caution None

References

- *modify ppp global* command

3.204 get ppp intf

Description Use this command to get information on a particular PPP interface or on all PPP interfaces

Command Syntax ***get ppp intf [ifname*** interface-name***]***

Parameters

Name	Description
ifname interface-name	This specifies the Interface for PPP Links. If this is not specified then information for all interfaces is displayed. **Type:** Optional **Valid values:** *ppp-0 - *, ...*

Mode Super-User, User

Example ***$ get ppp intf ifname*** **ppp-0**

Output

```
Entry Created

If-Name               : ppp-0          L2TP Call type        : inlac
Interface Sec Type    : Public         Phy Interface         : aal5-0
Configured IP Address : 0.0.0.0        NAT Direction         : OUT
Init MRU              : 1500           Magic                 : False
Encapsulation         : PPPOA          Service Name          : -
UseDhcp               : False          UseDns                : False
DRoute                : False          Status                : Start
Gateway IP Address    : 202.1.1.2     Associated Num If-Name : eth-0
Use Gateway           : remote
Configured MTU        : 300            Actual MTU            : 200
```

Output field description

Field	Description
If-Name	This specifies the PPP interface for the PPP Links: It may be: *ppp-0, ppp-1…*
L2TP Call Type	This field specifies the l2tp call type.
Interface Sec Type	Interface security type.
Phy Interface	This specifies Name of the lower interface on which PPP is running. It may be: *aal5-0, aal5-1…*
Configured IP Address	This specifies the IP Address for the PPP Link.
NAT Direction	This variable specifies whether this interface's address is inside or outside. It may be: *inside, outside, none*
Init MRU	The initial Maximum Receive Unit (MRU) that the local PPP entity will advertise to the remote entity
Magic	This specifies whether the local node will attempt to perform Magic Number negotiation with the remote node. It may be: *True, False*

Field	Description
Encapsulation	This specifies the lower layer protocol used below this PPP Link. It may be: *PPPOA, PPPOE*
Service Name	This specifies the service name used for PPPoE. It is generally the name of the ISP.
UseDhcp	This specifies whether DHCP is to be used for address negotiation. It may be either True or False
UseDns	This specifies whether DNS server addresses are to be obtained using IPCP or not.
Droute	Default Route
Status	This shows whether PPP session on this interface is active. It may be: *Start, Stop, StartOnData.*
Gateway IP Address	This specifies the IP Address of the Gateway.
Associated Num If-Name	This specifies the interface name of the associated numbered interface. A "-" indicates that this ppp interface is not associated with any numbered interface.
Use Gateway	This specifies whether local or remote gateway is to be used.
Configured MTU	This specifies the MTU value configured by the user for PPP interface.
Actual MTU	This specifies the MTU value actually operational for PPP interface.

Caution None.

References

- *delete ppp intf* command
- *create ppp intf* command
- *modify ppp intf* command
- *ppp lstatus* related commands
- *ppp security* related commands

3.205 get ppp ipinfo

Description Use this command to get PPP IP status on a particular PPP interface or on all the PPP interfaces.

Command Syntax ***get ppp ipsinfo [ifname*** interface-name***]***

Parameters

Name	Description
ifname interface-name	Identifies the interface. If no interface name is specified then information for all interfaces is retrieved. **Type:** Optional **Valid values:** *ppp-0 - *, ppp-1...*

Mode Super-User, User

Example ***$ get ppp ipinfo***

Output

```
If-name         :   ppp-0            Status            :  Opened
Self Ip Address  :  172.25.2.100     Peer Ip Address   :  175.30.2.100
Prim DSN Server :   123.24.1.100    Sec DNS Server     :  125.60.2.200
-------------------
```

Output field description

Field	Description
Self Ip Address	Self IP address of the PPP interface
Peer Ip Address	Remote IP Address of the PPP interface
Prim DNS Server	Primary DNS Server address.
Sec DNS Server	Secondary DNS Server address

Caution This command can be executed only when a valid PPP Interface exists.

References

- *create ppp intf* command
- *get ppp lstatus* command

3.206 get ppp lstatus

Description Use this command to get link status on a particular PPP interface or on all the PPP interfaces.

Command Syntax ***get ppp lstatus [ifname*** `interface-name`***]***

Parameters

Name	Description
ifname `interface-name`	Identifies the interface. If no interface name is specified then information for all interfaces is retrieved. **Type:** Optional **Valid values:** *ppp-0 - *, ...*

Mode Super-User, User

Example ***$ get ppp lstatus***

Output

```
If-name            : ppp-0     Lower-If           : aal5-0
Local MRU          : 1500      Remote MRU         : 1500
L2R Protocol Comp  : Enable    R2L Protocol Comp  : Enable
L2R AC Comp        : Enable    R2L AC Comp        : Enable
Operational Status: Down    Last Fail Cause     : No Valid PADO recvd

Current Auth Tries : 3
```

Output field description

Field	Description
If-name	The Interface of PPP on which IPCP is running. It may be: ppp-0 - *, ...
Lower-If	This identifies the lower-level interface over which this PPP Link is operating. It may be: aal5-0 - *
Local MRU	The current value of the MRU for the local PPP Entity. This value is the MRU that the remote entity is using when sending packets to the local PPP entity. The value of this object is meaningful only when the link has reached the open state, i.e., `Oper Status` as shown by `get interface stats` is *Up*
Remote MRU	The current value of the MRU for the local PPP Entity. This value is the MRU that the remote entity is using when sending packets to the local PPP entity. The value of this object is meaningful only when the link has reached the open state, i.e., `Oper Status` as shown by `get interface stats` is *Up*

Field	Description
L2R Protocol Comp	Indicates whether the local PPP entity will use Protocol Compression when transmitting packets to the remote PPP entity. The value of this object is meaningful only when the link has reached the open state, i.e., `Oper Status as` shown by `get interface stats` is *Up* It may be: *Enable, Disable*
R2L Protocol Comp	Indicates whether the remote PPP entity will use Protocol Compression when transmitting packets to the local PPP entity. The value of this object is meaningful only when the link has reached the open state, i.e., `Oper Status as` shown by `get interface stats` is *Up* It may be: *Enable, Disable*
L2R AC Comp	Indicates whether the local PPP entity will use Address and Control Compression when transmitting packets to the remote PPP entity. The value of this object is meaningful only when the link has reached the open state, i.e., `Oper Status as` shown by `get interface stats` is *Up* It may be: *Enable, Disable*
R2L AC Comp	Indicates whether the remote PPP entity will use Address and Control Compression when transmitting packets to the local PPP entity. The value of this object is meaningful only when the link has reached the open state, i.e., `Oper Status as` shown by `get interface stats` is *Up* It may be: *Enable, Disable*
Operational Status	The operational status of the interface. Values can be Up, Down, Lcp, Auth, Ncp, Dhcp.
Last Fail Cause	This gives the reason for last failure of PPP Link.It may be: - No Valid PADO recvd, No Valid PADS recvd, Stopped by User, No Activity, Auth Failure, Internal failure
Current Auth Tries	This field specifies the number of tries made for Authentication.

Caution This command can be executed only when a valid PPP Interface exists.

References

- *`create ppp intf`* command
- *`get ppp iptatus`* command
- create ipoa map
- delete ipoa map
- get ipoa map

3.207 get ppp security

Description Use this command to get information on a particular ppp security secrets entry or for all entries.

Command Syntax ***get ppp security [ifname*** interface-name***]***

Parameters

Name	Description
ifname interface-name	This specifies the PPP interface for which the security entry is to be displayed. If this is not specified then information for all PPP interfaces is displayed. **Type:** Optional **Valid values:** *ppp-0 - *, ..., default*

Mode Super-User, User

Example ***$ get ppp security ifname*** **ppp-0**

Output Verbose Mode On

```
IfName   : ppp-0      Protocol : PAP
Login    : abc
```

Verbose Mode Off

```
Entry Created
```

Output field description

Field	Description
IfName	This specifies the PPP interface for which the security entry has been displayed. It may be: *ppp –0 - *..., default.* The *default* entry gets used in case there is no specific entry for that interface.
Protocol	This is the protocol used for authentication It may be: *PAP, CHAP*
Login	This is the login name

Caution None.

References

- *delete ppp security* command
- *create ppp security* command
- *modify ppp security* command
- *ppp lstatus* related commands
- *ppp intf* related commands

3.208 get radius acctserv config

Description Use this command to get Radius Accounting Server Configuration

Command Syntax ***get radius acctserv config [index*** index ***]***

Parameter

Name	Description
index index	A number uniquely identifying each RADIUS Accounting server with which this client communicates **Type:** Optional **Valid values:** 1 - 2147483647

Mode Super-User, User

Example ***$ get radius acctserv config index*** 1

Output

```
Server Index       : 1          IP address      : 192.166.56.67
Port               : 1700       Retries         : 5
Start timeout(sec) : 60         On timeout(sec) : 60
Current State      : Start
```

Output field description

Field	Description
Server Index	A number uniquely identifying each RADIUS Accounting server with which this client communicates.
IP address	The IP address of the RADIUS server referred to in this table entry.
Port	The server port to which the client sends accounting requests.
Retries	The number of times the request packet shall be retransmitted to the server on getting timed out.
Start timeout(sec)	The time in seconds for which the client needs to wait before retransmitting the Accounting START request packet to the server.
On timeout(sec)	The time in seconds for which the client needs to wait before retransmitting the Accounting ON request packet to the server.
Current State	The current state of the accounting server.

Caution None

References

- *create radius acctserv config* command
- *delete radius acctserv config* command
- *modify radius acctserv config* command

3.209 get radius acctserv stats

Description Use this command to get Radius Accounting Server Statistics

Command Syntax ***get radius acctserv stats [index*** index ***]***

Parameter

Name	Description
index index	A number uniquely identifying each RADIUS Accounting server with which this client communicates **Type:** Optional **Valid values:** 1 - 2147483647

Mode Super-User, User

Example ***$ get radius acctserv stats index*** 1

Output

```
Server Index        : 1
IP address          : 192.166.56.67    Port               : 200
RTT(1/100th sec)    : 300              Requests Tx        : 30
Retransmissions     : 20               Responses Rx       : 20
Malformed Responses : 20               Bad Authenticators : 20
PendingRequests     : 20               Timeouts           : 10
Unknown Types       : 30               Packets Dropped    : 30
```

Output field description

Field	Description
Server Index	A number uniquely identifying each RADIUS Accounting server with which this client communicates.
IP address	The IP address of the RADIUS server referred to in this table entry.
Port	The server port to which the client sends accounting requests.
RTT(1/100th sec)	The time interval in hundredths of a second between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from this RADIUS Accounting server.
Requests Tx	The number of RADIUS Accounting-Request packets sent to this server. This does not include retransmissions.
Retransmissions	The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server. Retransmissions include retries where the Identifier and Acct-Delay have been updated, as well as those in which they remain the same.
Responses Rx	The number of RADIUS packets received on the accounting port from this server.

Field	Description
Malformed Responses	The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses
Bad Authenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Signature attributes received from this server
PendingRequests	The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Acess-Accept, Access-Reject or Access-Challenge, a timeout or retransmission.
Timeouts	The number of Accounting timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
Unknown Types	The number of RADIUS packets of unknown type which were received from this server on the Accounting port.
Packets Dropped	The number of RADIUS packets of which were received from this server on the Accounting port and dropped for some other reason.

Caution None

References

- *reset radius acctserv stats* command

3.210 get radius authserv config

Description Use this command to get Radius Authentication Server Configuration

Command Syntax ***get radius authserv config [index*** index ***]***

Parameter

Name	Description
index index	A number uniquely identifying each RADIUS Authentication server with which this client communicates **Type:** Optional **Valid values:** 1 - 2147483647

Mode Super-User, User

Example ***$ get radius authserv config index*** 1

Output

```
Server Index : 1
IP address   : 192.166.56.67    Port                          : 1800
Retries      : 5                Retransmission timeout(sec) : 60
```

Output field description

Field	Description
Server Index	A number uniquely identifying each RADIUS Authentication server with which this client communicates
IP address	The IP address of the RADIUS server referred to in this table entry.
Port	The server port to which the client sends authentication requests
Retries	The number of times the request packet shall be transmitted to the server on getting timed out.
Retransmission timeout(sec)	The time, in seconds, for which the client needs to wait before retransmitting the request packet to the server.

Caution None

References

- *create radius authserv config* command
- *delete radius authserv config* command
- *modify radius authserv config* command

3.211 get radius authserv stats

Description Use this command to get Radius Authentication Server Statistics

Command Syntax ***get radius authserv stats [index*** index ***]***

Parameter

Name	Description
index index	A number uniquely identifying each RADIUS Authentication server with which this client communicates. **Type:** Optional **Valid values:** 1 - 2147483647

Mode Super-User, User

Example ***$ get radius authserv stats index*** 1

Output

```
Server Index                : 1
IP address                  : 192.166.56.67     Port                : 200
RTT(1/100th sec)            : 300               Requests Tx         : 30
Retransmissions             : 20                Accepts             : 20
Rejects                     : 20                Challenges          : 20
Malformed Access Responses  : 20                Bad Authenticators  : 20
PendingRequests             : 20                Timeouts            : 10
Unknown Types               : 30                Packets Dropped     : 30
```

Output field description

Field	Description
Server Index	A number uniquely identifying each RADIUS Authentication server with which this client communicates.
IP address	The IP address of the RADIUS server referred to in this table entry.
Port	The server port to which the client sends authentication requests.
RTT(1/100th sec)	The time interval in hundredths of a second between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from this RADIUS authentication server.
Requests Tx	The number of RADIUS Access-Request packets sent to this server. This does not include retransmissions.
Retransmissions	The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.
Accepts	The number of RADIUS Access-Accept packets (valid or invalid) received from this server

Field	Description
Rejects	The number of RADIUS Access-Reject packets (valid or invalid) received from this server
Challenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from this server
Malformed Access Responses	The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or Signature attributes or unknown types are not included as malformed access responses.
Bad Authenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Signature attributes received from this server
PendingRequests	The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Acess-Accept, Access-Reject or Access-Challenge, a timeout or retransmission.
Timeouts	The number of authentication timeouts to this server.After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
Unknown Types	The number of RADIUS packets of unknown type which were received from this server on the authentication port.
Packets Dropped	The number of RADIUS packets of which were received from this server on the authentication port and dropped for some other reason.

Caution None

References

- *reset radius authserv stats* command

3.212 get radius global config

Description Use this command to get Radius Global Configuration

Command Syntax ***get radius global config***

Parameter None

Mode Super-User, User

Example ***$ get radius global config***

Output

```
Status                          : enable
Authentication Client Identifier : AuthClientIdentifier1
Accounting Client Identifier     : AcctClientIdentifier1
Interim Accounting Interval(sec) : 100
```

Output field description

Field	Description
Status	This field specifies the global status of radius client.This field being 'enable' implies this radius client is enabled, and 'disable' implies disabled.
Authentication Client Identifier	The name of the NAS identifier of the RADIUS authentication client. String of up to IAD_RADIUS_MAX_NAS_NAME_LEN characters (A-Z, a-z, 0-9,-,_)
Accounting Client Identifier	The name of the NAS identifier of the RADIUS accounting client. String of up to IAD_RADIUS_MAX_NAS_NAME_LEN characters (A-Z, a-z, 0-9,-,_)
Interim Accounting Interval(sec)	This field specifies the interval in seconds after which the interim accounting update will be sent to the server. If interim update attribute is received in access-accept response pkt from RADIUS server, it indicates that interim update is to be sent. Valid Values : 0 and between 60 and 4294967295, both inclusive. If configured interim update interval is not 0, then it is used, otherwise the time interval sent by RADIUS server is used.

Caution None

References

- *modify radius global config* command

3.213 get radius global stats

Description Use this command to get Radius Global Statistics

Command Syntax ***get radius global stats***

Parameter None

Mode Super-User, User

Example ***$ get radius global stats***

Output

```
Authentication Client Invalid Server Addresses : 10
Accounting Client Invalid Server Addresses     : 20
```

Output field description

Field	Description
Authentication Client Invalid Server Addresses	The number of RADIUS Access-Response packets received from unknown addresses.
Accounting Client Invalid Server Addresses	The number of RADIUS Accounting-Response packets received from unknown addresses.

Caution None

References None

3.214 get rip global

Description Use this command to get the global parameters of RIP.

Command Syntax ***get rip global***

Parameters None.

Mode Super-User and User

Example ***get rip global***

Output Verbose Mode On

```
RIP status               : enable
RIP route update time(sec): 30
RIP route age time(sec)   : 180
```

Verbose Mode Off

```
RIP status               : enable
RIP route update time(sec): 30
RIP route age time(sec)   : 180
```

Output field description

Field	Description
RIP status	This tells whether RIP is enabled or disabled
RIP route update time	This tells the timer frequency at which the RIP would broadcast its routes to all its neighbors
RIP route age time	This tells the timer frequency at which RIP would age a route, if an update is not received for this duration.

Caution None.

References

- *get rip intf* command
- *modify rip* global
- *create rip intf* command

3.215 get rip intf

Description Use this command to get RIP protocol parameters on the specified IP Interface.

Command Syntax ***get rip intf [ifname*** interface-name***]***

Parameters

Name	Description
ifname interface-name	Specifies the IP Interface name on which RIP is to be started. **Type:** Optional **Valid values:** *veth-0-*, ppp-0,ppp-0-*, eoa-0-*, ipoa-0-*, usb-0*

Mode Super-User and User

Example ***get rip intf ifname ppp-0***

Output Verbose Mode On

```
IP Interface Name    : ppp-0      RIP Interface Metric : 1
RIP Send Mode        : rip1       RIP Receive Mode     : rip1
RIP Send Def Route   : Enable     RIP Recv Def Route   : Disable
RIP packet auth      : None
```

Verbose Mode Off

```
IP Interface Name    : ppp-0      RIP Interface Metric : 1
RIP Send Mode        : rip1       RIP Receive Mode     : rip1
RIP Send Def Route   : Enable     RIP Recv Def Route   : Disable
RIP packet auth      : None
```

Output field description

Field	Description
RIP Interface Name	This tells the name of the IP Interface, or on all RIP interfaces, on which information is requested.
RIP Interface Status	This tells whether the RIP Interface is enabled or disabled.
RIP Interface Metric	This tells the metric value attached to the interface. The metric is used by RIP in deciding which among alternate routes is the most optimal
RIP Send Mode	This tells the packet format used for sending RIP updates and requests
RIP Receive Mode	This tells the packet format accepted while receiving RIP updates and requests and responses
RIP Send Def Route	This tells whether default route is to be included in the updates sent on the interface, or not.

Field	Description
RIP Recv Def Route	This tells whether default route is to be processed in the updates received on the interface or not.
RIP packet auth	This tells whether RIP authentication is enabled or not

Caution None.

References

- *get rip global* command
- *create rip intf* command

3.216 get rip stats

Description Use this command to view RIP stats.

Command Syntax ***get rip stats***

Parameters None.

Mode Super-User and User

Example ***get rip stats***

Output Verbose Mode On

```
Requests sent             : 10    Responses sent            : 20
Request pkts received     : 30    Pkts with bad RIP version : 10
Pkts with bad addr family : 3     Pkts with bad req format  : 5
Pkts with bad metrics     : 10    Pkts with bad resp format : 3
Resp from non-RIP port    : 5     Pkts rejected             : 7
Response packets received : 70    Unrecognized packets      : 15
Pkts from non-neighbors   : 3     Failed authentication     : 2
Route changes made by RIP : 7
```

Verbose Mode Off

```
Requests sent             : 10    Responses sent            : 20
Request pkts received     : 30    Pkts with bad RIP version : 10
Pkts with bad addr family : 3     Pkts with bad req format  : 5
Pkts with bad metrics     : 10    Pkts with bad resp format : 3
Resp from non-RIP port    : 5     Pkts rejected             : 7
Response packets received : 70    Unrecognized packets      : 15
Pkts from non-neighbors   : 3     Failed authentication     : 2
Route changes made by RIP : 7
```

Output field description

Field	Description
Requests sent	Number of RIP requests sent
Responses sent	Number of RIP responses sent
Request pkts received	Number of RIP packets received for request
Pkts with bad RIP version	Number of RIP packets received with invalid version
Pkts with bad address family	Number of packets received with incorrect address family
Pkts with bad request format	Number of request packets received with invalid format
Pkts with bad metrics	Number of packets received with metric value not between 1 to 15
Pkts with bad response format	Number of response packets received with invalid format
Resp from non-RIP port	Number of packets received from a port other than specified RIP port

Field	Description
Pkts rejected	Number of packets rejected
Response packets received	Number of RIP packets received for response
Unrecognized packets	Number of unrecognizable packets
Pkts from non-neighbors	Number of packets received from non-neighbor nodes
Failed authentication	Number of requests for which packet authentication has failed
Route changes made by RIP	Number of times the routing table has changed

Caution None.

References None.

3.217 get rmon eventgrp

Description Use this command to get event group information for all event groups or event groups with a specific name.

Command Syntax ***get rmon eventgrp [rname*** event-grp-name***]***

Parameters

Name	Description
rname event-grp-name	This specifies the name of the event group whose information is to be displayed. **Type:** Optional **Valid values:** String of Max. 8 Characters('A'- 'Z', 'a'-'z', '0'-'9','-','_')

Mode Super-User

Example ***$ get rmon eventgrp***

Output

```
Name      Event Flags  Tasks Waiting  First Task
-----------------------------------------------
BUFAVA    0            1              0xa27bc0
EROOT1    0            1              0xc2d578
```

Output field description

Field	Description
Name	This specifies the event group's name.
Event Flags	This indicates the current event flags.
Tasks Waiting	This indicates the no. of tasks waiting on the event flag group.
First Task	This is the address of the first suspended task.

Caution None.

References

- *get rmon* commands for queue, semaphore, mpool and task.

3.218 get rmon mpool

Description Use this command to get memory pool information for all memory pools or memory pools with the specified name.

Command Syntax ***get rmon mpool [rname*** mem-pool-name***]***

Parameters

Name	Description
rname mem-pool-name	This specifies the name of the memory pool whose information is to be displayed. **Type:** Optional **Valid values:** String of Max. 8 Characters('A'- 'Z', 'a'-'z', '0'-'9','-','_')

Mode Super-User

Example ***$ get rmon mpool rname*** **MDGAG**

Output

```
Name          : MDGAG          Size          : 0x270
Min           : 0x28           Free          : 0x0
Tasks Waiting : 0              Suspend Type  : FIFO
Start Addr    : 0x807554       First Task    : 0x0
..
```

Output field description

Field	Description
Name	This specifies the name of the memory pool whose information is to be displayed.
Size	This indicates the total number of bytes in the memory pool.
Min	This indicates the minimum no. of bytes for each allocation from this pool.
Free	This indicates the no. of bytes available in the pool.
Tasks Waiting	This indicates the number of tasks waiting on the dynamic-memory pool.
Suspend Type	This indicates the task suspend type. It may be: *FIFO, PRIORITY*
Start Addr	This is the starting address of the pool.
First Task	This is the address of the first suspended task.

Caution None.

References

- *get rmon* commands for queue, semaphore, task and eventgrp.

3.219 get rmon queue

Description Use this command to get queue information for all queues or queues with a specific name.

Command Syntax ***get rmon queue [rname*** queue-name***]***

Parameters

Name	Description
rname queue-name	This specifies the name of the queue whose information is to be displayed. **Type:** Optional **Valid values:** String of Max. 8 Characters('A'- 'Z', 'a'-'z', '0'-'9','-','_')

Mode Super-User

Example ***$ get rmon queue rname*** **qucli**

Output

```
Name            : QUCLI              Start Addr      : 0x807348
Size            : 0x8                Available Size  : 0x8
Pending Msgs    : 0                  Msg Type        : FIXED
Msg Size        : 0x1                Suspend Type    : PRIORITY
Tasks Waiting   : 0                  First Task Addr : 0x0
..
```

Output field description

Field	Description
Name	This specifies the name of the Queue whose information is being displayed.
Start Addr	This specifies the Starting address for the queue in memory.
Size	This indicates the total number of 4 byte data elements in the queue
Available Size	This indicates the number of 4 byte data elements available in the queue
Pending Msgs	This indicates the no. of messages already in the queue
Msg Type	This specifies the type (depending on size) of messages supported by the queue. This may be: *FIXED, VARIABLE*
Msg Size	This indicates the no. of 4 byte data elements in each queue message. If the queue supports variable length messages, then this no. is the maximum message size.
Suspend Type	This indicates the task suspend type. It may be: *FIFO, PRIORITY*

Field	Description
Tasks Waiting	This indicates the no. of tasks waiting on the queue.
First Task Addr	This is the address of the first suspended task.

Caution None.

References

- *get rmon* commands for task, semaphore, mpool and eventgrp.

3.220 get rmon semaphore

Description Use this command to get semaphore information for all semaphores or semaphores with a specific name.

Command Syntax ***get rmon semaphore [rname*** semaphore-name***]***

Parameters

Name	Description
rname semaphore-name	This specifies the name of the semaphore whose information is to be displayed. **Type:** Optional **Valid values:** String of Max. 8 Characters ('A'- 'Z', 'a'-'z', '0'-'9','-','_')

Mode Super-User

Example ***$ get rmon semaphore rname*** **TCP**

Output

```
Name        Count       Suspend Type   Tasks Waiting    First Task Addr
-------------------------------------------------------------------------
TCP         1           FIFO           0                0x0
```

Output field description

Field	Description
Name	This specifies the name of the semaphore.
Count	This is the current instance count of the semaphore.
Suspend Type	This indicates the task suspend type. It may be: *FIFO, PRIORITY*
Tasks Waiting	This indicates the no. of tasks waiting on the queue.
First Task Addr	This is the address of the first suspended task.

Caution None.

References

- *get rmon* commands for queue, task, mpool and eventgrp.

3.221 get rmon task

Description Use this command to get task information for all tasks or tasks with a specific name.

Command Syntax ***get rmon task [rname*** task-name***]***

Parameters

Name	Description
rname task-name	This specifies the name of the task whose information is to be displayed. **Type:** Optional **Valid values:** String of Max. 8 Characters('A'- 'Z', 'a'-'z', '0'-'9','-','_')

Mode Super-User

Example ***$ get rmon task rname roottask***

Output

```
Name           : ROOTTASK            Status         : PURE SUSPEND
Sched Count    : 69                  Priority       : 1
Preempt        : Yes                 Time Slice     : 0
Stack Base     : 0xfb0050            Stack Size     : 0x400
Min Stack Size : 0x0
```

Output field description

Field	Description
Name	The name of the task information related to which is being displayed
Status	Current Status of the Task. It may be: *READY, PURE SUSPEND, FINISHED, TERMINATED, SLEEP SUSPEND, MAILBOX SUSPEND, QUEUE SUSPEND, PIPE SUSPEND, EVENT SUSPEND, SEMAPHORE SUSPEND, MEMORY SUSPEND, PARTITION SUSPEND, DRIVER SUSPEND*
Sched Count	The No. of times the task has been scheduled
Priority	The priority of the task. The lower the value, the higher is the priority of the task.
Preempt	This indicates whether the task is preemptable or not. It may be: *Yes, No*
Time Slice	This indicates the task's time slice value. A value of *0* indicates that time slicing for this task is disabled.
Stack Base	This is the starting address of the task's stack.

Field	Description
Stack Size	This indicates the total no. of bytes in the task's stack
Min Stack Size	This indicates the minimum no. of bytes left in the task's stack

Caution None.

References

- *get rmon* commands for queue, task, mpool and eventgrp.

3.222 get sizeinfo

Description Use this command to get the configuration of the system sizing parameters.

Command Syntax ***get sizeinfo***

Parameters None.

Mode User

Example ***$ get sizeinfo***

Output

```
Entry Created

Max PPE Sessions          : 8         Max TBG MAC address : 256
Max VCs                   : 8         Max 1483 VCs        : 8
Max PFRaw Rules           : 64        Max PFRaw Subrules  : 68
Max IPF Rules              : 50       Max L2TP Tunnel     : 1
Max L2TP Sess pwer Tunnel  : 1        Max L2TP Peer RWS   : 4

Output field description
```

Field	Description
Max PPE Sessions	This specifies the maximum number of PPPoE sessions supported in the system.
Max TBG MAC address	This specifies the maximum number of MAC address that can be learned by bridging module.
Max VCs	This specifies the maximum number of VCCs supported over all ATM ports.
Max 1483 VCs	This specifies the maximum 1483 connections used for MEA5.
Max PFRaw Rules	This specifies the maximum number of raw filter rules that can be created in the system.
Max PFRaw Subrules	This specifies the maximum number of raw filter subrules that can be created in the system.
Max IPF Rules	This specifies the maximum number of IP filter rules that can be created in the system.
Max l2tp Tunnel	Maximum number of L2TP tunnels supported in the system
Max L2TP Sess pwer Tunnel	Maximum number of PPP sessions supported per L2TP tunnel.
Max L2TP Peer RWS	Maximum size of peer receive window size that can be handled

Caution None.

References

- *size* command

3.223 get smtp servaddr

Description Use this command to get SMTP server address.

Command Syntax ***get smtp servaddr***

Parameters None.

Mode User, Super-User

Example ***$ get smtp servaddr***

Output Verbose Mode on/off

```
Server Address    Server Domain Name
-------------------------------------------------
192.168.1.1       abc.def.com
```

Output field description

Field	Description
Server Address	IP address of the SMTP server..
Server Domain Name	The fully qualified domain name of the SMTP server.

Caution None.

References

- *modify smtp servaddr* command

3.224 get snmp comm

Description This command is used for getting information about entries in the community table.

Command Syntax ***get snmp comm [community*** comm-name***]***

Parameters

Name	Description
community comm-name	This specifies the Community name. If no community name is specified then information for all communities is displayed. **Type:** Optional **Valid values:** String of Max. 50 Characters('A'- 'Z', 'a'-'z', '0'-'9','-','_')

Mode Super-User, User

Example ***$ get snmp comm***

Output

```
Access          Community
------------------------
RO              public
```

Output field description

Field	Description
Community	This specifies the Community name
Access	This specifies the access permissions given to managers with this community name. It may be: *RO* (Read Only), *RW* (Read-Write)

Caution None.

References

- *create snmp comm* command
- *delete snmp comm* command
- *snmp trap* related commands
- *snmp host* related commands
- *snmp stats* related commands

3.225 get snmp host

Description Use this command to get information about all entries in the SNMP host table.

Command Syntax ***get snmp host***

Parameters None.

Mode Super-User, User

Example ***$ get snmp host***

Output

```
Host Address              Community
-----------------------------------
192.168.1.3               public
```

Output field description

Field	Description
Host Address	This specifies the IP address of the manager that has access permissions for the modem.
Community	This specifies the Community name.

Caution None.

References

- *create snmp* host command
- *delete snmp* host command
- *SNMP trap* related commands
- *SNMP comm* related commands
- *SNMP stats* related commands.

3.226 get snmp stats

Description Use this command to display global SNMP statistics.

Command Syntax ***get snmp stats***

Parameters None.

Mode Super-User, User

Example ***$ get snmp stats***

Output

```
Rx Pkts count           : 0          Tx Pkts count           : 0
Rx Bad Versions count   : 0          Rx Bad Comm count       : 0
Rx Bad Comm Use count   : 0          Rx ASN Errs count       : 0
Rx Too Big count        : 0          Tx Too Big count        : 0
Rx NoSuchName count     : 0          Tx NoSuchName count     : 0
Rx Bad Values count     : 0          Tx Bad Values count     : 0
Rx Gen Errs count       : 0          Tx Gen Errors count     : 0
Rx Tot Req Vars count   : 0          Rx Tot Set Vars count   : 0
Rx Get Req count        : 0          Tx Get Req count        : 0
Rx Get Next Req count   : 0          Tx Get Next Req count   : 0
Rx Set Req count        : 0          Tx Set Req count        : 0
Rx Get Response count   : 0          Tx Get Response count   : 0
Rx Traps count          : 0          Tx Traps count          : 0
Rx Read Onlys count     : 0
```

Output field description

Field	Description
Rx Pkts count	The total number of messages delivered to the SNMP entity from the transport service.
Tx Pkts count	The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service.
Rx Bad Versions count	The total number of SNMP Messages which were delivered to the SNMP protocol entity and were for an unsupported SNMP version.
Rx Bad Community count	The total number of SNMP Messages delivered to the SNMP protocol entity which used a SNMP community name not known to said entity.
Rx Bad Comm Uses count	The total number of SNMP Messages delivered to the SNMP protocol entity which represented an SNMP operation which was not allowed by the SNMP community named in the Message.
Rx ASN Errs count	The total number of ASN.1 or BER errors encountered by the SNMP protocol entity when decoding received SNMP Messages.
Rx Too Big count	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is *tooBig*.

Field	Description
Tx Too Big count count	The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field is *tooBig*.
Rx NoSuchName count	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is *noSuchName*
Tx NoSuchName count	The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field is *noSuchName*
Rx Bad Values count	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is *Badvalue*
Tx Bad Values count	The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field is *BadValue*.
Rx Gen Errs count	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is *genErr*.
Tx Gen Errors count	The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field is *genErr'*
Rx Tot Req Vars count	The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs
Rx Tot Set Vars count	The total number of MIB objects which have been altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs
Rx Get Requests count	The total number of SNMP Get-Request PDUs which have been accepted and processed by the SNMP protocol entity
Tx Get Requests count	The total number of SNMP Get-Request PDUs which have been generated by the SNMP protocol entity.
Rx Get Next Req count	The total number of SNMP Get-Next PDUs which have been accepted and processed by the SNMP protocol entity
Tx Get Next Req count	The total number of SNMP Get-Next Request PDUs which have been generated by the SNMP protocol entity
Rx Set Requests count	The total number of SNMP Set-Request PDUs which have been accepted and processed by the SNMP protocol entity
Tx Set Requests count	The total number of SNMP Set-Request PDUs which have been generated by the SNMP protocol entity.

Field	Description
Tx Too Big count count	The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field is *tooBig*.
Rx NoSuchName count	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is *noSuchName*
Tx NoSuchName count	The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field is *noSuchName*
Rx Bad Values count	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is *Badvalue*
Tx Bad Values count	The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field is *BadValue*.
Rx Gen Errs count	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is *genErr*.
Tx Gen Errors count	The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field is *genErr*'
Rx Tot Req Vars count	The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs
Rx Tot Set Vars count	The total number of MIB objects which have been altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs
Rx Get Requests count	The total number of SNMP Get-Request PDUs which have been accepted and processed by the SNMP protocol entity
Tx Get Requests count	The total number of SNMP Get-Request PDUs which have been generated by the SNMP protocol entity.
Rx Get Next Req count	The total number of SNMP Get-Next PDUs which have been accepted and processed by the SNMP protocol entity
Tx Get Next Req count	The total number of SNMP Get-Next Request PDUs which have been generated by the SNMP protocol entity
Rx Set Requests count	The total number of SNMP Set-Request PDUs which have been accepted and processed by the SNMP protocol entity
Tx Set Requests count	The total number of SNMP Set-Request PDUs which have been generated by the SNMP protocol entity.

Field	Description
Rx Get Response count	The total number of SNMP Get-Response PDUs which have been accepted and processed by the SNMP protocol entity.
Tx Get Response count	The total number of SNMP Get-Response PDUs which have been generated by the SNMP protocol entity
Rx Traps count	The total number of SNMP Trap PDUs which have been accepted and processed by the SNMP protocol entity
Tx Traps count	The total number of SNMP Trap PDUs which have been generated by the SNMP protocol entity.
Rx Read Onlys count	The total number valid SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is *readOnly*.

Caution None.

References

- *snmp host* related commands
- *snmp trap* related commands
- *snmp comm* related commands
- *snmp stats* related commands.

3.227 get snmp trap

Description Use this command to get the SNMP trap status and check whether it is enabled or disabled.

Command Syntax ***get snmp trap***

Parameters None.

Mode Super-User, User

Example ***$ get snmp trap***

Output

```
Snmp Trap Enabled
```

Output field description

Field	Description
Snmp Trap	This is the SNMP Trap Status. It may be: *Enabled, Disabled*

Caution None.

References

- *modify snmp trap* command
- *snmp host related* commands
- *snmp comm* related commands
- *snmp stats* related commands.

3.228 get sntp cfg

Description Use this command to get SNTP configuration information.

Command Syntax ***get sntp cfg***

Parameters None

Mode Super-User, User

Example ***$ get sntp cfg***

Output

```
Status : Enable
```

Output field description

Field	Description
Status	SNTP service is enabled or disabled.

Caution None.

References

- *create sntp servaddr* command
- *delete sntp servaddr* command
- *modify sntp cfg* command
- *get sntp cfg* command
- *get sntp stats* command
- *reset sntp stats* command

3.229 get sntp servaddr

Description Use this command to get SNTP server address information.

Command Syntax ***get sntp servaddr [<ip-address> | dname <domain-name>]***

Parameters

Name	Description
<ip-address> | dname <domain-name>	This parameter specifies the IP address or fully qualified domain name of the SNTP server for which information is required. **Type**: Optional **Valid values**: Valid IP address or fully qualified domain name.

Mode Super-User, User

Example ***$ get sntp servaddr 192.68.1.1***

Output

```
Server Addr : 192.168.1.1 Status : Active
Domain Name : abc.com
```

Output field description

Field	Description
Server Addr	IP address of the SNTP server.
Status	Operational Status of the SNTP server address entry.
Domain Name	The fully qualified domain name of the SNTP server.

Caution None.

References

- *create sntp servaddr* command
- *delete sntp servaddr* command
- *modify sntp cfg* command
- *get sntp cfg* command
- *get sntp stats* command
- *reset sntp stats* command

3.230 get sntp stats

Description Use this command to get statistical information about SNTP.

Command Syntax ***get sntp stats [<ip-address> | dname <domain-name>]***

Parameters None

Mode Super-User, User

Example ***$ get sntp stats***

Output

```
Requests count         : 20       Response count      : 19
Invalid Response count : 19       Lost Response count : 20
Last Time Stamp [MM/DD/YYYY::HH:MM:SS]   : 01/01/2002:00:00:00
```

Output field description

Field	Description
Requests count	Number of SNTP Requests sent to SNTP server.
Response count	Number of valid SNTP responses received from SNTP server.
Invalid Response count	Number of Invalid SNTP Responses received from SNTP server.
Lost Response count	The number of lost responses against the SNTP request
Last Time Stamp	Time at which the local clock was last set or corrected.

Caution None.

References

- *create sntp servaddr* command
- *delete sntp servaddr* command
- *get sntp servaddr* command
- *modify sntp cfg* command
- *get sntp cfg* command
- *reset sntp stats* command

3.231 get stp info

Description Use this command to display the current status of the Spanning Tree Protocol Group.

Command Syntax ***get stp info***

Parameters None.

Mode Super-User, User

Example ***$ get stp info***

Output

```
Protocol Spec.     : IEEE 8021D                 Priority            : 0x8000
Top. Changes       : 1                          Curr Top. Age(sec)  : 35.0
Desig Root         : 80:00:00:10:5A:6C:DB:20     Root Cost           : 0
Root If-name       : None                       Hold Time (sec)     : 1.0
Br Max Age(sec)    : 20                         Curr Max Age (sec)  : 20.0
Br Hello Time(sec): 2                           Curr Hello Time(sec) : 2.0
Br Fwd Delay(sec)  : 15                         Curr Fwd Delay (sec) : 15.0
Status             : Enable
```

Output field description

Field	Description
Protocol Spec	This indicates the Spanning Tree Protocol running. It may be: *DECLB100, IEEE 8021D, Unknown*
Priority	Bridge Priority. It is equal to the value of the 1st 2 octets of the designated Bridge Id. The value as given in '`bridge static`' commands represents the last 6 octets of the Id.
Top. Changes	This specifies the number of times the topology was changed since reset
Curr Top. Age (Sec)	This specifies the time elapsed (in seconds) since the last topology change
Desig Root	This specifies The Bridge Id of the root of the spanning tree as determined by the STP running on this node. This value is used as the Root Identifier parameter in all Configuration Bridge PDUs originated by this node.
Root Cost	The cost of the path to the root as seen from this bridge
Root If-name	The interface which offers the lowest cost path from this bridge to the root bridge
Hold Time (Sec)	This minimum time interval in seconds, between two Configuration bridge PDUs transmitted by this node.

Field	Description
Br Max Age (Sec)	The maximum age (in seconds) of Spanning Tree Protocol information learned from the network on any port before it is discarded when this Bridge is the root of the Spanning Tree. It may range between *6* and *40*.
Curr Max Age (Sec)	The actual maximum age (in seconds) of Spanning Tree Protocol information learned from the network on any port before it is discarded.It is derived from the Br Max Age of the Root Node. 802.1D-1990 specifies that the range for this parameter is related to the value of "Br Hello Time"
Br Hello Time (Sec)	The value (in seconds) that all bridges use for Hello-Time when this bridge is acting as the root. It may range between: *1* and *10*
Curr Hello Time (Sec)	The actual amount of time between the transmission of Configuration bridge PDUs by this node on any port
Br Fwd Delay (Sec)	The value (in seconds) that all bridges use for Forward Delay when this bridge is acting as the root. 802.1D-1990 specifies that the range for this parameter is related to the value of "Br Max Age". It may range between: *4* and *30*
Curr Fwd Delay (Sec)	This actual time value, (in seconds) which determines how fast a port changes its spanning state when moving towards the Forwarding state. It is used to determine how long the port stays in each of the Listening and Learning states, which precede the Forwarding state. It is also used when a topology change has been detected and is underway, to age all dynamic entries in the Forwarding Database.
Status	Global status of STP

Caution None.

References

- *modify stp global* command
- *stp port related* commands.

3.232 get stp port

Description Use this command to display port specific information for the Spanning Tree Protocol, for all ports, or for the specified port.

Command Syntax ***get stp port info [ifname*** interface-name***]***

Parameters

Name	Description
ifname interface-name	The port for which this entry contains Spanning Tree Protocol management information. If no interface name is specified, then information for all entries is displayed. **Type** : Optional **Valid values:** *eth-0, eoa-0*, usb-0**

Mode Super-User, User

Example ***$ get stp port ifname*** **eth-0**

Output

```
Port Name    : eth-0                    Priority          : 0x0
State        : Forwarding               Status            : Enable
Path Cost    : 100                      Desig Cost        : 0
Desig Root:  : 00:20:00:10:5A:6C:DB:20  Desig Bridge:     : 00:20:00:10:5A:6C:DB:20
Desig Port   : 0x0020                   Fwd Transitions   : 2
```

Output field description

Field	Description
Port Name	The port for which this entry contains Spanning Tree Protocol management information
Priority	Port Priority. It is contained in the first octet of the 2 octet Port Id. The other octet is used to derive the port name above.
State	The port's current state for STP. This state controls what action a port takes on reception of a frame. For example, a malfunctioning port will be placed in the broken state. The valid values are: Disabled, Blocking, Listening, Learning, Forwarding, Broken
Status	The Admin Status of the port. The possible values are: *Enable, Disable*
Path Cost	The contribution of this port to the path cost of paths towards the spanning tree root which included this port. 802.1D-1990 recommends that the default value of this parameter be in inverse proportion to the speed of the attached LAN.

Field	Description
Desig Cost	The path cost of the Designated Port of the segment connected to this port. This value is compared to the Root Path Cost field in received
Desig Root	The unique Bridge Identifier of the Bridge recorded as the Root in the Configuration BPDUs transmitted by the Designated Bridge for the segment to which the port is attached
Desig Bridge	The Bridge Identifier of the bridge which this port considers to be the Designated Bridge for this port's segment
Desig Port	The Port Identifier of the port on the Designated Bridge for this port's segment
Fwd Transitions	The number of times this port has transitioned from the Learning state to the Forwarding state

Caution None.

References

- *modify stp port* command
- *stp global* related commands
- *bridge ports* related commands

3.233 get system

Description Use this command to display the system parameters.

Command Syntax ***get system***

Parameters None.

Mode Super-User, User

Example ***$ get system***

Output

```
Model           : Titanium
Name            : Name of the unit
Domain Name     : conexant.com
Description     : DSL Modem
Location        : Conexant Systems, Inc.,100 Schulz Drive, Red Bank,NJ 07701,U.S.A
Contact         : Conexant Systems,Inc.,100 Schulz Drive, Red Bank,NJ 07701,U.S.A
Vendor          : Conexant Systems,Inc.,100 Schulz Drive, Red Bank,NJ 07701,U.S.A
LogThreshold    : 0
Object-id       : 1.3.6.1.4.1.200
HwVersion       : 810012
SwVersion       : VIK-1.37.020618f/T93.3.16
DSL Version     : T93.3.16
System Time     : Thu Jan 01 00:00:10 1970
Time Zone       : GMT
DST             : Off
Services        : physical datalink internet end-to-end applications
UpTime(HH:MM:SS): 0:0:10
Backup Interval(mins): 10
```

Output field description

Field	Description
Model	This specifies the model-name of the system
Name	This specifies the host name of the modem
Domain Name	This specifies the domain name of this modem
Description	This is description of the DSL modem
Location	This specifies the physical location of this modem
Contact	This shows the textual identification of the contact person for this modem, together with information on how to contact this person.
Vendor	This shows the vendor-specific information
LogThreshold	This specifies the severity level of trap equal to or lower than which shall be logged. 1 is the lowest level representing critical traps.
Object-id	This shows the vendor's authoritative identification of the network management subsystem contained in the modem.
HwVersion	This specifies the hardware and firmware version of the modem
SwVersion	This specifies the software version of the modem

Field	Description
DSL Version	This specifies the DSL-version of the system
System Time	This shows the current system time.
Time Zone	This specifies the time zone that has been set on the modem.
DST	This specifies whether Daylight Saving Time has been enabled or not.
Services	This specifies the functionality provided by this modem. These may be: *physical, datalink, internet, end-to-end, applications*
Up Time	This specifies the time in Hours:Min:Sec since the modem was up
Backup Interval(mins)	This specifies the backup interval (mins) of the dhcp server. A value of "immediate" will indicate that flash backups are to be done whenever the configuration gets updated. A value of "disable" will indicate that backups are never done by DHCP.

Caution None.

References

- `modify system` command

3.234 get tcp conn

Description Use this command to get all the TCP connection entries.

Command Syntax ***get tcp conn***

Parameters None.

Mode Super-User, User

Example ***$ get tcp conn***

Output

```
Local Addr       Local Port   Remote Addr      Remote Port
-------------------------------------------------------------------------
192.168.1.11     80           202.34.4.5       80
```

Output field description

Field	Description
Local Addr	The local IP address for the TCP connection.
Local Port	The local port number for the TCP connection.
Remote Addr	The remote IP address for the TCP connection
Remote Port	The remote port number for the TCP connection.

Caution None.

References

- *delete tcp conn* command
- *get tcp stats* command
- *get udp listen* command.

3.235 get tcp stats

Description Use this command to display global TCP statistics.

Command Syntax ***get tcp stats***

Parameters None.

Mode Super-User, User

Example ***$ get tcp stats***

Output

```
ReTx Algorithm        : VANJ          ReTx Min Timeout(ms)  : 250
ReTx Max Timeout(ms)  : 240000        Max Connections       : 30
Active Opens          : 0             Passive Opens         : 0
Failed Attempts       : 0             Establish Resets      : 0
Current Establishes   : 0             In Segments           : 0
Out Segments          : 0             ReTx Segments         : 0
In Errors             : 0             Out Resets            : 0
```

Output field description

Field	Description
ReTx Algorithm	The algorithm used to determine the timeout value used for retransmitting unacknowledged octets. It may be: *VANJ*
ReTx Min Timeout	The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds
ReTx Max Timeout	The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds
Max Connections	The limit on the total number of TCP connections the entity can support
Active Opens	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state
Passive Opens	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
Failed Attempts	The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.
Establish Resets	The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state
Current Establishes	The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT
In Segments	The total number of segments received, including those received in error. This count includes segments received on currently established connections

Field	Description
Out Segments	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
ReTx Segments	The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
In Errors	The total number of segments received in error (e.g., bad TCP checksums).
Out Resets	The number of TCP segments sent containing the RST flag

Caution None.

References

- *delete tcp conn* command
- *get tcp conn* command
- *get udp stats* command
- *get icmp stats* command.

3.236 get trace cfg

Description Use this command to display the trace configuration for a specific module or for all modules.

Command Syntax ***get trace cfg [module*** module-name|***all]***

Parameters

Name	Description
module module-name|***all***	This is a string representing the trace stream the information pertaining to which is to be displayed. If no module name is specified then information for all is displayed. **Type:** Optional **Valid values:** *GCOS, ALPS, MEA5, OAM, CIN, and so on*

Mode Super-User, User

Example ***$ get trace cfg module GAG***

Output

```
Module    Flow          Level         Type       Destn              Port
-------------------------------------------------------------------------
GAG       0x0           0x0           Stdout     0.0.0.0            0
```

Output field description

Field	Description
Module	This specifies the module for trace/log config whose information is being displayed: It can be: GCOS, ALPS, MEA5, OAM, CIN, GAG, CDB, LED, CLI, SAG, HAG, PPE, ATM, DCL, EOA, TBG, PPP, EMAC, DSL, USB, SPI, NVM, SPAN, SSI
Flow	This indicates a Hexadecimal bitmask which sets the filter for trace flow.
Level	This indicates a Hexadecimal bitmask which sets the filter for trace level.
Type	This specifies the type of logging to be done. It may be: Syslog, Net, Stdout
Destn	This specifies the IP address for host for logging for trace type syslog and net. It is invalid incase of trace type stdout
Port	Port number on which host is listening for trace info to be logged incase of trace type syslog and net. It is invalid incase of trace type stdout

Caution None.

References

- *modify trace cfg* command
- *get trace stats* command.

3.237 get trace stats

Description Use this command to display trace statistics.

Command Syntax ***get trace stats***

Parameters None.

Mode Super-User, User

Example ***$ get trace stats***

Output

```
Bytes Logged: 2744          Bytes Discarded : 40595
Msgs Logged : 19            Msgs Discarded  : 1045
```

Output field description

Field	Description
Bytes Logged	This specifies the number of bytes logged by the tracing/logging module
Bytes Discarded	This specifies the number of bytes discarded by the tracing/logging module due to filtering
Msgs Logged	This specifies the number of message logged by the tracing/logging module
Msgs Discarded	This specifies the number of messages discarded by the tracing/logging module due to filtering

Caution None.

References

- *get trace cfg* command
- *modify trace cfg* command

3.238 get traps

Description This command can be used to get the listing of all traps or the last few traps.

Command Syntax ***get traps*** ***[***num-of-traps***]***

Parameters

Name	Description
num-of-traps	This specifies the maximum number of (entries) traps to be displayed from trap log table; if not specified then all entries are displayed. **Type:** Optional **Valid values:** *0 to 4294967295*

Mode Super-User, User

Example ***$ get traps***

Output

```
Thu Jan 01 00:00:13 1970 : STATUS ALARM : ATM VC Up :Interface Name- aal5-0
```

Output field description The output fields in this command are separated by a ":"

Field	Description
Trap time	This specifies the time at which the trap was logged.
Trap severity	This specifies the severity level of the trap. It can be – CRITICAL ALARM MAJOR ALARM WARNING STATUS ALARM IPOA Interface Up/Down

Field	Description
Trap name	This specifies the name of the trap. It can be – ***System Init Failed*** - This trap is originated at the time of system initialization failures. The failure could be due to an internal error or due to a wrong/corrupted configuration file. Trap parameters are *Module* and *Cause.* ***System Up*** - This trap is originated after the modem boots up successfully. ***DSL Interface Up*** - This trap indicates that the DSL loop is up. ***DSL Interface Down*** - This trap indicates that the DSL loop is down. ***ATM Interface Up*** - This trap indicates that the ATM port is operationally up. Trap parameter is *Interface No.* ***ATM Interface Down*** - This trap indicates that the ATM port is operationally down. Trap parameter is *Interface No.* ***ETHER Interface Up*** - This trap indicates that the Ethernet port is operationally up. Trap parameter is *Interface No.* ***ETHER Interface Down*** - This trap indicates that the Ethernet port is operationally down. Trap parameter is *Interface No.* ***ATM VC Up*** - This trap indicates that the ATM VC is operationally up. Trap parameter is *Interface Name.* ***ATM VC Down*** - This trap indicates that the ATM VC is operationally down. Trap parameter is *Interface Name.* ***PPP Interface Up*** - This trap indicates that the PPP link is operationally up. Trap parameter is *Interface No.* ***PPP Interface Down*** - This trap indicates that the PPP link is operationally down. Trap parameter is *Interface No.* ***ATM VC Congested*** - This trap indicates that the ATM VC is congested. Trap parameter is *Interface Name.* ***PPP Authorization Failed*** - This trap indicates that the PPP user authorization with peer has failed. Trap parameter is *Interface No.* ***User Authorization Failed*** - This trap indicates that the modem's user authentication has failed. Trap parameter is *<user name>.* ***DHCP Server Address Pool Threshold Low*** - This trap indicates that number of free ip addresses in a pool has gone below the threshold set for the pool by the user. Trap parameter is *IP*. ***DHCP Server Duplicate Address Request*** - This trap indicates that the DHCP server tried to assign an IP address from one of its pools to a client but found that the address was already being used by some host on the LAN (without the DHCP server's knowledge). The server then marks this address as allocated in its pool and doesn't try to assign it to a client again. Trap parameter is *IP*. ***Failed To Get IP Address*** - This trap indicates that DHCP client or PPP link couldn't get an ip address from DHCP server or remote peer respectively. Trap parameter is *Interface No.* ***DHCP Server Intf Create Failed*** - This trap indicates that DHCP server could not be enabled on an interface. Trap parameter is *Interface No.* ***DHCP Relay Intf Create Failed*** - This trap indicates that DHCP relay could not be enabled on an interface. Trap parameter is *Interface No.* ***Raw Filter Intf Create Failed*** - This trap indicates that raw filter could not be enabled on an interface. Trap parameter is *Interface No.*

Field	Description
Trap Name (cont'd)	***Cold Start recvd from ILMI NW side*** – This trap indicates that cold start has been received from network side. Trap parameter is *Interface No.* ***VCC change recvd from ILMI NW side*** - This trap indicates that the VCC change trap has been received from network side. Trap parameters are *Port, VPI* and *VCI.* ***Ilmi AC - Config Mismatch*** - This trap indicates that there is a difference in the configuration of at least one VC between the local copy (retrieved earlier from network side) and the current retrieved copy. The difference could be addition, deletion or modification of one or more VC at the network-side. In this condition, the system comes up with the retrieved configuration along with the user configured VCs. If this trap is generated immediately after the system is started then the user should reconfigure the interfaces above the VCs such as EOA, PPP and so on, as the procedure discards local configuration above VCs. However, if this trap is followed by *Ilmi AC initiated - Link up* trap, it indicates that the procedure has detected a difference between the configuration at network side and the local configuration. To retrieve the latest configuration, the user should reboot the system. Trap parameters are *Port, VPI* and *VCI.* ***Ilmi AC - Unsupported Protocol*** - This trap indicates that the modem does not support the given layer-2/layer-3 access protocol. Trap parameters are *Port, ProtID, Layer-2*/*Layer-3.* ***Ilmi AC - Unsupported Srvc category*** - This trap indicates that traffic descriptor parameter(s) received for given VC is not supported. Trap parameters are *Port, VPI* and *VCI.* ***Ilmi AC - AAL not supported*** - This trap indicates that AAL type for given VC is not supported. Trap parameters are *Port, VPI* and *VCI.* ***Ilmi AC - Invalid Vpi/Vci*** - This trap indicates that the VPI and VCI values are greater than those supported. Trap parameters are *Port, VPI* and *VCI.* ***Ilmi AC - Max VCCs limit exceeded*** - This trap indicates that the VCs received from network side are more than supported. Trap parameter is *Interface No.* ***Ilmi AC - Incomp Config*** - This trap indicates that the entries corresponding to index are not present either in AAL or in Service type table. Trap parameters are *Port, VPI, VCI* and *Tbl.* ***Ilmi AC - Inconsistent Information -*** This trap indicates that the configuration information received from network side is inconsistent. Trap parameter is *Interface No.* ***Ilmi AC - System Up from Local Copy -*** This trap indicates that ILMI auto configuration could not be started because of ATM link being down and that the system has come up with the local copy. Trap parameter is *Interface No.* ***Ilmi AC initiated - Link up -*** This trap indicates that ILMI auto configuration has started its operation after the link has come up. Trap parameter is *Interface No.* ***Ilmi connection lost with network side*** – This trap indicates that ILMI connectivity with network side has been lost. Trap parameter is *Interface No.* ***USB Interface Up:*** This trap indicates that the USB port is operationally up. The trap parameter is Interface No.

Field	Description
Trap Name (cont'd)	***USB Interface Down:*** This trap indicates that the USB port is operationally down. The trap parameter is Interface No. ***LOFS Threshold:*** This trap indicates that Loss of Framing threshold has reached. The trap parameters are the current and threshold values. ***LOSS Threshold:*** This trap indicates that Loss of Signal threshold has reached. The trap parameters are the current and threshold values. ***ESS Threshold:*** This trap indicates that Errored Seconds threshold has reached. The trap parameters are the current and threshold values. ***SES Threshold*:** This trap indicates that Severely Errored Seconds threshold has reached. The trap parameters are the current and threshold values. ***UAS Threshold:*** This trap indicates that Unavailable Errored Seconds threshold has reached. The trap parameters are the current and threshold values. ***SVC Created:*** This trap indicates that the SVC has been created. The trap parameters are ATM port, VPI & VCI values. ***SVC Deleted:*** This trap indicates that the SVC has been deleted. The trap parameters are VC If index, ATM port, VPI & VCI values. ***SVC Creation Failed:*** This trap indicates that the SVC creation has failed. The trap parameters are VC If index and fail cause. ***IPOA Interface Up:*** This trap indicates that the IPOA interface is operationally up. The trap parameter is Interface No. ***IPOA Interface Down:*** This trap indicates that the IPOA interface is operationally down. The trap parameter is Interface No. ***ADET Successful:*** This trap indicates that Auto Detection is successful. There are no trap parameters. ***ADET Failed:*** This trap indicates that Auto Detection has failed. There are no trap parameters. ***ADET Invalid Entry:*** During an autodetect configuration procedure, this trap indicates that some entry in the autoconfiguration file is incorrect. ***L2TP Tunnel Up:*** This trap indicates that the L2TP tunnel is operationally up. The trap parameter is tunnel if index. ***L2TP Tunnel Down:*** This trap indicates that the L2TP tunnel is operationally down. The trap parameter is tunnel if index. ***L2TP Session Up**:* This trap indicates that the L2TP session is operationally up. The trap parameter is session if index. ***L2TP Session Down:*** This trap indicates that the L2TP session is operationally down. The trap parameter is session if index. ***Hardware Reboot:*** When a reboot is given or the reset button is pressed, this trap indicates that the system is verifying whether there is any task writing anything into the flash. If there is, then the system waits for the flash access to finish before initiating the reboot. ***PPPOE Interface Up:*** This trap indicates that the PPPOE interface is operationally up. The trap parameter is Interface No. ***PPPOE Interface Down:*** This trap indicates that the PPPOE interface is operationally down. The trap parameter is Interface No.

Field	Description
Trap Name (cont'd)	***PPP Authorization Successful:*** This trap indicates that the PPP user authorization with the peer has succeeded. The trap parameter is Interface No. ***SAAL Up:*** This trap indicates that SAAL is operationally up. ***SAAL Down***: This trap indicates that SAAL is operationally down. ***System Memory Low:*** This trap indicates that the system memory is running low. The trap parameter is the free system memory.
Trap parameters	This specifies additional parameters describing the trap. Different traps have different combinations of trap parameters. There are also some traps with no additional parameters. The parameters can be - Module - <module name> Cause - <failure cause> Interface No - <interface index> Interface Name - <interface name> <user name> IP - <IP address> Port - <port number> VPI - <vpi> VCI - <vci> Tbl - <table name> ProtID - <protocol number> <Layer-2/Layer-3>

Caution None.

References

- *reset traps* command.
- *logthresh* parameter in *modify system* and *get system* commands

3.239 get trapprints

Description Use this command to get the current status of trap prints on CLI.

Command Syntax ***get trapprints***

Parameters None

Mode Super-User, User

Example ***$ get trapprints***

Output

```
Trap Prints Enabled
```

Output field description None

Caution None.

References

- *modify trapprints* command

3.240 get udp listen

Description This command is used to display UDP listener table entries.

Command Syntax ***get udp listen***

Parameters None.

Mode Super-User, User

Example ***$ get udp listen***

Output

```
Local Addr          Local Port
------------------------------
0.0.0.0             161
127.0.0.1           6005
127.0.0.1           6006
127.0.0.1           6007
127.0.0.1           6008
```

Output field description

Name	Description
Local Addr	The local IP address for this UDP listener. In the case of a UDP listener which is willing to accept datagrams for any IP interface associated with the node, the value 0.0.0.0 is used.
Local Port	The local port number for this UDP listener.

Caution None.

References

- *delete tcp conn* command
- *get tcp conn* command
- *get udp stats* command.

3.241 get udp stats

Description Use this command to display global UDP statistics.

Command Syntax ***get udp stats***

Parameters None.

Mode Super-User, User

Example ***$ get udp stats***

Output

```
In Datagrams : 4              Out Datagrams          : 4
In Errors    : 0              Invalid Port Datagrams : 0
```

Output field description

Field	Description
In Datagrams	The total number of UDP datagrams delivered to UDP users.
Out Datagrams	The total number of UDP datagrams sent from this entity.
In Errors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
Ports	The total number of received UDP datagrams for which there was no application at the destination port.

Caution None.

References

- *delete tcp conn* command
- *get tcp conn* command
- *get udp stats* command
- *get tcp stats* command
- *get udp listen* command
- *get icmp stats* command.

3.242 get usagectrl

Description Use this command to get Usage Control Configuration.

Command Syntax ***get usagectrl***

Parameters None

Mode Super-User, User

Example ***$ get usagectrl***

Output Verbose mode on/off

```
Max Data Users     Status          Login         Arp Check Interval(mins)
-------------------------------------------------------------------------------
5                  disable         enable               21
```

Output field description

Field	Description
Max Data Users	This field specifies the maximum number of data users, which can have simultaneous access to the WAN side. It can also have the value 'nolimit' which specifies that all users are allowed to access the WAN side. It can also have the value 'nolimit' which specifies that all users are allowed to access the WAN side.
Status	This field specifies the status of usage control.
Login	This field specifies whether data user login is required for authentication. If disabled, the user is allowed access whenever he does a WAN access, provided the maxusers limit is not reached.
Arp Check Interval(mins)	This field specifies the interval (in minutes) after which an ARP check is to be done to ascertain whether the authenticated user is still online or not.

Caution None.

References

- *modify usagectrl* command
- *get datauserslist* command
- *reset datauserslist* command.

3.243 get usb stats

Description Use this command to get statistical information about a specific or all USB interfaces.

Command Syntax ***get usb stats [ifname*** interface-name***]***

Parameters

Name	Description
ifname interface-name	This parameter specifies the interface for which information is desired. In case the field is not specified, then the information for all valid USB interfaces is displayed. **Type:** Optional **Valid values:** *usb-0.*

Mode Super-User, User

Example ***$ get usb intf ifname usb-0***

Output

```
If-Name    : usb-0
Mode       : PA
Tx Correct Frames count   : 3       Tx Error Frames count      : 3
Rx Correct Frames count   : 2       Rx Error Frames count      : 2
Tx Dir Mode Bytes count   : 0       Tx Dir Mode Frames count   : 0
Rx Dir Mode Bytes count   : 0       Rx Dir Mode Frames count   : 0
Tx Mcast Mode Bytes count : 5000    Tx Mcast Mode Frames count : 50
Rx Mcast Mode Bytes count : 6000    Rx Mcast Mode Frames count : 60
Tx Bcast Mode Bytes count : 4000    Tx Bcast Mode Frames count : 45
Rx Bcast Mode Bytes count : 5000    Rx Bcast Mode Frames count : 50
"Mode : P - Promiscuous,  A - All MCast,  M - MultiCast, B - BroadCast,
        D - Directed"
```

Output field description

Field	Description
If-Name	This specifies the physical Interface name: It can be: *usb-0*
Mode	The mode of the USB interface specified (*Promiscuous*/*Direct*/ *Broadcast*/*Multicast*/*Simplex*).
Tx correct Frames count	The number of Frames Transmitted OK
Rx correct Frames count	The number of Frames Received OK
Tx Error Frames count	The number of Frames Transmitted with Error
Rx Error Frames count	The number of Frames Received with Error
Dir Mode Tx Bytes count	The number of Bytes Transmitted in Directed Mode.
Dir Mode Tx Frames count	The number of Frames Transmitted in Directed Mode

Field	Description
Dir Mode Rx Bytes count	The number of Bytes Received in Directed Mode
Dir Mode Rx Frames count	The number of Frames Received in Directed Mode
Mcast Mode Tx Bytes count	The number of Bytes Transmitted in Multicast Mode
Mcast Mode Tx Frames count	The number of Frames Transmitted in Multicast Mode
Mcast Mode Rx Bytes count	The number of Bytes Received in Multicast Mode
Mcast Mode Rx Frames count	The number of Frames Received in Multicast Mode
Bcast Mode Tx Bytes count	The number of Bytes Transmitted in Broadcast Mode
Bcast Mode Tx Frames count	The number of Frames Transmitted in Broad-cast Mode
Bcast Mode Rx Bytes count	The number of Bytes Received in Broadcast Mode
Bcast Mode Rx Frames count	The number of Frames Received in Broadcast Mode.
Mode	The mode flag of the USB interface specified - PAMBD. P - Promiscuous A - All MCast M - MultiCast B - BroadCast D - Directed

Caution None.

References

- *create usb intf* command
- *delete usb intf* command
- *modify usb intf* command
- *get usb intf* command.

3.244 get usb intf

Description Use this command to get information on a particular USB interface or on all the USB interfaces.

Command Syntax ***get usb intf [ifname*** interface-name***]***

Parameters

Name	Description
ifname interface-name	This parameter specifies the interface for which information is desired. In case the field is not specified, then the information for all valid USB interfaces is displayed. **Type:** Optional **Valid values:** *usb-0.*

Mode Super-User, User

Example ***$ get usb intf ifname usb-0***

Output

```
IfName   If SecType  Ip Address     Mask           Nat Dir      Oper      MTU
-------------------------------------------------------------------------------
usb-0    Public     192.168.1.1    255.255.255.0   Inside       Down      300
```

Output field description

Field	Description
IfName	The name of the interface, which has been created.
Ip Address	IP address assigned to the USB interface.
Mask	Network mask to be applied to the IP Address.
Nat Dir	This specifies the NAT direction, which may be: *inside, outside or none*.
Oper	The actual/current state of the interface. It can be either *Up* or *Down*
If SecType	Interface security type
MTU	This specifies the MTU Size configured for Ethernet over USB interface

Caution None.

References

- *create usb intf* command
- *delete usb intf* command
- *modify usb intf* command
- *get usb stats* command

3.245 get user

Description Use this command to display information of all the users. Password information is not displayed.

Command Syntax ***get user***

Parameters None.

Mode Super-User, Intermediate, User

Example ***$ get user***

Output

```
Privilege     UserName
--------------------------
  root            iad
  user            user1
```

Output field description

Field	Description
UserName	This represents the valid user logins for the modem.
Privilege	This represents the privilege level associated with the user log-ins. It may be: *user, intermediate, root*. In CLI, intermediate privilege has the same previliges as the user. In HTTP, the intermediate privilege has ALL the privileges as the "user" except that he can also modify the ATM VPI and VCI values and the PPP username and password.

Caution None.

References

- *delete user* command
- *create user* command
- *passwd* command

3.246 get wlan fwinfo

Description Use this command to get 802.11 Firmware Information

Command Syntax ***get wlan fwinfo***

Parameter None

Mode Super-User, User

Example ***$ get wlan fwinfo***

Output

```
Agere AP firmware version      : AP Firmware 1.0
Agere Primary firmware version : Primary Firmware 1.0
NIC ID version                 : NIC ID version 1.0
```

Output field description

Field	Description
Agere AP firmware version	This specifies the version of Agere AP firmware downloaded to the card (Major.Minor.Variant).
Agere Primary firmware version	This specifies the version of primary firmware in Agere MAC (Major.Minor.Variant).
NIC ID version	This specifies the version NIC ID Agere MAC.

Caution None.

References None.

3.247 get wlan intf

Description Use this command to get 802.11 Interface

Command Syntax ***get wlan intf [ifname*** ifname ***]***

Parameter

Name	Description
ifname ifname	Name of the wireless interface. **Valid Values:** wlan-0 - wlan-* **Type:** Optional

Mode Super-User, User

Example ***$ get wlan intf ifname*** wlan-0

Output

```
Interface                : wlan-0
Encryption Type          : 64bit            Default Tx Key Id      : 1
Default Channel          : 1                Rts Threshold          : 1
Fragmentation Threshold  : 1                Service set identifier : Viking
Relay packets between BSS : enable          IP address             : 192.168.3.4
Mask                     : 255.255.255.0    Nat Dir                : inside
Use DHCP                 : false            Security Type          : public
Microwave robustness     : enable
Maximum Transmission Unit : 1500
```

Output field description

Field	Description
Interface	Name of the wireless interface.
Encryption Type	WEP Encryption Type. Disabled for no encryption. 64-bit for 40bit encryption.128-bit for 128-bit encryption.
Default Tx Key Id	Combined with WepEncryption attribute, determines which encryption key (between 0-3) to use by default. The actual key is picked up from the 802.11 WEP Keys MO.
Default Channel	Default Channel
Rts Threshold	Maximum packet size to use RTS/CTS With
Fragmentation Threshold	Minimum packet size to use fragmentation with
Service set identifier	Service set identifier of upto 32 characters which each 802.11b station uses.
Relay packets between BSS	Relay packets between BSS (AP)
IP address	This specifies the IP address configured for the interface.
Mask	This specifies the network mask configured for the interface.

Field	Description
Nat Dir	This variable specifies whether this interface's address is inside or outside. This is used by NAT.
Use DHCP	DHCPclient will do/not do link address negotiation locally/remotely depending on the UseDHCP values of local/remote or false
Security Type	This specifies the interface type from firewall point of view.
Microwave robustness	Enable/Disable Microwave robustness
Maximum Transmission Unit	This specifies the maximum transmission unit for interface.

Caution None.

References

- *create wlan intf* command
- *delete wlan intf* command
- *modify wlan intf* command

3.248 get wlan stats

Description Use this command to get 802.11 Interface Statistics

Command Syntax ***get wlan stats [ifname*** ifname ***]***

Parameter

Name	Description
ifname ifname	Name of the wireless interface. **Valid Values:** wlan-0 - wlan-* **Type:** Optional

Mode Super-User, User

Example ***$ get wlan stats ifname*** wlan-0

Output

```
Interface                : wlan-0     Tx Unicast Packets         : 10
Tx Multicast Packets     : 10         Tx Fragments               : 10
Tx Unicast Octets        : 10         Tx Multicast Octets        : 10
Tx Deferred Transmission : 10         Tx Discards                : 10
Rx Unicast Packets       : 10         Rx Multicast Packets       : 10
Rx Fragments             : 10         Rx Unicast Octets          : 10
Rx Multicast Octets      : 10         Rx Fcs Errors              : 10
Rx Discards NoBuffer     : 10         Discards WepUndecryptable  : 10
Tx Single Retry Frames   : 10         Tx Multiple Retry Frames   : 10
Tx Retry Limit Exceeded  : 10         Tx Discards Wrong SA       : 10
Rx Message In MsgFrags   : 10         Rx Message In Bad MsgFrags : 10
Rx Discards WEP ICV Error: 10         Rx Discards WEP Excluded   : 10
Rx Discards NoBuf        : 10         InfoDrops                  : 10
Resets                   : 10         Rx Discards Buff Too Small : 10
Tx Q Depth Limited       : 10         Tx Packet Too Big          : 10
Tx Errored Packet        : 10         Tx Errored Packet Retry    : 10
Tx Errored Packet Aged   : 10         Tx Errored Packet Disconn  : 10
Tx Errored Packet Form   : 10         Tx Packet Port Down        : 10
No Space On CmdQ         : 10         Tx 8021x Drop              : 10
Rx 8021x Drop            : 10
```

Output field description

Field	Description
Interface	Name of the wireless interface.
Tx Unicast Packets	Total number of unicast packets transmitted.
Tx Multicast Packets	Total number of multicast packets transmitted.
Tx Fragments	Total number of fragments transmitted.
Tx Unicast Octets	Total number of unicast octets transmitted.
Tx Multicast Octets	Total number of multicast octets transmitted.
Tx Deferred Transmission	Total number of deferred transmissions.
Tx Discards	Total number of packets discarded.
Rx Unicast Packets	Total number of unicast packets received.
Rx Multicast Packets	Total number of multicast packets received.

Field	Description
Rx Fragments	Total number of fragments received.
Rx Unicast Octets	Total number of unicast octets received.
Rx Multicast Octets	Total number of multicast octets received.
Rx Fcs Errors	Total number of packets received with FCS errors.
Rx Discards NoBuffer	Total number of packets discarded (because of no receive buffers available).
Discards WepUndecryptable	Total number of packets discarded (because of WEP undecryptable).
Tx Single Retry Frames	Frames transmitted with single retry.
Tx Multiple Retry Frames	Frames transmitted with multiple retries.
Tx Retry Limit Exceeded	Number of frames whose retry limit exceeded.
Tx Discards Wrong SA	Transmissions discarded because of wrong SA.
Rx Message In MsgFrags	Number of received message in message fragments.
Rx Message In Bad MsgFrags	Number of received message in bad message fragments.
Rx Discards WEP ICV Error	Number of discards because of WEP ICV error.
Rx Discards WEP Excluded	Number of discards because of WEP excluded.
Rx Discards NoBuf	Packets discarded as allocate buffer failed.
InfoDrops	Number of times we have seen the InfoDrop event.
Resets	Number of times the reset command has been issued.
Rx Discards Buff Too Small	Packets discarded as they did not fit in the CYAN buffer.
Tx Q Depth Limited	Packet not transmitted as queue depth too big.
Tx Packet Too Big	Packet to be sent was larger than H2 max size.
Tx Errored Packet	Packets returned to us marked as errored.
Tx Errored Packet Retry	Returned packet due to excess retries.
Tx Errored Packet Aged	Packet exceeded lifetime before tx.
Tx Errored Packet Disconn	Packet was sent to an unconnected MAC address.
Tx Errored Packet Form	Transmit Frame Structure was invalid.
Tx Packet Port Down	Transmit packet dropped because port is down.
No Space On CmdQ	awlan_WorkerQCommand failed due to lack of space.

Field	Description
Tx 8021x Drop	TX Packet was dropped because not autheticated.
Rx 8021x Drop	RX Packet was dropped because not autheticated.

Caution None.

References None.

3.249 get wlan key

Description Use this command to get 802.11 Wired Equivalent Privacy Keys

Command Syntax ***get wlan key [ifname*** ifname ***] [encrtype*** 64bit | 128bit ***] [keyid*** keyid ***]***

Parameter

Name	Description
ifname ifname	Name of the wireless interface. **Valid Values:** wlan-0 - wlan-* **Type:** Optional
encrtype 64bit | 128bit	Encryption type with which this key is to be used(64 bit or 128 bit). **Type:** Optional
keyid keyid	Key index. Used to identify which key to use as the default key on the interface. **Type:** Optional **Valid values:** 0 - 3

Mode Super-User, User

Example ***$ get wlan key ifname*** wlan-0 ***encrtype*** 64bit ***keyid*** 1

Output

```
Interface       : wlan-0
Encryption Type : 64bit
Key Id          : 1
```

Output field description

Field	Description
Interface	Name of the wireless interface.
Encryption Type	Encryption type with which this key is to be used (64 bit or 128 bit).
Key Id	Key index. Used to identify which key to use as the default key on the interface.

Caution None.

References

- *create wlan key* command
- *delete wlan key* command
- *modify wlan key* command

3.250 get 8021x global

Description Use this command to get 802.1x Global Configuration

Command Syntax ***get 8021x global***

Parameter None

Mode Super-User, User

Example ***$ get 8021x global***

Output

```
802.1x global status
----------------------------
enable
```

Output field description

Field	Description
802.1x global status	Global Status of 802.1x feature

Caution None

References

- *modify 8021x global* command

3.251 get 8021x intf

Description Use this command to get Dot1x Interface Configuration

Command Syntax ***get 8021x intf [ifname*** ifname ***]***

Parameter

Name	Description
ifname ifname	Interface index **Type:** Optional **Valid values:** 1 - 4294967295

Mode Super-User, User

Example ***$ get 8021x intf ifname*** wan-0

Output

```
If Index                : wan-0
802.1x status           : enable      Admin dir           : both
Port Control            : Auto        Association         : many_to_one
Quiet Period(secs)      : 60          Tx Period(secs)     : 30
Supplicant Timeout(secs) : 30         Server Timeout(secs) : 30
Max Request             : 2           ReAuth Enabled      : true
ReAuth Period(secs)     : 3600        ReAuth Max requests : 2
Key Tx Enabled          : true        Dynamic Supp Allowed : true
ReKey timeout(secs)     : 600
```

Output field description

Field	Description
If Index	Interface index
802.1x status	Feature 802.1x status on this Interface
Admin dir	This specifies the controlled directions for the port. If set to both, then the port needs to be authenticated for traffic to flow either to or from it. If set to in, then traffic going out via this port does not require it to be authenticated.
Port Control	This allows administrative control over the Port's authorization status. If set to ForceUnAuth, the port is never authorized. If set to ForceAuth, the port is autorized unconditionally. If set to Auto, the port's authorization status is determined by outcome of the authentication exchanges between Supplicant PAE, Authenticator PAE, and the Authentication Server.
Association	This specifies whether there will be one supplicant or many supplicants per port .
Quiet Period(secs)	The Authenticator state machine uses a timer to define periods of time during which it will not attempt to acquire a Supplicant. The initial value of this timer is quietPeriod.

Field	Description
Tx Period(secs)	The Authenticator state machine uses a timer to determine when an EAPOL PDU is to be transmitted. The initial value of this timer is txPeriod.
Supplicant Timeout(secs)	The initialization value used for timing out the supplicant. Its default value is 30 s; however, if the type of challenge involved in the current exchange demands a different value of timeout (for example, if the challenge requires an action on the part of the user), then the timeout value is adjusted accordingly.
Server Timeout(secs)	The initialization value used for timing out the Authentication Server. Its default value is 30 s; however, the timeout value may be adjusted to take account of the communication medium being used to communicate with the Authentication Sever.
Max Request	The maximum number of times that the state machine will retransmit an EAP Request packet to the Supplicant before it times out the authentication session.
ReAuth Enabled	A constant that defines whether regular reauthentication will take place on this Port.
ReAuth Period(secs)	A constant that defines a nonzero number of seconds between periodic reauthentication of the Supplicant
ReAuth Max requests	The number of reauthentication attempts that are permitted before the Port becomes Unauthorized.
Key Tx Enabled	Controls transmission of key information after the port has been authorized.
Dynamic Supp Allowed	This controls whether only management-created Supplicants or both management-created and Dynamically-learnt Supplicants are allowed.
ReKey timeout(secs)	Timer period after which keys will be transmitted to all the supplicants in the port.

Caution None.

References

- *create 8021x intf* command
- *delete 8021x intf* command
- *modify 8021x intf* command

3.252 get 8021x authstats

Description Use this command to get statistics Information for each Authenticator PAE corresponding to a Supplicant.

Command Syntax ***get 8021x authstats [ifname interface-name] [macaddr mac-address]***

Parameter

Name	Description
ifname <ifname>	This specifies the Interface Index of a port. **Type:** Optional **Valid Values:**
macaddr <macaddr>	This specifies the MAC address of a supplicant for which individual authenticator state machines are running. **Type:** Optional **Valid Values:** A Valid mac-address.

Mode Super-User, User

Example ***$ get 8021x authstats ifname wlan-0 macaddr 0x0085a000004***

Output

```
If Index             : wlan-0          Mac address            : 0x0085a00004
Num Frames Rx        : 3000            Num Frames Tx          : 200
Num Start Frames Rx  : 120             Num Req Frames Tx      : 200
Num RespId Frames Rx : 100             Num ReqId FramesTx     : 200
Num Resp Frames Rx   : 100             Num LogOff Frames Rx   : 100
Num Invalid Frames Rx: 200             Num Len Error Frames Rx: 200
Last Frame Version   : 2               Last Frame Address     : 0x0085a00005
```

Output Field Description

Field	Description
If Index	This specifies the Interface Index of a port.
Mac address	This specifies the MAC aaddress of a supplicant for which statistics Information is fetched.
Num Frames Rx	This specifies the number of Valid EAPOL frames received (of any type)
Num Frames Tx	This specifies the number of EAPOL frames transmitted (of any type)
Num Start Frames Rx	This specifies the number of EAPOL Start frames received.
Num Req Frames Tx	This specifies the number of EAP Request frames transmitted excluding Req/ID frames
Num RespId Frames Rx	This specifies the number of EAP Resp/ID frames received.

Field	Description
Num ReqId FramesTx	This specifies the number of EAP Req/ID frames transmitted.
Num Resp Frames Rx	This specifies the number of valid EAP Resp frames received excluding Resp/ID frames.
Num LogOff Frames Rx	This specifies the number of EAPOL LogOff frames received.
Num Invalid Frames Rx	This specifies the number of EAPOL frames received with invalid frame type.
Num Len Error Frames Rx	This specifies the number of EAPOL frames received with invalid Packet Body length.
Last Frame Version	This specifies the Protocol Version carried in last EAPOL frame.
Last Frame Address	This specifies the Source MAC address carried in last EAPOL frame.

Caution None

References

- *reset 8021x authstats* command

3.253 get 8021x sessstats

Description Use this command to get Session Statistics Information for each Authenticator PAE corresponding to a Supplicant.

Command Syntax ***get 8021x sessstats [ifname interface-name] [macaddr mac-address]***

Parameters

Name	Description
ifname <ifname>	This specifies the Interface Index of a port. **Type:** Optional **Valid Values:**
macaddr <macaddr>	This specifies the MAC address of a supplicant for which individual authenticator state machines are running. **Type:** Optional **Valid Values:** A Valid mac-address.

Mode Super-User, User

Example ***$ get 8021x sessstats ifname wlan-0 macaddr 0x0085a000004***

Output

```
If Index               : wlan-0          Mac address       : 0x0085a00004
Num Octets Rx          : 3000            Num Octets Tx     : 200
Num Data Frames Rx     : 120             Num Data Frames Tx: 200
Auth Session Id        : xyz             Auth Method       : local
Auth Session Time(secs): 20              Terminate Cause   : Re-auth Failed
User Name              : titanium
```

Output field description

Field	Description
If Index	This specifies the Interface Index of a port.
Mac address	This specifies the MAC aaddress of a supplicant for which statistics information is fetched.
Num Octets Rx	This specifies the number of Octets received in User data during the session.
Num Octets Tx	This specifies the number of Octets transmitted in User data during the session.
Num Data Frames Rx	This specifies the number of User Data frames received during the session.
Num Data Frames Tx	This specifies the number of User Data frames Transmitted during the session.
Auth Session Id	This specifies a unique ID for the session. It is a displayable string of at least 3 characters.
Auth Method	This specifies the authentication method used to establish the session.

Field	Description
Auth Session Time(secs)	This specifies the duration of session in seconds.
Terminate Cause	This specifies the reason for session termination.
User Name	This specifies the User-name representing the identity of supplicant.

Caution None

References

- *reset 8021x sessstats* command

3.254 help

Description Use this command for a listing of all the user inputs permissible at the point. In case Help is asked for as a parameter of any incomplete command then it displays a list of all the pending/Extra parameters input by the user. In all other cases the next set of permissible keywords required in order to shortlist a command displays. The incomplete command keyed in by the user is made available again after the help.

Command Syntax

help?
OR
<Any Incomplete Command>?

Parameters None.

Mode Super-User, User.

Example An example session is shown.

```
$help
Command        Description
-------        -----------
alias          To Alias a command
commit         Commit the active config to the flash
create         Create a new entry of specified type
delete         Delete the specified entry
.
.


$delete ?
Command        Description
-------        -----------
arp            IP Net To Media Table
atm            ATM Commands
bridge         Bridge Commands
dhcp           DHCP Commands
.
.
$delete dhcp ?
Command        Description
-------        -----------
relay          DHCP Relay Commands
server         DHCP Server Commands

$delete dhcp server ?
Command        Description
-------        -----------
exclude        DHCP Server Pool Exclusion Table
host           DHCP Server Host Table
pool           DHCP Server Pool/ Range Table

$delete dhcp server exclude ?
Parameter                        Description
---------                        -----------
pool <decvalue>                   Pool Identifier
ip <ddd.ddd.ddd.ddd>              IP Address to be excluded

$delete dhcp server exclude pool 3 ?
Parameter                        Description
---------                        -----------
ip <ddd.ddd.ddd.ddd>              IP Address to be excluded

$delete dhcp server exclude pool 3 ip 1.1.1.1 ?
Command is complete
$delete dhcp server exclude pool 3 ip 1.1.1.1
```

Output field description None.

Caution Currently help cannot be asked for between a parameter name and its value. Thus, in the above example if user asked for help after `ip` then an error would result.

References None.

3.255 list

Description This command is used to list the Configuration or binary files stored on the modem

Command Syntax ***list***

Parameters None.

Mode Super-User.

Example ***$ list***

Output Verbose Mode On

```
myconfig.cfg
newcode.bin
```

Verbose Mode Off

```
myconfig.cfg
newcode.bin
```

Output field description The output shows the configuration and binary files stored on the modem.

Caution None.

References

- *get autoupdate* command
- *modify autoupdate* command
- *remove* command.
- *apply* command.
- *download* command.

3.256 logout

Description	Use this command to exit from the CLI shell.
Command Syntax	***Logout*** | ***quit*** | ***exit***
Parameters	None.
Mode	Super-User, User
Example	***$ logout***
Output	None.
Output field description	None.
Caution	None.
References	None.

3.257 modify atm port

Description Use this command to enable or disable the admin status of the atm port.

Command Syntax ***modify atm port ifname*** interface-name ***{enable|disable}***

Parameters

Name	Description
ifname interface-name	This specifies the ATM port being modified **Type:** Mandatory **Valid values:** *atm-0*
enable|disable	The desired admin status of the ATM port **Type:** Mandatory **Valid values:** *enable, disable*

Mode Super-User.

Example ***$ modify atm port ifname*** **atm-0** ***disable***

Output Verbose Mode On

```
If-Name          : atm-0            MaxVccs          : 4
CBRPriority      : 5                UBRPriority      : 1
RTVBRPriority    : 4                NRTVBRPriority   : 3
GFRPriority      : 2                Latency          : fast
MaxConfVccs      : 0
OAMSrc           : 0xffffffffffffffffffffffffffffffff
Oper Status      : Down             Admin Status  : Up

Set Done

If-Name          : atm-0            MaxVccs          : 4
CBRPriority      : 5                UBRPriority      : 1
RTVBRPriority    : 4                NRTVBRPriority   : 3
GFRPriority      : 2                Latency          : fast
MaxConfVccs      : 0
OAMSrc           : 0xffffffffffffffffffffffffffffffff
Oper Status      : Down             Admin Status    : Down
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
If-Name	This specifies the name of the ATM port. It can be: *atm-0*
MaxVccs	This specifies The maximum number of VCCs (PVCCs and SVCCs) supported at this ATM interface. It may be: 0-64

Field	Description
UBRPriority	Priority of the best effort traffic. A value 0 means no traffic of this class is supported. Higher the value, higher the priority. It may be: *1-3*
GFRPriority	This specifies the priority of GFR class. A value 0 means no traffic of this class is supported. Higher the value higher the priority. It may be: 1-*3*
CBRPriority	Priority of the CBR Class. Value 1 means lowest priority and higher the value higher the priority. It may be *1-3*.
Latency	Type of DSL channel in use on the underlying DSL port. It may be: *fast, interleaved*
MaxConfVccs	This specifies the current number of VCCs configured on this port. It may be:*0* - *v*alue defined in MaxVCCs.
OAMSrc	Loop back source id assigned to the ATM port. The ATM port will respond to all loopback cells which carry this OAM ID.
Oper Status	The actual/current state of the interface. It can be either *Up* or *Down*
Admin Status	The desired state of the interface. It may be either *Up* or *Down*

Caution None.

References

- *atm trfdesc* related commands
- *atm vc* related commands
- *oam lpbk* command
- Other *atm port* related commands
- *atm statistics* related commands.

3.258 modify atm svccfg

Description Use this command to modify atm svc configuration.

Command Syntax ***modify atm svccfg ifname <interface-name> start|stop***

Parameters

Name	Description
ifname interface-name	Interface name of the SVC to be configured **Type:** Mandatory **Valid values:** *atm-0*
start|stop	This specifies the action to be taken on the svc interface **Type:** Mandatory **Valid values:** *start, stop*

Mode Super-User.

Example ***$ modify atm svccfg ifname aal5-0 start***

Output Verbose Mode On/Off

```
Set Done
```

Output field description None

Caution None.

References

- *create atm svccfg* commands
- *get atm svccfg* commands
- *delete atm svccfg* command

3.259 modify atm vc intf

Description Use this command to enable or disable ATM VC.

Command Syntax ***modify atm vc intf ifname*** interface-name ***{enable|disable|lpbk}***

Parameters

Name	Description
ifname interface-name	Interface name of the VC being modified **Type:** Mandatory **Valid values:** *aal5-0 - **
Enable|disable	This specifies the Admin Status of the VC **Type:** Mandatory

Mode Super-User.

Example ***$ modify atm vc intf ifname*** **aal5-0** ***enable***

Output Verbose Mode On

```
LowIf              : atm-0       VPI              : 10          VCI         10
VC IfName           : aal5-0     VC Type           : PVC
Admin Status        : Down       Oper Status       : Down
Aal5 Tx Size        : 9200       Aal5 Rx Size      : 9200
AAL Type            : AAL5       AAL5 Encap        : LLC Mux
Max Aal5 Proto      : 3          Trf Descr Index   : 2
VC Weight           : 10

Set Done

LowIf              : atm-0      VPI               : 10       VCI           : 10
VC IfName           : aal5-0      VC Type          : PVC
Admin Status        : Up         Oper Status       : Up
Aal5 Tx Size        : 9200       Aal5 Rx Size      : 9200
AAL Type            : AAL5       AAL5 Encap        : LLC Mux
Max Aal5 Proto      : 3          Trf Descr Index   : 2
VC Weight           : 10
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
Lowif	Interface index of the underlying ATM port. It is always: *atm-0*
VPI	It is the Virtual Path Identifier.
VCI	It is the Virtual Circuit Identifier.
VC If-Name	Interface name of the VC being modified. It can be: *aal5-0, 11l5-1…*

Field	Description
VC Type	This field specifies whether VC type is PVC or SVC.
Oper Status	The actual/current state of the interface. It can be either *Up* or *Down*
Admin Status	The desired state of the interface. It may be either *Up*, *Down or Loopback. Loopback* has a special significance. A Loopback VC will loop back whatever cells it receives.
Aal5 Tx Size	This specifies the transmit CPCS SDU size to be used
Aal5 Rx Size	This specifies the receive CPCS SDU size to be used
AAL Type	AAL type in use for the VC
AAL5 Encap	This specifies the data multiplexing method to be used over the AAL5 SSCS layer. It may be: *VC Mux, LLC Mux*
Max Aal5 Proto	This specifies the maximum number of protocols that are supported over the VC
Trf Descr Index	This identifies the transmit traffic parameters in use. It corresponds to a valid entry in the traffic descriptor table
VC Weight	This specifies the priority of the VC. Higher value means higher priority

Caution None.

References

- Other *atm vc intf* commands
- *atm trfdesc* commands
- *oam lpbk* command
- *atm port* commands
- *atm statistics* commands.

3.260 modify autodetect cfg

Description Use this command to modify the status of automatic detect mode.

Command Syntax ***modify autodetect cfg [enable | disable] [mode bridge|router|both][pppdetect padilcp|fullblown] [vcrange all|fromfile]***

Parameters

Name	Description
enable|disable	Status of the Automatic Detect Mode. **Type:** Mandatory **Valid values:** enable or disable **Default value:** enable
mode bridge|router|both	This specifies whether modem is configured for bridging or routing or both modes. **Type:** Optional **Valid values:** router or bridge or both
pppdetect padilcp|fullblown	Auto detection procedure used. **Type:** Optional **Valid values:** padilcp or fullblown
vcrange all|fromfile	Range of VC values for which auto detection procedure will be followed. **Type:** Optional **Valid values:** all or fromfile

Mode Super-User

Example ***$ modify autodetect cfg*** *enable* ***mode*** *bridge*

Output Verbose Mode On:

```
Auto Detect Mode : Disable     Mode            : Router
Detect PPP       : PADI LCP    VC Range        : From file


Set Done


Auto Detect Mode : Enable      Mode            : Bridge
Detect PPP       : PADI LCP    VC Range        : From file
```

Verbose Mode Off:

```
Set Done
```

Output field description

Field	Description
Auto Detect Mode	Status of the Automatic Detect Mode.
Mode	This specifies whether modem is configured for bridging or routing mode, or both modes.
Detect PPP	This specifies the auto detection procedure.
VC Range	This specifies the range of VC values for which auto detection procedure will be followed.

Caution None

References

- *get autodetect cfg*

3.261 modify autoupdate

Description Use this command to modify the autoupdate flag.

Command Syntax ***modify autoupdate true|false***

Parameters

Name	Description
true|false	Desired autoupdate flag value. If it is *True* then any file downloaded using the *download command* is applied immediately after being downloaded (in case of a *.cfg* file its commands would be immediately executed; in case of a *.bin* file the code in it will get programmed into the flash and the modem will reboot with the new code). If the flag is *False* then the file is simply downloaded and not executed **Type:** Mandatory **Valid values:** *true, false*

Mode Super-User.

Example ***$ modify autoupdate true***

Output Verbose Mode On

```
Auto Update: False

Set Done

Auto Update: True
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
Auto Update	This specifies the value of the autoupdate flag. If it is *True* then any file downloaded using the *download command* is applied immediately after being downloaded (in case of a *.cfg* file its commands would be immediately executed; in case of a *.bin* file the code in it will get programmed into the flash and the modem will reboot with the new code). If the flag is *False* then the file is simply downloaded and not executed.

Caution None.

References

- *apply* command
- *set autoupdate* command
- *remove* command.
- *list* command

3.262 modify autodetect status

Description Use this command to modify the status of automatic detection mode.

Command Syntax ***$ modify autodetect status vci <decvalue> vpi <decvalue> [port <ifname>]***

Parameters

Name	Description
vci <decvalue>	This specifies the VCI detected. **Type :** Mandatory **Valid values:** 0-65535
vpi <decvalue>	This specifies the VPI detected. **Type :** Mandatory **Valid values:** 0-255
[port <ifname>]	This specifies the port on which VPI and VCI have been detected. **Type :** Optional **Valid values:** atm-0*

Mode .Super-User

Example ***$ modify autodetect status vci 102 vpi 9 port atm-0 ipoanon1577***

Output Verbose Mode On

```
VPI         : 9                 VCI             : 102
Port        : atm-0
Protocol    :  DHCP IPOA1577

Set Done

VPI         : 9                 VCI             : 102
Port        : atm-0
Protocol    :  IPOANon1577
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
VPI	This specifies the VPI detected
VCI	This specifies the VCI detected
Port	This specifies the port on which VPI and VCI have been detected
Protocol	This specifies the range of protocols, which have been detected.

Caution None.

References

- *get autodetect status* command

3.263 modify bras cfg

Description Use this command to modify BRAS Configuration.

Command Syntax ***modify bras cfg [status enable | disable] [selfppe restart]***

Parameters

Name	Description
***status enable	disable***	This field specifes whether Bridge Router Auto Sense (BRAS) feature is enabled or disabled. If enabled, the modem's PPoE client is disabled when a PPoE client is detected on the LAN. **Type:** Optional **Default value:** 0
selfppe restart	This is used to restart self PPoE clients in case they had got disabled because of a LAN PPoE client being detected earlier. **Type:** Optional

Mode Super-User

Example ***$ modify bras cfg status enable selfppe restart***

Output Verbose Mode on

```
Status : Enable

Set Done
```

Verbose Mode off

```
Set Done
```

Output field description

Field	Description
Status	This field specifes whether Bridge Router Auto Sense (BRAS) feature is enabled or disabled. If enabled, the modem's PPoE client is disabled when a PPoE client is detected on the LAN.

Caution None.

References

- *get bras cfg* command.

3.264 modify bridge tbg info

Description Use this command to modify the aging timeout of dynamically learned forwarding information by the bridge.

Command Syntax ***modify bridge tbg info aging*** aging-timeout

Parameters

Name	Description
aging aging-timeout	Specifies the timeout period in seconds for aging out dynamically learned forwarding information. 802.1D-1990 recommends a default of 300 seconds. **Type:** Mandatory **Valid values:** *30-1000000*

Mode Super-User.

Example ***$ modify bridge tbg info aging*** **400**

Output Verbose Mode On

```
Learned Entry Discards : 0
Aging Timeout(sec)     : 300
MacAddress             : 00:00:00:00:00:00
No. of Ports           : 5
Base Type              : Transparent

Set Done

Learned Entry Discards : 0
Aging Timeout(sec)     : 300
MacAddress             : 00:00:00:00:00:00
No. of Ports           : 5
Base Type              : Transparent
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
Learned Entry Discards	The total number of Forwarding Database entries, which have been or would have been learnt, but have been discarded due to a lack of space to store them in the Forwarding Database. If this counter is increasing, it indicates that the Forwarding Database is regularly becoming full (a condition which has unpleasant performance effects on the subnetwork). If this counter has a significant value but is not presently increasing, it indicates that the problem has been occurring but is not persistent.
Aging TimeOut(sec)	The timeout period in seconds for aging out dynamically learned forwarding information.
MacAddress	The MAC address used by this bridge when it must be referred to in a unique fashion. It is the address of the ethernet port.
No. of Ports	The maximum number of ports that can be controlled by this bridge.
Base Type	Indicates what type of bridging this bridge can perform. It is always *Transparent*.

Caution None.

References

- *get bridge tbg info* command
- *bridge* related commands
- *bridge port stats* command
- *bridge static* related commands
- *bridge forwarding* related commands.

3.265 modify bridge mode

Description Use this command to enable or disable the bridging on the unit.

Command Syntax ***modify bridge mode [enable|disable] [wan2wan enable|disable]***

Parameters

Name	Description
enable|disable	Desired state of Bridging Mode. **Type:** Mandatory **Valid values:** *enable, disable*
wan2wan enable|disable	Desired state of WAN-to-WAN bridging mode. **Type:** Optional **Valid values:** enable, disable

Mode Super-User.

Example ***$ modify bridge mode enable wan2wan enable***

Output Verbose Mode On

```
Bridging     Wan to Wan Bridging
-------------------------------------------
enable          disable

 Set Done

Bridging     Wan to Wan Bridging
-------------------------------------------
enable         enable
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
Bridging	This specifies whether bridging mode is enabled or disabled.
Wan to Wan bridging	This specifies whether WAN-to-WAN bridging mode is enabled or disabled.

Caution None.

References

- *get bridge mode* command
- *bridge port* related commands
- *bridge port stats* command
- *bridge static* related commands
- *bridge forwarding* related commands

3.266 modify bridge static

Description Use this command to modify the set of interfaces associated with an existing bridge static entry.

Command Syntax ***modify bridge static macaddr*** mac-address ***inifname*** interface-name|***all [ifname*** interface-name|***all]+***

Parameters

Name	Description
macaddr mac-address	This identifies the entry for which the information is to be modified. It is the destination MAC address in a frame to which this entry's filtering information applies. **Type:** Mandatory **Valid values:** *0:0:0:0:0:0 to FF:FF:FF:FF:FF:FF*
Inifname interface-name|***all***	Interface from which a frame must be received in order for this entry's filtering information to apply. A value of *all* indicates that this entry applies on all interfaces of the bridge for which there is no other applicable entry. **Type:** Mandatory **Valid values:** eth-0, eoa-0 - *, usb-0
ifname interface-name	The interface to which frames destined for the given MAC address are allowed to be forwarded. Any number of such interfaces may be specified together. **Type:** At least 1 should be specified. **Valid values:** *eth-0, eoa-0 - *,usb-0*

Mode Super-User.

Example ***$ modify bridge static macaddr 1:1:1:1:1:1 inifname all ifname usb-0***

Output Verbose Mode On

```
MAC Address        : 01:01:01:01:01:01       Incoming Interface : ALL
Interfaces         : eth-0

Set Done

MAC Address        : 01:01:01:01:01:01       Incoming Interface : ALL
Interfaces         : aal5-0
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
MAC Address	The destination MAC address in a frame to which this entry's filtering information applies
Incoming Interface	Interface from which a frame must be received in order for this entry's filtering information to apply. A value of all indicates that this entry applies on all interfaces of the bridge for which there is no other applicable entry.
Interfaces	The interfaces to which frames destined for the given MAC address are allowed to be forwarded. Any number of such interfaces may be specified together. They may be: *eth-0, eoa-0 - *, …*

Caution The existing list of interfaces is replaced by the new list.

References

- *delete bridge static* command
- *get bridge static* command
- *create bridge static* command
- *bridge mode* related commands
- *bridge forwarding* related commands
- *bridge port stats* related commands
- *bridge static* related commands.

3.267 modify dhcp relay cfg

Description Use this command to modify the DHCP relay configuration.

Command Syntax ***modify dhcp relay cfg [enable|disable] [ip*** serv-ip**]**

Parameters

Name	Description
ip serv-ip	This specifies the IP Address where the DHCP Server is running **Type:** Optional **Valid values:** Any valid class A/B/C IP address
enable|disable	This specifies the Admin Status of the DHCP Relay **Type:** Optional **Valid values:** *enable, disable*

Mode Super-User.

Example ***$ modify dhcp relay cfg enable***

Output Verbose Mode On

```
Status          : Disable
Server IP Addr  : 202.64.23.4

Set Done

Status          : Enable
Server IP Addr  : 202.64.23.4
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
Status	This specifies the Admin Status of the DHCP Relay. It may be: *Enable, Disable*
Server IP Addr	This specifies the IP Address where the DHCP Server is running.

Caution DHCP Server and Relay both cannot be enabled at the same time

References

- *get dhcp relay cfg* command
- *dhcp server* related commands
- *dhcp relay stats* related commands

3.268 modify dhcp server cfg

Description Use this command to enable or disable the dhcp server.

Command Syntax ***modify dhcp server cfg {enable|disable}***

Parameters

Name	Description
enable|disable	The state the DHCP Server is to be set in. **Type:** Mandatory **Valid values:** *enable, disable*

Mode Super-User.

Example ***$ modify dhcp server cfg disable***

Output Verbose Mode On

```
Status             : enable
Def Pri DNS Server : 172.25.8.9     Def Sec DNS Server   : 172.25.7.67

Set Done

Status             : Disable
Def Pri DNS Server : 172.25.8.9      Def Sec DNS Server  : 172.25.7.67
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
Status	The state of the DHCP Server. It may be either *Enable* or *Disable*
Def Pri DNS Server	The default primary DNS server assigned by the DHCP server when user does not specify a primary DNS server in the DHCP pool configuration
Def Sec DNS Server	The default secondary DNS server assigned by the DHCP server when user does not specify a secondary DNS server in the DHCP pool configuration

Caution Both DHCP Relay and DHCP Server cannot be enabled together.

References

- *Get dhcp server cfg* command
- *dhcp client* related commands
- *dhcp server* related commands
- *dhcp server pool* related commands.

3.269 modify dhcp server host

Description Use this command to modify an entry in the host table.

Command Syntax

```
modify dhcp server host ip ip-address [dname domain-name]
({pop3|nntp|web|irc|wins|swins|dns|sdns|gwy|smtp}
ip-address)* [dlease default-lease-time] [mlease max-lease-
time]
```

Parameters

Name	Description
ip ip-address	This specifies the IP address of the host the information pertaining to which is to be modified. **Type:** Mandatory **Valid values:** *Any valid class A/B/C IP address*
dname domain-name	Specifies the domain name configured for this host **Type:** Optional **Valid values:** String of length 64 with valid characters 'a'-'z', 'A'-'Z', '0'-'9', '-', '_'and '.' **Default value:** *Null*
gwy ip-address	This specifies the default gateway IP address **Type:** Optional **Valid values:** *Any valid class A/B/C IP address* **Default value:** *0.0.0.0*
pop3 ip-address	This specifies the IP address of the POP3 Server **Type:** Optional **Valid values:** *Any valid class A/B/C IP address* **Default value:** *0.0.0.0*
nntp ip-address	This specifies the IP address of the NNTP Server **Type:** Optional **Valid values:** *Any valid class A/B/C IP address* **Default value:** *0.0.0.0*
web ip-address	This specifies the IP address of the WWW Server **Type:** Optional **Valid values:** *Any valid class A/B/C IP address* **Default value:** *0.0.0.0*
irc ip-address	This specifies the IP address of the IRC Server **Type:** Optional **Valid values:** *Any valid class A/B/C IP address* **Default value:** *0.0.0.0*
wins ip-address	This specifies the IP address of the primary WIN Server **Type:** Optional **Valid values:** *0.0.0.0 – 255.255.255.255* **Default value:** *0.0.0.0*

Name	Description
swins ip-address	This specifies the IP address of the secondary WIN Server **Type:** Optional **Valid values:** *Any valid class A/B/C IP address* **Default value:** *0.0.0.0*
dns ip-address	This specifies the IP address of the primary Domain Name Server **Type:** Optional **Valid values:** *Any valid class A/B/C IP address* **Default value:** *0.0.0.0*
sdns ip-address	This specifies the IP address of the secondary Domain Name Server **Type:** Optional **Valid values:** *Any valid class A/B/C IP address* **Default value:** *0.0.0.0*
smtp ip-address	This specifies the IP address of the SMTP Server **Type:** Optional **Valid values:** *Any valid class A/B/C IP address* **Default value:** *0.0.0.0*
dlease default-lease-time	This specifies the lease period for which the server assigns an IP address to a client in case the client does not request for a specific lease period itself. **Type:** Optional **Valid values:** *0 -mlease* **Default value:** *2592000* seconds (this equals 30 days)
mlease max-lease-time	This specifies the maximum period for which the DHCP server can lease out an IP address to a DHCP client. **Type:** Optional **Valid values:** *0 – 4294967295* **Default value:** *31536000* seconds (this equals 1 year)

Mode Super-User.

Example ***$ modify dhcp server host ip*** **192.168.1.7** ***dname*** **www.test.net**

Output Verbose Mode On

```
Host Ip          : 192.168.1.7        Hardware Addr    : 12:34:45:56:03:02
Def Lease(sec)   : 2592000            Max Lease(sec)   : 31536000
Domain Name      :

Subnet Mask      : 255.255.255.0
Gateway Ip       : 0.0.0.0            Smtp Ip          : 0.0.0.0
Dns Ip           : 0.0.0.0            Sec. Dns Ip      : 0.0.0.0
Pop3 Ip          : 0.0.0.0            Nntp Ip          : 0.0.0.0
Www Ip           : 0.0.0.0            Irc Ip           : 0.0.0.0
Wins Ip          : 0.0.0.0            Sec. Wins Ip     : 0.0.0.0
```

```
Set Done

Host Ip          : 192.168.1.7        Hardware Addr    : 12:34:45:56:03:02
Def Lease(sec)   : 2592000            Max Lease(sec)   : 31536000
Domain Name      : www.test.net
Subnet Mask      : 255.255.255.0
Gateway Ip       : 0.0.0.0            Smtp Ip          : 0.0.0.0
Dns Ip           : 0.0.0.0            Sec. Dns Ip      : 0.0.0.0
Pop3 Ip          : 0.0.0.0            Nntp Ip          : 0.0.0.0
Www Ip           : 0.0.0.0            Irc Ip           : 0.0.0.0
Wins Ip          : 0.0.0.0            Sec. Wins Ip     : 0.0.0.0
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
Host Ip	This specifies the IP address provided to this host
Hardware Addr	This specifies the hardware address of the client
Def Lease(sec)	This specifies the lease period for which the server assigns an IP address to a client in case the client does not request for a specific lease period itself.
Max Lease(sec)	This specifies the maximum period for which the DHCP server can lease out an IP address to a DHCP client.
Domain Name	Specifies the domain name configured for this host
Subnet Mask	This specifies the subnet mask to be provided to the host
Gateway Ip	This specifies the default gateway IP address
Smtp Ip	This specifies the IP address of the NNTP Server
Dns Ip	This specifies the IP address of the primary Domain Name Server
Sec. Dns Ip	This specifies the IP address of the secondary Domain Name Server
Pop3 Ip	This specifies the IP address of the POP3 Server
Nntp Ip	This specifies the IP address of the SMTP Server
Www Ip	This specifies the IP address of the WWW Serve
Irc Ip	This specifies the IP address of the IRC Server
Wins Ip	This specifies the IP address of the primary WIN Server
Sec. Wins Ip	This specifies the IP address of the secondary WIN Server

Caution None.

References

- *create dhcp server host* command
- *delete dhcp server host* command
- *get dhcp server host* command
- *dhcp server* related commands

3.270 modify dhcp server pool

Description Use this command to modify the configuration of an existing DHCP pool.

Command Syntax

```
modify dhcp server pool pool-id pool-id [dname domain-name]
{{pop3|nntp|web|irc|wins|swins|dns|sdns|gwy|smtp} ip-
address}* [enabled|disabled] [lthres low-threshold]
[dlease default-lease-time] [mlease max-lease-time]
```

Parameters

Name	Description
pool-id pool-id	This identifies the pool whose configuration is to be modified. **Type:** Mandatory **Valid values:** *0 - 255*
dname domain-name	Domain name used per subnet. **Type:** Optional **Valid values:** String of length 64 with valid characters 'a'-'z', 'A'-'Z', '0'-'9', '-', '_'and '.' **Default value:** *Null*
gwy ip-address	This specifies the default gateway IP address **Type:** Optional **Valid values:** *0.0.0.0 – 255.255.255.255* **Default value:** *0.0.0.0*
pop3 ip-address	This specifies the IP address of the POP3 Server **Type:** Optional **Valid values:** *0.0.0.0 – 255.255.255.255* **Default value:** *0.0.0.0*
nntp ip-address	This specifies the IP address of the NNTP Server **Type:** Optional **Valid values:** *0.0.0.0 – 255.255.255.255* **Default value:** *0.0.0.0*
web ip-address	This specifies the IP address of the WWW Server **Type:** Optional **Valid values:** *0.0.0.0 – 255.255.255.255* **Default value:** *0.0.0.0*
irc ip-address	This specifies the IP address of the IRC Server **Type:** Optional **Valid values:** *0.0.0.0 – 255.255.255.255* **Default value:** *0.0.0.0*
wins ip-address	This specifies the IP address of the primary WIN Server **Type:** Optional **Valid values:** *0.0.0.0 – 255.255.255.255* **Default value:** *0.0.0.0*

Name	Description
swins ip-address	This specifies the IP address of the secondary WIN Server **Type:** Optional **Valid values:** *0.0.0.0 – 255.255.255.255* **Default value:** *0.0.0.0*
dns ip-address	This specifies the IP address of the primary Domain Name Server **Type:** Optional **Valid values:** *0.0.0.0 – 255.255.255.255* **Default value:** *0.0.0.0*
sdns ip-address	This specifies the IP address of the secondary Domain Name Server **Type:** Optional **Valid values:** *0.0.0.0 – 255.255.255.255* **Default value:** *0.0.0.0*
smtp ip-address	This specifies the IP address of the SMTP Server **Type:** Optional **Valid values:** *0.0.0.0 – 255.255.255.255* **Default value:** *0.0.0.0*
dlease default-lease-time	This specifies the lease period for which the server assigns an IP address to a client in case the client does not request for a specific lease period itself. **Type:** Optional **Valid values:** *0 -mlease* **Default value:** *2592000 seconds (this equals 30 days)*
mlease max-lease-time	This specifies the maximum period for which the DHCP server can lease out an IP address to a DHCP client. **Type:** Optional **Valid values:** *0 – 4294967295* **Default value:** *31536000 seconds (this equals 1 year)*
Enable | ***disable***	The state the pool is to be set in. **Type:** Optional **Valid values:** *enable, disable* **Default value:** *enable*
lthres low-threshold	Specifies the lowest threshold value on the number of available IP addresses for a particular shared network. If the number of free IP addresses fall below this value, then a trap is raised. This value has to be less than the pool size specified using the start and end ip addresses. **Type:** Optional **Valid values:** *0 – 255* **Default value:** *0*

Mode Super-User.

Example ***$ modify dhcp server poolid 0 Enable***

Output Verbose Mode On

```
Pool Id          : 0                 Status           : Disable
Start Ip         : 192.168.1.1       End Ip           : 192.168.1.200
Def Lease(sec)   : 2592000           Max Lease(sec)   : 31536000
Range Inuse      : 0                 Outstd Offers    : 0
Low Thres        : 0                 Subnet Mask      : 255.255.255.0
Domain Name      :

Gateway Ip       : 0.0.0.0           Smtp Ip          : 0.0.0.0
Dns Ip           : 0.0.0.0           Sec. Dns Ip      : 0.0.0.0
Pop3 Ip          : 0.0.0.0           Nntp Ip          : 0.0.0.0
Www Ip           : 0.0.0.0           Irc Ip           : 0.0.0.0
Wins Ip          : 0.0.0.0           Sec. Wins Ip     : 0.0.0.0

Set Done

Pool Id          : 0                 Status           : Enable
Start Ip         : 192.168.1.1       End Ip           : 192.168.1.200
Def Lease(sec)   : 2592000           Max Lease(sec)   : 31536000
Range Inuse      : 0                 Outstd Offers    : 0
Low Thres        : 0                 Subnet Mask      : 255.255.255.0
Domain Name      :

Gateway Ip       : 0.0.0.0           Smtp Ip          : 0.0.0.0
Dns Ip           : 0.0.0.0           Sec. Dns Ip      : 0.0.0.0
Pop3 Ip          : 0.0.0.0           Nntp Ip          : 0.0.0.0
Www Ip           : 0.0.0.0           Irc Ip           : 0.0.0.0
Wins Ip          : 0.0.0.0           Sec. Wins Ip     : 0.0.0.0
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
PoolId	This is the pool identifier
Status	This defines the Admin status of the entry. It may either be *enable* or *disable*.
Start Ip	The IP address of the first address in the range.
End Ip	The IP address of the last address in the range.
Def Lease(sec)	This specifies the lease period for which the server assigns an IP address to a client in case the client does not request for a specific lease period itself.
Max Lease(sec)	This specifies the maximum period for which the DHCP server can lease out an IP address to a DHCP client.
Range Inuse	The number of addresses in this range that are currently in use. This number includes addresses that have not expired and those that have been reserved.

Field	Description
Outstd Offers	The number of outstanding DHCOOFFER messages for this range is reported with this value. An offer is outstanding if if the server has sent a DHCPOFFER message to a client, but has not yet received a DHCPREQUEST message from the client nor has the server-specific timeout, within which a client can respond to the offer message, for the offer message expired.
Low Thres	This specifies the lowest threshold value on the number of available/ free IP addresses for a particular shared network
Subnet Mask	The subnet mask provided to any client offered an address from this range
Domain Name	Domain name used per subnet.
Gateway Ip	This specifies the default gateway IP address
Smtp Ip	This specifies the IP address of the NNTP Server
Dns Ip	This specifies the IP address of the primary Domain Name Server
Sec. Dns Ip	This specifies the IP address of the secondary Domain Name Server
Pop3 Ip	This specifies the IP address of the POP3 Server
Nntp Ip	This specifies the IP address of the SMTP Server
Www Ip	This specifies the IP address of the WWW Serve
Irc Ip	This specifies the IP address of the IRC Server
Wins Ip	This specifies the IP address of the primary WIN Server
Sec. Wins Ip	This specifies the IP address of the secondary WIN Server

Caution None.

References

- *get dhcp server pool* command
- *create dhcp server pool* command
- *delete dhcp server pool* command
- *get dhcp server host* command
- *dhcp server cfg* related commands
- *dhcp server exclude* related commands
- *dhcp server address* related commands.

3.271 modify dns relay cfg

Description Use this command to enable or disable DNS relay.

Command Syntax ***modify dns relay cfg [enable|disable][pollstatus enable|disable] [pollinterval <decvalue>]***

Parameters

Name	Description
enable|disable	This specifies whether to enable or disable DNS relay. Type: Optional Valid values : enable or disable
pollstatus enable|disable	If enabled, the DNS servers are probed periodically to see if they can be reached. **Type :** Optional **Valid values:** *enable* or *disable*
pollinterval <decvalue>	The periodic interval after which DNS servers are probed (if polling is enabled). **Type :** Optional **Valid values:** 1 .. 65535

Mode Super-User.

Example ***$ modify dns relay cfg enable enable pollstatus disable pollinterval 3***

Output Verbose Mode On

```
Status      : Disable
Poll Status :  enable          Poll interval: 2

 Set Done

Status      : Disable
Poll Status :  enable         Poll interval: 2
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
Status	This specifies whether DNS relay is enabled or disabled.
Poll Status	If enabled, the DNS servers are probed periodically to see if they can be reached.
Poll interval	The periodic interval after which DNS servers are probed (if polling is enabled).

Caution None.

References

- get dns relay cfg
- get dns relay stats
- reset dns relay stats
- create dns servaddr
- get dns servaddr
- delete dns servadd

3.272 modify dsl config

Description User can modify the default parameters for DSL in the system using this command

Command Syntax

modify dsl config [t1413|glite|gdmt|multi|rsrv|lgdmt|lglite|lg2|adicisco|alctanxb|alct41anxb|autosensegdmtfirst|gdmtorlite|autosenset1413first][annex annexa|annexb|annexc] [trellis enable|disable][expanded|short][txatten <decvalue>][gain <decvalue>][maxbits <decvalue>][txstart <decvalue>][txend <decvalue>] [txbinadj enable|disable] [rxstart <decvalue>][rxend <decvalue>][rxbinadj enable|disable][fastretrain enable|disable][escfastretrain enable|disable] [bitswap enable|disable][duallatency enable|disable][pmode enable|disable][pilotreq enable|disable][whip enable | disable] [loop start|stop][acmodeitem fbm|dbm][acpilotreq enable|disable][acttrroffset offset0|offset42][ecfdmmode < ec|fdm|fdmhp|fdmnaf>][maxdnrate <hexvalue>]

Parameters

Name	Description
t1413|glite|gdmt|multi|rsrv|lgdmt|lglite|lg2| adicisco| alctanxb|alct41anxb|autosensegdmtfirst| gdmtorlite| autosenset1413first	This specifies the standard to be supported for the DSL line. **Type:** Optional **Valid values:** *T1413, glite (G992.2), gdmt (G992.1), multi(multimode), rsrv(reserved), lgdmt, lglite, lg2, adicisco, alctanxb, alct41anxb (Alcatel 4.1 Annex B)* **Default value:** *G.dmt*
annex annexa|annexc	This specifies the Annex Type **Type:** Optional **Valid values:** Annex A, Annex B, Annex C
trellis enable|disable	This is used to enable or disable Trellis coding on the interface. **Type:** Optional **Valid values:** *enable|disable* **Default value:** *enable*
expanded|short	Expanded Exchange Sequence (EES) enable/disable, only valid for T1.413. This is largely for compatibility testing. **Type:** Optional **Valid values:** *expanded|short* **Default value:** *expanded*
framing0|framing1| framing2|framing3	Full overhead to reduced overhead (0x00-03). This value is ignored for G.lite. (G992.2). **Type:** Optional **Valid values:** *framing0|framing1|framing2|framing3* **Default value:** *framing3*
txatten tx-power-attenuation	This specifies the value of transmit power attenuation. Its range is from 0dB to 12dB. **Type:** Optional **Valid values:** *0 - 12* **Default value:** *0*

Name	Description
gain coding-gain|***auto***	Coding gain is the gain due to trellis/RS coding. Its value ranges from 0 to 7 dB in 1 dB increments. Recommended value is *auto*. **Type:** Optional **Valid values:** *0-7*, *8* (auto) **Default value:** *8* (auto)
maxbits max-bits-per-bin	Maximum number of receive bits per bin . **Type:** Optional **Valid values:** *0-15* **Default value:** *14*
txbinadj ***enable***|***disable***	Enable or disable automatic bin adjustment for transmit signal. **Type:** Optional **Valid values:** *enable*|*disable* **Default value:** *enable*
txstart tx-start-bin	Lowest bin number allowed for transmit signal **Type:** Optional **Valid values:** 255 or less, depending on annex **Default value:** *6*
txend tx-end-bin	Highest bin number allowed for transmit signal. **Type:** Optional **Valid values:** 255 or less, depending on annex **Default value:** *31*
rxbinadj ***enable***|***disable***	Enable or disable automatic bin adjustment for receive signal. **Type:** Optional **Valid values:** *enable*|*disable* **Default value:** *disable*
rxstart rx-start-bin	Lowest bin number allowed for receive signal **Type:** Optional **Valid values:** *32* **Default value:** *32*
rxend rx-end-bin	Highest bin number allowed for receive signal. **Type:** Optional **Valid values:** 255 or less, depending on annex **Default value:** *255*
fastretrain ***enable***|***disable***	Enable or disable fast retrain capability, Currently supported only in G.Lite mode. **Type:** Optional **Valid values:** *enable*|*disable* **Default value:** *disable*
escfastretrain ***enable***|***disable***	Enable or disable escape to fast retrain capability. **Type:** Optional **Valid values:** *enable*|*disable* **Default value:** *disable*
bitswap ***enable***|***disable***	Enable or disable bit swapping. **Type:** Optional **Valid values:** *enable*|*disable* **Default value:** *disable*

Name	Description
duallatency enable|disable	Enable or disable dependant upon support of dual latency. Valid only for T1.413 and G.DMT. **Type:** Optional **Valid values:** *enable*|*disable* **Default value:** *enable*
pmode enable|disable	If enable, use the upstream pilot for data if the CO is Conexant. **Type:** Optional **Valid values:** *enable*|*disable* **Default value:** *enable*
pilotreq enable|disable	Enable or disable request for pilot tone during training. **Type:** Optional **Valid values:** *enable*|*disable* **Default value:** *enable*
Whip enable|disable	Enable or disable Windows Based Host Interface Program **Type:** Optional **Valid values:** *enable*|*disable* **Default value:** *disable*
loop start|stop	Enables you to start or stop DSL connectivity **Type:** Optional **Valid values:** *start*|*stop* **Default value:** *start*
acmodeitem fbm|dbm	This specifies the bitmap transmission mode. **Type:** Optional **Valid values:** *fbm*: Time duplex transmission mode during FEXT symbols only *dbm*: Continuous transmission during NEXT and FEXT symbols with 2 bit loading profiles **Default value:** *fbm*
acpilotreq enable|disable	Enable/Disable reception of Pilot Tone during the next period in the FEXT bitmap mode. **Type:** Optional **Valid values:** *enable*|*disable* **Default value:** *enable*
acttroffset offset0|offset42	Offset from TTR_C (timing reference used in ATU-C) to TTR_R (timing reference used in ATU-R) **Type:** Optional **Valid values:** *offset0*|*offset42* **Default value:** *offset42*
ecfdmode ec|fdm|fdmhp|fdmnaf	This enables selection of echo cancellation and frequency division multiplexing modes. **Type:** Optional **Valid values:** *ec*: specifies echo cancellation mode *fdm*: specifies frequency division multiplexing mode, which also performs echo cancellation *fdmhp*: pure frequency division multiplexing (with no echo cancellation) *fdmnaf*: frequency division multiplexing with no analog filter **Default value:** *ec*

Mode Super-User.

Example

```
$ modify dsl config t1413 trellis enable expanded framing0
txatten 1 gain 8 maxbits 1 txbinadj enable txstart 1 txend 2
rxbinadj enable rxstart 1  rxend 2 fastretrain enable bitswap
enable duallatency enable pmode enable pilotreq enable whip
enable loopacmodeitem fbm loop start acpilotreq enable
actroffset offset0 ecfdmmode ec
```

Output

Verbose Mode On

```
Whip             : Disable        Annex Type       : Annex A
Standard         : Multimode      Trellis coding   : Enable
ExpExchSeq       : Expanded       Framing structure: Framing-3
TxAttenuation(dB): 0              Coding Gain      : Auto
TxBinAdjust      : Enable         RxBinAdju
TxStartBin       : 6              TxEndBin         : 31
RxStartBin       : 32             RxEndBin         : 255
Fast Retrain     : Disable        Esc Fast Retrain : Disable
MaxBits/bin On Rx: 14             Bit Swap         : Disable
Dual Latency     : Enable         Pmode            : Enable
Pilot Request    : Enable         Last Failed Status: 0x0
Oper Status      : Startup HShake Startup Progress : 0xa0
AC Mode item     : dbm            AC Ttr R Offset  : 42
AC Pilot Request : Disable        EC Fdm Mode      : EC

Set Done


Whip             : Disable        Annex Type       : Annex A
Standard         : Multimode      Trellis coding   : Enable
ExpExchSeq       : Expanded       Framing structure: Framing-3
TxAttenuation(dB): 0              Coding Gain      : Auto
TxBinAdjust      : Enable         RxBinAdjust      : Disable
TxStartBin       : 6              TxEndBin         : 31
RxStartBin       : 32             RxEndBin         : 255
Fast Retrain     : Disable        Esc Fast Retrain : Disable
MaxBits/bin On Rx: 14             Bit Swap         : Disable
Dual Latency     : Enable         Pmode            : Enable
Pilot Request    : Enable         Last Failed Status: 0x0
Oper Status      : Startup HShake Startup Progress : 0xa0
AC Mode item     : dbm            AC Ttr R Offset  : 42
AC Pilot Request : Disable        EC Fdm Mode      : EC
Max Down Rate     : 0xff
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
Whip	Windows Based Host Interface Program is enabled or disabled
Annex Type	The DSL annex type (A, B, or C)
Standard	This specifies the standard to be supported for the DSL line.
Trellis coding	This is used to enable or disable Trellis coding on the interface.
ExpExchSeq	Expanded Exchange Sequence (EES) enable/disable, only valid for T1.413. This is largely for compatibility testing.
Framing structure	Full overhead to reduced overhead (0x00-03). This value is ignored for G.lite (G992.2).

Field	Description
TxAttenuation (dB)	This specifies the value of transmit power attenuation. Its range is from 0dB to 12dB.
Coding Gain	Coding gain is the gain due to trellis/RS coding. Its value ranges from 0 to 7dB.
TxBinAdjust	Enable or disable automatic bin adjustment for transmit signal.
RxBinAdjust	Enable or disable automatic bin adjustment for receive signal.
TxStartBin	Lowest bin number allowed for transmit signal
TxEndBin	Highest bin number allowed for transmit signal.
RxStartBin	Lowest bin number allowed for receive signal
RxEndBin	Highest bin number allowed for receive signal.
Fast Retrain	Enable or disable fast retrain capability.
Esc Fast Retrain	Enable or disable escape to fast retrain capability.
MaxBits/bin On Rx	Maximum number of receive bits per bin.
Bit Swap	Enable or disable bit swapping,
Dual Latency	Enable or disable dependant upon support of dual latency. Valid only for T1.413 and G.DMT.
Pmode	If enable, use the upstream pilot for data if the CO is Conexant.
Pilot Request	Enable or disable request for pilot tone during training.
Last Failed Status	This value is reset to 0 each time a startup is attempted. If there is a failure, it indicates the reason for the failure.
Oper Status	Operational status of the transceiver. Values include Idle, Showtime/Data, Bootup Load, Startup HShake, Startup Trning, Framer Sync, Lcl Anlg Lpbk, Lcl Dig Lpbk, Spectrum Test.
Startup Progress	Detailed startup information to be used for debugging.
AC Mode Item	For Annex C, the bitmap transmission mode
AC Ttr R Offset	Offset from TTR_C (ATU-C timing reference) to TTR_R (ATU-R timing reference)
AC Pilot Request	Status of pilot tone for the NEXT period in the FEXT bitmap mode
EC Fdm Mode	Echo cancellation and/or frequency division multiplexing mode
Max Down Rate	This specifies the Maximum Down Rate.

Caution None.

References

- *get dsl config* command

3.273 modify eoa intf

Description Use this command to modify the properties of an eoa interface.

Command Syntax ***modify eoa intf ifname interface-name [ip ip-address] [mask net-mask] [usedhcp true|false] [gwy <ddd.ddd.ddd.ddd>] [droute true|false]][mtu <decvalue>]***

Parameters

Name	Description
ifname interface-name	This parameter specifies the interface name whose properties are to be modified. **Type:** Mandatory **Valid values:** *eoa-0,eoa-1 etc.*
ip ip-address	The IP address to be assigned to the eoa interface. **Type:** Optional **Valid values:** Any valid class A/B/C IP address **Default value:** *0.0.0.0*
mask net-mask	This parameter specifies the subnet mask to be applied to the IP address. **Type:** *Optional* **Valid values:** *255.0.0.0 - 255.255.255.255* **Default value:** *255.0.0.0*
usedhcp true|false	This specifies whether a DHCP client is to be triggered to obtain an IP address for this interface from a DHCP server. **Type:** *Optional* **Valid values:** *true or false* **Default value:** *false*
gwy <ddd.ddd.ddd.ddd>	This specifies the gateway IP address **Type:** Optional **Valid values:** Any valid class A/B/C IP address **Default value:** 0.0.0.0
droute true|false	This specifies the default route **Type:** Optional **Valid values:** true or false **Default value:** false
mtu <decvalue>	This specifies the MTU Size configured for EOA interface **Type:** Optional **Valid values :** 120 ..65535

Mode Super-User.

Example **$ modify eoa intf ifname eoa-0 droute true gwy 172.25.12.1**

Output Verbose Mode On

```
IfName                : eoa-0        Interface Sec Type: public
Configured IP Address  : 192.168.1.1  Mask              : 255.255.255.0
```

```
Low IfName             : aal5-0        NAT Direction : None
Gateway               : 0.0.0.0       Droute        : false
Oper Status            : Down          Admin Status  : Up
UseDHCP                : false
Configured MTU         : 500           Actual MTU    : 300

Set Done

IfName                 : eoa-0         Interface Sec Type: public
Configured IP Address  : 192.168.1.1   Mask : 255.255.255.0
Low IfName             : aal5-0        NAT Direction : None
Gateway               : 0.0.0.0       Droute : false
Oper Status            : Down          Admin Status : Up
UseDHCP                : false
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
IfName	The name of the interface which is being modified.
Configured IpAddress	IP address assigned to the eoa interface.
Mask	Network mask to be applied to the IP Address.
LowIfName	Specifies the lower interface.
NatDir	This specifies the NAT direction which may be: *inside, outside or none*.
UseDhcp	Whether or not a DHCP client is used to obtain the IP address for this interface from a DHCP server
OperStatus	The actual/current state of the interface. It can be either *Up* or *Down*
AdminStatus	The desired state of the interface. It may be either *Up* or *Down*
Droute	Default route
Interface sec Type	Interface security type.
Gateway	Gateway IP address
Configured MTU	This specifies the MTU value configured by the user for EOA interface.
Actual MTU	This specifies the MTU value actually operational for EOA interface

Caution None.

References

- *eoa stats* command
- *interface stats* command.

3.274 modify ethernet intf

Description Use this command to modify the NAT direction of the Ethernet interface.

Command Syntax ***modify ethernet intf ifname*** interface-name ***[ip*** ip-address***]*** ***[mask*** net-mask***]*** ***[usedhcp local|remote|false]*** ***[mtu <decvalue]***

Parameters

Name	Description
ifname interface-name	This parameter specifies the interface to be modified. **Type:** Mandatory **Valid values:** *eth-0, veth-0 - **
ip ip-address	The IP address to be assigned to the ethernet interface. **Type:** Optional **Valid values:** *Any valid class A/B/C IP address* **Default value:** *0.0.0.0*
mask net-mask	This parameter specifies the subnet mask to be applied to the IP address. Mask not allowed when **usedhcp** is **true**, with ip 0.0.0.0 **Type:** Optional **Valid values:** *255.0.0.0 – 255.255.255.255* **Default value:** *255.0.0.0*
usedhcp local|remote|false	Local: IP address for this interface is obtained from a local DHCP server Remote: DHCP client is used to obtain the IP address for this interface from a remote DHCP server False: DHCP client is not used. Usedhcp is allowed only with eth-0 interface. **Type:** Optional **Valid values:** *local, remote, false* **Default value:** *false*
inside|outside|none	This specifies the NAT direction for the interface.**Type:** Optional for physical (eth) interfaces Not allowed for virtual (veth) interfaces **Valid values:** *inside*, *outside*, *none* **Default value:** *none*
mtu <decvalue>	This specifies the MTU Size configured on ethernet interface Type: Optional Valid values : 120 ..1500

Mode Super-User.

Example ***$ modify ethernet intf ifname eth-0 ip 172.25.7.8***

Output Verbose Mode On

```
Interface          : veth-0                MTU                  : 300
Interface Sec Type  : Public               Configured IP Address : 192.168.1.1
```

```
Mask                : 255.255.255.0          UseDhcp              : False
Physical Interface  : eth-0                   Nat Direction        : None
Duplex              : half                    Speed                : 10BT
Operational Status  : Up                      Admin Status         : Up


Set Done


Interface           : veth-0                  MTU                  : 300
Interface Sec Type  : Public                 Configured IP Address : 192.168.1.1
Mask                : 255.255.255.0          UseDhcp              : False
Physical Interface  : eth-0                   Nat Direction        : None
Duplex              : half                    Speed                : 10BT
Operational Status  : Up                      Admin Status         : Up
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
Interface	The name of the interface which has been created.
Interface Sec Type	Interface security type.
Configured Ip Address	IP address assigned to the Ethernet port.
Mask	Network mask to be applied to the IP Address.
UseDhcp	Local: IP address for this interface is obtained from a local DHCP server Remote: DHCP client is used to obtain the IP address for this interface from a remote DHCP server False: DHCP client is not used.
Physical Interface	Valid only in case of virtual interfaces i.e. the Type is not *eth*. It can only be *eth-0*
Nat Direction	This specifies the NAT direction which may be: *inside, outside or none*.
Duplex	The duplex mode used by the interface.
Speed	Line speed used by Ethernet interface
Operational Status	The actual/current state of the interface. It can be either *up* or d*own*
Admin Status	The desired state of the interface. It may be either *up* or *down*
MTU	This specifies the MTU Size configured on ethernet interface

Caution None.

References

- *ethernet stats* command
- *interface stats* command.
- *create ethernet* command.

3.275 modify fwl global

Description Use this command to modify global configuration of IP Firewall.

Command Syntax ***modify fwl global [attackprotect*** *enable|disable]* ***[dosprotect*** *enable|disable]* ***[blistprotect*** *enable|disable]* ***[blistperiod*** *<decvalue>]* ***[maxtcpconn*** *<decvalue>]* ***[maxicmpconn*** *<decvalue>]* ***[maxsinglehostconn*** *<decvalue>]* ***[logdest*** *email|trace|both|none]* ***[emailid1*** *email-id]* ***[emailid2*** *email-id]* ***[emailid3*** *email-id]* ***[minlogtime<decvalue>]***

Parameters

Name	Description
attackprotect enable|disable	This specifies the status of attack protection in firewall. **Type**: Optional **Valid values** : *enable, disable*
dosprotect enable|disable	This specifies the status of DOS protection in firewall. **Type**: Optional **Valid values** : *enable, disable*
blistprotect enable|disable	This specifies the status of blacklist protection in firewall. **Type: Optional** **Valid values** : *enable, disable*
blistperiod <decvalue>	It specifies the duration to blacklist an attacking host. **Type**: Optional **Valid values** : 0 - 43200
minlogtime<decvalue>	It specifies the minimum time between logging of an individual attack. **Type:** Optional **Valid values:** 0 - 65535
maxtcpconn <decvalue>	It specifies the % of total connections that can be in a TCP half open state. **Type**: Optional **Valid values** : 0-100
maxicmpconn <decvalue>	It specifies the % of total connections that can be ICMP connections. **Type**: Optional **Valid values** : 0-100
maxsinglehostconn <decvalue>	It specifies the % of total connections that can be from a single host. **Type**: Optional **Valid values** : 0-100
Logdest email|trace|both|none	This specifies the destination type for firewall logs. **Type**: Optional **Valid values** : email,trace,both|none

Name	Description
emailid1 email-id	This field specifies the email address of the firewall administrator1 **Type**: Optional **Valid values** : Display string of length 64 char.
emailid2 email-id	This field specifies the email address of the firewall administrator2 **Type**: Optional **Valid values** : Display string of length 64 char.
emailid3 email-id	This field specifies the email address of the firewall administrator3 **Type**: Optional **Valid values** : Display string of length 64 char.

Mode Super-User.

Example ***$ modify fwl global attackprotect*** *enable* ***dosprotect*** *enable* ***blistperiod*** *20* ***maxtcpconn*** *20* ***maxicmpconn*** *35* ***maxsinglehostconn*** *50* ***logdest email emailid1*** *abc.yahoo.comcom* ***minlogtime*** *10*

Output Verbose Mode On

```
Attack Protection      : Disable    Max Half Open TCP Conn (%)  : 25
DOS Protection         : Disable    Max ICMP Conn (%)          : 25
Blacklist Status       : Enable     Max Single Host Conn(%)   : 100
Blacklist Period (min) : 10         Min Log Time(min)         :10
Log Destination        : Trace
E-Mail 1               : -
E-Mail 2               : -
E-Mail 3               : -

Set Done

Attack Protection      : Enable     Max Half Open TCP Conn (%): 20
DOS Protection         : Enable     Max ICMP Conn (%)         : 35
Blacklist Status       : Enable     Max Single Host Conn(%)    : 50
Blacklist Period (min): 20          Min Log Time(min)          :10
Log Destination        : Email
E-Mail 1               : abc.yahoo.com
E-Mail 2               : -
E-Mail 3               : -
```

Verbose Mode Off

```
Set Done
```

Output field description

Name	Description
attackprotect enable|disable	This specifies the status of attack protection in firewall.
dosprotect enable|disable	This specifies the status of DOS protection in firewall.
blistprotect enable|disable	This specifies the status of blacklist protection in firewall.
blistperiod <decvalue>	It specifies the duration to blacklist an attacking host.
Min Log Time(min)	It specifies the minimum time between logging of an individual attack.
maxtcpconn <decvalue>	It specifies the % of total connections that can be in a TCP half open state.
maxicmpconn <decvalue>	It specifies the % of total connections that can be ICMP connections.
maxsinglehostconn <decvalue>	It specifies the % of total connections that can be from a single host.
Logdest email|trace|both|none	This specifies the destination type for firewall logs.
emailid1 email-id	This field specifies the email address of the firewall administrator1
emailid2 email-id	This field specifies the email address of the firewall administrator2
emailid3 email-id	This field specifies the email address of the firewall administrator3

Caution None.

References

- *get fwl global* command

3.276 modify hdlceoc cfg

Description Use this command to modify HDLC Global Configuration

Command Syntax ***modify hdlceoc cfg [status*** disable | enable | loopback ***] [sar*** disable | enable ***]***

Parameter

Name	Description
status disable | enable | loopback	This provides Administrative control to enable/disable the HDLC over DSL channel on the modem **Type:** Optional **Default value:** disable
sar disable | enable	This provides control to enable/disable SAR(Segmentation & reassembly) of HDLC frames **Type:** Optional **Default value:** disable

Mode Super-User

Example ***$ modify hdlceoc cfg status*** disable ***sar*** disable

Output Verbose Mode On:

```
HDLC Status         SAR Status
-------------------------------------------------------------------------------
disable              disable

Set Done
```

Verbose Mode Off:

```
Set Done
```

Output field description

Field	Description
HDLC over DSL Status	This provides Administrative control to enable/disable the HDLC over DSL channel on the modem
SAR Status	This provides control to enable/disable SAR(Segmentation & reassembly) of HDLC frames

Caution None

References

- *get hdlceoc cfg* command

3.277 modify ilmi access protocol

Description

Use this command to modify the protocol which has to be configured for a particular ATM VC.

Command Syntax

modify ilmi access protocol ifname interface-name vpi vpinum vci vci-num proto pppoa|bridging|bbrouter|bpppoe|ipoa|classip|pppoe|any

Parameter

Name	Description
ifname interface-name	This specifies the ATM port for the VC(s) for which the access protocol is to be modified. **Type:** Optional **Valid values:** atm-0
vpi vpi-number	VPI of the VC(s) for which the access protocol is to be displayed. **Type:** Optional **Valid values:** 0-255
vci vci-number	VCI of the VC for which the access protocol is to be displayed. **Type:** Optional **Valid values:** 0-65535
proto pppoa|bridging|bbrouter|bpppoe|ipoa|classip|pppoe|any	Protocol to be configured for the VC

Mode

Super-User

Example

$ modify ilmi access protocol ifname atm-0 vpi 10 vci 5 proto pppoa

Output

```
Interface : atm-0              VPI             : 10
VCI       : 5                  Access Protocol : Any

Set Done

Interface : atm-0             VPI             : 10
VCI       : 5                 Access Protocol : PPPoA
```

Output field description

Field	Description
Interface	The ATM port of the VC for which information is being displayed.
VPI	VPI of the VC for which information is being displayed.

Field	Description
VCI	VCI of the VC, for which information is being displayed.
Access Protocol	Protocol, which has been configured for the shown VC.

Caution None

References None.

3.278 modify ipoa intf

Description Use this command to modify an IPoA (IP over ATM) interface.

Command Syntax ***modify ipoa intf ifname interface-name [ip ip-address] [mask net-mask][gwy <ddd.ddd.ddd.ddd>] [droute true|false] [usedhcp true/false]][mtu <decvalue>]***

Parameters

Name	Description
ifname interface-name	This parameter uniquely identifies the name of the IPoA interface. **Type:** Mandatory **Valid values:** ipoa-0-*,ipoa-1 etc.,.
ip ip-address	The IP address to be assigned to the interface. **Type:** Optional **Valid values:** *Valid IP address*
mask net-mask	This parameter specifies the subnet mask to be applied to the IP address. **Type:** *Optional* **Valid values:** *255.0.0.0 - 255.255.255.255*
gwy <ddd.ddd.ddd.ddd>	This parameter specifies the Gateway IP address. **Type:** *Optional* **Valid values:** *Valid Gateway IP Address.*
droute true|false	This specifies the default route **Type:** *Optional* **Valid values:** *true or false*
Usedhcp true/false	This specifies whether a DHCP client is to be triggered, to obtain an IP address for this interface, from a DHCP server. **Type:** *Optional* **Valid values:** *true or false*
mtu <decvalue>	This specifies the MTU Size configured for IPOA interface **Type:** Optional **Valid values:** 120 ..65535

Mode Super-User.

Example **$ modify ipoa intf ifname ipoa-0 ip 172.25.12.74**

Output Verbose Mode On

```
IfName              : ipoa-0          UseDHCP            : false
Type                : non1577         Interface Sec Type: Public
Configured IP Address: 172.25.12.12   Mask               : 255.255.0.0
DRoute              : False           Gateway            : 0.0.0.0
NAT Direction       : OUT             Oper Status        : Down
```

```
Configured MTU      : 300            Actual MTU: 200

Set Done

IfName               : ipoa-0          UseDHCP            : false
Type                 : non1577         Interface Sec Type: Public
Configured IP Address: 172.25.12.74    Mask               : 255.255.0.0
DRoute               : False           Gateway            : 0.0.0.0
NAT Direction        : OUT             Oper Status        : Down
Configured MTU       : 300             Actual MTU         : 200
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
IfName	The name of the IPoA interface which has been created.
UseDHCP	This specifies if a DHCP client is used to obtain the IP address for this interface from a DHCP server, or not.
Type	This specifies the type of IPoA interface.
Interface sec Type	VPI to be used for ILMI SNMP message exchanges
Configured IP Address	IP address assigned to the IPoA interface.
Mask	Network mask to be applied to the IP Address.
Droute	The time-interval in seconds, ILMI should use to poll for peer IL-MI's availability.
Gateway	Number of times ILMI should retry before declaring ILMI con-nectivity as lost.
Nat Direction	This specifies the NAT direction, which may be: inside, outside or none.
Oper Status	The actual/current state of the interface. It can be either Up or Down
Configured MTU	This specifies the MTU value configured by the user for IPOA interface.
Actual MTU	This specifies the MTU value actually operational for IPOA in-terface.

Caution IPoA interface will come up only when ipoa map is created from that interface.

References

- *get ipoa intf* command
- *delete ipoa intf* command
- *create ipoa map* command
- *delete ipoa map* command

3.279 modify ilmi intf

Description Use this command to modify ILMI based auto configuration parameters on the specified ATM interface.

Command Syntax ***modify ilmi intf ifname*** interface-name ***[enable|disable] [vpi*** vpi-number***] [vci*** vci-number***] [timeout*** time-out***] [keepalive*** keep-alive***] [maxretry*** max-retry***]***

Parameters

Name	Description
ifname interface-name	It specifies the ATM port on which the ILMI based auto configuration parameters are to be modified **Type:** Mandatory **Valid values:** *atm-0.*
enable|disable	Whether ILMI based auto configuration is enabled or not on this interface **Type:** Optional **Valid values:** *enable, disable* **Default value:** *disable*
vpi vpi-number	VPI to be used for ILMI SNMP message exchanges **Type:** Optional **Valid values:** *0-65535* **Default value:** *0*
vci vci-number	VCI to be used for ILMI SNMP message exchanges **Type:** Optional **Valid values:** *0-65535* **Default value:** *16*
timeout time-out	Timeout value in seconds, for SNMP Get/ Set messages exchanged between peer Interface Management Entities (IMEs) **Type:** Optional **Valid values:** *1-65535* **Default value:** *1*
keepalive keep-alive	The time-interval in seconds, ILMI should use to poll for peer ILMI's availability. **Type:** Optional **Valid values:** *1-65535* **Default value:** *5*
maxretry max-retry	Number of times ILMI should retry before declaring ILMI connectivity as lost. **Type:** Optional **Valid values:** 0-65535 **Default value:** 4

Mode Super-User.

Example ***$ modify ilmi intf ifname atm-0 enable vpi*** 10 ***vci*** 5 ***timeout*** 3 ***keepalive*** 5 ***maxretry*** 11

Output Verbose Mode On

```
Interface    : atm-0      Status           : Disable
VPI          : 12         VCI              : 50
Timeout(sec) : 1          Keep Alive (sec) : 3
Max Retries  : 3          Version          : 4.0

Set Done

Interface    : atm-0      Status           : Enable
VPI          : 10         VCI              : 5
Timeout(sec) : 3          Keep Alive (sec) : 5
Max Retries  : 11             Version      : 4.0
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
Interface	It specifies the ATM port on which the ILMI based auto configuration parameters are being modified
Status	Whether ILMI based auto configuration is enabled or not on this interface.
VPI	VPI to be used for ILMI SNMP message exchanges
VCI	VCI to be used for ILMI SNMP message exchanges
Timeout	Timeout value in seconds, for SNMP Get/ Set messages exchanged between peer Interface Management Entities (IMEs).
Keep Alive	The time-interval in seconds, ILMI should use to poll for peer ILMI's availability.
Max Retries	Number of times ILMI should retry before declaring ILMI connectivity as lost.
Version	The version of ILMI

Caution Enabling the ILMI interface only marks the state of the interface as enabled. The actual procedure begins only after the *trigger ilmi* command is given, or after the modem is rebooted. On the other hand, to disable the procedure, it is sufficient set the ILMI interface state as disabled.

References

- *create ilmi intf* command
- *get ilmi intf* command
- *modify ilmi trigger* command
- *trigger ilmi* command
- *get ilmi access protocol* command

3.280 modify ilmi access protocol

Description Use this command to modify the protocol, which has been configured by ILMI-based auto configuration for a particular ATM VC..

Command Syntax

```
modify ilmi access protocol ifname interface-name vpi vpinum
vci vci-num [proto
pppoa|bridging|bbrouter|bpppoe|ipoa|classip|any ]
```

Parameters

Name	Description
ifname interface-name	This specifies the ATM port for the VC(s) for which the access protocol is to be displayed. In case the field is not specified, then the information for all configured VCs is displayed. **Type :** Mandatory **Valid values:** atm-0.
vpi vpi-number	VPI of the VC(s) for which the access protocol is to be displayed. This can be specified only if ifname has also been specified. **Type :** Mandatory **Valid values :** 0-255 **Default value :** 0
vci vci-number	VCI of the VC for which the access protocol is to be displayed. This can be specified only if ifname and vpi have also been specified. **Type :** Mandatory **Valid values :** 0-65535 **Default value:** 16
proto pppoa|bridging|bbrouter|bpppoe|ipoa|classip|any	This specifies the Access Protocol. **Type :** Mandatory **Valid values :** *pppoa,bridging,bbrouter,bpppoe,ipoa,classip or any* **Default value:** *any*

Mode Super-User.

Example

```
$ modify ilmi access protocol ifname atm-0 vpi 10 vci 5 proto
classip
```

Output Verbose Mode On/Off

```
Interface  : atm-0      VPI             : 10
VCI        : 5          Access Protocol  : PPPoA
```

Output field description

Field	Description
Interface	The ATM port of the VC for which information is being displayed
VPI	VPI of the VC for which information is being displayed.
VCI	VCI of the VC for which information is being displayed.
Access Protocol	Protocol, which has been configured by ILMI-based auto configuration for the shown VC.

Caution None.

References

- *get ilmi access protocol* command

3.281 modify ip cfg

Description Use this command to modify IP Stack configuration parameters.

Command Syntax ***modify ip cfg [forwarding {enable|disable}] [ttl*** time-to-live***][arptimeout arp-timeout]***

Parameters

Name	Description
Forwarding enable|disable	This indicates whether this entity is acting as an IP gateway in respect to the forwarding of datagrams received by, but not addressed to, this entity **Type:** Optional **Valid values:** *enable, disable*
ttl time-to-live	This specifies the default value which will be inserted into the Time-To-Live field of the IP header of datagrams originated at this entity, whenever this is not supplied by the transport layer protocol **Type:** Optional **Valid values:** *1-255*
arptimeout arp-timeout	This specifies the duration, in seconds, after which an ARP entry is aged out. **Type :** Optional **Valid values:** 1.. 4294967295

Mode Super-User.

Example ***$ modify ip cfg forwarding*** **enable** ***ttl*** **50 arptimeout 410**

Output Verbose Mode On

```
Forwarding             : Disabled
TTL(sec)               : 64
Arp Ageing Timeout(sec):  400

Set Done

Forwarding             : Disabled
TTL(sec)               : 50
Arp Ageing Timeout(sec) :  400
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
Forwarding	This indicates whether this entity is acting as an IP gateway in respect to the forwarding of datagrams received by, but not addressed to, this entity. It may be: *Enabled, Disabled*
TTL	The default value inserted into the Time-To-Live field of the IP header of datagrams originated at this entity, whenever this is not supplied by the transport layer protocol. Here it will always be *64.*
Arp Ageing Timeout (sec)	This specifies the duration, in seconds, after which an ARP entry is aged out.

Caution None.

References

- *get ip cfg* command
- *ip stats* related commands
- *ip address* related commands
- *arp* related commands.

3.282 modify ipf global

Description Use this command to modify the global configuration.

Command Syntax ***modify ipf global [seclevel*** *high|medium|low|none]* ***[pubdefact*** *accept|deny]* ***[pvtdefact*** *accept|deny]* ***[dmzdefact*** *accept|deny]*

Parameters

Name	Description
seclevel high|medium|low|none	This specifies the service protection level applied to the system. **Type**: Optional **Valid values**: high,medim,low,none
pubdefact accept|deny	Specifies the default action when a packet does not match any of the Security rules on a public interface. **Type**: Optional **Valid values** : accept,deny
pvtdefact accept|deny	Specifies the default action when a packet does not match any of the Security rules on a private interface. **Type**: Optional **Valid values** : accept,deny
dmzdefact accept|deny	Specifies the default action when a packet does not match any of the Security rules on a DMZ interface. **Type**: Optional **Valid values** : accept,deny

Mode Super-User.

Example ***$ modify ipf global seclevel*** *high* ***pubdefact*** *accept* ***pvtdefact*** *deny* ***dmzdefact*** *accept*

Output Verbose mode on:

```
Security Level        : None       DMZ Default Action    : Deny
Public Default Action : Deny       Private Default Action : Accept

Set Done

Security Level        : High       DMZ Default Action    : Accept
Public Default Action : Accept     Private Default Action : Deny
```

Verbose mode off:

```
Set Done
```

Output Field description

Field	Description
Security Level	This specifies the service protection level applied to the system.
Public Default Action	Specifies the default action when a packet does not match any of the Security rules on a public interface.
Private Default Action	Specifies the default action when a packet does not match any of the Security rules on a private interface.
DMZ Default Action	Specifies the default action when a packet does not match any of the Security rules on a DMZ interface.

Caution None

References

- get ipf global

3.283 modify ipf rule entry

Description This command is used for modifying an IP filter rule for filtering.

Command Syntax ***modify ipf rule entry ruleid*** rule-id ***[log enable|disable] [enable|disable]***

Parameters

Name	Description
ruleid rule-id	This is index given by caller to identify the Rule entry. **Type**: Mandatory **Valid values** : *1-4294967295*
[log enable|disable]	This flag controls the logging of matched packets. Each log will contain IP Header and TCP/UDP header or ICMP fields, if available. **Type**: Optional **Valid values:** *enable* or *disable*
enable|disable	Specifies the status of rule entry. **Type:** Optional **Valid values:** *enable* or *disable*

Mode Super-User.

Example ***$ modify ipf rule entry ruleid 1 enable log enable***

Output Verbose Mode On

```
Rule id           : 1Interface         : eth-0
Rule Admin status : DisableRule Oper Status  : Disable
In interface      : ALLDirection         : Out
Security Level    : HighBlacklist Status         : Enable
Logging           : DisableAction            : Accept
Log Tag           : -
IP Frag Pkt       : Yes         IP Opt Pkt        : No
TCP Flag          : SynStore State       : Enable
Src Addr    : Equal          172.25.8.76
Dest Addr   : Range          172.25.8.70          172.25.8.90
Src Port    : Out Of Range   10                   20
Dest Port   : Not Equal      3
ICMP Code   : Not Equal      10
ICMP Type   : Equal          unreach
TransProt   : Equal          TCP
IP Pkt Size : Less Than      10
TOD Rule    : Enable Between  01:02:30              02:01:30


Set Done

Rule id          : 1              Interface        : eth-0
Rule Admin status: Enable         Rule Oper Status : Disable
In interface      : ALLDirection         : Out
Security Level    : HighBlacklist Status        : Enable
Logging           : EnableAction            : Accept
Log Tag           : -
IP Frag Pkt       : Yes         IP Opt Pkt        : No
TCP Flag          : SynStore State       : Enable
Src Addr    : Equal          172.25.8.76
Dest Addr   : Range          172.25.8.70          172.25.8.90
Src Port    : Out Of Range   10                   20
Dest Port   : Not Equal      3
```

```
ICMP Code   : Not Equal      10
ICMP Type   : Equal          unreach
TransProt   : Equal          TCP
IP Pkt Size : Less Than      10
TOD Rule    : Enable Between  01:02:30              02:01:30
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
Rule id	The index given by the caller to identify the rule entry.
Rule Admin Status	Specifies administrative status of the rule entry.
Interface	Specifies the IP-enabled physical interface to be associated to this rule. *All* indicates that the rule is to be associated to all interfaces.
In Interface	Specifies the input interface ID which may be used to dictate the rules such as deny/accept all traffic from a specific interface. This field can be specified only if the direction is *out*.
Direction	Specifies the direction of data flow on which filtering is to be applied.
Action	Specifies the action to be taken when a packet matches a rule.
Logging	This flag controls the logging of matched packets. Each log will contain IP header and TCP/UDP header or ICMP fields, if available.
Log Tag	This specifies the Filter logging tag, which will be added to all the logs generated due to the rule
Src Addr	This field specifies the matching criteria for source IP Address along with the source IPAddress value and the destination IP-Address value. The source or destination or both are shown depending on whether the matching criteria is relational, range, erange, any or self.
Dest Addr	This field specifies the matching criteria for source IP Address along with the source IPAddress value and the destination IP-Address value. The source or destination or both are shown depending on whether the matching criteria is relational, range, erange, any or self.
Src Port	This field specifies the matching criteria for source port along with the start of src port and the end of src port. The start or end or both are shown depending on whether the matching criteria is relational, range, erange, any or bcast.

Field	Description
Dest Port	This field specifies the matching criteria for destination Port along with the start dest port and the end dest port. The start or end or both are shown depending on whether the matching criteria is relational, range, erange, any or bcast.
ICMP Code	This field specifies the matching criteria for ICMP code value along with the code field in ICMP header in case of ICMP packets.
ICMP Type	This field specifies the matching criteria for ICMP Type along with the type field in ICMP header in case of ICMP packets.
TransProt	This field specifies the matching criteria for transport protcol field along with the transport layer protocol number as per IANA.
TCP Flag	This specifies filtering criteria for TCP packet types.
Store State	This specifies whether stateful filtering is done or not
Security Level	This specifies the association of rule with system wide service protection level.
Blacklist Status	This specifies whether source of the packet should be put in blacklist if it matches with the rule. It will be applicable to deny kind of rules
IP Frag Pkt	This specifies whether the rule is applicable to fragmented packets, non fragmented packets or in both cases.
IP Opt Pkt	This specifies whether the rule is applicable to IP packet with or without IP options or in both cases.
IP Pkt Size	This field specifies the matching criteria for IP Pkt Size along with IP packet filtering attribute . It should be compared against the packet size value in IP header.
ToD Rule	This field specifies whether the rule should be applied for the duration specified."Enable Between" indicates that the rule is applied between the specified time duration."Disable Between" indicates that rule is not applicable between the specified duration, but it is applicable for remaining time of the day.
Rule Oper Status	A rule will be operationally enabled if and only if it is administratively enabled, its Time of Day status as per current time is Enable, and if the rule's security level matches the global security level as shown by get ipf global.

Caution None.

References

- *create ipf rule entry* command
- *get ipf rule entry* command
- *delete ipf rule entry* command

3.284 modify l2tp global config

Description Use this command to modify L2tp global configuration.

Command Syntax ***modify l2tp global config timeout*** {infinite|{num <decValue>}}

Parameters

Name	Description
timeout {infinite|{ num <decValue>}}	This field defines the period of time (in secs) that a peer will wait for the response. A value of "Infinite" indicates an infinite wait. **Type:** mandatory **Valid values:** 1 ..3600, infinite

Mode Super-User.

Example ***$ modify l2tp global config timeout num*** *300*

Output Verbose mode on:

```
Response timeout (secs)  : 350

Set Done

Response timeout (secs)  : 300
```

Verbose mode off:

```
Set Done
```

Output Field description:

Field	Description
Response Timeout(secs)	Defines the period of time (in secs) that a peer will wait for the response. A value of "Infinite" indicates an infinite wait.

Caution None.

References

- get l2tp global config

3.285 modify l2tp tunnel config

Description Use this command to modify L2tp tunnel configuration.

Command Syntax

```
modify l2tp tunnel config
ifname interface-name
[localip local-ip-address]
[localhostname local-host-name]
[remoteip remote-ip-address]
[remotehostname remote-host-name]
[start|stop]
[authtype  simple|challenge|none]
[secret tunnel-secret]
[hellointerval hello-interval]
[idletimeout {infinite|{num <decValue>}}]
[crws contol-recv-windowsize]
[maxretx max-retransmission]
[maxretxtimeout max-retransmission-timeout]
[payloadseq  never|always}]
[transport udpip]
[initiator local|remote]
```

Parameters

Name	Description
ifname interface-name	Identifies the interface name for L2TP layer. **Type**: Mandatory **Valid values:** l2t-0-l2t-*.
localip local-ip-address	This field specifies the address of the local endpoint of the tunnel, or 0.0.0.0 if the device is free to choose any of its addresses at tunnel establishment time. **Type:** Optional **Valid values:**
localhostname host-name	Name of the local End-point of the tunnel. **Type:** Optional **Valid values:** Display string of 255 characters
remoteip remote-ip-address	This field specifies the address of the remote end-point of the tunnel to which the tunnel is to be established. **Type:** Optional **Valid values:**
remotehostname peer-dns-name	Name of the remote End-point of the tunnel **Type:** Optional **Valid values:** Display string of 255 characters.
start|stop	This attribute specifies the action to be taken for the tunnel. True establishes the Tunnel. False tears the tunnel down. **Type:** Optional **Valid values:** start, stop

Name	Description
authtype simple|challenge|none	This object describes how L2TP tunnel peers are to be authenticated **Type:** optional **Valid values:** simple, challenge, none
secret tunnel-secret	This object is used to configure the shared secret used during the tunnel authentication phase of tunnel establishment if authtype is challenge. **Type:** optional **Valid values:** Hex Value - maximum of 64 octet length.
Hellointerval hello-interval	This object defines the interval (in sec) in which Hello packets are to be sent to the tunnel peer. A value '0' indicates that Hello packets will not be sent to tunnel peer. **Type:** optional **Valid values:** 0..3600(sec)
idletimeout idle-timeout	This object defines the period of time (in seconds) that an established tunnel with no sessions will wait before disconnecting the tunnel.A value of '0' indicates that the tunnel will disconnect immediately after the last session disconnects. "infinite" leaves the tunnel up indefinitely. **Type:** optional **Valid values:** 0.86400(sec), infinite
crws contol-recv-windowsize	This object defines the control channel receive window sizeIt specifies the maximum number of packets the tunnel peer can send without waiting for an acknowledgement from this peer **Type:** optional **Valid values:** 1..10
maxretx max-retransmission	This object defines the number of retransmissions, which the tunnel will attempt before assuming that the peer is no longer responding.A value of '0' indicates that this peer will not attempt to retransmit an unacknowledged control packet. **Type:** optional **Valid values:** 0..32
maxretxtimeout max-retransmission-timeout	This object defines the maximum retransmission timeout interval that the tunnel will wait before retransmitting a control packet that has not been acknowledged. **Type:** optional **Valid values:** 1..32

Name	Description
payloadseq never|always	This object determines whether or not session payload packets will be requested to be sent with sequence numbers from tunnel peer's. **Type:** optional **Valid values:** never, always
transport udpip	This object defines the underlying transport media that is in use for this tunnel entry. **Type:** optional **Valid values:** udpip
initiator local|remote	This object indicates whether the tunnel will be initiated locally or not. **Type:** optional **Valid values:** local, remote

Mode Super-User.

Example

```
$ modify l2tp tunnel config ifname l2t-0 localip 178.10.1.2
remoteip 178.10.2.1 hellointerval 100 idletimeout 200
```

Output Verbose mode on:

```
If Name             : l2t-0
Status              : Start              Oper Status        : Up
Local IP-address    : 178.10.10.10     Remote IP-address  : 178.10.11.10
Hello Interval      : 300               Idle Timeout       : 100
Max Retx Attempt    : 10                Max Retx Timeout   : 10
Initiator           : local             Payload Sequencing : always
Authentication Type : simple            Transport          : udpip
Control RWS         : 5
Shared Secret       : passwd
Local Host name     : titanium
Remote Host name    : Columbia

Set Done

If Name             : l2t-0
Status              : Start              Oper Status        : Up
Local IP-address    : 178.10.10.10     Remote IP-address  : 178.10.11.10
Hello Interval      : 300               Idle Timeout       : 100
Max Retx Attempt    : 10                Max Retx Timeout   : 10
Initiator           : local             Payload Sequencing : always
Authentication Type : simple            Transport          : udpip
Control RWS         : 5
Shared Secret       : passwd
Local Host name     : titanium
Remote Host name    : Columbia
Remote Host name    : Columbia
```

Verbose mode off:

```
Set Done
```

Output Field description:

Field	Description
If-name	Identifies the interface name for L2TP layer.
Local IP-address	This field specifies the address of the local endpoint of the tunnel
Local Host name	This field specifies the address of the local endpoint of the tunnel
Remote IP-address	This field specifies the address of the remote endpoint of the tunnel to which the tunnel is to be established.
Status	This field specifies the status of the of the l2tp interface.
Oper Status	This field specifies the Operstatus of the of the l2tp interface.
Remote Host name	This field specifies the hostname of the remote endpoint of the tunnel to which the tunnel is to be established.
Hello Interval	Defines the interval (in sec) in which Hello packets are to be sent to the tunnel peer
Idle Timeout	Defines the period of time (in seconds) that an established tunnel with no sessions will wait before disconnecting the tunnel.
Control RWS	Defines the control channel receive window size
Max Retx Timeout	Defines the maximum retransmission timeout interval that the tunnel will wait before retransmitting a control packet that has not been acknowledged.
Initiator	This indicates whether the tunnel will be initiated locally or not.
Payload Sequencing	This object determines whether or not session payload packets will be requested to be sent with sequence numbers from tunnel peer's. The value never(2) indicates that L2TP will never initiate sequencing but will do sequencing if asked. The value always(3) indicates that L2TP will send the sequencing Required AVP during session establishment
Authentication Type	Describes how L2TP tunnel peers are to be authenticated
Transport	Defines the underlying transport media that is in use for this tunnel entry.

Field	Description
Shared Secret	Shared secret is used during the tunnel authentication phase of tunnel establishment if authtype is challenge
Max Retx Attempt	Defines the number of retransmissions, which the tunnel will attempt before assuming that the peer is no longer responding.

Caution None.

References

- delete l2tp tunnel config
- get l2tp tunnel config
- create l2tp tunnel config

3.286 modify l2wall cfg

Description Use this command to modify the L2WALL global configuration.

Command Syntax ***modify l2wall cfg [off|on|auto] [inacttime*** *inactive-time**]***

Parameters

Name	Description
off|on|auto	Status of the L2wall configuration.. **Type:** Optional **Valid values:** on, off or auto **Default value:** off
inacttime *inactive-time*	Time since last recorded activity in minutes. **Type:** Optional **Valid values:** 0 – 4294967295 **Default value:** 5

Mode Super-User

Example ***$ modify l2wall cfg on inacttime 20***

Output Verbose Mode On:

```
Status : off                    Inactive Time(min) : 5
Set Done
Status : on                     Inactive Time(min) : 20
```

Verbose Mode Off:

```
Set Done
```

Output field description

Field	Description
`Status`	Status of the L2wall configuration.
`Inactive Time(min)`	Time since last recorded activity in minutes.

Caution None.

References

- *get l2wall cfg*

3.287 modify mctl access

Description Use this command to modify Management Control-Access Configuration

Command Syntax

```
modify mctl access  [ httpwanaccess enable | disable ] [
httplanaccess enable | disable ] [ telnetwanaccess enable |
disable ] [ telnetlanaccess enable | disable ] [ ftpwanaccess
enable | disable ] [ ftplanaccess enable | disable ] [
tftpwanaccess enable | disable ] [ tftplanaccess enable |
disable ] [ snmpwanaccess enable | disable ] [ snmplanaccess
enable | disable ]
```

Parameter

Name	Description
httpwanaccess enable | disable	This is used to enable or disable HTTP access to the modem from its WAN interfaces. WAN interfaces are those for which the IP Filter security type is marked as public. The IP addresses allowed are picked up from the Management Control Allowed IP addresses list. If there are no entires in this list, then access is allowed to all addresses. **Type:** Optional **Default value:** enable
httplanaccess enable | disable	This is used to enable or disable HTTP access to the modem from its LAN interfaces. LAN interfaces are those for which the IP Filter security type is marked as private or DMZ. If enabled, HTTP access is allowed to all LAN hosts. LAN access cannot be controlled for specific hosts. **Type:** Optional **Default value:** enable
telnetwanaccess enable | disable	This is used to enable or disable Telnet access to the modem from its WAN interfaces. WAN interfaces are those for which the IP Filter security type is marked as public. The IP addresses allowed are picked up from the Management Control Allowed IP addresses list. If there are no entires in this list, then access is allowed to all addresses. **Type:** Optional **Default value:** enable
telnetlanaccess enable | disable	This is used to enable or disable Telnet access to the modem from its LAN interfaces. LAN interfaces are those for which the IP Filter security type is marked as private or DMZ. If enabled, Telnet access is allowed to all LAN hosts. LAN access cannot be controlled for specific hosts. **Type:** Optional **Default value:** enable

Name	Description
ftpwanaccess enable | disable	This is used to enable or disable FTP access to the modem from its WAN interfaces. WAN interfaces are those for which the IP Filter security type is marked as public. The IP addresses allowed are picked up from the Management Control Allowed IP addresses list. If there are no entires in this list, then access is allowed to all addresses. **Type:** Optional **Default value:** enable
ftplanaccess enable | disable	This is used to enable or disable FTP access to the modem from its LAN interfaces. LAN interfaces are those for which the IP Filter security type is marked as private or DMZ. If enabled, FTP access is allowed to all LAN hosts. LAN access cannot be controlled for specific hosts. **Type:** Optional **Default value:** enable
tftpwanaccess enable | disable	This is used to enable or disable TFTP access to the modem from its WAN interfaces. WAN interfaces are those for which the IP Filter security type is marked as public. The IP addresses allowed are picked up from the Management Control Allowed IP addresses list. If there are no entires in this list, then access is allowed to all addresses. **Type:** Optional **Default value:** enable
tftplanaccess enable | disable	This is used to enable or disable TFTP access to the modem from its LAN interfaces. LAN interfaces are those for which the IP Filter security type is marked as private or DMZ. If enabled, TFTP access is allowed to all LAN hosts. LAN access cannot be controlled for specific hosts. **Type:** Optional **Default value:** enable
snmpwanaccess enable | disable	This is used to enable or disable SNMP access to the modem from its WAN interfaces. WAN interfaces are those for which the IP Filter security type is marked as public. The IP addresses allowed are picked up from the Management Control Allowed IP addresses list. If there are no entires in this list, then access is allowed to all addresses. **Type:** Optional **Default value:** enable
snmplanaccess enable | disable	This is used to enable or disable SNMP access to the modem from its LAN interfaces. LAN interfaces are those for which the IP Filter security type is marked as private or DMZ. If enabled, SNMP access is allowed to all LAN hosts. LAN access cannot be controlled for specific hosts. **Type:** Optional **Default value:** enable

Mode Super-User

Example

```
$ modify mctl access  httpwanaccess enable httplanaccess
enable telnetwanaccess enable telnetlanaccess enable
ftpwanaccess enable ftplanaccess enable tftpwanaccess enable
tftplanaccess enable snmpwanaccess enable snmplanaccess
enable
```

Output Verbose Mode On:

```
HTTP Wan Access   : enable  HTTP Lan Access   : enable
Telnet Wan Access : enable  Telnet Lan Access : enable
FTP Wan Access    : enable  FTP Lan Access    : enable
TFTP Wan Access   : enable  TFTP Lan Access   : enable

Set Done
```

Verbose Mode Off:

```
Set Done
```

Output field description

Field	Description
HTTP Wan Access	This is used to enable or disable HTTP access to the modem from its WAN interfaces. WAN interfaces are those for which the IP Filter security type is marked as public. The IP addresses allowed are picked up from the Management Control Allowed IP addresses list. If there are no entires in this list, then access is allowed to all addresses.
HTTP Lan Access	This is used to enable or disable HTTP access to the modem from its LAN interfaces. LAN interfaces are those for which the IP Filter security type is marked as private or DMZ. If enabled, HTTP access is allowed to all LAN hosts. LAN access cannot be controlled for specific hosts.
Telnet Wan Access	This is used to enable or disable Telnet access to the modem from its WAN interfaces. WAN interfaces are those for which the IP Filter security type is marked as public. The IP addresses allowed are picked up from the Management Control Allowed IP addresses list. If there are no entires in this list, then access is allowed to all addresses.
Telnet Lan Access	This is used to enable or disable Telnet access to the modem from its LAN interfaces. LAN interfaces are those for which the IP Filter security type is marked as private or DMZ. If enabled, Telnet access is allowed to all LAN hosts. LAN access cannot be controlled for specific hosts.

Field	Description
FTP Wan Access	This is used to enable or disable FTP access to the modem from its WAN interfaces. WAN interfaces are those for which the IP Filter security type is marked as public. The IP addresses allowed are picked up from the Management Control Allowed IP addresses list. If there are no entires in this list, then access is allowed to all addresses.
FTP Lan Access	This is used to enable or disable FTP access to the modem from its LAN interfaces. LAN interfaces are those for which the IP Filter security type is marked as private or DMZ. If enabled, FTP access is allowed to all LAN hosts. LAN access cannot be controlled for specific hosts.
TFTP Wan Access	This is used to enable or disable TFTP access to the modem from its WAN interfaces. WAN interfaces are those for which the IP Filter security type is marked as public. The IP addresses allowed are picked up from the Management Control Allowed IP addresses list. If there are no entires in this list, then access is allowed to all addresses.
TFTP Lan Access	This is used to enable or disable TFTP access to the modem from its LAN interfaces. LAN interfaces are those for which the IP Filter security type is marked as private or DMZ. If enabled, TFTP access is allowed to all LAN hosts. LAN access cannot be controlled for specific hosts.

Caution None

References

- *get mctl access* command

3.288 modify nat global

Description Use this command to modify NAT global info.

Command Syntax

```
modify nat global [tcpidletimeout tcp-idle-timeout]
[tcpclosewait tcp-close-wait] [tcptimeout tcp-timeout]
[udptimeout udp-timeout] [gretimeout gre-timeout] [esptimeout
esp-timeout] [icmptimeout icmp-timeout] [defnatage default-
nat-timeout] [{enable|disable}] [portstart port-start]
[portend port-end]
```

Parameters

Name	Description
tcpidletimeout tcp-idle-timeout	The Time out (in seconds) which is used to expire out Idle TCP Nat Translations **Type:** Optional **Valid values:** *1-4294967295*
tcpclosewait tcp-close-wait	The Wait time (in seconds) after which a TCP connection is closed **Type:** Optional **Valid values:** *1-4294967295*
tcptimeout tcp-timeout	The default timeout (in seconds) in case of errors. **Type:** Optional **Valid values:** *1-4294967295*
udptimeout udp-timeout	The time (in seconds) for UDP timeout **Type:** Optional **Valid values:** *1-4294967295*
icmptimeout icmp-timeout	The time (in seconds) for ICMP timeout **Type:** Optional **Valid values:** *1-4294967295*
gretimeout gre-timeout	The time (in seconds) for GRE timeout **Type:** Optional **Valid values:** *1-4294967295*
esptimeout esp-timeout	The time (in seconds) for ESP timeout **Type:** Optional **Valid values:** *1-4294967295*
defnatage default-nat-timeout	The default Nat Time Out (in seconds). **Type:** Optional **Valid values:** *1-4294967295*
enable|disable	This is used to enable or disable NAT operations in the IAD **Type:** Optional

Name	Description
portstart port-start	The port value from which the port range can start. This value can be set only when the Nat is disabled. **Type:** Optional **Valid values:** *50000 - 60000*
portend port-end	The port value at which the port range ends. This value can be set only when the Nat is disabled. **Type:** Optional **Valid values:** *50000 - 60000*

Mode Super-User

Example ***$ modify nat global disable***

Output Verbose Mode On

```
TCP Idle Timeout(sec): 86400          TCP Close Wait(sec)  : 60
TCP Def Timeout(sec) : 60             UDP Timeout(sec)     : 300
ICMP Timeout(sec)    : 60             GRE Timeout (sec)    : 200
ESP Timeout(sec)      : 300           Default Nat Age(sec) : 240
NAPT Port Start      : 50000          NAPT Port End        : 51023
Admin Status         : Disable
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
TCP Idle Timeout	The Time out (in seconds) which is used to expire out Idle TCP Nat Translations
TCP Close Wait	The Wait time (in seconds) after which a TCP connection is closed
TCP Def Timeout	The default timeout (in seconds) in case of errors.
UDP Timeout	The time (in seconds) for UDP timeout
ICMP Timeout	The time (in seconds) for ICMP timeout
GRE Timeout	The time (in seconds) for GRE timeout
ESP Timeout	The time (in seconds) for ESP timeout
Default Nat Age	The default NAT Time Out (in seconds).
NAPT Port Start	The port value from which the port range can start
NAPT Port End	The port value at which the port range ends.
Admin Status	The desired NAT Status. It may be: *Enable, Disable*

Caution None.

References

- *get nat global* command
- *nat rule status* related commands
- *nat rule stats* related commands
- *nat rule entry* related commands.

3.289 modify nbsize

Description Use this command to modify sizing parameters. The modification takes effect only after the next reboot.

Command Syntax ***modify nbsize [maxipsess*** *max-num-ip-sessions]* ***[httpport*** *http-port]* ***[telnetport*** *telnet-port]* ***[ftpport*** *ftp-port]* ***[serialauth enable|disable]***

Parameters

Name	Description
Maxipsess max-num-ip-sessions	This specifies the maximum number of active IP sessions. **Type:** Optional **Valid values:** *100-2000*
Httpport http-port	This specifies the HTTP port. **Type:** Optional **Valid values:** 80 or from 61000 to 62000
Telnetport telnet-port	This specifies the telnet port. **Type:** Optional **Valid values:** 23 or from 61000 to 62000
Ftpport ftp-port	This specifies the FTP port. **Type:** Optional **Valid values:** 21 or from 61000 to 62000
serialauth enable|disable	This specifies Serial Port Authentication Mode. **Type:** Optional **Valid Values:** *Enable, Disable*

Mode Super-User.

Example ***$ modify nbsize maxipsess*** 200 **serialauth** enable

Output Verbose Mode On

```
Max IP Session : 100       HTTP Port : 80
Telnet Port    : 23        FTP Port  : 21
Serial Auth    : disable

Set Done

Max IP Session : 200      HTTP Port : 80
Telnet Port    : 23        FTP Port  : 21
Serial Auth    : enable
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
Max IP Session	This specifies the maximum number of active IP sessions.
HTTP Port	This specifies the HTTP port.
Telnet Port	This specifies the telnet port.
FTP Port	This specifies the FTP port
Serial Auth	This specifies whether Serial Port Authentication is enabled or disabled.

Caution None.

References

- *get nbsize* command

3.290 modify oam cc vc

Description Use this command to to activate or de-activate OAM F5 end to end continuity check mechanism..

Command Syntax ***modify oam cc vc ifname*** *interface-name* ***[mode*** *auto|manual]* ***[action*** *act|deact]* ***[dir*** *src|sink|both]* ***[ethercheck*** *enable|disable]*

Parameters

Name	Description
ifname interface-name	This parameter specifies the VC interface on which the continuity check is to be activated or de-activated. **Type**: Mandatory **Valid values**: aal5-*
mode auto|manual	This specifies the mode of activation/deactivation of continuity check.Manual activates/de-activates immediately.Auto activates/de-activates through OAM activation/de-activation procedure. **Type**: Optional **Valid values**: auto or manual **Default Value** : auto
action act|deact	This field specifies the CC action to be taken. This is used along with "dir" field.Act is activation.Deact is de-activation. **Type:** Optional **Valid values:** act or deact.
dir src|sink|both	This field specifies the direction for CC activation/deactivation. Direction could be source (src), sink or both. **Type**: Optional **Valid values**: src, sink, both
ethercheck enable|disable	This field specifies whether ethernet device status should be checked before transmitting a CC cell. **Type**: Optional **Valid values**: enable, disable **Default Value** : disable.

Mode Super-User.

Example ***$ modify oam cc vc ifname*** *aal5-0* ***mode*** *auto* ***action*** *act* ***dir*** *both* ***ethercheck*** *enable*

Output Verbose Mode On

```
Ifname   Mode   SourceOperStatus EtherCheck  SinkOperStatus Initiator
-------------------------------------------------------------------------
aal5-0  manual deactivated      disable      deactivated     -

Set Done

Ifname   Mode  SourceOperStatus EtherCheck SinkOperStatusInitiator
-------------------------------------------------------------------------
aal5-0  auto  activated        enable      activated        Self
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
Ifname	This parameter specifies VC interface.
Mode	This specifies the mode of activation/deactivation of continuity check.
SourceOperStatus	This field specifies the current operational state of source point of the VCC.
EtherCheck	This field specifies whether ethernet device status should be checked before transmitting a CC cell.
SinkOperStatus	This field specifies the current operational state of sink point of the VCC.
Initiator	This field is valid only in auto mode and it specifies the current initiator of CC Activation/Deactivation.

Caution

1. This command will not work if operational status of VC is DOWN.
2. In auto mode, if CC is activated then the next activate command will fail.
3. In manual mode, the activation state of source/sink is the combined effect of the activation commands issued. i.e. if the user gives activate source and then activate sink, then the final result will be that both source and sink will be in activated state. Similarly, if the user has given activate both direction and then gives activate sink, the final result will be that both source and sink will be in activated state.
4. Manual to auto mode transition is allowed only when the source and sink are in deactivated state. There is no such restriction in auto to manual mode transition.

References

- *get oam cc vc* command.

3.291 modify oam lpbk vc

Description Use this command to start or stop OAM loopback.

Command Syntax ***modify oam lpbk vc ifname*** interface-name ***[lbid*** **oam-loopback-location-id*]*** ***[e2e|seg]***

Parameters

Name	Description
vc ifname interface-name	This parameter specifies the interface for which information is desired. In case the field is not specified, then the information for all valid aal5 interfaces should be displayed. **Type:** Mandatory **Valid values:** *aal5-0 - **
lbid oam-loopback-location-id	This defines the loop back site which will loop-back the cell. **Type:** Optional **Valid values:** 0x followed by 32 Hexadecimal No. **Default value:** *0xffffffffffffffffffffffffffffffff*
e2e|seg	This specifies the loop back type to be used. It may be either end-to-end or segment. **Type:** Optional **Valid values:** *e2e, seg* **Default value:** *e2e*

Mode Super-User.

Example ***$ modify oam lpbk vc ifname*** **aal5-0** ***seg***

Output Verbose Mode On

```
If-Name             : aal5-0   VPI            : 1        VCI        : 1
LB Type             : e2e
OAM Location Id     : 0xffffffffffffffffffffffffffffffff
OAM LB Result       : E2e Succeeded

Set Done

If-Name             : aal5-0   VPI            : 1        VCI        : 1
LB Type             : seg
OAM Location Id     : 0xffffffffffffffffffffffffffffffff
OAM LB Result       : Test In Progress
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
If-Name	The name of the aal5 (*aal5-0* etc.) interface whose statistics are to be retrieved.
VPI	This is the Virtual Port Identifier
VCI	This is the Virtual Circuit Identifier
LB Type	This specifies the loop back type used. It may be: *e2e* or *seg*
OAM Location Id	This defines the loop back site which was used to loopback the cell.
OAM LB Result	This specifies the result of the loop back test. It may be *Result Unavailable*, *Seg Succeeded*, *Seg Failed*, *E2e Succeeded*, *E2e Failed*, *Test Aborted*, or *Test In Progress*

Caution None.

References

- `get oam lpbk` command
- `atm trfdesc` related commands
- `atm vc` related commands
- `atm port` and `statistics` related commands.

3.292 modify pfraw block

Description Use this command to modify the pfraw block status for a given protocol.

Command Syntax ***modify pfraw block protocol IPV6MCAST|8021Q|ARP|BPDU|IPX|NETBEUI|APPLETALK|RARP|IPMCAST|PPE enable|disable***

Parameters

Field	Description
protocol IPV6MCAST|8021Q|ARP|BPDU|IPX|NETBEUI|APPLETALK|RARP|IPMCAST|PPE	This specifies the protocol for which pfraw rule needs to be blocked/unblocked. **Type:** Mandatory **Valid Values:** *IPV6MCAST, 8021Q, ARP, BPDU, IPX, NETBEUI, APPLETALK, RARP, IPMCAST, PPE*
enable|disable	This specifies the rule status of the Pfraw Rule. **Type:** Mandatory **Valid Values:** enable, disable

Mode Super-User.

Example ***$ modify pfraw block protocol L2WALL disable***

Output Verbose Mode On

```
Protocol        : L2WALL          Rule status : enable

Set Done

Protocol        : L2WALL          Rule status : disable
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
Protocol	This object specifies the protocol for which pfraw rule needs to be blocked/unblocked.
Rule status	This specifies the rule status of the pfraw Rule.

Caution None.

References

- *get pfraw block* command

3.293 modify pfraw global

Description Use this command to modify global parameters of raw filter.

Command Syntax ***modify pfraw global [enable|disable] [accept|deny|callmgmt]***

Parameters

Field	Description
enable*|*disable	This identifies whether to enable the raw filter feature or to disable it. **Type:** Optional **Valid values:** *enable* or *disable*
***accept*|*deny*|callmgmt**	This identifies the default action incase the packet does not match any of the rules. **Type:** Optional **Valid values:** *accept* , *deny* or *callmgmt*

Mode Super-User.

Example ***$ modify pfraw global enable***

Output Verbose Mode On

```
Status         : Disable
Default action : Deny

Set Done

Status         : Enable
Default action : Deny
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
status	This field indicates whether the raw filter status is enabled or disabled.
default action	This field indicates the default action to be taken if the packet does not match any of the rules specified.

Caution None.

References

- *modify pfraw rule entry* command
- *modify pfraw subrule entry* command

3.294 modify pfraw rule entry

Description Use this command to modify the attributes of a rule.

Command Syntax ***modify pfraw rule entry ruleid*** rule-id ***[enable|disable] [log disable|match|nomatch|all] [act accept|deny|callmgmt] [ssb ssb] [ssbmask ssbmask] [priority priority] [inifname*** incoming-if-name|***all|public|private|dmz] [outifname out-ifname]***

Parameters

Name	Description
ruleid rule-id	This identifies the rule index of the rule whose attributes need to be changed. **Type:** Mandatory **Valid values:** 0 -65535 Only existing rule ids accepted as input.
enable|disable	This specifies whether this rule should be enabled or disabled. **Type:** Optional **Valid values:** enable or disable
log disable|match|nomatch|all	This specifies the log option of this rule. **Type:** Optional **Valid values:** disable or match or nomatch or all
Act accept|deny|callmgmt	This specifies the action to be taken when a packet matches this rule. **Type:** Optional **Valid values:** accept or deny or callmgmt.
ssb ssb	Service Specification Byte value to be set in the packet **Type:** Optional **Valid values:** any hexadecimal pattern beginning with 0x and of length 2
ssbmask ssbmask	Service Specification Byte value mask **Type:** Optional **Valid values:** any hexadecimal pattern beginning with 0x and of length 2
inifname incoming-if-name	In case of a rule for an outgoing interface, this specifies the incoming interface. Only packets which are received on the *inifname* and which are going out via the *ifname* will be matched against this rule. **Type:** Optional **Valid values:** *eth-0, veth-0, veth-1, veth-2, veth-3, eoa-0 - *, ppp-0 - *, all.* This can be specified only when the direction is out. **Default value:** *all*

Name	Description
inifname incoming-if-name	In case of a rule for an outgoing interface, this specifies the incoming interface. Only packets which are received on the *inifname* and which are going out via the *ifname* will be matched against this rule. **Type:** Optional **Valid values:** *eth-0, veth-0, veth-1, veth-2, veth-3, eoa-0 - *, ppp-0 - *, all.* This can be specified only when the direction is out. **Default value:** *all*
outifname outIfName	In case of a rule for an incoming interface, this specifies the outgoing interface. Only packets which are received on the outifname and which are coming in via the ifname will be matched against this rule. **Type:** Optional **Valid values:** eth-0, veth-0, veth-1, veth-2, veth-3, eoa-0 - *, ppp-0 - *, all. This can be specified only when the direction is **in**. **Default value:** all

Mode Super-User

Example ***$ modify pfraw rule entry ruleid 2 log match ssb 0x34 ssbmask 0xff priority 1***

Output Verbose Mode On:

```
Rule id        : 2                 Rule status   : Enable
Interface      : eth-0             In interface  : All
Direction      : Out               SSB           : 0x44
SSB Mask : 0x1f                    Priority      : 2
Action         : Accept             Logging     : Disable
Out interface : ALL

Set Done

Rule id        : 2                 Rule status   : Enable
Interface      : eth-0             In interface  : All
Direction      : Out               SSB           : 0x44
SSB Mask       : 0x1f              Priority      : 2
Action         : Accept            Logging        : Match
Out interface  : ALL
```

Verbose Mode Off:

```
Set Done
```

Output field description

Field	Description
Rule id	This identifies the rule index of the rule.
Rule Status	This specifies whether this rule is enabled or disabled.
Interface	This specifies the interface name for a rule.

Field	Description
In Interface	This specifies the incoming interface for the given outgoing interface.
Direction	This specifies the filtering direction to which this rule is applied.
SSB	Service Specification Byte value to be set in the packet.
SSB Mask	Service Specification Byte value mask
Priority	Priority value to be attached to the packet
Action	This specifies the action taken when a packet matches this rule
Logging	This specifies the log option of this rule
Out interface	This specifies the outgoing interface. Only packets which are received on the outifname and which are coming in via the ifname will be matched against this rule.

Caution None.

References

- *modify pfraw global* command
- *modify pfraw subrule entry* command

3.295 modify pfraw subrule entry

Description Use this command to modify the attributes of a sub-rule of an already existing rule.

Command Syntax ***modify pfraw subrule entry ruleid*** rule-id ***subruleid*** sub-rule-id ***[mask*** mask-value***] [start linkh|iph|tcph|tcpd|udph|udpd|icmph|icmpd] [offset*** offset***] [enable|disable] [cmpt {eq|neq|lt|lteq|gt|gteq val}|{range low-val high-val}|{any}]***

Parameters

Name	Description
ruleid rule-id	This identifies the rule index of the rule for which the sub-rule has to be modified. **Type:** Mandatory **Valid values:** *0 - 65535* Only existing rule ids accepted as input.
subruleid sub-rule-id	This specifies the sub-rule index of the sub-rule which has to be modified. **Type:** Mandatory **Valid values:** *0 - 254* Only existing sub rule ids accepted as input.
mask mask-value	This specifies the mask. The mask length cannot be modified. **Type:** Optional **Valid values:** any hexadecimal pattern starting with 0x.
start linkh|iph|tcph|tcpd|udph|udpd|icmph|icmpd	This specifies the beginning position in the packet for an offset. The start position can be the beginning of the header or data portions of various protocols as listed below. **Type:** Optional **Valid values:** *linkh|iph|tcph|tcpd|udph|udpd|icmph|icmpd*
offset offset	This specifies the offset with in the header or data part of the packet, calculated from the *start*. **Type:** Optional **Valid values:** *0—4294967295*
enable|disable	This specifies whether this subrule should be enabled or disabled. **Type:** Optional **Valid values:** *enable* or *disable*
Cmpt {eq|neq|lt|lteq|gt|gteq val}|{range low-val high-val***}|{any}***	This specifies the type of comparison that can be done on the extracted data and the comparison value(s). **Type:** Optional **Valid values:** *val*, *low-val* and *high-val* are hexadecimal patterns to be used for comparison. *low-val* and *high-val* are used when range related comparison is to be done else *val* is used. The value(s) should start with 0x. If no comparison has to be done then *any* is given on the command line

Mode Super-User.

Example ***$ modify pfraw subrule entry ruleid 2 subruleid 1 offset 10***

Output Verbose Mode On

```
Sub Rule id : 1 Rule id : 2
Sub Rule status : Enable Offset from : Linkh
Offset : 6
Comp operation : Range
Low value : 0x00000000ff000000
High value : 0x00000000ffcd0000
Mask : 0x00000000ffff0000

Set Done

Sub Rule id : 1 Rule id : 2
Sub Rule status : Disable Offset from : Linkh
Offset : 10
Comp operation : Range
Low value : 0x00000000ff000000
High value : 0x00000000ffcd0000
Mask : 0x00000000ffff0000
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
Sub Rule id	This identifies the sub-rule index of the sub-rule.
Rule id	This specifies the rule index of the rule of which this is the subrule
Sub Rule status	This specifies whether this subrule is enabled or disabled.
Offset from	This specifies the beginning position in the packet for an offset. The start position can be the beginning of the header or data portions of various protocols.
Offset	This specifies the offset with in the header or data part of the packet.
Comp Operation	This specifies the type of comparison that is done on the extracted data and the comparison value(s)
Low Value	This is hexadecimal pattern to be used for comparison when comparison type is Range.
High Value	This is hexadecimal pattern to be used for comparison when comparison type is Range.
Value	This is hexadecimal pattern to be used for comparison when comparison type is Relational.
Mask	This is hexadecimal pattern which specifies the mask

Caution None.

References

- *modify pfraw global* command
- *modify pfraw rule entry* command

3.296 modify ppe cfg

Description Use this command to modify PPPoE global configuration parameters.

Command Syntax ***modify ppe cfg [padimax*** max-padi-attempts***] [padrmax*** max-padr-attempts***] [discmax*** max-discovery-attempts***] [paditime*** initial-padi-time-difference***] [padrtime*** initial-padr-time-difference***] [first-come|serv-to-ac][padiperpadt padi-per-padt]***

Parameters

Name	Description
padimax max-padi-attempts	This specifies the maximum number of PADI attempts that shall be made by PPPoE on not receiving PADO. **Type:** Optional **Valid values:** *1-255*
padrmax max-padr-attempts	This specifies the maximum number of PADR attempts that shall be made by PPPoE on not receiving PADS. **Type:** Optional **Valid values:** *1-255*
discmax max-discovery-attempts	This specifies the maximum number of discovery attempts that shall be made by PPPoE **Type:** Optional **Valid values:** *1-255*
paditime initial-padi-time-difference	This specifies the initial PADI time difference (in seconds). **Type:** Optional **Valid values:** *1-255*
padrtime initial-padr-time-difference	This specifies the initial PADR time difference (in seconds) **Type:** Optional **Valid values:** *1-255*
first-come|serv-to-ac	This specifies the default AC selection policy used by the PPPoE. **Type:** Optional
padiperpadt padi-per-padt	This specifies the number of PADI to be sent before each PADT. **Type:** Optional **Valid Values:** 1..255

Mode Super-User.

Example ***$ modify ppe cfg serv-to-ac***

Output Verbose Mode On

```
Max PADI Attempts              : 3    Max PADR Attempts              : 3
Max Disc Attempts              : 3    Initial PADI Time Diff (sec)   : 5
Initial PADR Time Diff (sec)   : 5    AC Selection Policy            : first-come
PADI per PADT                  : 1

Set Done

Max PADI Attempts              : 3    Max PADR Attempts              : 3
Max Disc Attempts              : 3    Initial PADI Time Diff (sec)   : 5
Initial PADR Time Diff (sec)   : 5    AC Selection Policy            : serv-to-ac
PADI per PADT                  : 1
```

Verbose Mode Off

```
Set Done
```

\Output field description

Field	Description
Max PADI Attempts	This specifies the maximum number of PADI attempts that shall be made by PPPoE on not receiving PADO.
Max PADR Attempts	This specifies the maximum number of PADR attempts that shall be made by PPPoE on not receiving PADS
Max Disc Attempts	This specifies the maximum number of discovery attempts that shall be made by PPPoE
Initial PADI Time Diff (Secs)	This specifies the initial PADI time difference (in seconds).
Initial PADR Time Diff (Secs)	This specifies the initial PADR time difference (in seconds)
AC Selection Policy	This specifies the default AC selection policy used by the PPPoE. It may be: *first-come, serv-to-ac*
PADI per PADT	This specifies the number of PADI to be sent before each PADT

Caution None.

References

- *get ppe cfg* command
- *ppe pconf* related commands
- *ppe stats global* related commands
- *ppe stats session* related commands

3.297 modify ppp global

Description Use this command to modify PPP global information.

Command Syntax

```
modify ppp global [pppsesstimer ppp-sess-timer]
[ignorewantolan true|false][keepalive enable|disable|auto]
[maxlcpecho lcp-echo][maxauthtries <decvalue>|infinite]
[authretrydelay auth-retry-delay]
```

Parameters

Name	Description
Pppsesstimer ppp-sess-timer	Inactivity timeout for PPP sessions. **Type:** Optional **Valid values :** 1 - 4294967295
Ignorewantolan true|false	Flag indicating whether to ignore WAN to LAN traffic for PPP Session timeout. **Type:** Optional **Valid Values :** true or false
keepalive enable|disable|auto	“Enable” causes restarting of PPP link if the number of consecutive missing LCP echo replies exceed maxlcpecho. If set to “disable”, LCP echoes are still sent till missing replies exceed maxlcpecho. However, no further action is taken. If set to “auto”, a few LCP echo requests are initially sent to determine if the remote end supports LCP echoes. If it does, then theKkeep alive feature will be enabled, else it will stay disabled. **Type :** Optional **Valid Values:** enable, disable, auto
maxlcpecho max-lcp-echo	This specifies the number of unanswered LCP echo requests. **Type :** Optional **Valid Values:** 1..255
[maxauthtries <decvalue>|infinite] [authretrydelay auth-retry-delay]	This parameter specifies the Max Number of tries for Authentication. **Type:** Optional **Valid Values:** 1.. 4294967295, Infinite
authretrydelay auth-retry-delay	This parameter specifies the Delay in retries for authentication. For no delays between retries, 0 is accepted. **Type:** Optional **Valid Values:** 0.. 4294967295

Mode Super-User.

Example

```
$ modify ppp global pppsesstimer 10 keepalive disable
maxlcpecho 20 maxauthtries infinite authretrydelay 10
```

Output Verbose Mode On

```
PPP Inactivity Timeout    : 0         Ignore WAN to LAN traffic : False
PPP Keep Alive            : enable   Max LCP Echo Requests     : 10
Max Auth Tries            :  4       Auth Retry Delay(sec)     : 0

Set Done.

PPP Inactivity Timeout    : 10         Ignore WAN to LAN traffic : False
PPP Keep Alive            : enable    Max LCP Echo Requests     : 10
Max Auth Tries            :  4        Auth Retry Delay(sec)     : 0
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
PPP Inactivity Timeout	This specifies the Inactivity timeout for PPP sessions.
Ignore WAN to LAN traffic	Flag indicating whether to ignore WAN to LAN traffic for PPP Session timeout.
PPP Keep Alive	This specifies whether the PPP Keep alive feature is enabled, disabled or auto.
Max LCP Echo Requests	This specifies the number of unanswered echo requests.
Max Auth Tries	This field specifies Max Number of tries for Authentication.
Auth Retry Delay(sec)	This field specifies the Delay between 2 successive tries for Authentication.

Caution None.

References

- *get ppp global* command

3.298 modify ppp intf

Description Use this command to modify PPP interface parameters.

Command Syntax ***modify ppp intf ifname*** interface-name ***[start|stop|statondata] [mru<decvalue>] [magic true|false] [l2tpcalltype outlns|outlac|inlns|inlac][droute {true|false}]][mtu <decvalue>]***

Parameters

Name	Description
ifname interface-name	This specifies the PPP interface which is to be modified. **Type:** Mandatory **Valid values:** *ppp-0 - *, ...*
mru<decvalue>	Maximum Receive unit
magic true|false	Magic number negotiation
start|stop|startondata	Setting of this object results in start and stop of the PPP session on this interface. If the session is already started then only stop value can be set. startondata will cause the PPP link to start only after there is some data activity. **Type:** Optional
l2tpcalltype outlns|outlac|inlns|inlac	This object indicates the l2tp call type. **Type**: optional **Values**: outlac, outlns, inlac, inlns
droute {true|false}	If set to **true**, then the default route is chosen through this interface. **Type :** Optional **Valid Values:** true, false.
mtu <decvalue>	This specifies the MTU Size configured for PPP interface. **Type:** Optional **Valid values:** 120 ..65535

Mode Super-User.

Example ***$ modify ppp intf ifname ppp-0 usedhcp true l2tpcalltype outlns mtu 500***

Output Verbose Mode On

```
If-Name               : ppp-0          L2TP Call type        : inlac
Interface Sec Type    : Public         Phy Interface         : aal5-0
Configured IP Address : 0.0.0.0        NAT Direction         : OUT
Init MRU              : 1500           Magic                 : False
Encapsulation         : PPPOA          Service Name          : -
UseDhcp               : False          UseDns                : False
DRoute                : False          Status                : Start
Gateway IP Address    : 202.1.1.2    Associated Num If-Name : eth-0
Use Gateway           : remote
```

```
Configured MTU        : 300          Actual MTU            : 200

Set Done

If-Name               : ppp-0         L2TP Call type        : inlac
Interface Sec Type    : Public        Phy Interface         : aal5-0
Configured IP Address : 0.0.0.0       NAT Direction         : OUT
Init MRU              : 1500          Magic                 : False
Encapsulation         : PPPOA         Service Name          : -
UseDhcp               : False         UseDns                : False
DRoute                : False         Status                : Start
Gateway IP Address    : 202.1.1.2     Associated Num If-Name : eth-0
Use Gateway           : remote
Configured MTU        : 300          Actual MTU            : 200
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
If-Name	This specifies the PPP interface for the PPP Links: It may be: *ppp-0, ppp-1…*
L2TP Call Type	This field specifies the l2tp call type.
Interface Sec Type	Interface security type.
Phy Interface	This specifies Name of the lower interface on which PPP is running. It may be: *aal5-0, aal5-1…*
Configured IP Address	This specifies the IP Address for the PPP Link.
NAT Direction	This variable specifies whether this interface's address is inside or outside. It may be: *inside, outside, none*
Init MRU	The initial Maximum Receive Unit (MRU) that the local PPP entity will advertise to the remote entity
Magic	This specifies whether the local node will attempt to perform Magic Number negotiation with the remote node. It may be: *True, False*
Encapsulation	This specifies the lower layer protocol used below this PPP Link. It may be: *PPPOA, PPPOE*
Service Name	This specifies the service name used for PPPoE. It is generally the name of the ISP.
UseDhcp	This specifies whether DHCP is to be used for address negotiation. It may be either True or False
UseDns	This specifies whether DNS server addresses are to be obtained using IPCP or not.
Droute	Default Route
Status	This shows whether PPP session on this interface is active. It may be: *Start, Stop, StartOnData.*
Gateway IP Address	This specifies the IP Address of the Gateway.

Field	Description
Associated Num If-Name	This specifies the interface name of the associated numbered interface. A "-" indicates that this ppp interface is not associated with any numbered interface.
Use Gateway	This specifies whether local or remote gateway is to be used.
Configured MTU	This specifies the MTU value configured by the user for PPP interface.
Actual MTU	This specifies the MTU value actually operational for PPP interface.

Caution None.

References

- *delete ppp intf* command
- *create ppp intf* command
- *get ppp intf* command
- *ppp lstatus* related commands
- *ppp security* related commands.

3.299 modify ppp security

Description Use this command to change the login or password setting for the PPP Interface.

Command Syntax ***modify ppp security ifname*** interface-name ***[pap|chap] [login*** login-name***] [passwd*** password***]***

Parameters

Name	Description
ifname interface-name	This specifies the PPP interface for which the security entry is to be modified. **Type:** Mandatory **Valid values:** *ppp-0 - *, ..., default.* The *default* entry gets used in case there is no specific entry for that interface.
pap|chap	This is the protocol used for authentication **Type:** Optional **Default value:** pap
login login-name	This is the login name **Type:** Optional **Valid values:** String of up to 128 Characters('A'- 'Z', 'a'-'z', '0'-'9','-','_') and any combination of printable characters excluding ';'
passwd password	This is the password used to authenticate the user **Type:** Optional **Valid values:** String of Upto 128 Characters('A'- 'Z', 'a'-'z', '0'-'9','-','_') and any combination of printable characters excluding ';'

Mode Super-User.

Example ***$ modify ppp security ifname ppp-0 login xyz passwd wer***

Output Verbose Mode On

```
IfName   : ppp-0     Protocol : PAP
Login    : abc

Set Done

IfName   : ppp-0     Protocol : PAP
Login    : xyz
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
IfName	This specifies the PPP interface for which the security entry has been modified It may be: *ppp-0 - *, ..., default*. The *default* entry gets used in case there is no specific entry for that interface.
Protocol	This is the protocol used for authentication It may be: *PAP, CHAP*
Login	This is the login name.

Caution None.

References

- *delete ppp security* command
- *get ppp security* command
- *create ppp security* command
- *ppp lstatus* related commands
- *ppp intf* related commands

3.300 modify rip global

Description This command is used for modifying global parameters of RIP.

Command Syntax ***modify rip global*** ***[*****enable**|**disable****]*** ***[updatetime*** update-time**]** ***[agetime*** age-time***]***

Parameters

Name	Description
enable**|**disable	Dynamically Enable/Disable RIP on IAD. **Type:** Optional **Valid values:** *enable* or *disable*
Updatetime update-time	This is the timer frequency at which the RIP would broadcast its routes to all its neighbors **Type:** Optional **Valid values:** *1-4294967295*
agetime age-time	This is the timer frequency at which RIP would age a route, if an update is not received for this duration. This value should be larger than the ripUpdateTime. It is recommended for ripAgeTime = 6*ripUpdateTime. **Type:** Optional **Valid values:** *1-4294967295*

Mode Super-User

Example ***$ modify rip global enable updatetime 10***

Output Verbose Mode On

```
RIP status                : enable
RIP route update time(sec): 20
RIP route age time(sec)   : 20

Set Done

RIP status           : enable
RIP route update time(sec): 10
RIP route age time(sec)   : 20
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
RIP status	This tells whether RIP is enabled or disabled
RIP route update time	This tells the timer frequency at which the RIP would broadcast its routes to all its neighbors
RIP route age time	This tells the timer frequency at which RIP would age a route, if an update is not received for this duration.

Caution None.

References

- *get rip global* command.

3.301 modify radius acctserv config

Description Use this command to modify Radius Accounting Server Configuration.

Command Syntax ***modify radius acctserv config index*** index ***[retries*** retries ***]*** ***[starttimeout*** starttimeout ***] [ontimeout*** ontimeout ***] [secret*** secret ***]***

Parameter

Name	Description
index index	A number uniquely identifying each RADIUS Accounting server with which this client communicates **Type:** Mandatory **Valid values:** 1 - 2147483647
retries retries	The number of times the request packet shall be retransmitted to the server on getting timed out. **Type:** Optional **Valid values:** 10 **Default value:** 5
starttimeout starttimeout	The time in seconds for which the client needs to wait before retransmitting the Accounting START request packet to the server. **Type:** Optional **Valid values:** 30 **Default value:** 5
ontimeout ontimeout	The time in seconds for which the client needs to wait before retransmitting the Accounting ON request packet to the server. **Type:** Optional **Valid values:** 30 **Default value:** 5
secret secret	The secret shared between this server and the client. String of up to 64 characters (All printable characters excluding ";") **Type:** Optional

Mode Super-User

Example ***$ modify radius acctserv config index*** 1 ***retries*** 5 ***starttimeout*** 60 ***ontimeout*** 60 ***secret*** 0x1090

Output Verbose Mode On:

```
Server Index       : 1          IP address      : 192.166.56.67
Port               : 1700       Retries         : 5
Start timeout(sec) : 60         On timeout(sec) : 60
Current State      : Start

Set Done
```

Verbose Mode Off:

```
Set Done
```

Output field description

Field	Description
Server Index	A number uniquely identifying each RADIUS Accounting server with which this client communicates.
IP address	The IP address of the RADIUS server referred to in this table entry.
Port	The server port to which the client sends accounting requests.
Retries	The number of times the request packet shall be retransmitted to the server on getting timed out.
Start timeout(sec)	The time in seconds for which the client needs to wait before retransmitting the Accounting START request packet to the server.
On timeout(sec)	The time in seconds for which the client needs to wait before retransmitting the Accounting ON request packet to the server.
Current State	The current state of the accounting server.

Caution None

References

- *get radius acctserv config* command
- *create radius acctserv config* command
- *delete radius acctserv config* command

3.302 modify radius authserv config

Description Use this command to modify Radius Authentication Server Configuration

Command Syntax ***modify radius authserv config index*** index ***[retries*** retries ***]*** ***[retxtimeout*** retxtimeout ***] [secret*** secret ***]***

Parameter

Name	Description
index index	A number uniquely identifying each RADIUS Authentication server with which this client communicates **Type:** Mandatory **Valid values:** 1 - 2147483647
retries retries	The number of times the request packet shall be transmitted to the server on getting timed out. **Type:** Optional **Valid values:** 0 - GS_CFG_RADC_MAX_SRV_RETRIES **Default value:** GS_CFG_RADC_DEF_SRV_RETRIES
retxtimeout retxtimeout	The time, in seconds, for which the client needs to wait before retransmitting the request packet to the server. **Type:** Optional **Valid values:** 0 - GS_CFG_RADC_MAX_SRV_RETRNS_TOUT **Default value:** GS_CFG_RADC_DEF_SRV_RETRNS_TOUT
secret secret	The secret shared between this server and the client. String of up to GS_CFG_RADC_MAX_SRV_SHRDSCRT_LEN characters (All printable characters excluding ";") **Type:** Optional

Mode Super-User

Example ***$ modify radius authserv config index*** 1 ***retries*** 5 ***retxtimeout*** 60 ***secret*** 0x1090

Output Verbose Mode On:

```
Server Index : 1
IP address   : 192.166.56.67    Port                          : 1800
Retries      : 5                Retransmission timeout(sec) : 60

Set Done
```

Verbose Mode Off:

```
Set Done
```

Output field description

Field	Description
Server Index	A number uniquely identifying each RADIUS Authentication server with which this client communicates.
IP address	The IP address of the RADIUS server referred to in this table entry.
Port	The server port to which the client sends authentication requests.
Retries	The number of times the request packet shall be transmitted to the server on getting timed out.
Retransmission timeout(sec)	The time, in seconds, for which the client needs to wait before retransmitting the request packet to the server.

Caution

References

- *get radius authserv config* command
- *create radius authserv config* command
- *delete radius authserv config* command

3.303 modify radius global config

Description Use this command to modify Radius Global Configuration

Command Syntax ***modify radius global config [enable | disable] [authid*** authid ***] [acctid*** acctid ***] [acctintrvl*** acctintrvl ***]***

Parameter

Name	Description
enable | ***disable***	This field specifies the global status of radius client.This field being enable implies this radius client is enabled, and disable implies disabled. **Type:** Optional **Default value:** enable
authid authid	The name of the NAS identifier of the RADIUS authentication client. String of up to 128 characters. (A-Z, a-z, 0-9,-,_) **Type:** Optional
acctid acctid	The name of the NAS identifier of the RADIUS accounting client. String of up to 128 characters (A-Z, a-z, 0-9,-,_) **Type:** Optional
acctintrvl acctintrvl	This field specifies the interval in seconds after which the interim accounting update will be sent to the server. If interim update attribute is received in access-accept response pkt from RADIUS server, it indicates that interim update is to be sent. Valid Values : 0 and between 60 and 4294967295, both inclusive. If configured interim update interval is not 0, then it is used otherwise the time interval sent by RADIUS server is used. **Type:** Optional **Default value:** 0

Mode Super-User

Example

```
$ modify radius global config  enable authid
AuthClientIdentifier1 acctid AcctClientIdentifier1
acctintrvl 100
```

Output Verbose Mode On:

```
Status                          : enable
Authentication Client Identifier : AuthClientIdentifier1
Accounting Client Identifier     : AcctClientIdentifier1
Interim Accounting Interval(sec) : 100

Set Done
```

Verbose Mode Off:

```
Set Done
```

Output field description

Field	Description
Status	This field specifies the global status of radius client.This field being enable implies this radius client is enabled, and disable implies disabled.
Authentication Client Identifier	The name of the NAS identifier of the RADIUS authentication client. String of up to IAD_RADIUS_MAX_NAS_NAME_LEN characters (A-Z, a-z, 0-9,-,_)
Accounting Client Identifier	The name of the NAS identifier of the RADIUS accounting client. String of up to IAD_RADIUS_MAX_NAS_NAME_LEN characters (A-Z, a-z, 0-9,-,_)
Interim Accounting Interval(sec)	This field specifies the interval in seconds after which the interim accounting update will be sent to the server. If interim update attribute is received in access-accept response pkt from RADIUS server, it indicates that interim update is to be sent. Valid Values : 0 and between 60 and 4294967295, both inclusive. If configured interim update interval is not 0, then it is used otherwise the time interval sent by RADIUS server is used.

Caution None

References

- *get radius global config* command

3.304 modify rip intf

Description Use this command to modify RIP protocol parameters on the specified IP Interface.

Command Syntax

```
modify rip intf ifname interface-name [send
{rip1|rip2|rip1compat|none}] [senddefroute {enable|disable}]
[receive {rip1|rip2|both|none}] [recvdefroute
{enable|disable}] [auth {none|text password}]
```

Parameters

Name	Description
ifname interface-name	Specifies the IP Interface name on which RIP is to be started. **Type:** Mandatory **Valid values:** *eth-0, veth-0 - *, ppp-0, ppp-0-* eoa-0 - *,ipoa-0-*, usb-0*
send {rip1|rip2|rip1compat|none}	This specifies the packet format to be used for sending RIP updates and requests **Type:** Optional **Valid values:** *rip1, rip2, rip1compat, none*
senddefroute {enable|disable}	If Default route is to be included in the updates sent on the interface, or not. **Type:** Optional **Valid values:** *enable* or *disable*
receive {rip1|rip2|both|none}	This specifies the packet format to be accepted while receiving RIP updates and requests and responses **Type:** Optional **Valid values:** *rip1, rip2, both, none*
Recvdefroute {enable|disable}	If Default route is to be processed in the updates received on the interface or not. **Type:** Optional **Valid values:** *enable* or *disable*
auth none|*auth text* password	If ripAuthentication has been enabled, what should be the password. If ripAuthentication is **Text** then ripAuthPasswd cannot be left blank **Type:** Optional **Valid values:** *none* or if text then *password* of length 16

Mode Super-User

Example ***modify rip intf ifname ppp-0 metric 2 senddefroute disable***

Output Verbose Mode On:

```
IP Interface Name    : ppp-0      RIP Interface Metric : 1
RIP Send Mode        : rip1RIP Receive Mode     : rip1
RIP Send Def Route   : EnableRIP Recv Def Route   : Disable
RIP packet auth      : None

Set Done

IP Interface Name    : ppp-0RIP Interface Metric : 2
RIP Send Mode        : rip1RIP Receive Mode     : rip1
RIP Send Def Route   : EnableRIP Recv Def Route   : Disable
RIP packet auth      : None
```

Verbose Mode Off:

```
Set Done
```

Output field description

Field	Description
IP Interface Name	This tells the IP Interface name on which RIP is to be stopped.
RIP Interface Metric	This tells the metric value attached to the interface. The metric is used by RIP in deciding which among alternate routes is the most optimal.
RIP Send Mode	This tells the packet format used for sending RIP updates and requests
RIP Receive Mode	This tells the packet format accepted while receiving RIP updates and requests and responses
RIP Send Def Route	This tells whether default route is to be included in the updates sent on the interface, or not.
RIP Recv Def Route	This tells whether default route is to be processed in the updates received on the interface or not.
RIP packet auth	This tells whether RIP authentication is enabled or not.

Caution None.

References None.

3.305 modify smtp servaddr

Description Use this command to modify SMTP server address.

Command Syntax ***modify smtp servaddr*** *[ip-address|**dname** domain-name]*

Parameters

Name	Description
ip-address|dname domain-name	This parameter specifies the IP address or fully qualified domain name used for configuring the SMTP server address. 0.0.0.0 IP address will remove the existing server address. **Type:** Mandatory **Valid values:** Valid IP address or fully qualified domain name.

Mode Super-User

Example ***$ modify smtp servaddr*** *192.168.1.1*

Output Verbose Mode On:

```
Server Address      Server Domain Name
-------------------------------------------------
192.168.10.20       abc.xyz.com

Set Done


Server Address       Server Domain Name
-------------------------------------------------
192.168.1.1          def.wxy.com
```

Verbose Mode Off:

```
Set Done
```

Output field description

Field	Description
Server Address	IP address of the SMTP server.
Server Domain Name	The fully qualified domain name of the SMTP server.

Caution None.

References

- *get smtp servaddr* command

3.306 modify snmp trap

Description Use this command to enable or disable SNMP traps.

Command Syntax ***modify snmp trap {enable|disable}***

Parameters

Name	Description
enable|disable	This specifies whether SNMP Traps are to be enabled or disabled. **Type:** Mandatory

Mode Super-User.

Example ***$ modify snmp trap disable***

Output Verbose Mode On

```
Snmp Trap Enabled

Set Done

Snmp Trap Disabled
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
Snmp Trap	This is the SNMP Trap Status. It may be: *Enabled, Disabled*

Caution None.

References

- *get snmp trap* command
- *snmp host* related commands
- *snmp comm* related commands
- *snmp stats* related commands.

3.307 modify sntp cfg

Description Use this command to modify the SNTP configuration.

Command Syntax ***modify sntp cfg [enable|disable]***

Parameters

Name	Description
enable|disable	SNTP service is enabled or disabled. **Type**: Optional **Valid values**: enable or disable

Mode Super-User.

Example ***$ modify sntp cfg enable***

Output Verbose Mode On

```
Status : Disable

Set Done

Status : Enable
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
Status	SNTP service is disabled or enabled.

Caution None.

References

- *create sntp servaddr* command
- *get sntp servaddr* command
- *delete sntp servaddr* command
- *get sntp cfg* command
- *get sntp stats* command
- *reset sntp stats* command

3.308 modify stp info

Description Use this command to alter the configuration for the spanning tree protocol group.

Command Syntax ***modify stp info [priority priority-value] [maxage maximum-age] [htime hello-time] [fdelay forward-delay] [enable|disable]***

Parameters

Name	Description
priority priority-value	The priority value accorded to the bridge. This should be input in Hexadecimal Format. It forms the 1st two octets of the Designated Bridge Id. **Type:** Optional **Valid values:** *0-65535*
maxage maximum-age	The value (in seconds) that all bridges use for Max-Age when this bridge is acting as the root. **Type:** Optional **Valid values:** *6-40*
htime hello-time	The value (in seconds) that all bridges use for Hello-Time when this bridge is acting as the root **Type:** Optional **Valid values:** *1-10*
fdelay forward-delay	The value (in seconds) that all bridges use for Forward Delay when this bridge is acting as the root. **Type:** Optional **Valid values:** *4-30*
Enable|disable	Global status of STP

Mode Super-User.

Example ***$ modify stp info priority 0x20 maxage 25 htime 5 fdelay 20 enable***

Output Verbose Mode On

```
Protocol Spec.     : IEEE 8021D               Priority : 0x8000
Top. Changes       : 1                        Curr Top. Age(sec): 35.0
Desig Root         : 80:00:00:10:5A:6C:DB:20  Root Cost : 0
Root If-name       : None                     Hold Time (sec) : 1.0
Br Max Age(sec)    : 20                       Curr Max Age (sec): 20.0
Br Hello Time(sec) : 2                        Curr Hello Time(sec) : 2.0
Br Fwd Delay(sec)  : 15                       Curr Fwd Delay (sec) : 15.0
Status             : Disable

Set Done

Protocol Spec.     : IEEE 8021D               Priority : 0x8000
Top. Changes       : 1                        Curr Top. Age(sec): 35.0
Desig Root         : 80:00:00:10:5A:6C:DB:20  Root Cost : 0
Root If-name       : None                     Hold Time (sec) : 1.0
Br Max Age(sec)    : 20                       Curr Max Age (sec): 20.0
Br Hello Time(sec) : 2                        Curr Hello Time(sec) : 2.0
```

```
Br Fwd Delay(sec)  : 15                    Curr Fwd Delay (sec) : 15.0
Status             : Enable
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
Protocol Spec	This indicates the Spanning Tree Protocol running. It may be: DECLB100, IEEE 8021D, Unknown
Priority	Bridge Priority. It is equal to the value of the 1st 2 octets of the designated Bridge Id. The value as given in '`bridge static`' commands represents the last 6 octets of the Id.
Top. Changes	This specifies the number of times the topology was changed since reset
Curr Top. Age(Sec)	This specifies the time elapsed (in seconds) since the last topology change
Desig Root	This specifies The Bridge Id of the root of the spanning tree as determined by the STP running on this node. This value is used as the Root Identifier parameter in all Configuration Bridge PDUs originated by this node.
Root Cost	The cost of the path to the root as seen from this bridge
Root If-name	The interface which offers the lowest cost path from this bridge to the root bridge
Hold Time (Sec)	This minimum time interval in seconds, between two Configuration bridge PDUs transmitted by this node.
Br Max Age(Sec)	The maximum age (in seconds) of Spanning Tree Protocol information learned from the network on any port before it is discarded when this Bridge is the root of the Spanning Tree. It may range between *6* and *40*.
Curr Max Age (Sec)	The actual maximum age (in seconds) of Spanning Tree Protocol information learned from the network on any port before it is discarded.It is derived from the Br Max Age of the Root Node. 802.1D-1990 specifies that the range for this parameter is related to the value of "Br Hello Time"
Br Hello Time(Sec)	The value (in seconds) that all bridges use for Hello-Time when this bridge is acting as the root. It may range between: *1* and *10*
Curr Hello Time(Sec)	The actual amount of time between the transmission of Configuration bridge PDUs by this node on any port

Field	Description
Br Fwd Delay(Sec)	The value (in seconds) that all bridges use for Forward Delay when this bridge is acting as the root. 802.1D-1990 specifies that the range for this parameter is related to the value of “Br Max Age”. It may range between: *4* and *30*
Curr Fwd Delay (Sec)	This actual time value (in seconds) which determines how fast a port changes its spanning state when moving towards the Forwarding state. It is used to determine how long the port stays in each of the Listening and Learning states, which precede the Forwarding state; and also when a topology change has been detected and is underway, to age all dynamic entries in the Forwarding Database.
Status	Gloabal status of STP

Caution None.

References

- *get stp global* command
- *STP port* related commands.

3.309 modify stp port

Description Use this command to alter the configuration for the spanning tree protocol.

Command Syntax ***modify stp port info ifname interface-name [enable|disable] [pcost path-cost] [priority priority-value]***

Parameters

Name	Description
ifname interface-name	The port number of the port for which modifications are to be done. **Type:** Mandatory **Valid values:** *eth-0, eoa-0*, usb-0**
enable*|*disable	Admin status of Port. **Type:** Optional **Valid values:** *enable, disable*
pcost path-cost	The contribution of this port to the path cost of paths towards the spanning tree root which included this port. **Type:** Optional **Valid values:** *1-65535*
priority priority-value	The value of the priority field. It should be input in Hexadecimal Format. **Type:** Optional **Valid values:** *0x0 to 0xFF*

Mode Super-User.

Example ***$ modify stp port ifname*** **eth-0 disable** ***pcost*** **1000** ***priority*** **0x10**

Output Verbose Mode On

```
Port Name  : eth-0                    Priority    : 0x0
State      : Forwarding               Status      : Enable
Path Cost  : 100                      Desig Cost  : 0
Desig Root : 80:00:00:10:5A:6C:DB:20  Desig Bridge: 80:00:00:10:5A:6C:DB:20
Desig Port  : 0x8000                  Fwd Transitions  : 1

Set Done

Port Name   : eth-0                    Priority         : 0x10
State       : Disabled                 Status           : Disable
Path Cost   : 1000                     Desig Cost       : 0
Desig Root  : 80:00:00:10:5A:6C:DB:20  Desig Bridge     : 80:00:00:10:5A:6C:DB:20
Desig Port  : 0x8000                   Fwd Transitions  : 1
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
Port Name	The port for which this entry contains Spanning Tree Protocol management information
Priority	Port Priority. It is contained in the first octet of the 2 octet Port Id. The other octet is used to derive the port name above.
State	The port's current state for STP. This state controls what action a port takes on reception of a frame. For example, a malfunctioning port will be placed in the broken state. The valid values are: Disabled, Blocking, Listening, Learning, Forwarding, Broken
Status	The Admin Status of the port. The possible values are: *Enable, Disable*
Path Cost	The contribution of this port to the path cost of paths towards the spanning tree root which included this port. 802.1D-1990 recommends that the default value of this parameter be in inverse proportion to the speed of the attached LAN.
Desig Cost	The path cost of the Designated Port of the segment connected to this port. This value is compared to the Root Path Cost field in received
Desig Root	The unique Bridge Identifier of the Bridge recorded as the Root in the Configuration BPDUs transmitted by the Designated Bridge for the segment to which the port is attached
Desig Bridge	The Bridge Identifier of the bridge which this port considers to be the Designated Bridge for this port's segment
Desig Port	The Port Identifier of the port on the Designated Bridge for this port's segment
Fwd Transitions	The number of times this port has transitioned from the Learning state to the Forwarding state

Caution The specified interface should be an existing bridge interface. Please refer to the *create bridge port intf* command.

References

- *get stp port* command
- *create bridge port* command
- *stp global* related commands
- *bridge ports* related commands

3.310 modify system

Description Use this command to modify the system parameters.

Command Syntax ***modify system [contact sys-contact] [model model-name] [location sys-location] [vendor sys-vendor-info] [logthresh sys-log-threshold] [systime systime] [dst <on|off>] [timezone <timezone>] [name <name>] [dname <domain>][bkpinterval disable|immediate|<decvalue>]***

Parameters

Name	Description
contact sys-contact	This contains the textual identification of the contact person for this modem, together with information on how to contact this person **Type:** Optional **Valid values:** String of upto 64 ASCII Characters
model model-name	This specifies the name of the modem **Type:** Optional **Valid values:** String of upto 64 ASCII Characters
location sys-location	This specifies the physical location of this modem **Type:** Optional **Valid values:** String of upto 64 ASCII Characters
vendor sys-vendor-info	This contains the vendor-specific information **Type:** Optional **Valid values:** String of upto 64 ASCII Characters
logthresh sys-log-threshold	This specifies the severity level of trap equal to or lower than that shall be logged. 1 is the lowest and represents critical traps. **Type:** Optional **Valid values:** *0-4*
systime systime	This specifies the current system time **Type:** Optional **Valid values:** System Time String in format. The total string length must be 20 characters. Single digits should be prepended with a '0', e.g. '1' should be given as '01' mon dd hh:mm:ss year e.g. *"Feb 01 21:20:10 2001"*
name <name>	This contains the host name for this modem **Type**: Optional **Valid values:** String of upto 64 ASCII Characters

Name	Description
dst <on|off>	This specifies if the Daylight Savings Time has been enabled or not. **Type:** Optional **Valid values:** on|off
timezone <timezone>	This specifies the timezone that has been set on the modem **Type:** Optional **Valid values:** +hhmm
dname <domain>	This contains the domain name for this modem. **Type:** Optional **Valid values:** String of upto 63 ASCII Characters
bkpinterval disable|immediate|<decvalue>	This specifies the backup interval (mins) of the dhcp server. A value of "immediate" will indicate that flash backups are to be done whenever the configuration gets updated. A value of "disable" will indicate that backups are never done by DHCP. **Type:** Optional **Valid Values:** disable, immediate, 0.. 4294967295

Mode Super-User.

Example

```
$ modify system systime "Feb 01 21:20:10 2001" model
"titanium" dname "conexant"  bkpinterval disable
```

Output Verbose Mode On

```
Model       : Titanium
Name        : Name of the unit
Domain Name : Conexant
Description : DSL Modem
Location    : Conexant Systems, Inc.,100 Schulz Drive, Red Bank,NJ 07701,U.S.A
Contact     : Conexant Systems, Inc.,100 Schulz Drive, Red Bank,NJ 07701,U.S.A
Vendor      : Conexant Systems,,100 Schulz Drive, Red Bank,NJ 07701,U.S.A
LogThreshold: 0
Object-id   : 1.3.6.1.4.1.200
HwVersion   : 71fb0922
SwVersion   : VIK-1.37.020524a/T93.3.8
DSL Version : T93.3.8
System Time : Feb 01 21:20:10 2001
Time Zone   : GMT
DST         : Off
Services    : physical datalink internet end-to-end applications
UpTime(HH:MM:SS): 0:0:9
Backup Interval(mins): 10

Set Done
Model           : Titanium
Name            : Name of the unit
Domain Name     : Conexant
Description     : DSL Modem
Location        : Conexant Systems, Inc.,100 Schulz Drive, Red Bank,NJ 07701,U.S.A
Contact         : Conexant Systems, Inc.,100 Schulz Drive, Red Bank,NJ 07701,U.S.A
Vendor          : Conexant Systems, Inc.,100 Schulz Drive, Red Bank,NJ 07701,U.S.A
LogThreshold    : 0
Object-id       : 1.3.6.1.4.1.200
HwVersion       : 71fb0922
SwVersion       : VIK-1.37.020524a/T93.3.8
DSL Version     : T93.3.8
System Time     : Feb 01 21:20:10 2001
Time Zone       : GMT
DST             : Off
Services        : physical datalink internet end-to-end applications
UpTime(HH:MM:SS) : 0:0:9
Backup Interval(mins): 10
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
Model	This specifies the name of the system
Name	This specifies the host name of the modem
Domain name	This specifies the domain name of the modem.
Description	This is textual description of the entity
Location	This specifies the physical location of this node
Contact	This shows the textual identification of the contact person for this managed node, together with information on how to contact this person.
Vendor	This shows the vendor-specific information

Field	Description
LogThreshold	This specifies the severity level of trap equal to or lower than that shall be logged. 1 is the lowest and represents critical traps.
Object-id	This shows the vendor's authoritative identification of the network management subsystem contained in the entity.
HwVersion	This specifies the hardware and firmware version of the system.
SwVersion	This specifies the software version of the system
DSL Version	This specifies the DSL-version of the system
System Time	This shows the current system time.
Time Zone	This specifies the time zone that has been set on the modem.
DST	This specifies whether Daylight Saving Time has been enabled or not.
Services	This specifies the functionality provided by this node. These may be: *physical, datalink, internet, end-to-end, applications*
Up Time	This specifies the time in seconds since the system is up
Backup Interval(mins)	This specifies the backup interval(mins) of the dhcp server. A value of "immediate" will indicate that flash backups are to be done whenever the configuration gets updated. A value of "disable" will indicate that backups are never done by DHCP.

Caution None.

References

- `get system` command
- `commit` command.

3.311 modify trace cfg

Description Use this command to modify the trace and log configuration for a specific module.

Command Syntax

```
modify trace cfg  module module-name|all [flow trace-flow]
[level trace-level] [syslog|net|stdout] [dest ip-address]
[port port-number]
```

Parameters

Name	Description
module module-name|**all**	This specifies the module whose trace/log configuration is to be modified. **Type:** Mandatory **Valid values:** *GCOS, ALPS, MEA5, OAM, CIN, GAG, CDB, LED, CLI, SAG, HAG, PPE, ATM, DCL, EOA, TBG, PPP, EMAC, DSL, USB, SPI, NVM, SPAN, SSI*
flow trace-flow	This indicates a Hexadecimal bitmask which sets the filter for trace flow **Type:** Optional **Valid values:** *0x0 to 0xffffffff*
level trace-level	This indicates a Hexadecimal bitmask which sets the filter for trace level **Type:** Optional **Valid values:** *0x0 to 0xffffffff*
syslog|**net**|**stdout**	This specifies the type of logging to be done. Incase *net* or *syslog* is specified then `dest` and `port` must be specified. **Type:** Optional
dest ip-address	This specifies the IP address for host for logging for trace type *syslog* and *net.* It is invalid incase of trace type *stdout* **Type:** Mandatory when type is modified to *net* or *syslog; e*lse it is invalid **Valid values:** Any valid class A/B/C IP address
port port-number	Port number on which host is listening for trace info to be logged incase of trace type *syslog* and *net*. It is invalid incase of trace type *stdout* **Type:** Mandatory when type is modified to *net* or *syslog; e*lse it is invalid **Valid values:** *0-4294967295*

Mode Super-User.

Example

```
$ modify trace cfg module GAG flow 0x1 level 0x1
```

Output Verbose Mode On

```
Module    Flow          Level         Type       Destn              Port
-------------------------------------------------------------------------
GAG       0x0           0x0           Stdout     0.0.0.0            0

Set Done

Module    Flow          Level         Type       Destn              Port
-------------------------------------------------------------------------
GAG       0x1           0x1           Stdout     0.0.0.0            0
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
Module	This specifies the module for trace/log config whose information is being displayed: It can be: GCOS, ALPS, MEA5, OAM, CIN, GAG, CDB, LED, CLI, SAG, HAG, PPE, ATM, DCL, EOA, TBG, PPP, EMAC, DSL, USB, SPI, NVM, SPAN, SSI
Flow	This indicates a Hexadecimal bitmask which sets the filter for trace flow.
Level	This indicates a Hexadecimal bitmask which sets the filter for trace level.
Type	This specifies the type of logging to be done. It may be: Syslog, Net, Stdout
Destn	This specifies the IP address for host for logging for trace type syslog and net. It is invalid incase of trace type stdout
Port	Port number on which host is listening for trace info to be logged incase of trace type syslog and net. It is invalid incase of trace type stdout

Caution None.

References

- *get trace cfg* command
- *get trace stats* command

3.312 modify trapprints

Description Use this command to enable or disable trap prints on CLI.

Command Syntax ***modify trapprints enable|disable***

Parameters

Name	Description
enable|disable	Desired state of Trap prints. **Type :** Mandatory **Valid values:** *enable, disable*

Mode Super-User.

Example ***$ modify trapprints enable***

Output

```
Trap Prints Enabled
```

Output field description None

Caution None.

References

- *get trapprints* command

3.313 modify upnp cfg

Description Use this command to modify UPNP global configuration.

Command Syntax ***modify upnp cfg [nbstatus enable | disable] [advcacheage advcacheage]***

Parameters

Name	Description
nbstatus enable | disable	This field specifies the next boot status of UPNP module. **Type:** Optional **Default value:** disable
advcacheage advcacheage	This field specifies the advertisement cache age in seconds of Internet Gateway Device **Type:** Optional **Valid values:** 40 - 4294967295 **Default value:** GS_CFG_EWU_CACHE_AGE
Current Status	This field specifies the current status of UPNP module.

Mode Super-User.

Example ***$ modify upnp cfg nbstatus enable advcacheage 40***

Output Verbose Mode On

```
Next Boot Status            : enable
Advertisement Cache Age(sec) : 40
Current Status              : enable

Set Done
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
Next Boot Status	This field specifies the next boot status of UPNP module.
Advertisement Cache Age(sec)	This field specifies the advertisement cache age in seconds of Internet Gateway Device
Current Status	This field specifies the current status of UPNP module.

Caution None.

References

- *get upnp cfg* command

3.314 modify usagectrl

Description Use this command to modify Usage Control Configuration.

Command Syntax

```
$modify usagectrl [ enable|disable ]
[ maxusers <decvalue>|nolimit ] [ login enable|disable ]
[ arpcheck <decvalue> ]
```

Parameters

Name	Description
maxusers <decvalue>	This field specifies the maximum number of data users, who can have simultaneous access to the WAN side. A value of 'nolimit specifies that all users are allowed to access the WAN side. **Type:** Optional **Valid values:** *1 - 8, nolimit*
enable|disable	This specifies the usage control status. **Type:** Optional **Valid Value:** *enable, disable*
login enable|disable	This field specifies whether data user login is required for authentication. **Type :** Optional **Valid Values:** enable, disable
Arpcheck <decvalue>	This field specifies the interval (in minutes). after which, an ARP check is to be done. **Type :** Optional **Valid Values:** 0.. 4294967295

Mode Super-User

Example

```
$ modify usagectrl enable login enable arpcheck 10
```

Output Verbose Mode On

```
Max Data Users     Status           Login         Arp Check Interval(mins)
-------------------------------------------------------------------------------
5                 disable          disable        21


Set Done

Max Data Users     Status           Login         Arp Check Interval(mins)
-------------------------------------------------------------------------------
5                 enable            enable         10
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
Max Data Users	This field specifies the maximum number of data users, who can have simultaneous access to the WAN side. It can also have the value 'nolimit' which specifies that all users are allowed to access the WAN side.
Status	This field specifies the status of usage control.
Login	This field specifies whether data user login is required for authentication. If disabled, the user is allowed access whenever he does a WAN access, provided the maxusers limit is not reached.
Arp Check Interval(mins)	This field specifies the interval (in minutes) after which an ARP check is to be done to ascertain whether the authenticated user is still online.

Caution None.

References

- *get usagectrl* command
- *get datauserslist* command
- *reset datauserslist* command.

3.315 modify usb intf

Description Use this command to modify the properties of an USB interface.

Command Syntax ***modify usb intf ifname*** interface-name ***[ip*** ip-address***]*** ***[mask*** *net-mask***][mtu <decvalue>]***

Parameters

Name	Description
ifname interface-name	This parameter specifies the name assigned to this interface. **Type:** Mandatory **Valid values:** *usb-0*
ip ip-address	The IP address to be assigned to interface. **Type:** Optional **Valid values:** Any valid class A/B/C IP address **Default value:** *0.0.0.0*
mask net-mask	This parameter specifies the subnet mask to be applied to the IP address. **Type:** Optional **Valid values:** *128.0.0.0 – 255.255.255.254* **Default value:** *0.0.0.0*
mtu <decvalue>	This specifies the MTU Size configured for Ethernet over USB interface **Type:** Optional **Valid values :** 120 ..1500

Mode Super-User

Example ***$ modify usb intf ifname usb-0 ip 172.25.8.100***

Output Verbose Mode On

```
IfName   If SecType  Ip Address     Mask           Nat Dir      Oper    MTU
-------------------------------------------------------------------------------
usb-0     Public    192.168.1.1    255.255.255.0    Inside      Down    300

Set Done

IfName   If SecType  Ip Address     Mask           Nat Dir      Oper    MTU
-------------------------------------------------------------------------------
usb-0     Public     172.25.8.100   255.255.255.0  Inside       Down    300
```

Verbose Mode Off

```
Set Done
```

Output field description

Field	Description
IfName	The name of the interface, which has been created.
Ip Address	IP address assigned to the USB interface.

Field	Description
Mask	Network mask to be applied to the IP Address.
Nat Dir	This specifies the NAT direction, which may be: *inside, outside or none*.
Oper	The actual/current state of the interface. It can be either *Up* or *Down*
If Sec Type	Interface security type.
MTU	This specifies the MTU Size configured for Ethernet over USB interface

Caution None.

References

- *create usb intf* command
- *delete usb intf* command
- *get usb intf intf* command
- *get usb stats* command.

3.316 modify wlan intf

Description Use this command to modify 802.11 Interface

Command Syntax

```
modify wlan intf  ifname ifname [ encrtype disable | 64bit | 128bit ] [ deftxkeyid deftxkeyid ] [ defchannel defchannel ] [ rtsthreshold rtsthreshold ] [ fragthreshold fragthreshold ] [ essid "essid" ] [ micwaverobust enable | disable ] [ intrabssrelay enable | disable ] [ ip ip ] [ mask mask ] [ usedhcp false | remote | local ]
```

Parameter

Name	Description
ifname ifname	Name of the wireless interface. **Valid Values:** wlan-0 - wlan-* **Type:** Mandatory
encrtype disable | 64bit | 128bit	WEP Encryption Type.Disabled for no encryption.64bit for 40bit encryption.128bit for 128bit encryption. **Type:** Optional **Default value:** disable
deftxkeyid deftxkeyid	Combined with WepEncryption attribute, determines which encryption key (between 0-3) to use by default. The actual key is picked up from the 802.11 WEP Keys MO. **Type:** Optional **Valid values:** 0 - 3 **Default value:** 0
defchannel defchannel	Default Channel **Type:** Optional **Valid values:** 0 - 2147483647 **Default value:** 0
rtsthreshold rtsthreshold	Maximum packet size to use RTS/CTS With **Type:** Optional **Valid values:** 0 - 2147483647 **Default value:** 2347
fragthreshold fragthreshold	Minimum packet size to use fragmentation with **Type:** Optional **Valid values:** 0 - 2147483647 **Default value:** 2346
essid essid	Service set identifier of upto 32 characters which each 802.11b station uses. **Type:** Optional **Default value:** "Viking"
micwaverobust enable | disable	Enable/Disable Microwave robustness **Type:** Optional **Default value:** enable

Name	Description
intrabssrelay enable | disable	Relay packets between BSS (AP) **Type:** Optional **Default value:** disable
ip ip	This specifies the IP address configured for the interface. **Type:** Optional **Default value:** 0
mask mask	This specifies the network mask configured for the interface. **Type:** Optional **Default value:** 0
usedhcp false | remote | local	DHCPclient will do/not do link address negotiation locally/remotely depending on the UseDHCP values of local/remote or false **Type:** Optional **Default value:** false

Mode Super-User

Example

```
$ modify wlan intf  ifname wlan-0 encrtype 64bit deftxkeyid 1
defchannel 1 rtsthreshold 1 fragthreshold 1 essid "Viking"
micwaverobust enable intrabssrelay enable ip 192.168.3.4 mask
255.255.255.0 usedhcp false mtu 1500
```

Output Verbose Mode On:

```
Interface                 : wlan-0
Encryption Type           : 64bit            Default Tx Key Id      : 1
Default Channel           : 1                Rts Threshold          : 1
Fragmentation Threshold   : 1                Service set identifier : Viking
Relay packets between BSS : enable           IP address             : 192.168.3.4
Mask                      : 255.255.255.0    Nat Dir                : inside
Use DHCP                  : false            Security Type          : public
Microwave robustness      : enable
Maximum Transmission Unit : 1500

Set Done
```

Verbose Mode Off:

```
Set Done
```

Output field description

Field	Description
Interface	Name of the wireless interface.
Encryption Type	WEP Encryption Type. Disabled for no encryption. 64-bit for 40-bit encryption.128-bit for 128-bit encryption.
Default Tx Key Id	Combined with WepEncryption attribute, determines which encryption key (between 0-3) to use by default. The actual key is picked up from the 802.11 WEP Keys MO.

Field	Description
Default Channel	Default Channel
Rts Threshold	Maximum packet size to use RTS/CTS With
Fragmentation Threshold	Minimum packet size to use fragmentation with
Service set identifier	Service set identifier of upto 32 characters which each 802.11b station uses.
Relay packets between BSS	Relay packets between BSS (AP)
IP address	This specifies the IP address configured for the interface.
Mask	This specifies the network mask configured for the interface.
Nat Dir	This variable specifies whether this interface's address is inside or outside. This is used by NAT.
Use DHCP	DHCPclient will do/not do link address negotiation locally/remotely depending on the UseDHCP values of local/remote or false
Security Type	This specifies the interface type from firewall point of view.
Microwave robustness	Enable/Disable Microwave robustness
Maximum Transmission Unit	This specifies the maximum transmission unit for interface.

Caution None.

References

- *get wlan intf* command
- *create wlan intf* command
- *delete wlan intf* command

3.317 modify wlan key

Description Use this command to modify 802.11 Wired Equivalent Privacy Keys

Command Syntax ***modify wlan key ifname*** ifname ***encrtype*** 64bit | 128bit ***keyid*** keyid ***[keyval*** keyval ***]***

Parameter

Name	Description
ifname ifname	Name of the wireless interface. **Valid Values:** wlan-0 - wlan-* **Type:** Mandatory
encrtype 64bit | 128bit	Encryption type with which this key is to be used (64 bit or 128 bit). **Type:** Mandatory
keyid keyid	Key index. Used to identify which key to use as the default key on the interface. **Type:** Mandatory **Valid values:** 0 - 3
keyval keyval	64 or 128 bit Encryption key.Value to be given in Hex. **Type:** Optional

Mode Super-User

Example ***$ modify wlan key ifname*** wlan-0 ***encrtype*** 64bit ***keyid*** 1 ***keyval*** 0x3455678902345678

Output Verbose Mode On:

```
Interface       : wlan-0
Encryption Type : 64bit
Key Id          : 1

Set Done
```

Verbose Mode Off:

```
Set Done
```

Output field description

Field	Description
Interface	Name of the wireless interface.
Encryption Type	Encryption type with which this key is to be used(64 bit or 128 bit).
Key Id	Key index. Used to identify which key to use as the default key on the interface.

Caution None.

References

- *get wlan key* command
- *create wlan key* command
- *delete wlan key* command

3.318 modify zipb cfg enable

Description Use this command to either enable or disable the ZIPB mode of the modem.

Command Syntax ***modify zipb cfg enable***

Parameters None.

Mode Super-User

Example ***modify zipb cfg enable***

Output field description None.

Caution None.

References

- *get zipb cfg* command.

3.319 modify 8021x global

Description Use this command to modify 802.1x Global Configuration

Command Syntax ***modify 8021x global [enable | disable]***

Parameter

Name	Description
***enable	disable***	Global Status of 802.1x feature **Type:** Optional **Default value:** enable

Mode Super-User

Example ***$ modify 8021x global*** `enable`

Output Verbose Mode On:

```
802.1x global status
--------------------------------------------------------------------------------
enable

Set Done
```

Verbose Mode Off:

```
Set Done
```

Output field description

Field	Description
802.1x global status	Global Status of 802.1x feature

Caution None

References

- *get 8021x global* command

3.320 modify 8021x intf

Description Use this command to modify Dot1x Interface Configuration

Command Syntax

```
modify 8021x intf  ifname ifname [ enable | disable  ] [
admindir both | in ] [ portcontrol ForceUnAuth | Auto |
ForceAuth ] [ assoc one_to_one | many_to_one ] [ qperiod
qperiod ] [ txperiod txperiod ] [ supptimeout supptimeout ] [
servtimeout servtimeout ] [ maxreq maxreq ] [ reauthenabled
true|false ] [ reauthperiod reauthperiod ] [ reauthmax
reauthmax ] [ keytxenabled true|false ] [ dynamicsuppallow
true|false ] [ rekeytimeout rekeytimeout ]
```

Parameter

Name	Description
ifname ifname	Interface index **Type:** Mandatory **Valid values:** 1 - 4294967295
enable | ***disable***	Feature 802.1x status on this Interface **Type:** Optional **Default value:** enable
admindir both | in	This specifies the controlled directions for the port. If set to **both**, then the port needs to be authenticated for traffic to flow either to or from it. If set to **in**, then traffic going out via this port does not require it to be authenticated. **Type:** Optional **Default value:** both
portcontrol ForceUnAuth | Auto | ForceAuth	This allows administrative control over the Port's authorization status. If set to ForceUnAuth, the port is never authorized. If set to ForceAuth, the port is autorized unconditionally. If set to Auto, the port's authorization status is determined by outcome of the authentication exchanges between Supplicant PAE, Authenticator PAE, and the Authentication Server. **Type:** Optional **Default value:** Auto
assoc one_to_one | many_to_one	This specifies whether there will be one supplicant or many supplicants per port . **Type:** Optional **Default value:** one_to_one
qperiod qperiod	The Authenticator state machine uses a timer to define periods of time during which it will not attempt to acquire a Supplicant. The initial value of this timer is quietPeriod. **Type:** Optional **Valid values:** 0 - 65535 **Default value:** 60

Name	Description
txperiod txperiod	The Authenticator state machine uses a timer to determine when an EAPOL PDU is to be transmitted. The initial value of this timer is txPeriod. **Type:** Optional **Valid values:** 1 - 65535 **Default value:** 30
supptimeout supptimeout	The initialization value used for timing out the supplicant. Its default value is 30 s; however, if the type of challenge involved in the current exchange demands a different value of timeout (for example, if the challenge requires an action on the part of the user), then the timeout value is adjusted accordingly. **Type:** Optional **Valid values:** 1 - 65535 **Default value:** 30
servtimeout servtimeout	The initialization value used for timing out the Authentication Server. Its default value is 30 s; however, the timeout value may be adjusted to take account of the communication medium being used to communicate with the Authentication Sever. **Type:** Optional **Valid values:** 1 - 65535 **Default value:** 30
maxreq maxreq	The maximum number of times that the state machine will retransmit an EAP Request packet to the Supplicant before it times out the authentication session. **Type:** Optional **Valid values:** 1 - 10 **Default value:** 2
reauthenabled true|false	A constant that defines whether regular reauthentication will take place on this Port. **Type:** Optional **Valid values:** False, True **Default value:** GS_TRUE
reauthperiod reauthperiod	A constant that defines a nonzero number of seconds between periodic reauthentication of the Supplicant **Type:** Optional **Valid values:** 1 - 65535 **Default value:** 3600
reauthmax reauthmax	The number of reauthentication attempts that are permitted before the Port becomes Unauthorized. **Type:** Optional **Valid values:** 1 - 65535 **Default value:** 2

Name	Description
keytxenabled true|false	Controls transmission of key information after the port has been authorized. **Type:** Optional **Valid values:** False, True **Default value:** GS_FALSE
dynamicsuppallow true|false	This controls whether only management-created Supplicants or both management-created and Dynamically-learnt Supplicants are allowed. **Type:** Optional **Valid values:** False, True **Default value:** GS_TRUE
rekeytimeout rekeytimeout	Timer period after which keys will be transmitted to all the supplicants in the port. **Type:** Optional **Valid values:** 20 - 3600 **Default value:** 600

Mode Super-User

Example

```
$ modify 8021x intf  ifname wan-0  enable admindir both
portcontrol Auto assoc many_to_one qperiod 60 txperiod 30
supptimeout 30 servtimeout 30 maxreq 2 reauthenabled true
reauthperiod 3600 reauthmax 2 keytxenabled true
dynamicsuppallow true rekeytimeout 600
```

Output Verbose Mode On:

```
If Index                : wan-0
802.1x status           : enable      Admin dir            : both
Port Control            : Auto        Association          : many_to_one
Quiet Period(secs)      : 60          Tx Period(secs)      : 30
Supplicant Timeout(secs) : 30         Server Timeout(secs) : 30
Max Request             : 2           ReAuth Enabled       : true
ReAuth Period(secs)     : 3600        ReAuth Max requests  : 2
Key Tx Enabled          : true        Dynamic Supp Allowed : true
ReKey timeout(secs)     : 600

Set Done
```

Verbose Mode Off:

```
Set Done
```

Output field description

Field	Description
If Index	Interface index
802.1x status	Feature 802.1x status on this Interface
Admin dir	This specifies the controlled directions for the port. If set to both, then the port needs to be authenticated for traffic to flow either to or from it. If set to in, then traffic going out via this port does not require it to be authenticated.

Field	Description
Port Control	This allows administrative control over the Port's authorization status. If set to ForceUnAuth, the port is never authorized. If set to ForceAuth, the port is autorized unconditionally. If set to Auto, the port's authorization status is determined by outcome of the authentication exchanges between Supplicant PAE, Authenticator PAE, and the Authentication Server.
Association	This specifies whether there will be one supplicant or many supplicants per port .
Quiet Period(secs)	The Authenticator state machine uses a timer to define periods of time during which it will not attempt to acquire a Supplicant. The initial value of this timer is quietPeriod.
Tx Period(secs)	The Authenticator state machine uses a timer to determine when an EAPOL PDU is to be transmitted. The initial value of this timer is txPeriod.
Supplicant Timeout(secs)	The initialization value used for timing out the supplicant. Its default value is 30 s; however, if the type of challenge involved in the current exchange demands a different value of timeout (for example, if the challenge requires an action on the part of the user), then the timeout value is adjusted accordingly.
Server Timeout(secs)	The initialization value used for timing out the Authentication Server. Its default value is 30 s; however, the timeout value may be adjusted to take account of the communication medium being used to communicate with the Authentication Sever.
Max Request	The maximum number of times that the state machine will retransmit an EAP Request packet to the Supplicant before it times out the authentication session.
ReAuth Enabled	A constant that defines whether regular reauthentication will take place on this Port.
ReAuth Period(secs)	A constant that defines a nonzero number of seconds between periodic reauthentication of the Supplicant
ReAuth Max requests	The number of reauthentication attempts that are permitted before the Port becomes Unauthorized.
Key Tx Enabled	Controls transmission of key information after the port has been authorized.
Dynamic Supp Allowed	This controls whether only management-created Supplicants or both management-created and Dynamically-learnt Supplicants are allowed.
ReKey timeout(secs)	Timer period after which keys will be transmitted to all the supplicants in the port.

Caution None.

References

- *get 8021x intf* command
- *create 8021x intf* command
- *delete 8021x intf* command

3.321 modify 8021x supp

Description Use this command to modify a dot1x supplicant.

Command Syntax

```
modify 8021x supp  ifname <ifname> macaddr <macaddr>
[reauth yes|no] [authcontrol forceauth|forceunauth|auto]
[qperiod <decvalue>] [authtxperiod <decvalue>] [authtimeout
<decvalue>][authservtimeout <decvalue>][authmaxreq
<decvalue>] [reauthmax <decvalue>] [reauthperiod <decvalue>]
[authkeytx enable|disable] [reauthenabled true|false]
```

Parameter

Name	Description
ifname <ifname>	This specifies the Interface Index of a port. **Type:** Mandatory **Valid Values:**
macaddr <macaddr>	This specifies the MAC aaddress of a supplicant for which individual authenticator state machines are running. **Type:** Mandatory **Valid Values:** A Valid mac address
reauth yes|no	This specifies the re-authentication control for this port. **Type:** Optional **Valid Values:** yes, no **Default Value:** no
authcontrol forceauth|forceunauth|auto	This specifies the Current value of auth control Parameter. **Type:** Optional **Valid Values:** forceauth, forceunauth, auto **Default Value:** auto
qperiod <decvalue>	This specifies the Value in seconds of Quiet Period constant used by authenticator PAE state machine. **Type:** Optional **Valid Values:** 0 - 65535 **Default Value:** 60
authtxperiod <decvalue>	This specifies the value in seconds of TxPeriod constant used by authenticator PAE state machine **Type** : Optional **Valid Values** : 0 - 65535 **Default Values:** 30
authtimeout <decvalue>	This specifies the value in seconds of SuppTimeout constant used by backend authenticator state machine. **Type:** Optional **Valid Values:** 0 - 65535 **Default Values:** 30

Name	Description
authservtimeout <decvalue>	This specifies the Value in seconds of ServerTime-out constant used by Backend authenticator state machine **Type** : Optional **Valid Values** : 0 - 65535 **Default Values:** 30
authmaxreq <decvalue>	This specifies the value of MaxReq constant used by backend authenticator state machine **Type:** Optional **Valid Values** : 1- 10 **Default Values:** 2
reauthmax <decvalue>	This specifies the value of ReAuthMax constant used by Authenticator PAE state machine. **Type** : Optional **Valid Values** : 1 - 65535 **Default Values:** 2
reauthperiod <decvalue>	This specifies the value in seconds of re-authenti-cate period constant used by re-authenticate state machine. **Type** : Optional **Valid Values** : 1 - 65535 **Default Values:** 3600
authkeytx enable|disable	This specifies the whether auth key Transmission is enabled or disabled. **Type** : Optional **Valid Values** : enable, disable **Default Values:** disable
reauthenabled true|false	This specifies whether re-authentication is enabled or disabled **Type** : Optional **Valid Values :** true, false **Default Value:** true

Mode Super-User

Example ***$ modify 8021x supp ifname wlan-0 macaddr 0x0085a00004 authcontrol forceunauth reauthmax 3 reauthperiod 3700***

Output Verbose Mode On:

```
If Index                : wlan-0            Mac address             :  0x0085a00004
Virtual port Number     : 3000              Owner                   : 802.1x
Protocol Version        : 2.0.1.1           Port capability         : Auth
Re- authenticate        : no                Auth Pae State          : forceauth
Auth backend state      : request           Auth Key Transmission   :  disable
Auth Admin dir          : both              Auth Oper dir           : both
Auth Control status     : authorized        Auth control value      : forceauth
Auth Q period(secs)     : 1000              Auth Tx Period(secs)    : 200
Auth Supp Timeout(sec)  : 30                Auth Server timeout(secs):30
Auth Max req            : 2                 Auth Re-auth max        : 2
Auth reauth Period(secs): 3600              Auth reauth enabled     : true

Set Done
```

```
If Index                : wlan-0            Mac address            :  0x0085a00004
Virtual port Number     : 3000              Owner                  : 802.1x
Protocol Version        : 2.0.1.1           Port capability        : Auth
Re- authenticate        : no                Auth Pae State         : forceauth
Auth backend state      : request           Auth Key Transmission  :  disable
Auth Admin dir          : both              Auth Oper dir          : both
Auth Control status     : authorized        Auth control value     : forceauth
Auth Q period(secs)     : 1000              Auth Tx Period(secs)   : 200
Auth Supp Timeout(sec)  : 30                Auth Server timeout(secs):30
Auth Max req            : 2                 Auth Re-auth max       : 2
Auth reauth Period(secs): 3600              Auth reauth enabled    : true
```

Verbose Mode Off:

```
Set Done
```

Output field description

Field	Description
If Index	This specifies the Interface Index of a port.
Mac address	This specifies the MAC aaddress of a supplicant for which individual authenticator state machines are running.
Virtual port Number	This specifies the virtual Port Number to be used for an authenticator PAE associated with a Supplicant.
Owner	This specifies of the owner of the entry.
Protocol Version	This specifies the EAPOL Protocol Version associated with this supplicant.
Port capability	This specifies the PAE functionality (authenticator or supplicant) supported by this port.
Re- authenticate	This specifies the Re-authentication control for this port (it will always be returned false while reading)
Auth Pae State	This specifies the Current State of Authenticator PAE state machine.
Auth backend state	This specifies the Current State of Backend Authentication state machine.
Auth Key Transmission	This specifies the Key Transmission enable/disable control parameter.
Auth Admin dir	This specifies the Administrative Controlled Direction Parameter.
Auth Oper dir	This specifies the Operational Controlled Direction Parameter.
Auth Control status	This specifies the Supplicant's Current Authentication Status.
Auth control value	This specifies the Current value of AuthControl Parameter.
Auth Q period(secs)	This specifies the Value in seconds of QuietPeriod constant used by authenticator PAE state machine.

Field	Description
Auth Tx Period(secs)	This specifies the Value in seconds of TxPeriod constant used by authenticator PAE state machine.
Auth Supp Timeout(sec)	This specifies the Value in seconds of SuppTimeout constant used by Backend authenticator state machine.
Auth Server timeout(secs)	This specifies the Value in seconds of ServerTimeout constant used by Backend authenticator state machine
Auth Max req	This specifies the Value of MaxReq constant used by Backend authenticator state machine.
Auth Re-auth max	This specifies the Value of ReAuthMax constant used by Authenticator PAE state machine.
Auth reauth Period(secs)	This specifies the Value in seconds of ReauthPeriod constant used by Re-authenticate state machine.
Auth reauth enabled	This specifies the Re-authentication enable/disable control parameter.

Caution None

References

- *create 8021x supp* command
- *modify 8021x supp* command
- *delete 8021x supp* command

3.322 passwd

Description Use this command to change the password associated with a user login. An ordinary user may change the password for another user if the old password is known to him. However, the root does not need to know a user's existing password before changing it. The passwords are not echoed onto the screen.

Command Syntax ***Passwd*** *[*user-id*]*

Parameters

Name	Description
user-id	The id of the user whose password is to be changed. If not specified then the current user is assumed. **Type:** Mandatory, if user is logged in through serial port and user authentication is disabled through serial port. Otherwise, Optional. **Valid values:** String of up to 128 characters (All printable characters except ';')

Mode Super-User, Intermediate, User

Example See Sessions below

Normal Usage

```
$passwd
Old Password:
New Password:
Confirm New Password:
Set Done.
```

Super User (for ordinary user)

```
$passwd User1
New Password:
Confirm New Password:
Set Done.
```

Output field description None.

Caution None.

References

- *get user* command

3.323 ping

Description This command is used to send one or more ICMP messages to another host for a reply.

Command Syntax ***ping*** ***{***ip-address|***dname*** domain-name***}*** ***[-t***|***-n*** number***]*** ***[-i*** time-to-live***]*** ***[-w*** seconds***]*** ***[-s*** size***]***

Parameters

Name	Description
ip-address|***dname*** domain-name	This specifies the Destination address to be pinged. **Type:** Mandatory **Valid values:** Any Valid IP Address (*0.0.0.0 – 255.255.255.255*) or Domain Name (String of Max 63 characters ('a'-'z', 'A'- 'Z', '0'-'9', '-', '_'and '.')
-t	This specifies to ping the host continuously until the user interrupts. **Type:** Optional
-n number	This specifies the number of pings to send to host. **Type:** Optional **Valid values:** *1-65535* **Default value:** *4*
-w seconds	This specifies the time interval between successive ping requests **Type:** Optional **Valid values:** *0-65535* **Default value:** *2*
-i time-to-live	This specifies the time to live to be filled in the ping request **Type:** Optional **Valid values:** *0 – 255* **Default value:** *64*
-s size	This specifies the size of payload for ping. **Type:** Optional **Valid values:** *4-1472* **Default value:***64*

Mode Super-User, user

Example ***$ ping 192.168.1.13***

Output

```
$ ping 192.168.1.13
64 bytes of data from 192.168.1.13, seq=0 ttl=64 rtt=0.000 msec
64 bytes of data from 192.168.1.13, seq=1 ttl=64 rtt=0.000 msec
64 bytes of data from 192.168.1.13, seq=2 ttl=64 rtt=0.000 msec
64 bytes of data from 192.168.1.13, seq=3 ttl=64 rtt=0.000 msec


-------------------- Ping Statistics --------------------
4 packets transmitted, 4 packets received, 0 percent packet loss
```

Output field description

Field	Description
64 bytes of...	This denotes the number of bytes in the ping packet and the source IP Address.
Seq	This denotes the ping attempt counter value.
Ttl	This is the Time to live for the packet.
Rtt	This denotes the Round trip Time for the packet. A value less than *10ms* is shown as *0*

Caution If there is only one user login with root privileges then that entry cannot be deleted.

References

- `traceroute` command.

3.324 prompt

Description Use this command to set the new CLI prompt.

Command Syntax ***prompt*** new-prompt

Parameters

Name	Description
new-prompt	The new prompt string. **Type:** Mandatory **Valid values:** String of upto 19 characters (All characters except ';', ' ', '?')

Mode User, Super-User.

Example ***$ prompt $$$***

Output

```
Set Done
$$$
```

Output field description None.

Caution The modified prompt is not saved across a reboot.

References None.

3.325 reboot

Description Use this command to reboot the modem and to set the boot configuration (the source from which to boot up).

Command Syntax ***reboot [default|backup|last|minimum|clean]***

Parameters

Name	Description
default|backup|last|minimum|clean	This specifies the boot configuration – the source from which to boot up. The boot configuration is set to *last* automatically whenever a *commit* command is given. The boot configuration being an optional parameter, if it is not specified, it retains the previous value. So giving *reboot* after a *commit* will result in a reboot from the committed configuration. *Default*: Use Default factory configuration while booting up. *Backup*: Use the Backup configuration to boot the modem. *Last* : Use last committed configuration to boot the modem. *Minimum:* Use a configuration in which: • the size command is executed. • the user (login name and password as root) is created. • an Ethernet interface with IP address 192.168.1.1 mask 255.255.0.0 is created. *Clean:* The modem comes up with nothing configured. **Type:** Optional **Default value:** If a reboot is being given for the first time, then the default value is *default*. Otherwise, the default value is the same as what was given the last time.

Mode Super-User, User.

Example ***$ reboot***

Output None.

Output field description None.

Caution None.

References
- `commit` command.

3.326 remove

Description Use this command to remove a configuration or binary file stored on the modem.

Command Syntax ***remove fname*** file-name

Parameters

Name	Description
file-name	This specifies the file name which needs to be removed. **Type:** mandatory **Valid values:** string of upto 128 characters (‘A’-’Z’, ‘a’-‘z’, ‘0’-‘9’, ’-‘, ’_’)

Mode Super-User.

Example ***$ remove fname*** *myconfig.cfg*

Output Verbose Mode On

```
File removed
```

Verbose Mode Off

```
File removed
```

Output field description None.

Caution None.

References

- *get autoupdate* command
- *modify autoupdate* command
- *apply* command.
- *list* command.
- *download* command.

3.327 reset atm aal5 stats

Description Use this command to reset AAL5 VC statistics for the specified interface.

Command Syntax ***reset atm aal5 stats ifname*** interface-name

Parameters

Name	Description
ifname interface-name	This parameter specifies the interface for which information is desired. In case the field is not specified, then the information for all valid aal5 interfaces should be displayed. **Type:** Mandatory **Valid values:** aal5-0 - *

Mode Super-User.

Example ***$ reset atm aal5 stats ifname aal5-0***

Output Verbose Mode On

```
Set Done
```

Verbose Mode Off

```
Set Done
```

Output field description None.

Caution None.

References

- *oam lpbk* command
- *atm trfdesc* related commands
- *atm vc* related commands
- *atm port* and *statistics* related commands

3.328 reset atm stats

Description Use this command to reset ATM Port statistics for the specified interface.

Command Syntax ***reset atm stats ifname*** interface-name

Parameters

Name	Description
ifname interface-name	This parameter specifies the ATM port for which statistics should be reset. **Type:** Mandatory **Valid values:** *atm-0*

Mode Super-User.

Example ***$ reset atm stats ifname*** **atm-0**

Output Verbose Mode On

```
Set Done
```

Verbose Mode Off

```
Set Done
```

Output field description None.

Caution None.

References

- *oam lpbk* command
- *get atm stats* command
- *atm trfdesc* related commands
- *atm vc* related commands
- *atm port* commands

3.329 reset atm vc stats

Description Use this command to reset statistical information about a specific atm virtual circuit.

Command Syntax ***reset atm vc stats ifname*** interface-name

Parameters

Name	Description
ifname interface-name	This specifies the Virtual Circuit whose statistics are to be reset. **Type:** Optional **Valid values:** *aal5-0* - *

Mode Super-User

Example ***$ reset atm vc stats ifname*** **aal5-0**

Output Verbose Mode On

```
Set Done
```

Verbose Mode Off

```
Set Done
```

Output field description None.

Caution The specified atm vc should exist. That is, *create atm vc intf* command should have been run for this interface.

References

- *oam lpbk* command
- *atm statistics* related commands
- *atm trfdesc* related commands
- *atm vc* related commands.
- *atm port* commands.

3.330 reset bridge port stats

Description Use this command to reset bridge port statistics.

Command Syntax ***reset bridge port stats ifname*** interface-name

Parameters

Field	Description
ifname interface-name	This specifies the bridge interface whose statistics are to be reset. **Type:** Optional **Valid values:** *eoa-0 - *, eth-0, usb-0*

Mode Super-User

Example

```
$ reset bridge port stats ifname eth-0
```

Output

```
Set Done
```

Output field description None.

Caution None.

References

- *bridge mode* related commands
- *bridge port intf* related commands
- *bridge static* related commands
- *bridge forwarding* related commands.

3.331 reset bridge tbg stats

Description Use this command to reset statistics related to transparent bridging.

Command Syntax ***reset bridge tbg stats***

Parameters None.

Mode Super-User

Example ***$ reset bridge tbg stats***

Output

```
Set Done
```

Output field description None.

Caution None.

References

- *bridge tbg info* related commands
- *bridge* related commands
- *bridge port stats* related commands
- *bridge static* related commands
- *bridge forwarding* related commands

3.332 reset datauserslist

Description Use this command to delete all data users.

Command Syntax ***reset datauserslist***

Parameters None.

Mode Super-User

Example ***$ reset datauserslist***

Output Verbose mode on/off

```
Set Done
```

Output field description None.

Caution None.

References

- *get datauserslist* command
- *get usagectrl* command
- *modify usagectrl* command.

3.333 reset dhcp relay stats

Description This command resets the global DHCP Relay statistics.

Command Syntax ***reset dhcp relay stats***

Parameters None.

Mode Super-User, User

Example ***$ reset dhcp relay stats***

Output Verbose Mode On

```
Set Done
```

Verbose Mode Off

```
Set Done
```

Output field description None.

Caution None.

References

- *get dhcp relay stats* command
- *dhcp relay cfg* related commands
- *dhcp relay intf* related commands

3.334 reset dhcp server stats

Description Use this command to reset the global DHCP Server statistics.

Command Syntax ***reset dhcp server stats***

Parameters None.

Mode Super-User

Example ***$ reset dhcp server stats***

Output Verbose Mode On

```
Set Done
```

Verbose Mode Off

```
Set Done
```

Output field description None.

Caution None.

References

- *get dhcp server stats* command
- *dhcp server cfg* related commands
- *dhcp server exclude* related commands
- *dhcp server address* related commands
- *dhcp server pool* related commands.

3.335 reset dns relay stats

Description Use this command to reset DNS relay statistics

Command Syntax ***reset dns relay stats***

Mode Super User

Output Verbose mode on

```
Set Done
```

Verbose mode off

```
Set Done
```

Caution: None

References

- modify dns relay cfg
- get dns relay stats
- get dns relay config
- create dns servaddr
- get dns servaddr
- delete dns servaddr

3.336 reset dsl stats cntrs

Description Use this command to reset DSL statistics error counters.

Command Syntax ***reset dsl stats cntrs***

Parameters None.

Mode Super-User.

Example ***$ reset dsl stats cntrs***

Output Verbose Mode On

```
Set Done
```

Verbose Mode Off

```
Set Done
```

Output field description None.

Caution None.

References

- *get dsl stats cntrs* command

3.337 reset dsl stats flrs

Description Use this command to reset dsl statistics failures.

Command Syntax ***reset dsl stats flrs***

Parameters None.

Mode Super-User.

Example ***$ reset dsl stats cntrs***

Output Verbose Mode On

```
Set Done
```

Verbose Mode Off

```
Set Done
```

Output field description None.

Caution None.

References

- *get dsl stats flrs* command

3.338 reset fwl stats

Description Use this command to reset firewall statistics.

Command Syntax ***reset fwl stats***

Parameters None.

Mode Super-User.

Example ***$ reset fwl stats***

Output Verbose Mode On/Off

```
Set Done
```

Output field description None.

Caution None.

References

- *get fwl stats* command

3.339 reset ipf session

Description Use this command to reset all IP filter sessions.

Command Syntax ***reset ipf session***

Parameters None

Mode Super-User

Example ***$ reset ipf session***

Output Verbose Mode On

```
Set Done
```

Verbose Mode Off

```
Set Done
```

Output field description None

Caution This command is valid only when IP filter is enabled.

References

- *get ipf session* command
- *delete ipf session* command

3.340 reset ipf rule stats

Description Use this command to reset IP filter stats for a specific rule ID.

Command Syntax ***reset ipf rule stats ruleid*** rule-id

Parameters

Name	Description
ruleid rule-id	The index given by the caller to identify the rule entry. **Type**: Mandatory **Valid values:** *1-4294967295*

Mode Super-User.

Example ***$ reset ipf rule stats ruleid 1***

Output Verbose Mode On

```
Set done
```

Verbose Mode Off

```
Set done
```

Output field description None.

Caution None.

References

- *get ipf rule stats* command
- *get ipf stats* command
- *reset ipf stats* command

3.341 reset ipf stats

Description Use this command to reset global statistics of the IP filter.

Command Syntax ***reset ipf stats***

Parameters None.

Mode Super-User.

Example ***$ reset ipf stats***

Output Verbose Mode On

```
Set done
```

Verbose Mode Off

```
Set done
```

Output field description None.

Caution None.

References

- *get ipf stats* command
- *get ipf rule stats* command
- *reset ipf rule stats* command

3.342 reset l2tp session stats

Description Use this command to reset l2tp session statistics for a L2TP session for particular PPP interface.

Command Syntax ***reset l2tp session stats [pppifname interface-name]***

Parameters

Name	Description
`pppifname interface-name`	Identifies the PPP interface name from which PPP packets are being tunneled **Type:** Optional **Valid values**: ppp-0, ppp-*

Mode Super-User

Output Verbose Mode On/Off

```
Set Done
```

Output field description None.

Caution None.

References

- *`get l2tp session stats`* command

3.343 reset l2tp tunnel stats

Description Use this command to reset l2tp tunnel statistics for a particular tunnel interface.

Command Syntax ***rreset l2tp tunnel stats ifname interface-name***

Parameters

Name	Description
`ifname interface-name`	Identifies the interface name for L2TP layer. **Type:** Optional **Valid values:** l2t-0-l2t-*

Mode Super-User

Example ***reset l2tp tunnel stats ifname l2t-0***

Output Verbose Mode On/Off

```
Set Done
```

Output field description None.

Caution None.

References

- *get l2tp tunnel stats* command

3.344 reset nat rule stats

Description Use this command to reset statistics for the specified NAT rule or for all rules.

Command Syntax ***reset nat rule stats [ruleid*** rule-id***]***

Parameters

Name	Description
Ruleid rule-id	This identifies the NAT rule, statistics pertaining to which are to be reset. If no rule ID is specified then Statistics for all the rules are reset. **Type:** Optional **Valid values:** *1-4294967295*

Mode Super-User

Example ***$ reset nat rule stats ruleid*** 1

Output Verbose Mode On

```
Set Done
```

Verbose Mode Off

```
Set Done
```

Output field description None.

Caution None.

References

- *get nat rule stats* command
- *nat rule status* related commands
- *nat rule entry* related commands

3.345 reset nat stats

Description Use this command to reset global NAT statistics.

Command Syntax ***reset nat stats***

Parameters None.

Mode Super-User

Example ***$ reset nat stats***

Output Verbose Mode On

```
Set Done
```

Verbose Mode Off

```
Set Done
```

Output field description None.

Caution None.

References

- *get nat stats* command
- *nat status info* commands.

3.346 reset pfraw rule stats

Description Use this command to reset raw filter stats for a specific rule id.

Command Syntax ***reset pfraw rule stats ruleid*** rule-id

Parameters

Name	Description
Ruleid rule-id	This identifies the rule index for which the statistics should be reset. **Type:** Mandatory **Valid values:** *0 - 65535* Only existing rule ids accepted as input.

Mode Super-User.

Example ***$ reset pfraw rule stats ruleid 1***

Output Verbose Mode On

```
Set done
```

Verbose Mode Off

```
Set done
```

Output field description None.

Caution None.

References *pfraw* related commands.

3.347 reset pfraw stats

Description Use this command to reset global statistics of the raw filter.

Command Syntax ***reset pfraw stats***

Parameters None

Mode Super-User.

Example ***$ reset pfraw stats***

Output Verbose Mode On

```
Set Done
```

Verbose Mode Off

```
Set Done
```

Output field description None.

Caution None.

References *pfraw* related commands.

3.348 reset ppp lstatus

NOTE: This command is not supported in the current release.

Description Use this command to reset statistics of a particular PPP interface.

Command Syntax ***$ reset ppp lstatus ifname*** *interface-name*

Parameters

Name	Description
ifname interface-name	This parameter specifies the PPP interface for which statistics should be reset. **Type** : Mandatory **Valid values:** *ppp-0**.

Mode Super-User.

Example ***$ reset ppp lstatus ifname ppp-0***

Output Verbose Mode On/Off

```
Set Done
```

Output field description None.

Caution None.

References *get ppp lstatus.*

3.349 reset radius acctserv stats

Description Use this command to reset Radius Accounting Server Statistics.

Command Syntax ***reset radius acctserv stats index*** index

Parameter

Name	Description
index index	A number uniquely identifying each RADIUS Accounting server with which this client communicates. **Type:** Mandatory **Valid values:** 1 - 2147483647

Mode Super-User

Example ***$ reset radius acctserv stats index*** 1

Output Verbose Mode On:

```
Set Done
```

Verbose Mode Off:

```
Set Done
```

Output field description None

Caution None

References

- *get radius acctserv stats* command

3.350 reset radius authserv stats

Description Use this command to reset Radius Authentication Server Statistics.

Command Syntax ***reset radius authserv stats index*** index

Parameter

Name	Description
index index	A number uniquely identifying each RADIUS Authentication server with which this client communicates. **Type:** Mandatory **Valid values:** 1 - 2147483647

Mode Super-User

Example ***$ reset radius authserv stats index*** 1

Output Verbose Mode On:

```
Set Done
```

Verbose Mode Off:

```
Set Done
```

Output field description None

Caution None

References

- *get radius authserv stats* command

3.351 reset rip stats

Description Use this command to reset RIP stats.

Command Syntax ***reset rip stats***

Parameters None.

Mode Super-User and User

Example ***reset rip stats***

Output Verbose Mode On

```
Set done
```

Verbose Mode Off

```
Set done
```

Output field description None.

Caution None.

References

- *get rip stats* commands.

3.352 reset sntp stats

Description Use this command to reset SNTP statistics.

Command Syntax ***reset sntp stats***

Parameters None.

Mode User, Super-User

Example ***$ reset sntp stats***

Output

```
Set Done
```

Output field description None.

Caution None.

References

- *create sntp servaddr command*
- *delete sntp servaddr command*
- *get sntp servaddr command*
- *modify sntp cfg command*
- *get sntp cfg command*
- *get sntp stats command*

3.353 reset stp stats

Description Use this command to reset stp global statistics.

Command Syntax ***reset stp stats***

Parameters None.

Mode Super-User

Example ***$ reset stp stats***

Output

```
Set Done
```

Output field description None.

Caution None.

References

- *modify stp info* command
- *stp port* related commands.

3.354 reset stp port stats

Description Use this command to reset the stp port stats for a specific interface.

Command Syntax ***reset stp port stats ifname*** interface-name

Parameters

Name	Description
ifname interface-name	The port for which this entry contains Spanning Tree Protocol management information. If no interface name is specified, then information for all entries is displayed. **Type:** Optional **Valid values:** *eth-0, aal5-0* - *

Mode Super-User

Example

```
$ reset stp port stats ifname eth-0
```

Output

```
Set Done
```

Output field description None.

Caution None.

References

- *modify stp port* command
- *stp global* related commands
- *bridge ports* related commands

3.355 reset surf profile reg

Description Use this command to reset the surfing profile registration.

Command Syntax ***reset surf profile reg***

Mode Super-User

Example ***$ reset surf profile reg***

Output Verbose mode on/off

```
Set Done
```

Output field description None.

Caution None.

References

- *get surf profile cfg* command.

3.356 reset traps

Description This command deletes all traps.

Command Syntax ***reset traps***

Parameters None.

Mode Super-User.

Example ***$ reset traps***

Output

```
Set Done
```

Output field description None.

Caution None.

References

- *get traps* command

3.357 reset 8021x authstats

Description Use this command to reset the statistics Information for each Authenticator PAE corresponding to a Supplicant.

Command Syntax ***reset 8021x authstats ifname interface-name macaddr mac-address***

Parameters

Name	Description
ifname <ifname>	This specifies the Interface Index of a port. **Type:** Mandatory **Valid Values:**
macaddr <macaddr>	This specifies the MAC address of a supplicant for which individual authenticator state machines are running. **Type :** Mandatory **Valid Values:** A Valid mac-address.

Mode Super-User.

Output Verbose Mode On

```
Set Done
```

Verbose Mode Off

```
Set Done
```

Output field description None.

Caution None.

References

- *get 8021x authstats* command

3.358 reset 8021x sessstats

Description Use this command to reset the session statistics Information for each Authenticator PAE corresponding to a Supplicant.

Command Syntax ***reset 8021x sessstats ifname interface-name macaddr mac-address***

Parameters

Name	Description
ifname <ifname>	This specifies the Interface Index of a port. **Type:** Mandatory **Valid Values:**
macaddr <macaddr>	This specifies the MAC address of a supplicant for which individual authenticator state machines are running. **Type :** Mandatory **Valid Values:** A Valid mac-address.

Mode Super-User.

Output Verbose Mode On

```
Set Done
```

Verbose Mode Off

```
Set Done
```

Output field description None.

Caution None.

References

- *get 8021x sessstats* command

3.359 size

Description Use this command to configure the system sizing information.

Command Syntax ***size*** ***[maxvc*** max-num-of-vcs***]*** ***[max1483vc*** max-1483-vc***]*** ***[maxppe*** max-ppe-session***]*** ***[maxmac*** max-num-of-mac-addresses***]*** ***[maxpfrawrule*** max-num-pfraw-rules***]*** ***[maxpfrawsubrule*** max-pfraw-subrules***]*** ***[maxipfrule*** max-num-ipf-rules***]*** ***[maxl2tpTunnel*** max-l2t-tunnel***]*** ***[maxl2tpSessPerTunnel*** *max-l2t-session-per-tunnel*] ***[maxl2tppeerrws*** *max-l2t-peer-recv-window*]

Parameters

Name	Description
Maxvc max-num-of-vcs	This specifies the maximum number of VCCs supported over all ATM ports. **Type:** Optional **Valid values:** *1- ** **Default value:** *2*
max1483vc max-1483-vc	This specifies the maximum AAL5 connections used for MEA5. **Type:** Optional **Valid values:** *1- ** **Default value:** *1*
maxppe max-ppe-session	This specifies the maximum number of PPPoE sessions supported in the system **Type:** Optional **Valid values:** *1- ** **Default value:** *1*
maxmac max-num-of-mac-addresses	This specifies the maximum number of MAC address that can be learnt by bridging module **Type:** Optional **Valid values:** *1 - ** **Default value:** *256*
maxpfrawrule max-num-pfraw-rules	Maximum total number of rules that can be stored in global rule table **Type:** Optional **Valid values:** *1 - ** **Default value:** *8*
maxpfrawsubrule max-pfraw-subrules	Maximum total number of sub-rules that can be stored in sub-rule table **Type:** Optional **Valid values:** *1 - ** **Default value:** *8*
maxipfrule max-num-ipf-rules	Maximum total number of rules that can be stored in global ipfilter rule table. **Type:** Optional **Valid values:** *1 - ** **Default Value:** *50*

Name	Description
maxl2tpTunnel mx-l2t-tunnel	Maximum number of L2TP tunnels supported in the system.
maxl2tpSessPerTunnel max-l2t-session-per-tunnel	Maximum number of PPP sessions supported per L2TP tunnel.
maxl2tppeerrws max-l2t-peer-recv-window	Maximum size of peer receive window size that can be handled.

Mode Super-User

Example ***$ size maxvc 4 max1483vc 2 maxppe 2 maxmac 6***

Output Verbose Mode On:

```
Entry Created
PPP Inactivity Timeout    : 0        Max PPE Sessions    : 2
Ignore WAN to LAN traffic : False    Max TBG MAC address : 6
Max VCs                   : 4        Max 1483 VCs        : 2
Max PFRaw Rules           : 8        Max PFRaw Subrules  : 8
Max IPF Rules              : 8       Max l2tp Tunnel: 2
Max l2tp Sess Per Tunnel   : 2       Max L2TP Peer RWS: 2
```

Verbose Mode Off:

```
Entry Created
```

Output field description

FIELD	DESCRIPTION
PPP Inactivity Timeout	This specifies the Inactivity timeout for PPP.
Ignore WAN to LAN traffic	Flag indicating whether to ignore WAN to LAN traffic for PPP Session timeout.
Max PPE Sessions	This specifies the maximum number of PPPoE sessions supported in the system.
Max TBG MAC address	This specifies the maximum number of MAC addresses that can be learned by the bridging module.
Max VCs	This specifies the maximum number of VCCs supported over all ATM ports.
Max 1483 VCs	This specifies the maximum AAL5 connections used for MEA5.
Max PFRaw Rules	Maximum total number of rules that can be stored in the global rule table.
Max PFRaw Subrules	Maximum total number of sub-rules that can be stored in the sub-rule table.
Max IPF Rules	Maximum total number of rules that can be stored in the global ipfilter rule table.
Max l2tp Tunnel	Maximum number of L2TP tunnels supported in the system.

FIELD	DESCRIPTION
Max l2tp Sess Per Tunnel	Maximum number of PPP sessions supported per L2TP tunnel.
Max L2TP Peer RWS	Maximum size of peer receive window size that can be handled.

Caution None.

References *get sizeinfo* command

3.360 traceroute

Description This command is used to trace the route to the specified destination.

Command Syntax ***traceroute*** {ip-address|***dname*** domain-name} {***ping***|***udp***} ***[-m*** num-of-hops***]*** ***[-w*** wait-time***]*** ***[-p*** udp-port-number***]*** ***[-q*** num-of-probes***]***

Parameters

Name	Description
ip-address|***dname*** domain-name	This specifies the Destination address to be pinged. **Type:** Mandatory **Valid values:** Any Valid IP Address (*0.0.0.0 – 255.255.255.255*) or Domain Name (String of Max 63 characters ('a'-'z', 'A'- 'Z', '0'-'9', '-', '_'and '.')
Ping|***udp***	Traceroute probe message type **Type:** Mandatory
-m num-of-hops	Maximum number of hops to search for ip-address **Type:** Optional **Valid values:** *0-255* **Default value:** *30*
-w wait-time	This specifies the timeout in seconds **Type:** Optional **Valid values:** *0-65535* **Default value:** *5*
-p udp-port-number	Destination UDP port to be used, only when Probe is Udp **Type:** Optional. **Valid values:** *0-65535* **Default value:** *32768*
-q num-of-probes	Number of probes to be sent for each TTL value **Type:** Optional **Valid values:** *0-255* **Default value:** *3*

Mode Super-User, User

Example ***$ traceroute 192.168.1.13 ping***

Output

```
Tracing route to [192.168.1.13]
Over a maximum of 30 hops
1    0.000000 ms  0.000000 ms  0.000000 ms   192.168.1.13
Trace complete.
```

Output field description

Field	Description
1	This denotes the hop counter value.
2-4	These are the Round trip timings of the 3 probe packets sent. A * denotes that this probe was missed.
5	This is the ip address of the intermediate/destination node.

Caution None.

References

- *ping* command.

3.361 trigger ilmi

Description Use this command to give a start trigger to the ILMI based auto configuration procedure. On receiving this trigger ILMI would initiate its procedures if ILMI is enabled.

Command Syntax ***trigger ilmi***

Parameters None.

Mode Super-User.

Example ***$ trigger ilmi***

Output None.

Caution The *trigger ilmi* command can be given after creating an ILMI interface in the enabled state using the *create ilmi intf* command, or after modifying the state to enabled using the *modify ilmi intf* command. Alternately, the triggering can be achieved automatically if the modem is rebooted after enabling the ILMI interface.

In case an ILMI interface is being created in the default configuration, the *create ilmi intf* command in the default configuration *must* be followed by a *trigger ilmi* command.

References

- *create ilmi intf* command

4 CLI – Quick Reference Sheet

4.1 ALG Commands

COMMANDS	PARAMETERS
create alg port	***[prot {any|tcp|udp|icmp|esp| num <prot-number>}] algtype {ftp|snmp|cuseeme|l2tp|ra|rcmd|mirc| h323_q931|h323_ras|pptp|rtsp|timbuktu|ldap|sgicompcore| msnmsgr|ike|esp|SIP|t120|icq}***
delete alg port	***portno*** port-no ***[prot {any|tcp|udp|***<prot- number>***}]***
get alg port	***[portno*** port-no***]***
get alg type	***none***

4.2 ATM Commands

(Sheet 1 of 2)

COMMANDS	PARAMETERS
create atm port	***ifname*** interface-name ***[maxvc max-num-vccs] [fast|interleaved] [oamsrc oam-src-id] [cbrpriority*** cbr-priority***] [rtvbrpriority*** rtvbr-priority***] [nrtvbrpriority*** nrtvbr-priority***] [gfrpriority*** gfr-priority***] [ubrpriority*** ubr-priority***] [enable|disable]***
create atm trfdesc	***create atm trfdesc trfindex traffic-descriptor-index [NOCLP_NOSCR|CLP_NOTAG_MCR|NOCLP_SCR|NOCLP_NOSCR_CDVT|NOCLP_SCR _CDVT] [UBR|GFR|CBR|RTVBR|NRTVBR] [pcr peak-cell-rate] [mcr minimum-cell-rate] [scr sustained-cell-rate] [mbs maximum-burst-size][cdvt cell-delay-variation-tolerance]***
create atm vc intf	***ifname*** interface-name ***vpi vpi vci vci lowif*** virtual-atm-port-interface-name ***[enable|disable] [trfindex*** traffic-descriptor-index***] [aal5] [a5txsize*** aal5-cpcs-tx-sdu-size***] [a5rxsize*** aal5-cpcs-rx-sdu-size***] [vcmux|llcmux|none] [a5maxproto*** max-protocol-per-aal5***] [vcweight*** vc-weight***]***
create atm svccfg	interface-name ***daddr*** dest-atm-address ***[pppoa|eoa|any] [nplan isdn|atmes] [trfindex*** traffic-descriptor-index***] [a5txsize*** aal5-cpcs-tx-sdu-size***] [a5rxsize*** aal5-cpcs-rx-sdu-size***] [vcmux|llcmux|none]***
create ipoa intf	***ifname interface-name ip ip-address mask net-mask [type 1577|non1577] [inside|outside|none] [ifsectype public|private|dmz] [gwy ip-address] [droute true|false][mtu <decvalue]***
modify ipoa intf	***ifname interface-name [ip ip-address] [mask net-mask] [gwy <ddd.ddd.ddd.ddd>] [droute true|false][mtu <decvalue>]***
delete atm port	***ifname*** interface-name
delete atm trfdesc	***trfindex*** traffic-descriptor-index
delete atm vc intf	***ifname*** interface-name
delete atm svccfg	***[ifname*** interface-name***]***
delete ipoa intf	***ifname*** interface-name
get atm 1483 stats	-
get atm aal5 stats	***[ifname*** interface-name***]***
get atm port	***[ifname*** interface-name***]***
get atm stats	***[ifname*** interface-name***]***
get atm svccfg	***[ifname*** interface-name***]***
get atm trfdesc	***trfindex [***traffic-descriptor-index***]***
get atm vc intf	***[ifname*** interface-name***]***
get atm vc stats	***[ifname*** interface-name***]***

(Sheet 2 of 2)

COMMANDS	PARAMETERS
get ipoa intf	***[ifname*** interface-name***]***
get oam lpbk vc	***[ifname*** interface-name***]***
modify oam cc vc	***[mode auto|manual] [action act|deact] [dir src|sink|both] [ethercheck enable|disable]***
get oam cc vc	***[ifname*** *interface-name*]***
modify atm port	***ifname*** interface-name ***{enable|disable}***
modify atm vc intf	***ifname*** interface-name ***{enable|disable}***
modify atm svccfg	***ifname <interface-name> start|stop***
modify oam lpbk vc	***ifname*** interface-name ***[lbid*** oam-loopback-location-id***] [e2e|seg]***
reset atm aal5 stats	***ifname*** interface-name
reset atm stats	***ifname*** interface-name
Reset atm vc stats	***ifname*** interface-name

4.3 AutoDetect Commands

COMMANDS	PARAMETERS
get autodetect cfg	***none***
modify autodetect cfg	***[enable | disable] [mode bridge|router|both] [pppdetect padilcp|fullblown] [vcrange all|fromfile]***
get autodetect status	***-***
modify autodetect status	***vci <decvalue> vpi <decvalue> [port <ifname>]***

4.4 Bridge Commands

COMMANDS	PARAMETERS
create bridge port intf	***ifname*** interface-name
create bridge static	***macaddr*** mac-address ***inifname*** interface-name|***all [ifname*** interface-name|***all]+***
delete bridge port intf	***ifname*** interface-name
delete bridge static	***macaddr*** mac-address ***inifname*** interface-name|***all***
get bridge forwarding	***[macaddr*** mac-address***]***
get bridge tbg info	***-***

COMMANDS	PARAMETERS
get bridge mode	-
get bridge port intf	*[ifname* interface-name*]*
get bridge port stats	*[ifname* interface-name*]*
get bridge static	*[macaddr* mac-address*] [inifname* interface-name|*all]*
get stp info	-
get stp port	*[ifname* interface-name*]*
modify bridge tbg info	*aging* aging-timeout
modify bridge mode	*{enable|disable}*
modify bridge static	*macaddr* mac-address *inifname* interface-name|*all [ifname* interface-name|*all]+*
modify stp info	*[priority priority-value] [maxage maximum-age] [htime hello-time] [fdelay forward-delay] [enable|disable]*
modify stp port	*ifname* interface-name *[enable|disable] [pcost path-cost] [priority* priority-value*]*

4.5 Bridge Router Autosense (BRAS) Commands

COMMANDS	PARAMETERS
get bras cfg	-
modify bras cfg	*[status enable | disable] [selfppe restart]*

4.6 DDNS Commands

COMMANDS	PARAMETERS
create ddns hostname	*ifname ifname name name*
create ddns intf	*ifname ifname srvcname tzo | dyndns username username passwd passwd [system dynamic | static | custom] [wildcard enable | disable] [mailexchger mailexchger] [mailbackup enable | disable] [offlinesupport enable | disable]*
delete ddns hostname	*ifname ifname name name*
delete ddns intf	*ifname ifname name name*
get ddns hostname	*[ifname ifname] [name name]*
get ddns intf	*[ifname* ifname *]*

4.7 DHCP Client Commands

COMMANDS	PARAMETERS
get dhcp client info	***[ifname*** interface-name***]***
get dhcp client stats	***[ifname*** interface-name***]***

4.8 DNS Commands

COMMANDS	PARAMETERS
modify dns relay cfg	***[enable|disable] [pollstatus enable|disable] [pollinterval <decvalue>]***
get dns relay cfg	-
create dns servaddr	***<ip-address>***
delete dns servaddr	***<ip-address>***
get dns servaddr	-
get dns relay stats	-
reset dns relay stats	-

4.9 DSL Commands

COMMANDS	PARAMETERS
get dsl config	-
get dsl stats cntrs	-

COMMANDS	PARAMETERS
get dsl stats curr	-
get dsl stats hist	*[sintrvl* start-interval-number*] [nintrvl* num-of-intervals*]*
modify dsl config	*[t1413|glite|gdmt|multi|rsrv|lgdmt|lglite|lg2|adicisco|alctanxb |alct41anxb|autosensegdmtfirst|gdmtorlite|autosenset1413first] [annex annexa|annexb|annexc] [trellis enable|disable] [expanded|short] [txatten <decvalue>] [gain <decvalue>] [maxbits <decvalue>] [txstart <decvalue>] [txend <decvalue>] [txbinadj enable|disable] [rxstart <decvalue>] [rxend <decvalue>] [rxbinadj enable|disable] [fastretrain enable|disable] [escfastretrain enable|disable] [bitswap enable|disable] [duallatency enable|disable] [pmode enable|disable] [pilotreq enable|disable] [whip enable | disable] [loop start|stop] [acmodeitem fbm|dbm] [acpilotreq enable|disable] [acttrroffset offset0|offset42] [ecfdmmode < ec|fdm|fdmhp|fdmnaf>] [maxdnrate <hexvalue>]*
reset dsl stats cntrs	-
get dsl stats flrs	-
reset dsl stats flrs	-

4.10 DHCP Relay Commands

COMMANDS	PARAMETERS
create dhcp relay intf	*ifname* interface-name
delete dhcp relay intf	*ifname* interface-name
get dhcp relay cfg	-
get dhcp relay intf	*[ifname* interface-name*]*
get dhcp relay stats	-
modify dhcp relay cfg	*[enable|disable] [ip* serv-ip*]*
reset dhcp relay stats	-

4.11 DHCP Server Commands

COMMANDS	PARAMETERS
create dhcp server exclude	***ip*** ip-address
create dhcp server host	***ip*** ip-address ***mask*** ip-address ***hwaddr hw-address [dname domain-name] ({pop3|nntp|web|irc|wins|swins|dns|sdns|gwy|smtp}*** ip-address ***)* [dlease default-lease-time] [mlease max-lease-time]***
create dhcp server pool	***[pool-id] start-ip*** ip-address ***end-ip*** ip-address ***mask*** ip-address ***[dname*** domain-name***]*** ***{{pop3|nntp|web|irc|wins|swins|dns|sdns|gwy|smtp}*** ip-address***}* [enabled|disabled] [lthres*** low-threshold***] [dlease*** default-lease-time***] [mlease*** max-lease-time***]***
delete dhcp server exclude	***ip*** ip-address
delete dhcp server host	***ip*** ip-address
delete dhcp server pool	pool-id
get dhcp server address	***[ip*** ip-address***]***
get dhcp server cfg	-
get dhcp server exclude	-
get dhcp server host	***[ip*** ip-address***]***
get dhcp server pool	***[***pool-id***]***
get dhcp server stats	-
modify dhcp server cfg	***{enable|disable}***
modify dhcp server host	***ip*** ip-address ***[dname*** domain-name***]*** ***({pop3|nntp|web|irc|wins|swins|dns|sdns|gwy|smtp}*** ip-address ***)* [dlease*** default-lease-time***] [mlease*** max-lease-time***]***
modify dhcp server pool	pool-id ***[dname*** domain-name***]*** ***{{pop3|nntp|web|irc|wins|swins|dns|sdns|gwy|smtp}*** ip-address***}* [enabled|disabled] [lthres*** low-threshold] ***[dlease*** default-lease-time***] [mlease*** max-lease-time***]***
Reset dhcp server stats	-

4.12 DNS Commands

COMMANDS	PARAMETERS
get dns relay	-
modify dns relay	***[enable|disable]***

4.13 EoA Commands

COMMANDS	PARAMETERS
create eoa intf	***ifname interface-name [ip ip-address] [mask net-mask] lowif low-interface-name [inside|outside|none] [usedhcp true|false] [ifsectype public|private|dmz] [gwy <ddd.ddd.ddd.ddd>] [mtu <decvalue>]***
get eoa intf	***[ifname*** interface-name***]***
delete eoa intf	***[ifname*** interface-name***]***
modify eoa intf	***ifname interface-name [ip ip-address] [mask net-mask] [usedhcp true|false] [gwy <ddd.ddd.ddd.ddd>] [droute true|false] [mtu <decvalue>]***

4.14 Ethernet Commands

COMMANDS	PARAMETERS
create ethernet intf	***ifname interface-name [ip ip-address] [mask net-mask] [phyif low-interface-name] [inside|outside|none] [usedhcp local|remote|false] [ifsectype public|private|dmz] [mtu <decvalue>]***
delete ethernet intf	***Ifname*** interface-name
get ethernet intf	***ifname*** interface-name
get ethernet stats	***ifname*** interface-name
modify ethernet intf	***ifname interface-name [ip ip-address] [mask net-mask] [usedhcp local|remote|false] [mtu <decvalue]***

4.15 Firewall Commands

COMMANDS	PARAMETERS
get fwl blacklist	-
delete fwl blacklist	-
modify fwl global	*[attackprotect enable|disable] [dosprotect enable|disable] [blistprotect enable|disable] [blistperiod <decvalue>] [maxtcpconn <decvalue>] [maxicmpconn <decvalue>] [maxsinglehostconn <decvalue>] [logdest email|trace|both|none] [emailid1 email-id] [emailid2 email-id] [emailid3 email-id]*
get fwl global	-
get fwl stats	-
reset fwl stats	-

4.16 HDLC Commands

COMMANDS	PARAMETERS
get hdlceoc cfg	-
modify hdlceoc cfg	*[status disable | enable | loopback] [sar disable | enable]*
get hdlceoc stats	-

4.17 ICMP Commands

COMMANDS	PARAMETERS
get icmp stats	-

4.18 IGMP Commands

COMMANDS	PARAMETERS
create igmp intf	***ifname*** <interface-name> ***[qinterval*** <query-interval>***]*** ***[robust*** <robustness-variable>***]*** ***[host|router]*** ***[version igmpv1|igmpv2]*** ***[qmaxresponsetime*** < ***qmaxresponsetime*** >***]*** ***[lmqinterval*** < ***lmqinterval*** >***]***
delete igmp intf	***ifname*** interface-name
get igmp intf	***[ifname*** <interface-name>***]***
get igmp groups	***[grpaddr*** <ddd.ddd.ddd.ddd>***]*** ***[ifname*** <interface-name>***]***

4.19 ILMI Commands

COMMANDS	PARAMETERS
create ilmi intf	***intf ifname*** interface-name ***[enable|disable]*** ***[vpi*** vpi-number***]*** ***[vci*** vci-number***]*** ***[timeout*** time-out***]*** ***[keepalive*** keep-alive***]*** ***[maxretry*** max-retry***]***
get ilmi intf	***intf [ifname*** interface-name***]***
modify ilmi intf	***intf ifname*** interface-name ***[enable|disable]*** ***[vpi*** vpi-number***]*** ***[vci*** vci-number***]*** ***[timeout*** time-out***]*** ***[keepalive*** keep-alive***]*** ***[maxretry*** max-retry***]***
modify ilmi access protocol	***ifname interface-name vpi vpinum vci vci-num [proto pppoa|bridging|bbrouter|bpppoe|ipoa|classip|any]***

4.20 IP Commands

(Sheet 1 of 2)

COMMANDS	PARAMETERS
create arp	***ifname*** interface-name ***ip*** ip-address ***macaddr*** mac-address
create ip route	***ip dest-***ip-address ***gwyip gwy-***ip-address ***mask*** net-mask
delete arp	***ifname*** interface-name ***ip*** ip-address
delete ip route	***ip dest-***ip-address ***mask*** net-mask
get arp	***[ifname*** interface-name***]*** ***[ip*** ip-address***]***
get interface stats	***[ifname*** interface-name***]***
get ip address	***[ip*** ip-address***]***

(Sheet 2 of 2)

COMMANDS	PARAMETERS
get ip cfg	*-*
get ip route	***[ip dest-***ip-address***] [mask*** net-mask***]***
get ip stats	*-*
get host info	***[ip <ipaddress>]***
modify ip cfg	***[forwarding {enable|disable}] [ttl*** time-to-live***][arptimeout arp-timeout]***

4.21 IP Filtering Commands

(Sheet 1 of 2)

COMMANDS	PARAMETERS
create ipf rule entry	***ruleid rule-id*** ***[ifname interface-name|public|private|dmz|all]*** ***[dir in|out]*** ***[inifname interface-name|public|private|dmz|all]*** ***[act accept|deny]*** ***[log enable|disable]*** ***[enable|disable]*** ***[srcaddr {lt|lteq|gt|gteq|eq|neq*** ***<ddd.ddd.ddd.ddd>}|{{range|erange} <ddd.ddd.ddd.ddd>*** ***<ddd.ddd.ddd.ddd>}|any|self]*** ***[destaddr {lt|lteq|gt|gteq|eq|neq*** ***<ddd.ddd.ddd.ddd>}|{{range|erange} <ddd.ddd.ddd.ddd>*** ***<ddd.ddd.ddd.ddd>}|any|bcast|self]*** ***[srcport {lt|lteq|gt|gteq|eq|neq {num*** ***<decvalue>}|echo|discard|chargen|ftp|telnet|smtp|dns|boot|tftp|*** ***http|pop3|snmp >}|{{range|erange} <decValue> <decValue>}|any]*** ***[destport {lt|lteq|gt|gteq|eq|neq {num*** ***<decvalue>}|echo|discard|chargen|ftp|telnet|smtp|dns|boot|tftp|*** ***http|pop3|snmp >}|{{range|erange} <decValue> <decValue>}|any]*** ***[icmpcode {eq|neq <decValue>}|any]*** ***[icmptype {eq|neq echoreq|unreach|redir|echorep|{num*** ***<decValue>}}|any]*** ***[transprot {eq|neq TCP|UDP|ICMP|{num <decValue>}}|any]*** ***[tcpflag syn|nosyn|any]*** ***[storestate enable|disable]*** ***[seclevel {high|medium|low}+] [blistprotect enable|disable]*** ***[logtag "log-tag"] [isfrag yes|no|ignore] [isipopt yes|no|ignore]*** ***[pktsize {lt|lteq|gt|gteq|eq|neq <decvalue>}|any]*** ***[todfrom <hh:mm:ss>] [todto <hh:mm:ss>] [todstatus*** ***enable|disable]***
delete ipf rule entry	***ruleid*** rule-id
get ipf global	*-*

(Sheet 2 of 2)

COMMANDS	PARAMETERS
get ipf rule entry	*[ruleid* rule-id*]*
get ipf rule stats	*[ruleid* rule-id*]*
get ipf stats	-
modify ipf global	*[enable|disable] [accept|deny]*
modify ipf rule entry	*ruleid* rule-id *[log enable|disable] [enable|disable]*
reset ipf rule stats	*ruleid* rule-id
get ipf session	-
reset ipf session	-
reset ipf stats	-

4.22 L2TP Commands

(Sheet 1 of 2)

COMMANDS	PARAMETERS
create l2tp tunnel config	*ifname interface-name* *localip local-ip-address* *localhostname local-host-name* *remoteip remote-ip-address* *remotehostname remote-host-name* *[start|stop]* *[authtype simple|challenge|none]* *[secret tunnel-secret]* *[hellointerval hello-interval]* *[idletimeout {infinite|{num <decValue>}}]* *[crws contol-recv-windowsize]* *[maxretx max-retransmission]* *[maxretxtimeout max-retransmission-timeout]* *[payloadseq never|always}]* *[transport udpip]* *[initiator local|remote]*
delete l2tp tunnel config	*ifname* interface-name
get l2tp global config	-
get l2tp tunnel config	*ifname interface-name*
get l2tp udp stats	*ifname interface-name*
get l2tp tunnel stats	*ifname interface-name*
get l2tp global info	-
get l2tp session stats	*pppifname interface-name*

(Sheet 2 of 2)

COMMANDS	PARAMETERS
modify l2tp global config	***timeout {infinite|{ num <decValue>}}***
modify l2tp tunnel config	***ifname*** interface-name ***[localhostname*** *local-host-name]* ***[remotehostname*** *remote-host-name]* ***[start|stop]*** ***[authtype*** *simple|challenge|none]* ***[secret*** *tunnel-secret]* ***[hellointerval*** *hello-interval]* ***[idletimeout*** *{infinite|{num <decValue>}}]* ***[crws*** *contol-recv-windowsize]* ***[maxretx*** *max-retransmission]* ***[maxretxtimeout*** *max-retransmission-timeout]* ***[payloadseq*** *never|always}]* ***[transport*** *udpip]* ***[initiator*** *local|remote]*
reset l2tp tunnel stats	***ifname interface-name***
reset l2tp session stats	***ifname interface-name***

4.23 L2Wall Commands

COMMANDS	PARAMETERS
get l2wall cfg	***none***
modify l2wall cfg	***[off|on|auto] [inacttime*** *inactive-time]*

4.24 Management Control Commands

COMMANDS	PARAMETERS
create mctl iplist	***ipaddress ipaddress***
delete mctl iplist	***ipaddress ipaddress***
get mctl iplist	***[ipaddress ipaddress]***
get mctl access	-
modify mctl access	***[httpwanaccess enable | disable] [httplanaccess enable | disable] [telnetwanaccess enable | disable] [telnetlanaccess enable | disable] [ftpwanaccess enable | disable] [ftplanaccess enable | disable] [tftpwanaccess enable | disable] [tftplanaccess enable | disable] [snmpwanaccess enable | disable] [snmplanaccess enable | disable]***

4.25 NAT Commands

COMMANDS	PARAMETERS
create nat rule entry	*ruleid rule-id {basic|filter|napt|bimap|rdr|pass} [prot {any|tcp|udp| icmp|num prot-number}] [ifname interface -name] [lcladdrfrom local-address-from] [lcladdrto local-address-to] [destaddrfrom dest-address-from] [destaddrto dest-address-to] [destportfrom {num <decvalue>}|echo|discard|chargen|ftp|telnet|smtp|dns|boot| tftp|http|pop3|snmp] [destportto {num <decvalue>}|echo|discard|chargen| ftp|telnet|smtp|dns|boot|tftp|http|pop3|snmp] [glbaddrfrom global-address-from] [glbaddrto global-address-to] [lclport {num <decvalue>}|echo|discard| chargen|ftp|telnet|smtp|dns|boot|tftp|http|pop3|snmp]*
delete nat rule entry	*ruleid* rule-id
get nat global	-
get nat rule entry	*[ruleid* rule-id*]*
get nat rule stats	*[ruleid* rule-id*]*
get nat rule status	*[ruleid* rule-id*]*
get nat stats	-
get nat status	-
get nat translation	-
modify nat global	*[tcpidletimeout tcp-idle-timeout] [tcpclosewait tcp-close-wait] [tcptimeout tcp-timeout] [udptimeout udp-timeout] [gretimeout gre-timeout][esptimeout esp-timeout] [icmptimeout icmp-timeout] [defnatage default-nat-timeout] [{enable|disable}] [portstart port-start] [portend port-end]*
reset nat rule stats	*[ruleid* rule-id*]*
reset nat stats	-

4.26 Raw Packet Filtering Commands

COMMANDS	PARAMETERS
create pfraw rule entry	***ruleid rule-id [ifname interface-name|public|private|dmz|all] [dir in|out] [inifname interface-name|public|private|dmz|all] [enable|disable] [log disable|match|nomatch|all] [act accept|deny|callmgmt] [ssb ssb] [ssbmask ssbmask] [priority priority]***
create pfraw subrule entry	***ruleid*** rule-id ***subruleid*** sub-rule-id ***mask*** mask-value ***[start linkh|iph|tcph|tcpd|udph|udpd|icmph|icmpd] offset offset [enable|disable] cmpt {eq|neq|lt|lteq|gt|gteq val}|{range*** low-val high-val***}|{any}***
delete pfraw rule entry	***ruleid*** rule-id
delete pfraw subrule entry	***ruleid*** rule-id ***subruleid*** sub-rule-id
get pfraw rule info	***[ifname*** interface-name***] [dir in|out] [ruleid*** rule-id***] [subruleid*** subrule-id***]***
get pfraw rule entry	***[ruleid*** rule-id ***]***
get pfraw subrule entry	***[ruleid rule-id] [subruleid subrule-id]***
modify pfraw rule entry	***ruleid rule-id [enable|disable] [log disable|match|nomatch|all] [act accept|deny|callmgmt] [ssb ssb] [ssbmask ssbmask] [priority priority] [inifname incoming-if-name|all|public|private|dmz] [outifname out-ifname]***
modify pfraw subrule entry	***ruleid*** rule-id ***subruleid*** sub-rule-id ***[mask*** mask-value***] [start linkh|iph|tcph|tcpd|udph|udpd|icmph|icmpd] [offset offset] [enable|disable] [cmpt {eq|neq|lt|lteq|gt|gteq val}|{range*** low-val high-val***}|{any}]***
modify pfraw global	***[enable|disable] [accept|deny|callmgmt]***
get pfraw global	***-***
get pfraw stats	***-***
get pfraw rule stats	***[ruleid*** rule-id***]***
get pfraw block	***protocol IPV6MCAST|8021Q|ARP|BPDU|IPX|NETBEUI|APPLETALK|RARP|IPMCAST|PPE enable|disable***
modify pfraw block	***protocol IPV6MCAST|8021Q|ARP|BPDU|IPX|NETBEUI|APPLETALK|RARP|IPMCAST|PPE enable|disable***

4.27 PPP Commands

COMMANDS	PARAMETERS
create ppp intf	*ifname interface-name lowif low-interface-name {PPOE|PPOA|L2TP} [ip ip-address] [usedhcp {true|false}] [inside|outside|none] [mru max-rx-unit] [magic {true|false}] [droute {true|false}] [sname service-name] [start|stop|startondata] [usedns true|false] [ifsectype public|private|dmz] [l2tpcalltype outlns|outlac|inlns|inlac] [usegwy local|remote] [gwyip <ddd.ddd.ddd.ddd>] [numif <name>] [mtu <decvalue>]*
create ppp security	***ifname*** interface-name *[pap|chap]* ***login*** login-name ***passwd*** password
delete ppp intf	***ifname*** interface-name
delete ppp security	***ifname*** interface-name
get ppp intf	*[**ifname** interface-name]*
get ppp ipinfo	*[**ifname** interface-name]*
get ppp lstatus	*[**ifname** interface-name]*
reset ppp lstatus	*ifname interface-name*
get ppp security	*[**ifname** interface-name]*
modify ppp intf	*ifname interface-name [start|stop|statondata] [mru<decvalue>] [magic true|false] [l2tpcalltype outlns|outlac|inlns|inlac] [mtu <decvalue>]*
get ppp global	-
modify ppp global	*[pppsesstimer ppp-sess-timer] [ignorewantolan true|false] [keepalive enable|disable|auto] [maxlcpecho lcp-echo] [maxauthtries <decvalue>|infinite] [authretrydelay auth-retry-delay]*
modify ppp security	***ifname*** interface-name *[**login** login-name] [**passwd** password] [pap|chap]*

4.28 PPPoE Commands

COMMANDS	PARAMETERS
create ppe pconf	*acname AC-name [**srvname** service-name]*
delete ppe pconf	*acname AC-name [**srvname** service-name]*

COMMANDS	PARAMETERS
get ppe acserv	***ifname*** interface-name
get ppe cfg	-
get ppe pconf	-
get ppe stats global	-
get ppe stats session	***[ifname*** interface-name***]***
modify ppe cfg	***[padimax*** max-padi-attempts***] [padrmax*** max-padr-attempts***] [discmax*** max-discovery-attempts***] [paditime*** initial-padi-time-difference***] [padrtime*** initial-padr-time-difference***] [***first-come|serv-to-ac***] [padiperpadt padi-per-padt]***

4.29 RADIUS Commands

COMMANDS	PARAMETERS
create radius acctserv config	***index index ip ip port port [retries retries] [starttimeout starttimeout] [ontimeout ontimeout] secret secret***
delete radius acctserv config	***index index***
get radius acctserv config	***[index index]***
get radius acctserv stats	***[index index]***
modify radius acctserv config	***index index [retries retries] [starttimeout starttimeout] [ontimeout ontimeout] [secret secret]***
reset radius acctserv stats	***index index***
create radius authserv config	***index index ip ip port port [retries retries] [retxtimeout retxtimeout] secret secret***
delete radius authserv config	***index index***
get radius authserv config	***[index index]***

COMMANDS	PARAMETERS
get radius authserv stats	*[index index]*
modify radius authserv config	*index index [retries retries] [retxtimeout retxtimeout] [secret secret]*
reset radius authserv stats	*index index*
get radius global config	*-*
get radius global stats	*-*
modify radius global config	*[enable | disable] [authid authid] [acctid acctid] [acctintrvl acctintrvl]*

4.30 RIP Commands

COMMANDS	PARAMETERS
modify rip global	*[enable|disable] [updatetime* update-time*] [agetime* age-time*]*
create rip intf	*{ifname* interface-name*} [metric* metric-value*] [send {rip1|rip2|rip1compat|none}] [senddefroute {enable|disable}] [receive {rip1|rip2|both|none}] [recvdefroute {enable|disable}] [auth {none|text* password*}]*
delete rip intf	*{ifname* interface-name*}*
get rip intf	*[ifname* interface-name*]*
modify rip intf	*{ifname* interface-name*} [metric* metric-value*] [send {rip1|rip2|rip1compat|none}] [senddefroute {enable|disable}] [receive {rip1|rip2|both|none}] [recvdefroute {enable|disable}] [auth {none|text password}]*

4.31 RMON Commands

COMMANDS	PARAMETERS
get rmon eventgrp	*[rname* event-grp-name*]*
get rmon mpool	*[rname* mem-pool-name*]*
get rmon queue	*[rname* queue-name*]*
get rmon semaphore	*[rname* semaphore-name*]*
get rmon task	*[rname* task-name*]*

4.32 SNMP Commands

COMMANDS	PARAMETERS
create snmp comm	***community*** comm-name ***[ro|rw]***
create snmp host	***ip*** ip-addr ***community*** comm-name
delete snmp comm	***community*** comm-name
delete snmp host	***ip*** ip-addr ***community*** comm-name
get snmp comm	***[community*** comm-name***]***
get snmp host	-
get snmp stats	-
get snmp trap	-
modify snmp trap	***{enable|disable}***

4.33 SMTP Commands

COMMANDS	PARAMETERS
modify smtp servaddr	-
get smtp servaddr	-

4.34 SNTP Commands

COMMANDS	PARAMETERS
create sntp servaddr	*<ip-address>*|***dname*** *<domain-name>*
delete sntp servaddr	***< ip-address|dname domain-name >***
get sntp servaddr	***[<ip-address>|dname <domain-name>]***
modify sntp cfg	***[enable|disable]***
get sntp cfg	-
get sntp stats	***[<ip-address>|dname <domain-name>]***
reset sntp stats	-

4.35 Surfing Profile Commands

COMMANDS	PARAMETERS
reset surf profile reg	-

4.36 TCP Commands

COMMANDS	PARAMETERS
delete tcp conn	***lclip local***-ip-address ***lclport*** local-port ***rmtip*** remote-ip-address ***rmtport*** remote-port
get tcp conn	-
get tcp stats	-

4.37 UDP Commands

COMMANDS	PARAMETERS
get udp listen	-
get udp stats	-

4.38 UNI Commands

COMMANDS	PARAMETERS
create atm uni	***ifname interface-name saddr source-atm-addr [nplan isdn|atmes] [version uni31|uni40]***
delete atm uni	***[ifname*** interface-name***]***
get atm uni	***[ifname*** interface-name***]***

4.39 UPnP Commands

COMMANDS	PARAMETERS
get upnp cfg	-
modify upnp cfg	***[nbstatus enable | disable] [advcacheage advcacheage]***

4.40 Usage Control Commands

COMMANDS	PARAMETERS
get usagectrl	-
modify usagectrl	***[enable|disable] [maxusers <decvalue>|nolimit] [login enable|disable] [arpcheck <decvalue>]][mtu <decvalue]***
get datauserslist	-
reset datauserslist	-

4.41 USB Commands

COMMANDS	PARAMETERS
create usb intf	***ifname interface - name [ip ip-address] [mask net-mask] [inside|outside|none] [ifsectype public|private|dmz]***
delete usb intf	***delete usb intf ifname*** interface-name
get usb intf	***get usb intf [ifname*** interface-name***]***
modify usb intf	***modify usb intf ifname*** interface-name ***[ip*** ip-address***] [mask*** net-mask***][mtu <decvalue>]***
get usb stats	***get usb stats [ifname*** interface-name***]***

4.42 ZIPB Commands

COMMANDS	PARAMETERS
modify zipb cgf enable	-

4.43 802.11 Interface Commands

COMMANDS	PARAMETERS
create wlan intf	*ifname ifname [encrtype disable | 64bit | 128bit] [deftxkeyid deftxkeyid] [defchannel defchannel] [rtsthreshold rtsthreshold] [fragthreshold fragthreshold] [essid essid] [micwaverobust enable | disable] [intrabssrelay enable | disable] [ip ip] [mask mask] [natdir none | inside | outside] [usedhcp false | remote | local] [ifsectype public | private | dmz] [mtu mtu]*
create wlan key	*fname ifname encrtype 64bit | 128bit keyid keyid keyval keyval*
delete wlan intf	ifname ifname
delete wlan key	*ifname ifname encrtype 64bit | 128bit keyid keyid*
get wlan fwinfo	-
get wlan intf	*[ifname ifname]*
get wlan stats	*[ifname ifname]*
get wlan key	*[ifname ifname] [encrtype 64bit | 128bit] [keyid keyid]*
modify wlan intf	*ifname ifname [encrtype disable | 64bit | 128bit] [deftxkeyid deftxkeyid] [defchannel defchannel] [rtsthreshold rtsthreshold] [fragthreshold fragthreshold] [essid essid] [micwaverobust enable | disable] [intrabssrelay enable | disable] [ip ip] [mask mask] [usedhcp false | remote | local]*
modify wlan key	*ifname ifname encrtype 64bit | 128bit keyid keyid [keyval keyval]*

4.44 802.1x Commands

COMMANDS	PARAMETERS
create 8021x intf	*ifname ifname [enable | disable] [admindir both | in] [portcontrol ForceUnAuth | Auto | ForceAuth] [assoc one_to_one | many_to_one] [qperiod qperiod] [txperiod txperiod] [supptimeout supptimeout] [servtimeout servtimeout] [maxreq maxreq] [reauthenabled true|false] [reauthperiod reauthperiod] [reauthmax reauthmax] [keytxenabled true|false] [dynamicsuppallow true|false] [rekeytimeout rekeytimeout]*
delete 8021x intf	*ifname ifname*
modify 8021x intf	*ifname ifname [enable | disable] [admindir both | in] [portcontrol ForceUnAuth | Auto | ForceAuth] [assoc one_to_one | many_to_one] [qperiod qperiod] [txperiod txperiod] [supptimeout supptimeout] [servtimeout servtimeout] [maxreq maxreq] [reauthenabled true|false] [reauthperiod reauthperiod] [reauthmax reauthmax] [keytxenabled true|false] [dynamicsuppallow true|false] [rekeytimeout rekeytimeout]*
get 8021x intf	*[ifname ifname]*
get 8021x global	*-*
modify 8021x global	*[enable | disable]*
create 8021x supp	*ifname <ifname> macaddr <macaddr> [reauth yes|no] [authcontrol forceauth|forceunauth|auto] [qperiod <decvalue>] [authtxperiod <decvalue>] [authtimeout <decvalue>][authservtimeout <decvalue>][authmaxreq <decvalue>] [reauthmax <decvalue>] [reauthperiod <decvalue>] [authkeytx enable|disable] [reauthenabled true|false]*
modify 8021x supp	*ifname <ifname> macaddr <macaddr> [reauth yes|no] [authcontrol forceauth|forceunauth|auto] [qperiod <decvalue>] [authtxperiod <decvalue>] [authtimeout <decvalue>][authservtimeout <decvalue>][authmaxreq <decvalue>] [reauthmax <decvalue>] [reauthperiod <decvalue>] [authkeytx enable|disable] [reauthenabled true|false]*
create 8021x supp	*ifname <ifname> macaddr <macaddr> [reauth yes|no] [authcontrol forceauth|forceunauth|auto] [qperiod <decvalue>] [authtxperiod <decvalue>] [authtimeout <decvalue>][authservtimeout <decvalue>][authmaxreq <decvalue>] [reauthmax <decvalue>] [reauthperiod <decvalue>] [authkeytx enable|disable] [reauthenabled true|false]*

COMMANDS	PARAMETERS
delete 8021x supp	*supp ifname <ifname> macaddr <macaddr> [reauth yes|no] [authcontrol forceauth|forceunauth|auto] [qperiod <decvalue>] [authtxperiod <decvalue>] [authtimeout <decvalue>] [authservtimeout <decvalue>] [authmaxreq <decvalue>] [reauthmax <decvalue>] [reauthperiod <decvalue>] [authkeytx enable|disable] [reauthenabled true|false]*
get 8021x supp	*[ifname interface-name] [macaddr mac-address]*
delete 8021x supp	*ifname interface-name macaddr mac-address*
get 8021x authstats	*[ifname interface-name] [macaddr mac-address]*
reset 8021x authstats	*ifname interface-name macaddr mac-address*
get 8021x sessstats	*[ifname interface-name] [macaddr mac-address]*

4.45 Other Commands

COMMANDS	PARAMETERS
apply	***fname*** file-name *[besteffort true|false] [sparams "<params>"]*
alias	*[alias-string =* aliased-command*]*
commit	-
create user	*name user-name passwd password [root|user|intermediate] useserial*
delete user	***name*** user-name
do getserialize	–
do getver	–
do serialize	MAC-address serial-number USB-MAC-address
download	***fname*** file-name ***ip*** ip-address
get autoupdate	-
get size info	-
get system	-
get trace cfg	*[**module** module-name]*
get trace stats	-
get traps	*[*num-of-traps*]*
get trapprints	-
get user	-

COMMANDS	PARAMETERS
get nbsize	
help	*|?*
list	***list***
logout	*|**quit**|**exit***
modify autoupdate	***modify autoupdate true|false***
modify system	***[contact sys-contact] [model model-name] [location sys-location] [vendor sys-vendor-info] [logthresh sys-log-threshold] [systime systime] [dst <on|off>] [timezone <timezone>] [name <name>] [dname <domain>]***
modify trace cfg	***module*** module-name ***[flow*** trace-flow***] [level*** trace-level***] [syslog|net|stdout] [dest*** ip-address***] [port*** port-number***]***
modify trapprints	***enable|disable***
passwd	***[user-id]***
ping	***{***ip-address|domain-name***} [-t|-n*** number***] [-i*** time-to-live***] [-w*** seconds***] [-s*** size***]***
prompt	new-prompt
reboot	***[default|backup|last|minimum|clean]***
remove	***remove fname*** file-name
reset traps	-
size	***[maxvc max-num-of-vcs] [max1483vc max-1483-vc] [maxppe max-ppe-session] [maxmac max-num-of-mac-addresses] [maxpfrawrule max-num-pfraw-rules] [maxpfrawsubrule max-pfraw-subrules] [maxipfrule max-num-ipf-rules] [maxl2tpTunnel max-l2t-tunnel] [maxl2tpSessPerTunnel max-l2t-session-per-tunnel] [maxl2tppeerrws max-l2t-peer-recv-window]***
traceroute	***{***ip-address|domain-name***} {ping|udp} [-m*** num-of-hops***] [-w*** wait-time***] [-p*** udp-port-number***] [-q*** num-of-probes***]***
unalias	***{all|***alias-string***}***
modify nbsize	***maxipsess max-num-ip-sessions] [httpport http-port] [telnetport telnet-port] [ftpport ftp-port][serialauth enable|disable]***
verbose	***{on|off}***
do getver	-
do serialize	***<Ethernet Mac Address> <Serial Number> <USB Mac Address>***