ATOS 6.1.12

Contents

Articles

References

AtosntUserGuide

Point to Point

POTS

PRI1

PTM

Quality of Service

Security

Serial V/X

Sharing

SNMP

SysLog

System

Storage

TR069

Voice Service

VOIP

VRRP

WEB

Wi-Fi

WWAN physical interfaces

xDSL (ADSL,VDSL,ADSL2+,SHDSL)

ManOverView

ATOSNT
Technical Reference Manual
Rev.6.1.12
Date: October 2015
Index

ManHowToUse

How to use ATOSNT

ATOSNT - Stands for **Aethra Telecommunications Operating System**

How to understand the ATOSNT structure using CLI commands

Configuration and Management

Local configuration and management are possible via the console port with **Command Line Interface** (CLI) commands. The console port is connected to a TTY asynchronous terminal (typically a Personal Computer with terminal emulation software[1]).

Procedures with CLI commands are used to:

- access diagnostics and command functions;
- monitor internal events;
- configure the device;
- update the operating system.

The configuration structure is of hierarchical type. To access a parameter, you must reach the corresponding node and enter the command.

Some CPE models like BG7420 are not provided with the console port, in this case the access to the CLI is made on behalf a USB/Serial adapter, a custom accessory provided by Aethra, that allows the connection between the PC serial port ended in a 25 pins Canon connector and the USB port of the CPE.

The features supported are the same as described below

How to start a CLI session

This section describes the CLI commands. Before accessing ATOSNT from CLI, you must:

- connect the PC to the device with the supplied console cable (MiniDin 8 pinout to DB-9);
- start the terminal emulation software, such as Windows HyperTerminal, and configure the serial port with the following parameters:

1. bits per second = 9.600;
2. data bits=8;
3. parity=none;
4. stop bits=1;
5. flow control = none;

Now you can switch on the device and start the configuration procedure. To access the CLI enter the username (1 character at least) and leave the password field empty. Once you have accessed the CLI, you can change the password as desired.

Table 1 explains how to access the CLI and navigate through the nodes.

Table 1: CLI navigation

Prompt	How to enter	How to exit
User name:	Enter any character	
Password:	The password field is empty by default; you can configure different passwords to differentiate User level from Administrator level.	
ATOSNT>	You have logged in as User. You can only view the configuration and make diagnostics tests (ping, atmping, etc). You cannot change the configuration parameters.	Enter quit to go back to User name:.
ATOSNT>>	You have logged in as Administrator. You have a full control over the device.	Enter quit to go back to User name:.
ATOSNT>>eth0 ATOSNT\eth0>> ATOSNT>>ATM ATOSNT\ATM>>quit	Enter the interface name (Eth0, Wanx) to access the configuration mode. Multiple commands are available for each node.	Enter top to go back to ATOSNT>> from any node. Enter quit from any node to exit the system. The next prompt is User name: .
ATOSNT\eth0>>port1 ATOSNT\eth0\port1>>up ATOSNT\eth0>>	You can access all nodes in cascade mode by entering the name of the most internal node from the most external node.	Enter up to go to the higher node, without going back to ATOSNT>>.

How to use the help or (?) commands

When you need help on commands or options you can use the **help** command or the **?** command.

Table 2: help and ?

Prompt	Description
ATOSNT>>help ATOSNT>>?	The help or ? command shows the commands and subnodes that are available in the current node.
ATOSNT\eth0>>help ATOSNT\eth0>>? ATOSNT>>help eth0	You can limit your search to a specific node. To do this, you can access the desired node and enter help (or ?) or you can add the node name to help.
ATOSNT\eth0>>set ? ATOSNT\ip\route>>add ?	The meaning changes if you enter the question mark after the set or add commands. In this case the syntax and configurable options are shown.

The <Tab> key can be used either as editing accelerator to complete “keywords”, or to togle to every possible command/node starting from the given digit.

The CLI syntax

The following syntax is used in the CLI:

- < > identifies a parameter;
- <value> indicates a numeric parameter;
- <string> indicates an alphanumeric parameter;
- <ip add> indicates an ip address with aaa.bbb.ccc.ddd format(for example 10.0.0.1);
- <ip name> indicates an ip host name, for example with www.xxx.ddd.com format (www.aethra.com [1]);
- the symbol | indicates an alternative parameter. For example, <value | TCP | UDP > indicates that the parameter can be a number, TCP or UDP keyword.

Configuration Commands

There are two types of configuration commands:

- Node-related commands:

  these commands can be used only if you are in the correct node. For example, the **download** command can only be used in the root node and is not accepted in any other node;

- General commands:

  these commands can be used in any node.

Node-related commands

This is an example of the Node-related commands:

```
download               Downloads a file from a server on node ATOSNT>>
upload                 Uploads a file to a server on node ATOSNT>>
logins                 Shows a list of logs on node ATOSNT\system>>
password               Sets user/admin/others passwords on node ATOSNT\system>>
privilege              Creates and configures privilege on node ATOSNT\system>>
list                   Lists the drive contents on node ATOSNT\storage>>
remove                 Removes the drive safely on node ATOSNT\storage>>
create                 Creates a file or folder on node ATOSNT\storage>>
erase                  Cancels a file or folder on node ATOSNT\storage>>
copy                   Copies a file or folder on node ATOSNT\storage>> and others
rename                 Renames a file or folder on node ATOSNT\storage>>
bitpertone             Retrieves the number of the bits per each tone on node ATOSNT\xdsl0>>
modify                 Modifies the mac address mode on node ATOSNT\wlan0\ap\mac-filter>>
connect                Opens a session on node ATOSNT\interfaces\eth0>>
disconnect             Closes a session on node ATOSNT\interfaces\eth0>>
loopeth                Enables/disables ethernet loop on node ATOSNT\interfaces\eth0>>
no-keepalive           Enables/disables no-keepalive on node ATOSNT\interfaces\eth0>>
clear                  Clears all entries on node ATOSNT\dhcpserver>> and others
npm-responders-status  Shows the responders status on node ATOSNT\npm>>
......
```

General commands

These are some of the General Commands that you can find in ATOSNT. To learn more about them read bellow; for each command you will find the following information:

- command definition
- command syntax with the CLI
- command parameters configuration (see tables)

```
up                      Moves one step up from the current node
top                     Backs to the root of the tree
quit                    Exits from CLI session
set                     Sets node options
add                     Adds a new option
del                     Removes an added option
conf                    Shows the configuration in CLI command format
full-conf               Shows full configuration in CLI command format
show                    Shows 'ATOSNT' settings
delete                  Deletes statistics
tree                    Shows the tree structure of CLI interface
help                    Helps with the item
info                    Shows the system informations
date                    Shows or allows to set the system date and time
save                    Saves the configuration data
restart                 Restarts the device
telnet                  Opens a telnet client session
ping                    Sends an ICMP ECHO request
atmping                 Sends an ATM loopback cells
tracert                 Displays a trace of the packet transmission
mtrace                  Displays a path for a multicast group
resolve                 Resolves a IP address or IP name
log                     Log Management
dump                    Dumps a system internal file
show-logging-level      Shows the logged level
.....
```

Tracert

Reports the hops from the source to the destination host.

```
tracert <dest host>[ttl <max hops>][timeout <timeout(sec)>][source <ip add|ifc>][numeric-only]
```

Table 3: tracert

Syntax	Description
dest host [max 128 char]	Ip address or name of the destination host (only if a DNS is configured in the device).
ttl <max hops> [1-255]	Specifies the maximum number of hops in the path to reach the destination (default: 30).
timeout <timeout(sec)> [2-86400]	Wait/answer timeout in seconds for each attempt (default: 2 seconds).
source <ip add | ifc > [0-15 char]	Defines the source ip address or the interface to use for the tests.
numeric-only	Only displays the address list (not the hop hosts).

Mtrace

Displays a path for a multicast group

```
mtrace <source host> [address <receiver>] [mgroup <group>] [options]
```

Table 4: mtrace

Syntax	Description
source host [max 128 char]	Ip address or name of the source host (only if a DNS is configured in the device).
address [max 128 char]	Ip address or name of the receiver host (name only if a DNS is configured in the device).
mgroup [aa.bb.cc.dd from 224.0.0.1 to 239.255.255.255]	Ip address of multicast group to which the receiver belongs to. If not specified default group is 224.2.0.1.

Options

Syntax	Description
timeout (sec) [2-86400]	Time (in seconds) to wait for a trace response (default 3 seconds).
ttl [1-255]	The *ttl* (time-to-live, or number of hops) for multicast trace queries and responses. Default is 64, except for local queries to the "all routers" multicast group which uses ttl 1.
stats-interval [1-1000]	The interval (in seconds) between statistics gathering traces (default 10 seconds).
extra-hops [0-60]	The number of extra hops to trace past nonresponsive routers.
source [0-15 char]	Local interface for sending the trace query.
gateway [aa.bb.cc.dd]	The last-hop router on the path from the intended *source* to the *receiver*, to send the trace query via unicast directly to the multicast router *gateway* rather than multicasting the query
max-num-of-hops [0-60]	The maximum number of hops that will be traced from the *receiver* back towards the *source*. Default is 32 hops.
num-of-queries [1-65535]	The maximum number of query attempts for any hop to *n*. Default is 3.
dest-for-response [aa.bb.cc.dd]	Send the trace response to *host dest-for-response* rather than to the host on which mtrace is being run, or to a multicast address other than the one registered for this purpose (224.0.1.32).
numeric-only [numeric-only]	Print hop addresses numerically rather than symbolically and numerically.
no-router-alert [no-router-alert]	The router alert IP option will not be added in the IP packet header.
verbose [verbose]	Show hop times and statistics display.
loop [loop]	Loop indefinitely printing packet.
mcast-in-resp [mcast-in-resp]	The response packet is forced to be sent in multicast.

passive-mode [passive-mode]	Listen passively for multicast responses from traces initiated by others.
loop-no-stats [loop-no-stats]	Loop indefinitely printing packet without statistics.
short-form [short-form]	Print output not including packet rate and loss statistics.
unicast-in-resp [unicast-in-resp]	The response packet is forced to be sent in unicast.
tunnel-stat [tunnel-stat]	Tunnel statistics mode: show loss rates for overall traffic.

Ping

Checks if the host can be reached. The device sends a special packet (ICMP Echo Request) to the destination host. The destination host acknowledges receipt with an ICMP Echo Reply packet.

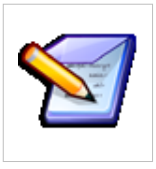
```
ping <dest host>[size <size-value>][tries <tries-value>][ttl <ttl-value>][timeout   <timeout(sec)>]
[numeric-only][continuous][quiet][source <ip add|ifc>]
```

Table 5: ping

Syntax	Description
dest host [max 128 char]	Ip address or name of the destination host (only if a DNS is configured in the device).
size <size-value>	Packet length (default: 32).
tries <tries-value>	Number of echo requests (default: 3).
ttl <ttl-value>	"Time-to-live" (ttl) parameter (default: 64).
timeout <timeout(sec)>	Wait/answer timeout in seconds for each attempt (default: 2 seconds).
numeric-only	Only displays the address list
Continuous	A continuous ping is sent to the “dest host” untill “Ctrl-C” sequence is pressed.
quiet	A “silent” ping sequence is sent to the “dest host”. At last only the summary result is shown.
source <ip add | ifc>	Defines the source ip address or the interface to use for the tests.

Atmping

Checks the connection integrity over the ATM network. The device sends a special loopback cell over the VPI and VCI. Once it has reached the destination, the cell is re-transmitted by the receiver.

	In ATM connections, VPI and VCI are permanent values assigned by the network administrator. For more information on values contact the network administrator.

```
atmping [F5-ETE|F5-STS|F4-ETE|F4-STS][ATMport_name]<vpi>[vci][tries <number tries>][continuous][quiet]
```

Table 6: atmping

Syntax	Description
F5-ETE	Generates a F5 loopback cell of end-to-end type (default).
F5-STS	Generates a F5 segment-to-segment ATM ping.
F4-ETE	Generates a F4 loopback cell of end-to-end type
F4-STS	Generates a F4 segment-to-segment ATM ping.
ATMport_name	In case of multiple ATM ports, it is possible to select which one will be used
vpi	VPI value (Virtual Path Identifier).
vci	VCI value (Virtual Channel Identifier).
tries <number tries>	Number of loopback requests (default: 5).
continuous	Number of loopback cell requests to infinity, alternatively to option “tries”. The operation ends when you press Ctrl-C.
quiet	A “silent” loopback cell requests sequence is sent. At the end only the summary result is shown.

Resolve

Resolves an IP address in a host name or a host name in an IP address. The <ip-add | ip-name> parameter can be the IP address or the name of the host to resolve.

```
resolve <ip-add|ip-name>
```

date

The command returns you the date and time when you call it without any options. If you want to set the local date and time you can use the following syntax:

```
ATOSNT>>date ?

date  help :  Show or setting system date and time
date  usage:
 [dd mm yyyy hh mm ss]

date command parameters:
 day     [1-31]
 <cr>
```

```
ATOSNT>>date
Date Monday 08 June 2015 Time 09:00:19
Command executed
```

Table 7: resolve

Syntax	Description
ip-add | ip-name	Ip address or name of the host to resolve.

Table 8: Other General Commands

Syntax	Description
show-logging-level	Shows the level of the current log session (e.g. administrator, user …)
Save	Saves the current configuration. All changes have been saved into the device and will be implemented when the device working conditions allows for it.
Tree	Shows the available nodes starting from the current one. When executed from the main node (root), it displays the entire node tree and allows to identify the parameter you want to change.
Help	Shows the available nodes starting from the current one, as well as the commands that can be applied for the current node.
Show Conf	Shows the configuration parameters of the current node and subnodes. The parameter values are not shown if the node is an ON/OFF configurable node and it is set OFF.
Show Work	Shows the working parameters of the current node and subnodes. If the node is configurable as ON/OFF and is set OFF, the node parameter values are not shown.
Up	Returns to the higher node.
Top	Returns to the main node (root).
Quit or ^R	Closes the CLI session (logout).
Info [verbose]	Displays information abour the device Hardware and Software versions. With the “verbose” option, you can get more details info.
↑↓	Displays the last typed commands

Prompt

The prompt **>>** preceded by the device name and the node path is always shown when you use the CLI for the configuration. The prompt is only preceded by the device name if you are in the main node.

For example, the following prompt is shown if you have assigned the name “ATOSNT” to the device:

ATOSNT>>

The prompt indicates that commands can be entered.

To change the current prompt, you should do this :

```
ATOSNT>>set system name PEPPE
Command executed
PEPPE>>
```

The command structure

The tree structure of the device is made up of the main node (root) and of the multiple subnodes. To reach the desired node, you can enter the subnode path or go from node to node until you reach the desired node.

To show the complete tree structure, you must enter the tree command from the main node. Look at an example:

```
ATOSNT>>tree
ATOSNT                    system                    timesync
                                                    intservices
                                                    privilege-map
                                                    scheduler
                          storage
                          xdsl0
                          eth0                      port1
                                                    port2
                                                    port3
                                                    port4
                          eth1
                          wlan0                     security
                                                    ap                        mac-filter
                          bri1
                          bri2
                          bri3
                          bri4
                          pots1
                          pots2
                          pots3
                          pots4
                          ptm                       ptm0
                          atm                       atm0
                          isdn                      isdn-bri1
                                                    isdn-bri2
                                                    isdn-bri3
                                                    isdn-bri4
                          point-to-point
                          aaa
                          syslog
                          bridges
                          classmap-profile
                          classifier-map
                          connectivity-monitor
                          interfaces                loopback0                 ip
                                                    eth0                      ip
                                                                              service-8023
                          firewall
                          dhcpserver
                          dhcpclient
                          security                  ike
```

```
                                    ipsec
                                    crypto
                    backup
                    dns             host
                    napt
                    arp
                    captive-portal
                    vrrp
                    ip              classifier
                                    network-groups
                                    route
                                    routemap
                                    rip
                                    ospf
                                    bgp
                                    multicast       igmp
                                                    pim
                    qos             p-fifo-default
                                    b-fifo-default
                    voip            call-setting    it
                                                    be
                                                    italy
                                                    belgium
                                    sip
                                    fax
                                    user-terminal
                                    terminal-group
                                    trunk
                                    call-mng
                    ddns
                    ethernet-oam
                    ethernet-cfm
                    sharing
                    snmp
                    tr069
                    npm

ATOSNT>>
```

Once you have identified the path to the subnode, you can enter the path directly.

Changing the system password

To change the local system password you should go to **password Command** section on the System node

How to show the system configuration

You can see the system configuration with the **show conf** command.

```
ATOSNT>>show conf
```

show conf shows the parameter configuration of the current node and of the active subnodes.

```
ATOSNT>>show work
```

show work command shows you the working parameters of the current node and of the active subnodes.

You can see the differences between configuration parameters and working parameters comparing **show conf** and **show work** results.

```
ATOSNT>>full-conf
```

Shows full configuration in CLI command format

```
ATOSNT>>conf ?

conf  help :  Show configuration in CLI command format
conf  usage:
 [which]

conf command parameters:
 which      [startup|default]
 <cr>
```

Shows the configuration in CLI command format.

- startup

  shows the parameters configuration realised by the user

- default

  shows the by default parameters configuration defined in a file according to the user requests.

How to save the configuration

When you save the configuration, you can see the changes in some configuration parameters. To see the changes in the other ones, you have to restart the device.

The **save** command is used to save modifications in a configuration file contained in a non-volatile memory. The file is loaded as the working configuration after typing the restart command.

Save command allows to save the current "user" configuration, as the default configuration. If you make a reset, the device will restart working with the "user" configuration, instead of the factory default configuration.

Notice that after the keyword "as-default", you must write the keyword "confirm" to avoid any mistake.

Look at the syntax of the command:

```
ATOSNT\system>>save ?

save  help :  Save configuration data
```

```
save  usage:
 [option]

save command parameters:
 option      [as-default]
 <cr>

ATOSNT\system>>save as-default ?

save command parameters:
 confirm     [confirm]

ATOSNT\system>>save as-default confirm

Command executed
```

Table : save

Syntax	Description
save	Keyword. Saves configuration data
as-default	Saves the user configuration as default configuration.
confirm	Keyword. Sets the current user configuration as the machine default configuration replacing the factory default configuration.

How to perform a reboot of the device and a default restore

To activate a new firmware after an upgrade or to activate a new configuration file, a reboot is necessary. To do that the following command is used:

```
ATOSNT>>restart ?
restart  help:  Restart device
restart usage:
   <option>[delay]

restart command parameters:
   option [no-save-conf|save-conf|restore-default-conf|restore-factory-default]
```

Table 9: restart

Syntax	Description
no-save-conf	A reboot is performed without saving the configuration
save-conf	A reboot is performed after saving the user configuration
restore-default-conf	This option removes all contents of the internal disks except: • firmware • default configuration • privilege configuration • imported web sites/app

restore-factory-default	This option removes all contents of the internal disks except: • firmware • default configuration.
delay (sec) [0-172800]	Specifies the time in seconds to delay to restart the device

How to upload a file to a PC

ATOSNT allows to upload a configuration file or a log file to a PC. This is possible using the CLI (or telnet/SSH), or the Web Browser with a FTP or TFTP server running on the PC.

The command to use via CLI is the following:

```
ATOSNT>>Upload ?

upload  help :  Upload file to a server
upload  usage:
 <TFTP><remote file name>[server-name][option]
 <FTP><remote file name>[server-name[:port]][option]
 <SCP><remote path/file-name>[server-name[:port]][option]
 <TO-DISK><local destination-file name>[option]

upload command parameters:
 protocol         [TFTP|FTP|SCP|TO-DISK]
```

Table 10: upload

Syntax	Description
TFTP | FTP | SCP | TO_DISK	Protocol type to use for the upload service.
remote file name [max 128 char]	File name to save (for example “my_config.txt).
server-name [:port][max 128 char]	Name or IP address and destination port of the host where the TFTP/FTP/SCP server is located.
port	Specifies the destination port
defaultconf| logs|nm-capture|local-file]	• If no option or “userconf” is used the user configuration file will be uploaded. • “defaultconf” the default configuration file stored into the device will be uploaded. • “logs” the log file stored into the device will be uploaded. • “nm-capture” the nm-capture is inherent to the "network-monitor" which allows to monitor one or more interfaces, and then to capture all the traffic in a file that can be upload it and view it offline at the PC using for example "wireshark" application or just to download it to the Pc at your convenience • “local-file” the given local-file will be uploaded.

How to download a file from a PC

Upgrading the operating system and the boot software is possible via CLI (or telnet/SSH) or the Web Browser, using a TFTP, FTP server on your PC.

The command to use via CLI is the following:

```
ATOSNT>>download ?

download  help :  Download file from a server
download  usage:
 <TFTP><remote file name>[server-name][option]
 <FTP><remote file name>[server-name[:port]][option]
 <SCP><remote path/file-name>[server-name[:port]][option]
 <HTTP><[username:password@]URL/file-name[:port]>[option]
 <FROM-DISK><local source-file name>[option]

download command parameters:
 protocol         [TFTP|FTP|HTTP|SCP|FROM-DISK]
```

Table 11: download

Syntax	Description
TFTP | FTP | HTTP | SCP | FROM_DISK	Protocol type to use for download service.
remote file name [max 128 char]	Name of the remote file to download into the device
server Name [max 128 char][:port]	Name or IP address and destination port of the host where the TFTP/FTP/HTTP/SCP server is located.
option [userconf|defaultconf|boot|firmware|package| banner-pre|welcome|license|local-file| certificate|banner-post]	• If no option or “userconf” option is used a configuration file will be downloaded; • “defaultconf” to download a default configuration file; • “boot” to download a boot file; • “firmware” to download a firmware • “package” to download a bundle file where different file types will be loaded. • “banner-pre” to download a welcome message to display before the login • “welcome” is a synonym of "banner-pre", kept for compatibility with older ATOSNT versions • “license” to download a license file • “local-file” to download a user local file. • “certificate” to download certificate for SSL protocols • “banner-post” to download a message to display after the login
server-name[:port]	Name or IP address or address:port of the host where the TFTP/FTP/HTTP/SCP server is located.

username:password@]URL/file-name[:port]	Username and password

Some of these parameters can be skipped if they have been configured in the relevant field on the “system” node

How to make a Prelogin and a Postlogin Banner

A banner is just a message that can be customized and displayed to the user.
ATOSNT offers the possibility to create and present welcome messages before the login and after the login.

There are two modes to create a banner; one is to write the message in a text file and then to import it using the "download" command; the other one is to use the "banner" command and the built-in nano editor to write the text of the message.
For more details, look at below

Making a Prelogin Banner with Download Command

A Prelogin Banner is a message to present the user before making the login.
Start writing the message and save it as a text file with name "**BannerPrelogin.txt**" for example.
Then use the download command to import the file

```
ATOSNT>>download TFTP BannerPrelogin.txt 192.168.111.36 banner-pre
Starting...
Downloading 'BannerPrelogin.txt' using TFTP protocol
BannerPrelogin.txt   100% |*******************************|  1305   0:00:00 ETA

Writing File! Do Not turn off!

Command executed
```

To check the result, you should open a telnet session and access the CPE

```
Entering character mode
Escape character is '^]'.


Thanks for choosing Aethra Telecommunications technology !!!


You can proceed with the login.........


--------------------------------------------------------------------------------
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.
You must have explicit permission to access or configure this device.
All activities performed on this device may be logged based on the Service Provider Security Policy.
Any violations of this policy may result in disciplinary action and may be reported to law enforcement.
--------------------------------------------------------------------------------
L'ACCESSO NON AUTORIZZATO A QUESTO DISPOSITIVO E' PROIBITO.
Per accedere o configurare questo apparato e' necessario ottenere un permesso esplicito.
Le violazioni a questa politica possono comportare azioni disciplinari e possono essere comunicate all'Autorita' Giudiziaria.
Le leggi sulla Privacy non sono vigenti per l'utilizzo di questo apparato.


login as:
```

Note that after displaying the welcome message, the system is asking for the login name and password information

Making a Prelogin Banner with Banner Command

```
ATOSNT>>banner ?

banner  help :  Edit pre and post login banners
banner  usage:
[pre-login|post-login]
banner command parameters:
type                 [pre-login|post-login]
ATOSNT>>banner pre-login ?

banner command parameters:
<cr>
```

At this point the built-in nano text editor appears and allows you to start editing the message text. Look at the below example

```
GNU nano  2.2.6       File:./DiskB/wmsg

Thanks for choosing Aethra telecommunications Technology !!!
You can proceed with the login.........

--------------------------------------------------------------------------------
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.
You must have explicit permission to access or configure this device.
There is no right to privacy on this device.
--------------------------------------------------------------------------------
L'ACCESSO NON AUTORIZZATO A QUESTO DISPOSITIVO E' PROIBITO.
Per accedere o configurare questo apparato e' necessario ottenere un permesso.



                              [ Read 8 lines ]
^G Get Help  ^O WriteOut  ^W Where Is  ^V Next Page ^U UnCut TextM-? Last Line
^X Exit      ^R Read File ^Y Prev Page ^K Cut Text  M-| First Lin^_ Go To Line
```

Making a Postlogin Banner with Download Command

A Postlogin Banner is a message to present the user after making the login.
Start writing the message and save it as a text file format with name "**BannerPostlogin.txt**". Then use the download command to import the file

```
ATOSNT>>download TFTP BannerPostlogin.txt 192.168.111.36 banner-post ?

download command parameters:
 expected size         [0-1000000000]
 <cr>
ATOSNT>>download TFTP BannerPostlogin.txt 192.168.111.36 banner-post
Starting...
Downloading 'BannerPostlogin.txt' using TFTP protocol
BannerPostlogin.txt  100% |*******************************|   927   0:00:00 ETA
```

```
Writing File! Do Not turn off!

Command executed
```

To check the result, you should open a telnet session and access the CPE.
Look at below for more details

```
ATOSNT Remote CLI


CTRL+d to exit


Init Command Line Interface...
ATOS Version: 6.0.0.rc1 (2@BVMEDtjuukbpjWcwovv)
ATOS Date: 21/05/2014 10:16
ATOS License: FullFeatures
Hardware: SV6044VW - 2320B
Product Code: 708190244
Serial Number: 310638
eth0 MAC Address: 00:D0:D6:48:87:E7
Wireless card: Atheros Communications, Inc. - AR9227 Wireless Network Adapter


User name :a
Password :
<a> logged at Administrator level


You have been successful with the login


Go to Start Menu and enjoy Aethra Technology !!!
--------------------------------------------------------------------------------
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.
You must have explicit permission to access or configure this device.
All activities performed on this device may be logged based on the Service Provider Security Policy.
Any violations of this policy may result in disciplinary action and may be reported to law enforcement.
--------------------------------------------------------------------------------
L'ACCESSO NON AUTORIZZATO A QUESTO DISPOSITIVO E' PROIBITO.
Per accedere o configurare questo apparato e' necessario ottenere un permesso esplicito.
Le violazioni a questa politica possono comportare azioni disciplinari e possono essere comunicate all'Autorita' Giudiziaria.
Le leggi sulla Privacy non sono vigenti per l'utilizzo di questo apparato.
ATOSNT>>
```

Making a Postlogin Banner with Banner Command

```
ATOSNT>>banner ?

banner  help :  Edit pre and post login banners
banner  usage:
[pre-login|post-login]
banner command parameters:
type                 [pre-login|post-login]
```

```
ATOSNT>>banner post-login ?

banner command parameters:
<cr>
```

At this point the built-in nano text editor appears and allows you to start editing the message text. Look at the below example

```
GNU nano  2.2.6       File:./DiskB/wmsg-post


You have been successful with the login


Go to Start Menu and enjoy Aethra Technology !!!

--------------------------------------------------------------------------------

UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.

You must have explicit permission to access or configure this device.

All activities performed on this device may be logged based on the Service Provider Security Policy.

Any violations of this policy may result in disciplinary action and may be reported to law enforcement.

--------------------------------------------------------------------------------

L'ACCESSO NON AUTORIZZATO A QUESTO DISPOSITIVO E' PROIBITO.

Per accedere o configurare questo apparato e' necessario ottenere un permesso esplicito.

Le violazioni a questa politica possono comportare azioni disciplinari e possono essere comunicate all'Autorita' Giudiziaria.

Le leggi sulla Privacy non sono vigenti per l'utilizzo di questo apparato.


                                [ Read 8 lines ]

^G Get Help  ^O WriteOut  ^W Where Is  ^V Next Page ^U UnCut TextM-? Last Line

^X Exit      ^R Read File ^Y Prev Page ^K Cut Text  M-| First Lin^_ Go To Line
```

How to show ATOSNT Software Version

If you want to know what ATOSNT software version is running in your CPE, use **info** command.

```
ATOSNT>>info
ATOS Version: 5.6.9 (2@BVMEDtjuukbpjWcwovv)
ATOS Date: 08/07/2013 11:29
ATOS License: TR069+AdvancedPlus
Hardware: SV6044VW - 2320B
Product Code: 708190244
Serial Number: 310638
eth0 MAC Address: 00:D0:D6:48:87:E7
Wireless card: Atheros Communications, Inc. - AR9287 Wireless Network Ar
Command executed
```

With **info verbose** command, you can get more information, see below

```
ATOSNT>>info verbose
ATOS Version: 5.6.9 (2@BVMEDtjuukbpjWcwovv)
ATOS Date: 08/07/2013 11:29
ATOS License: TR069+AdvancedPlus
Hardware: SV6044VW - 2320B
Product Code: 708190244
```

```
Serial Number: 310638
eth0 MAC Address: 00:D0:D6:48:87:E7
Wireless card driver: 9.2.0_U10.1020 - WPA/802.1x: ersion
dsl api release version: VDSL2_R10_ADSL_R6_oPOTS_CPE_30012009
dsl modem fw version: 9.6.3.2.0.5
dsl modem drv api version: 3.18.3
dsl modem mei bsp version: 1.6.9
dsl modem chip type: Ifx-Vinax
dsl modem hw version: VINAX-DFE_V1.4
LINUX kernel  : 2.6.35.3-SV6044 #40 Thu May 16 12:08:19 CEST 2013
Boot Loader   : U-Boot 2010.06.2.1.6 (May 03 2013 - 13:05:03) A.Tlc-SV64
CPLD Version  : 6
HW Device Id  : 133
CLEI Code     :
ATOSNT distro : 'V_5_6_X' (r12509) for SV6044V
FIRMWARE Image 1 (RUNNING, BOOTING)
 Firmware format : ATOS image
 Firmware version: SV6044V-fw-5.6.9-r12509
 Firmware date   : Mon Jul  8 10:31:39 2013
 Firmware size   : 15628/31232KB (50%)
FIRMWARE Image 2 (NOT-RUNNING)
 Firmware format : ATOS image
 Firmware version: SV6044V-fw-5.6.4-r12196
 Firmware date   : Thu May 30 11:37:38 2013
 Firmware size   : 15740/31232KB (50%)
Command executed
```

How to Swap Firmware

Important Note

Starting from ATOSNT Release 5.6.X and for CPEs that support dual image firmware, the swap-firmware is automatically run after the firmware download. To start the new firmware image, you should make a reboot with restart command (there is no longer need to use the swap-firmware command).

To learn more about how **swap-firmware** command works, look at the below section.

Start finding out what version of ATOSNT is installed in the CPE, look at here How to show ATOSNT software version

When you download a new ATOSNT firmare, this is saved in the flash memory but it is not running yet.

Actually in the flash memory there is a partition that allows to allocate 2 firmwares:

- firmware image 1 is the software version that is currently running on the CPE
- firmware image 2 instead is another software version that acts as a backup.

With "swap firmware" command you are instructing the CPE to change the current running software version from firmware image 1 to firmware image 2.

Warning: "firmware image 2" will be effective from next system restart

```
ATOSNT>>swap-firmware
Checking for swapping the FIRMWARE from image 1 to 2
```

```
 Firmware format : ATOS image
 Firmware version: SV6044V-fw-5.6.4-r12196
 Firmware date   : Thu May 30 11:37:38 2013
 Firmware size   : 15740/31232KB (50%)
Update bootloader settings...
FIRMWARE Image 2 will be used from next system restart
Command executed
```

Example of how to download a new software release of ATOSNT from your PC

Suppose that you have saved on your PC desktop the file (named bundle_12196sv6044v) you want to download it into the CPE.
To do this we will use TFTP protocol and a free application programm (it is the FTTP Server) like "Tftpd32 by Ph. Jounnin" already installed on your PC.
Follow the next steps:

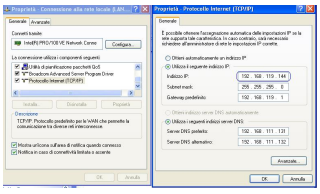
- **Start looking for the IP address of your PC and the CPE and make sure that both are installed on the same subnet.**

Looking for the CPE IP address:

ATOSNT>>set interfaces eth0 ip dhcp-client on
Command executed

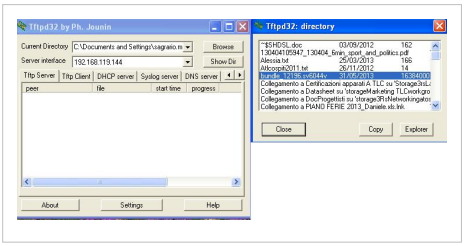
ATOSNT\interfaces\eth0>>show work
Show of ATOSNT interfaces eth0 ip
Level of log : 1
IP address : **192.168.119.50**
Netmask : 255.255.255.0
Default router : 192.168.119.1
MTU value : 1500
DHCP client : on
TCP MSS adjustment : path-mtu
Tx queue len : 1000

Looking for your PC IP address:



- **Launch Tftpd32 application**

Click **Browse** bottom and choose **Desktop**, then clik **Show Dir** and select the file's name bundle_12196sv6044v :



- **Download the file**

Downloading the file with FTTP protocol. "Server name" is just your PC IP address

ATOSNT>>download TFTP bundle_12196.sv6044v ?

download command parameters:
server Name [max 128 char]
option [userconf|defaultconf|boot|firmware|package|welcome|
license|local-file|certificate]
<cr>
ATOSNT>>download TFTP bundle_12196.sv6044v **192.168.119.144** package
Starting...
Downloading 'bundle_12196.sv6044v' using TFTP protocol
bundle_12196.sv6044v 100% |*******************************| 16000k 0:00:00
ETA
Checking bundle...
Received file is a valid bundle. Installing...
Executing pre-installation stage...
Installing ATOSNT package release 5.6.4...
Firmware format : ATOS image
Firmware version: SV6044V-fw-5.6.4-r12196
Firmware date : Thu May 30 11:37:38 2013
Bundle include bootloader image. Updating...
Writing File! Do Not turn off!
Erasing memory blocks
Erasing block: 2/2 (100%)
Writing kb: 248/248 (100%)
Bundle include firmware image. Updating...
Use firmware partition 2 (NOT-RUNNING)
Writing File! Do Not turn off!
Erasing memory blocks
Erasing block: 123/123 (100%)
Writing kb: 15740/15740 (100%)
Executing post-installation stage...
ATOSNT package release 5.6.4 installed
Command executed

- **Swap Firmware**

Swapping the FIRMWARE from image 1 to 2

WARNING: you have downloaded the new software version but it is not running yet on the CPE !!!.
Be aware that starting from ATOSNT Release 5.6.X and for CPEs that support dual image firmware, the swap-firmware is automatically run after the firmware download. To start the new firmware image, you should make a reboot with restart command (there is no longer need to use the swap-firmware command).
To learn more about how swap-firmware command works, look at the below section.

Actually in the flash memory there is a partition and 2 firmwares are saved: the one that is currently running on the device and the second one that acts as a backup.
With "swap firmware" command you are instructing the CPE to substitute the current firmware image 1 with firmware image 2 that you have just downloaded it.
ATOSNT>>swap-firmware
Checking for swapping the FIRMWARE from image 1 to 2
Firmware format : ATOS image
Firmware version: SV6044V-fw-5.6.4-r12196
Firmware date : Thu May 30 11:37:38 2013
Firmware size : 15740/31232KB (50%)
Update bootloader settings...
FIRMWARE Image 2 will be used from next system restart
Command executed

- **Use restart command or push on/off switch to make effective the new software version**

ATOSNT>>restart no-save-conf
System will be restarted in 1 sec
Command executed
ATOSNT>>Restarting...
.
ATOS-NT boot system V2.1.6
Starting OS.....Done
Starting ATOSNT...
ATOSNT is running
VDSL2 over POTS FW file is available
ADSL2plus/2/1 Annex A FW file is available
VDSL2 over ISDN FW file is available
ADSL2plus/2/1 Annex B FW file is available
Init Command Line Interface...
ATOS Version: 5.6.4 (6@BVMEDtjuukbpjWcwovv)
ATOS Date: 30/05/2013 12:35
ATOS License: TR069+AdvancedPlus
Hardware: SV6044VW - 2320B
Product Code: 708190244
Serial Number: 310638
eth0 MAC Address: 00:D0:D6:48:87:E7
Wireless card: Atheros Communications, Inc. - AR9287 Wireless Network Adapter

- **Whenever you need, use "info verbose" command to check what ATOSNT software version is running on your CPE**

ATOSNT>>info verbose

ATOS Version: 5.6.4 (6@BVMEDtjuukbpjWcwovv)

ATOS Date: 30/05/2013 12:35

ATOS License: TR069+AdvancedPlus

Hardware: SV6044VW - 2320B

Product Code: 708190244

Serial Number: 310638

eth0 MAC Address: 00:D0:D6:48:87:E7

Wireless card driver: 9.2.0_U10.1020 - WPA/802.1x: ersion

dsl api release version: VDSL2_R10_ADSL_R6_oPOTS_CPE_30012009

dsl modem fw version: 9.6.3.2.0.5

dsl modem drv api version: 3.18.3

dsl modem mei bsp version: 1.6.9

dsl modem chip type: Ifx-Vinax

dsl modem hw version: VINAX-DFE_V1.4

LINUX kernel : 2.6.35.3-SV6044 #40 Thu May 16 12:08:19 CEST 2013

Boot Loader : U-Boot 2010.06.2.1.6 (May 03 2013 - 13:05:03) A.Tlc-SV6044

CPLD Version : 6

HW Device Id : 133

CLEI Code :

ATOSNT distro : 'V_5_6_X' (r12196) for SV6044V

FIRMWARE Image 1 (**NOT-RUNNING**)

Firmware format : ATOS image

Firmware version: SV6044V-**fw-5.6.1**-r11936

Firmware date : Wed May 8 12:34:48 2013

Firmware size : 15684/31232KB (50%)

FIRMWARE Image 2 (**RUNNING**, BOOTING)

Firmware format : ATOS image

Firmware version: SV6044V-**fw-5.6.4**-r12196

Firmware date : Thu May 30 11:37:38 2013

Firmware size : 15740/31232KB (50%)

Command executed

Event logs

In ATOSNT, it is possible to record and manage the event logs that are helpful for troubleshooting. An event log is a file that contains events, which are entries to the log that notify the user of some occurrence relating to the operating system, network connection or applications running on the system.

The log level is configured for every single node. The list of events can be shown on the console port or by connecting to the Telnet internal server. The log files can be saved on an external storage memory (eg. USB) or on the CPU memory which is the default behavior.

When enabling logs, you must take into account that, depending on working conditions and amount of logs, performances of the equipment can be affected by logs themselves.

The following commands are available in any position of the different menus, with the exception of the **set loglevel** command that can only be given in enabled subnodes.

```
ATOSNT>>log ?

log  help :  Log Management
log  usage:
  <CONSOLE>[file]
  <START>[file]
  <STOP>[file]
  <FILE>
  <VIEW>[[type]<param>]

log command parameters:
 log type             [console|start|file|stop|view]
```

Table 12: log commands

Syntax	Description
log console	Shows the log events on the console. The visualization can be interrupted by pressing any key and restarted with the "log console" command.
log console file	Shows the log events on the console and save the log file on an external storage memory (eg. USB) or on the CPU memory which is the default behavior . The visualization can be interrupted by pressing any key, while capturing in file is interrupted by command "log stop file".
log start	Shows the log events "live" on the console. The visualization is interrupted by typing “log stop ” command.
log start file	Shows the log events on the console and save the log file on an external storage memory (eg. USB) or on the CPU memory which is the default behavior. The visualization can be interrupted by the "log stop" command, while capturing in file is interrupted by “log stop file” command.
log stop	Stops showing log events “live” on console.
log stop file	Stops capturing log events in an external storage memory (eg. USB) or on the CPU memory which is the default behavior.
log file	Saves the log events on an external storage memory (eg. USB) or on the CPU memory which is the default behavior. Capturing in file is interrupted by command “log stop file”.
log view [[type]<param>]	Shows the last acquisition made and saved on file. The logs capture must previously be stopped with “log stop file” command. The device returns: Nothing to show if the file contains no element.
type	• severity: specifies one level of severity to be shown • source: specifies the log source
param	• type severity: [error|warning-1|warning-2|log-1|log-2|debug-1|debug-2] • type source: name of the log source (e.g OFdsp)
set loglevel [0-5] [-s]	Configures the detail level used by ATOSNT to record the events: • 0 no type of anomalous event is saved; • 1 errors (i.e. protocol errors); • 2 errors and first level warnings; • 3 errors and second level warnings; • 4 errors, first and second level warnings, first level signaling; • 5 errors, first and second level warnings, first and second level signaling; • -s when you select this option from a node, ATOSNT configures the same log level on the current node and subnodes. This command cannot be executed from the main node.

[1] like Windows HyperTerminal

Index

References

[1] http://www.aethra.com/

ManARP

ARP node

Address Resolution Protocol (ARP) is a link layer protocol that allows to find the host's MAC address when its IP address is only known.

ARP protocol operates on local area networks or in a point-to point link. In particular on Ethernet networks, when a host wants to know the MAC address of another host, it sends an ARP request to the broadcast MAC address; each host in the LAN verifies, by ARP protocol, if the target address is its own IP address and if so it dispatches to the sender an unicast ARP REPLY containing its own MAC address.

ARP protocol in each host of the LAN stores the data of responses in a cache, where the single address resolution entry contains the association between IP address and MAC address as well as its timeout. Receiving a packet from a host entails the reset of address resolution entry timeout, whilst if no packets are received from a host within the timeout the address resolution entry is removed.

Furthermore it can often be useful to add permanent entries in the ARP cache, since these are not timeout dependent.

Starting from root node “arp” node occurs, where following actions can be carried out:

- Adding/deleting static ARP table entries by **add/del** command;
- Deleting one/all nonstatic entries by **clear** command;
- Modifying ARP timeout value of nonstatic entries by **set** command;
- Modifying, in ARP requests sent, the IP source address used by **set** command;
- Displaying static configuration by **show conf** command;
- Displaying complete configuration by **show work** command;
- Displaying ARP cache by **show status** command;
- Displaying per interface statistics of ARP packets by **show statistics** command.

```
ATOSNT\arp>>add ?

add  help:  Add an ARP static entry
add  usage:
 <ip address><mac address>

add command parameters:
 ip address  [aa.bb.cc.dd]

ATOSNT\arp>>add 192.168.110.3  00-00-aa-9a-0e-c2
Command executed

ATOSNT\arp>>show conf
Show of ATOSNT arp
```

```
Level of log      : 1
Used local address: any-addr

LIST OF ARP ENTRIES
 IP ADDRESS          MAC ADDRESS
 192.168.110.3       00-00-AA-9A-0E-C2
Command executed

ATOSNT\arp>>show work
Show of ATOSNT arp
Level of log      : 1
Used local address: any-addr

LIST OF ARP ENTRIES
 IP ADDRESS          MAC ADDRESS
 192.168.110.3       00-00-AA-9A-0E-C2
 192.168.110.1       00-0B-AC-38-F4-83
Command executed

ATOSNT\arp>>show status
IP ADDRESS          FLAGS          HW ADDRESS          DEVICE
192.168.110.3       static         00-00-AA-9A-0E-C2   eth1
192.168.110.1       dynamic        00-0B-AC-38-F4-83   eth1
Command executed

ATOSNT\arp>>clear ?

clear  help:  Clear dynamic ARP entries
clear  usage:
 [ip address]

clear command parameters:
 ip address  [aa.bb.cc.dd]
 <cr>

ATOSNT\arp>>set ?

Set command parameters:
 level of log        [loglevel]         Current value: 1
 used local address  [used-local-addr]  Current value: any-addr
```

Table 1: add

Parameter	Description
ip address [aa.bb.cc.dd]	Indicates the IP address of the entry to be created. This is a mandatory field.
mac address [aa.bb.cc.dd.ee.ff]	Indicates the mac address (hardware, Ethernet) of the entry to be created. This is a mandatory field.

Table 2: del

Parameter	Description
ip address [aa.bb.cc.dd]	Indicates the IP address of the entry to be removed. This is a mandatory field.

Table 3: clear

Parameter	Description
ip address [aa.bb.cc.dd]	Indicates the IP address of the entry to be removed. This is an optional field. If missing, all ARP table entries will be deleted.

Table 4: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the arp events. Default:1
used-local-addr [any-addr|addr-in-subnet|ifc-addr]	Defines the local source IP address used in the ARP requests. • **any-addr** Use any local address configured on any interface. • **addr-in-subnet** Try to avoid local addresses that are not in the target's subnet for this interface. This mode is useful when target hosts reachable via this interface require the source IP address in ARP requests to be part of their logical network configured on the receiving interface. When we generate the request we will check all our subnets that include the target IP and will preserve the source address if it is from such subnet. If there is no such subnet we select the source address according to the rules for "ifc-addr". • **ifc-addr** Always use the best local address for this target. In this mode we ignore the source address in the IP packet and try to select local address that we prefer for talks with the target host. Such local address is selected by looking for primary IP addresses on all our subnets on the outgoing interface that include the target IP address. If no suitable local address is found we select the first local address we have on the outgoing interface or on all other interfaces, with the hope we will receive reply for our request and even sometimes no matter the source IP address we announce. Default: any-addr

ManAutheAuthoAcc

Authentication, Authorization, Accounting

AAA stands for authentication, authorization and accounting. It refers to a security architecture for distributed systems, which enables control over which users are allowed access to which services, and how much of the resources they have used.

Authentication provides a way of identifying each user by login and password, challenge and response, messaging support and, depending on the security protocol selected, encryption.

Authorization checks and verifies the operations that the user is allowed to carry out in the network.

Accounting provides the possibility to trace the services that users are accessing and how much of the network's resources they are using.

ATOSNT implements the AAA authentication function using **RADIUS** (Remote Authentication Dial In User), **RAC** (Remote Access Configuration) of an internal user database and **TACACS+** protocols.

Authentication by RADIUS protocol

RADIUS protocol, based on a client/server model, carries authentication, authorization and configuration information between a NAS [1] and a RADIUS authentication server.

Transactions between the RADIUS client and server are authenticated using a shared private key.

The RADIUS client implemented in ATOSNT can support various authentication modes such as: login, PAP2 [2], CHAP3[3], MS-CHAP v1, MS-CHAP v2.

Authentication information can be provided to the RADIUS client:

- by the login prompt, when connecting to the device via serial or telnet
- by a link framing protocol such as PPP, for a VPN PPTP connection.

Once the client has obtained the information, it sends the server an Access-Request packet containing attributes such as username, password, ID client and port used.

If the password exists, it is encrypted using the MD5 alghoritm. If the client doesn't receive a reply from the server in a defined time period, the authentication request is sent a further three times. On failing to receive a reply from the first server, the client may send the request to other configured RADIUS servers. When authentication fails, the RADIUS server sends an Access-Reject packet that invalidates the user request. If the authentication conditions are satisfied, the RADIUS server sends an Access-Accept packet containing the information needed to supply the service requested. In PPP mode, for example, this information may include the keys for traffic encryption, wheras for the login it shows the device access level (user or admin).

For privilege management authentication the following attributes are needed (cfr RFC 2865):

- "Service-Type" attribute

  type = 6, length = 6, value = 6 for "Administrative User"

- "Vendor-Specific" attribute:

  type = 26, len ≥ 7, Vendor-Id (four octets) = 7745 for "aethra",

  Vendor type = 1 for"atlc-av-pair",

  Vendor length = <length>

  Attribute specific string=<format: attribute=value> example: shell:priv-lvl=15

  Note: Vendor-Id recognized in ATOSNT are only 7745 ("aethra") and 9 ("cisco"). See IANA Private Enterprise Numbers.

Authentication by TACACS+ protocol

TACACS+ protocol, based on a client/server model, is used to transfer authentication information between a NAS and a TACACS+ authentication server.

While RADIUS protocol uses UDP datagrams TACACS+ uses TCP datagrams.

Table 1:**TACAC+ user conf example**

```
# We also can define local users and specify a file where data is stored.
# That file may be filled using tac_pwd
user = mario {
default service = permit
login = cleartext mario
service = exec {
priv-lvl = 3
  }
}

user = rosa {
default service = permit
login = cleartext rosa
}
user = matteo {
default service = deny
login = cleartext matteo
service = exec {
priv-lvl = 1
  }
}
```

Authentication by RAC

RAC allows the creation of an authentication mechanism based on a local database containing a group of users. Group membership, password and access level (user, administrator, super-administrator) are specified for each database user. Data stored in the RAC database is used by NAS to validate the authentication request received from the user. For example, the username and password sent by the user for a login or a PPP authentication by PAP are compared with the recorded ones in the RAC database.

Authentication profiles

An authentication profile must be created in order to perform AAA authentication. Each profile can define up to two authentication modes: remote and local.

- Remote authentication

  can be achieved by towards one or more RADIUS and/or TACACS+ servers. In case more servers are defined they are sequentially addressed until one of them is successfully connected.

- Local authentication

  is based on RAC local database.In case for a single profile both RADIUS/TACACS servers and RAC data base are defined, the last one is only used if all RADIUS/TACACS servers are not reachable .

AAA - Commands

On **aaa** node, you can set, add and del the following parameters:

```
ATOSNT\aaa>>set ?

Nodes not available.
Set command parameters:
 level of log                           [loglevel]            Current value: 1
 local ip address (0.0.0.0 if notused)  [local-ip-address]    Current value: 0.0.0.0
 local ipv6 address                     [local-ipv6-address]  Current value: ::
```

Table 2: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the AAA events. Default: 1
local-ip-address [aa.bb.cc.dd]	Sets the client IP address. Default: 0.0.0.0
local ipv6 address [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]	Sets the client IPv6 address. Default: ::

Any value can be configured as "local ip address", but an interface should be created (e.g. loopback) in order to make it working.

ATOSNT\aaa>>set local-ip-address 192.168.110.77

Command executed

The log level (default is set to 1) can be changed from 0 to 5 to view internal events of the device with different detail level (max = 5)

ATOSNT\aaa>>set loglevel 5

Command executed

```
ATOSNT\aaa>>add ?

add  help:  Add a new AAA profile or a rac-account or rac-address
add  usage:
 <PROFILE><name>
 <RAC-ACCOUNT><name><user-name><password>[ProfileList]
 <RAC-ADDRESS><name><start-address><end-address>

add command parameters:
 PROFILE
 RAC-ACCOUNT
 RAC-ADDRESS
```

Table 3: add PROFILE

Syntax	Description
PROFILE	Keyword
name [max 16 char]	Sets the name of the new profile

Table 4: add RAC-ACCOUNT

Syntax	Description
RAC-ACCOUNT	Keyword
name [max 16 char]	Sets the name of a RAC Account group. Many accounts can belong to the same group (e.g. different access level). Entries created specifying the same group name automatically belong to the same group.
user-name [max 16 char]	Username of new RAC Account
password [max 32 char]	Password of new RAC Account
type [0-15|ADMIN|USER]	Access level of new RAC Account: • 0-15 choosing a number from 0 -15 you select an item in the "system privilege-map" on the System node, e.g. 0 corresponds to the association of the parameter "privilege level 0" to a certain privilege. • ADMIN Administrator access level • USER User access level
address [aa.bb.cc.dd|any]	Sets the IP address of some specific interface or the address of any other interface

Table 5: add RAC-ADDRESS

Syntax	Description
RAC-ADDRESS	Keyword
name [max 16 char]	Name of new RAC Address
start-address [aa.bb.cc.dd]	The first IP address of a range
end-address [aa.bb.cc.dd]	The last IP address of a range

Adding a new PROFILE under AAA node

ATOSNT\aaa>>add PROFILE Sales

Command executed

ATOSNT\aaa>>sales

ATOSNT\aaa\sales>>set ?

Adding a new RAC-ACCOUNT under AAA node (e.g. Production) with relevant user name and password, and defining the access level

ATOSNT\aaa>>add RAC_ACCOUNT Production Mario Pass ADMIN

Command executed

Adding a new RAC-ADDRESS, a range of IP address to be released (e.g. when acting as PPP server)

ATOSNT\aaa>>add RAC_ADDRESS 192.168.31.50 192.168.31.210

Command executed

```
ATOSNT\aaa>>del ?

del  help:  Remove a AAA profile or a rac-account or rac-address
del  usage:
 <PROFILE><name>
 <RAC-ACCOUNT><name><user-name>
 <RAC-ADDRESS><name>

del command parameters:
 PROFILE
 RAC-ACCOUNT
 RAC-ADDRESS
```

Table 6: del PROFILE

Syntax	Description
PROFILE	Keyword
name [max 16 char]	Name of the profile to be removed

Table 7: del RAC-ACCOUNT

Syntax	Description
RAC-ACCOUNT	Keyword
name [max 16 char]	Name of the RAC Account group to be removed.
user-name [max 16 char]	Username of the RAC Account to be removed.

Table 8: del RAC-ADDRESS

Syntax	Description
RAC-ADDRESS	Keyword
name [max 16 char]	Name of the RAC Address to be removed.

AAA\Profile name - Commands

```
ATOSNT\aaa>>add PROFILE Sales
Command executed

ATOSNT\aaa>>Sales
ATOSNT\aaa\sales>>set ?

Nodes not available.
Set command parameters:
 account name              [account-group]       Current value:
 nas identifier            [nas-id]              Current value:
 aaa server timeout (sec)  [aaa-server-timeout]  Current value: 5
```

```
 aaa server retries        [aaa-server-retries]  Current value: 4
 aaa authorization         [authorization]       Current value: off
 aaa accounting            [accounting]          Current value: off
```

Table 9: set

Syntax	Description
account-group	Name of the account group (created with "add rac-account") assigned to this profile. RAC authentication will be used if no RADIUS/TACACS+ server are defined or none is responding.
nas-id [max 32 char]	Sets the value of NAS identifier. It could be requested by the Authentication server.
aaa-server-timeout (sec) [1-300]	Sets the AAA server timeout. Default: 5
aaa server retries [1-999]	Sets the AAA server retries. Default: 4
authorization [on|off]	Enables/disables the AAA authorization. Default: off
accounting [on|off]	Enables/disables the AAA accounting. Default: off

```
ATOSNT\aaa\sales>>add ?

add  help:  Add a new server
add  usage:
 <name|server-ip-addr><key string>[authentication-port][server protocol]

add command parameters:
 name or server ip addr [max 256 char]
```

Table 10: add a new server

Syntax	Description
server-ip-addr [max 100 char]	RADIUS/TACACS+ server name can be specified either by its name or IP address.
key string [max 64 char]	Public key shared with the server
authentication-port [1-65535]]	Transport port used. Default: 1812 for RADIUS and 49 for TACACS+
radius|tacacs+	Sets the server protocol type

Adding a new SERVER RADIUS to a profile'

ATOSNT\aaa\sales>>add 192.168.31.201 pass 1812 radius

Command executed

ATOSNT\aaa\sales>>add 151.151.1.201 pass1 1812 radius

Command executed

ATOSNT\aaa\sales>>show work

Show of ATOSNT aaa sales

Account name :

NAS identifier :

AAA Server timeout (sec) : 5

AAA Server retries : 4

Show of ATOSNT aaa sales srv-192.168.31.201

Name or Server IP address : 192.168.31.201

Key : pass

Authentication port : 1812

Account port : 1813

Protocol type : radius

Show of ATOSNT aaa sales srv-151.151.201

Name or Server IP address : 151.151.201

Key : pass1

Authentication port : 1812

Account port : 1813

Protocol type : radius

Command executed

To enable the AAA profile for login authentication go to the System node and type: ATOSNT\system>>set aaa-profile AAAProfilename.

Notes

[1] Network Access Server

[2] Password Authentication Protocol

[3] Challenge Handshake Authentication Protocol

ManAtm

ATM Configuration

ATOSNT allows the configuration of multiple remote data connections. If you have subscribed multiple **ATM virtual circuits** with the Service Provider, you can establish simultaneous connections to different destinations provided that each destination is identified with VPI/VCI values.

For example, you can use one connection to reach your Internet Service Provider and another connection to reach the VoIP network or a Corporate LAN from a remote site.

On **ATM** node it's possible to create up to 8 VCC. The name assigned to the *Virtual Connection Channel* is **VCCx**, where x can have a value from 0 (VCC0) to 7 (VCC7). Once a new VCC has been created, this can be used on the Interfaces node to add and manage new virtual interfaces (for more details go to Interfaces node).

ATM – Commands

On **atm** node, you can set, add and del the following parameters:

```
ATOSNT\atm>>set ?

Available nodes:
                        atm0

Set command parameters:
 level of log  [loglevel]  Current value: 1
```

Table 1: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the ATM events (e.g. ATMPING command). Default: 1

To add a new VCC, you must use add command as follows:

```
ATOSNT\atm>>add ?

add  help:  Add a VCC
add  usage:
 <VCC>[numeric_suffix_name][atm_port]

add command parameters:
 VCC
```

Table 2: add

Syntax	Description
VCC	Keyword
numeric_suffix_name [max 3 decimal digits]	Up to 3 digits can be used to name the VCC. Even if the numeric suffix is not set, it will automatically add a progressive number to the VCC name (e.g. the first VCC name will be VCC0, the second VCC1 and so on).
atm_port	Sets the association between the atm port and the new VCC created. It is necessary only with CPE models with more than one ATM port present. Default: atm0

ATM - Nodes

To see the structure of the ATM node, use the **tree** command:

```
ATOSNT\atm>>tree
atm                     atm0
                        vcc0
                        vcc1
```

ATM0 – Commands

On the **atmx** subnode, it is only visible the log level and the xDSL port used:

```
ATOSNT\atm\atm0>>set ?

Nodes not available.
Set command parameters:
 level of log   [loglevel]  Current value: 1

ATOSNT\atm\atm0>>show work
Show of ATOSNT atm atm0
Level of log  : 1
Physical Port : xdsl0.0
```

Table 3: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the ATMx events. Default: 1

VCCx – Commands

VCCx node is used to configure the ATM connection parameters. By default, the first VCC created has VPI 8 and VCI 35, the second one has VPI 8 and VCI 36 and so on. "Traffic type" supported can be CBR, UBR, VBR-RT, VBR-NRT, UBR+. Default traffic type is UBR.

```
ATOSNT\atm\vcc0>>set ?

Nodes not available.
Set command parameters:
 level of log                    [loglevel]        Current value: 1
 atm port                        [atm-port]        Current value: atm0
 vpi                             [vpi]             Current value: 8
 vci                             [vci]             Current value: 35
 send buffer (bytes)             [send-buffer]     Current value: auto
 keep alive                      [keep_alive]      Current value: OFF
 polling time                    [polling_time]    Current value: 10
 retry time                      [retry_time]      Current value: 1
 up retry count                  [up_retry_cnt]    Current value: 3
 down retry count                [down_retry_cnt]  Current value: 5
 traffic type                    [traffic-type]    Current value: UBR 2304
```

Table 4: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the VCC events. Default: 1
atm-port	Sets the atm port. Default: atm0
vpi [0-255]	Sets the "Virtual Path Identifier" associated with the atm port. Default: 8 for any VCC created.
vci [32-65535]	Sets the "Virtual Channel Identifier" associated with the atm port. Default: 35 for VCC0, 36 for VCC1, etc.
send-buffer (bytes) [1-128000|auto]	Send buffer is the parameter that allows to dimension the size of a buffer developed to adapt the fast internal data transfer speed to the slower physical link and thus to reduce the latency. Default: auto
keep_alive [OFF|LOOPBACK-REQ]	Enables (LOOPBACK-REQ) or disables (OFF) the ATM keep alive. If enabled, the ATM ping requests are sent to the ATM network. Default: OFF
polling_time [5-300]	Sets the time in seconds between each sending loopback request. Default: 10
retry_time [1-60]	Sets the waiting time in seconds related to the loopback request. Default: 1
up_retry_cnt [1-20]	Configures the number of received loopback answers to wait before declaring that the logic ATM link is UP Default: 3
down_retry_cnt [1-20]	Configures the number of failure loopback answers to wait before declaring that the logic ATM link is DOWN Default: 5

traffic-type [CBR|UBR|VBR-RT|VBR-NRT|UBR+]	Sets ATM class of service: • CBR - Constant Bit Rate • UBR - Unspecified Bit Rate • VBR-RT - Real-Time Variable Bit Rate • VBR-NRT - Non Real-Time Variable Bit Rate PCR -Peak cell rate (kbit/sec) [0-65535]; Default: 2304 SCR - Sustainable Cell Rate (kbit/sec) [0-65535]; Default: 1024 MCR - Minimum cell rate (kbit/sec) [0-65535]; Default: 1024 Default value is UBR, 2304 kbit/s

VCCx - Configuration example

This example shows how to create a new VCC named VCC40 with VPI 8, VCI 45 and traffic type CBR with PCR sets to 640 kbit/sec:

add atm VCC 40 atm0
set atm vcc40 vci 45
set atm vcc40 traffic-type CBR 640

The result is the following:

ATOSNT\atm\vcc40>>**show work**
Show of ATOSNT atm vcc40
Level of log : 1
ATM Port : atm0
VPI : 8
VCI : 45
Send buffer (bytes) : auto
Keep alive : OFF
Polling time : 10
Retry time : 1
Up retry count : 3
Down retry count : 5
Traffic type : CBR PCR=640

VCCx - Status and Statistics

Here un example of VCC status and statistics:

Active state

ATOSNT>>show atm vcc0 status

status of atm aal5 channel vcc0

state: active

----------RX----------TX----------

f5-ais ete: OFF OFF

f5-rdi ete: OFF OFF

f5-ais sts: OFF OFF

f5-rdi sts: OFF OFF

Inactive state

ATOSNT\atm\vcc0>>show status

status of atm aal5 channel vcc0

state: inactive

----------RX----------TX----------

f5-ais ete: OFF OFF

f5-rdi ete: OFF OFF

f5-ais sts: OFF OFF

f5-rdi sts: OFF OFF

Statistics

ATOSNT>>show atm vcc0 statistics

statistics of atm aal5 channel vcc0

******* upstream direction *******

packets: 1571

errors: 0

oam f5 ete ais: 0

oam f5 sts ais: 0

oam f5 ete rdi: 0

oam f5 sts rdi: 0

oam f5 ete loopback: 0

oam f5 sts loopback: 0

****** downstream direction ******

packets: 393

errors: 0

drops: 0

oam f5 ete ais: 0

oam f5 sts ais: 0

oam f5 ete rdi: 0

oam f5 sts rdi: 0

oam f5 ete loopback: 0

oam f5 sts loopback: 0

oam f5 ete others: 0

oam f5 sts others: 0

oam discarded: 0

oam crc10 err: 0

Status and Statistics with keep alive enabled

ATOSNT>>show atm vcc0 status

status of atm aal5 channel vcc0

state: active

pvc status: up

----------RX----------TX----------

f5-ais ete: OFF OFF

f5-rdi ete: OFF OFF

f5-ais sts: OFF OFF

f5-rdi sts: OFF OFF

ATOSNT\atm\vcc0>>show statistics

statistics of atm aal5 channel vcc0

******* upstream direction *******

packets: 54

errors: 0

oam f5 ete ais: 0

oam f5 sts ais: 0

oam f5 ete rdi: 0

oam f5 sts rdi: 0

oam f5 ete loopback: 23

oam f5 sts loopback: 0

****** downstream direction ******

packets: 19

errors: 0

drops: 0

oam f5 ete ais: 0

oam f5 sts ais: 0

oam f5 ete rdi: 0

oam f5 sts rdi: 0

oam f5 ete loopback: 23

oam f5 sts loopback: 0

oam f5 ete others: 0

oam f5 sts others: 0

oam discarded: 0

oam crc10 err: 0

****** keep alive ******

stopped: 0

pvc up: 1

pvc down retry: 0

pvc up retry: 0

pvc down: 0

ATOSNT>>show atm vcc0 status

status of atm aal5 channel vcc0

state: inactive

pvc status: stopped

----------RX----------TX----------

f5-ais ete: OFF OFF

f5-rdi ete: OFF OFF

f5-ais sts: OFF OFF

f5-rdi sts: OFF OFF

ATOSNT>>show atm vcc0 statistics

statistics of atm aal5 channel vcc0

******* upstream direction *******

packets: 62

errors: 0

oam f5 ete ais: 0

oam f5 sts ais: 0

oam f5 ete rdi: 0

oam f5 sts rdi: 0

oam f5 ete loopback: 27

oam f5 sts loopback: 0

****** downstream direction ******

packets: 19

errors: 0

drops: 0

oam f5 ete ais: 0

oam f5 sts ais: 0

oam f5 ete rdi: 0

oam f5 sts rdi: 0

oam f5 ete loopback: 27

oam f5 sts loopback: 0

oam f5 ete others: 0

oam f5 sts others: 0

oam discarded: 0

oam crc10 err: 0

****** keep alive ******

stopped: 2

pvc up: 2

pvc down retry: 1

pvc up retry: 0

pvc down: 0

Table 5: VCC Status

Syntax	Description
state	Virtual Circuit state. It can assume the following values: • **Active** if it works properly • **Inactive** if it is declared down • **vcc is not used** if it is not associated to any interface
PVC status	Only available if keep alive is not disabled. It can assume the following values:

	• **Up** if it works properly (the keep alive receives the right answer) • **Stopped** if the PVC is not able to transmit loopback keep alive (e.g. the pysical connection is down) • **Down** if it doesn't work properly (e.g. the keep alive doesn't receive the right answer to declare the PVC Up) • **Up retry** if it is waiting to declare the logic ATM link UP (e.g. the number of keep alive "Up_retry_cnt" is not reach yet to declare the ATM link UP) • **Down-retry** if it is waiting to declare the logic ATM link DOWN (e.g. the number of keep alive "DOWN_retry_cnt" is not reach yet to declare the ATM link DOWN)
f5-ais ete	Number of F5 Alarm Indication Signal (AIS) End to End (ete) sent / received
f5-rdi ete	Number of F5 Remote Defect Indication (RDI) End to End (ete) sent / received
f5-ais sts	Number of F5 Alarm Indication Signal (AIS) Segment to Segment (sts) sent / received
f5-rdi sts	Number of F5 Remote Defect Indication (RDI) Segment to Segment (sts) sent / received

Table 6: ***VCC statistics (upstream / downstream)***

Table 1: set

Syntax	Description
packets	Number of packets sent / received by the selected VCC
errors	Number of errors. In upstream means packets not sent for any error occured; in downstram means packets not recognized.
Drops(only downstream)	Number of received packets, dropped for any reason.
oam f5 ete ais	Number of oam f5 ete ais sent / received by the selected VCC
oam f5 sts ais	Number of oam f5 sts ais sent / received by the selected VCC
oam f5 ete rdi	Number of oam f5 ete rdi sent / received by the selected VCC
oam f5 sts rdi	Number of oam f5 sts rdi sent / received by the selected VCC
oam f5 ete loopback	Number of oam f5 ete loopback sent / received by the selected VCC
oam f5 sts loopback	Number of oam f5 sts loopback sent / received by the selected VCC
oam f5 ete others(only Downstream)	Number of others oam f5 ete received by the selected VCC
oam f5 sts others(only downstream)	Number of others oam f5 sts received by the selected VCC
oam discarded(only downstream)	Number of received oam packets, discarded by ATOSNT
oam crc10 err	Number of oam crc10 error received
****** keep alive ******	
stopped	Number of keep alive process stops occours
pvc up	Number of PVC UP event
pvc down retry	Number of "down retry" event
pvc up retry	Number of "up retry" event
pvc down	Number of times that the PVC has been declared DOWN

Index

ManBackup

Backup

Backup is used to provide an alternative connection when an interface stops to work. Backup procedure is set on by the physical layer, “PPP” or “IP” events.

This feature is available configuring a backup profile, which consists of a set of interfaces (LAN or WAN) carrying the same traffic (routing or bridging) and a priority assignment. The traffic will actually flow on the interface which is in up status and has higher priority.

Backup manager receives alarm messages (up and down) from interfaces, then:

- if the interface where traffic currently flows goes down

  it switches the traffic (modifying routes) on the interface belonging to the profile which has the highest priority.

- if an interface belonging to a profile goes from down to up and has priority higher than the profile interface currently in use

  it becomes the active interface.

Backup – Commands

On the **backup** node you can set the following command parameters:

```
ATOSNT\backup>>set ?

Nodes not available.
Set command parameters:
 level of log  [loglevel]  Current value: 1
```

Table 1: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the backup events. Default: 1

```
ATOSNT\backup>>add ?

add  help :  Add a new Backup profile
add  usage:
 <PROFILE>[name]

add command parameters:
 PROFILE

ATOSNT\backup>>add PROFILE profile
```

```
Command executed
```

Table 2: add PROFILE

Syntax	Description
PROFILE	Keyword
name [max 16 char]	Name of the profile to create.

```
ATOSNT\backup>>del ?

del  help:  Remove a Backup profile
del  usage:
 <PROFILE>[name]

del command parameters:
 PROFILE
```

Table 3: del PROFILE

Syntax	Description
PROFILE	Keyword
name [max 16 char]	Name of the profile to be removed.

PROFILE name – Commands

Each profile creates dynamically a subnode “profile”, which needs to be associated to an interfaces list having different priorities.

```
ATOS\backup>>profile

ATOSNT\backup\profile>>set ?

Nodes not available.
Set command parameters:
 level of log         [loglevel]       Current value: 1
 description          [description]    Current value:
 startup delay (sec)  [startup-delay]  Current value: 60
```

Table 4: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the backup events. Default: 1
description [max 100 char]	Sets a brief description of the profile
startup-delay (sec) [1-300]	Sets the waiting time before activating the backup process at the CPE reboot. The purpose of this parameter is to avoid that interfaces with less priority can be activated just because primary interface (e.g. ADSL) takes longer time for the first activation. Default: 60 sec.

```
ATOS\backup\PROFILEname>>add ?

add  help :  Add a new interface
add  usage:
 <IFC><name><priority>

add command parameters:
 IFC
```

Table 3: add IFC

Syntax	Description
IFC	Keyword
name	Name of the interface to use for backup profile (ETHx, VCCx,...)
priority [1-60]	Priority value associated to the interface

del command removes the association between interface and profile:

```
ATOSNT\backup\profilename>>del ?

del  help:  Remove an interface
del  usage:
 <IFC><name>

del command parameters:
 IFC
```

Backup Configuration Example

ATOSNT\backup\PROFILEname>>add
IFC eth0 60
Command executed

ATOSNT\backup\PROFILEname>>add
IFC vcc0 50
Command executed

ATOSNT\backup\backup>>**show conf**
Show of ATOSNT
backup
Level of log : 1
Description :
Startup delay (sec) :
60

LIST OF
INTERFACES

Interface	Priority
eth0	60
vcc0	50

Index

ManBri

BRI-X – Commands

From the application (e.g. VoIP) point of view, the “physical” configuration of an ISDN port includes layer 1 (that is the actual physical layer) and layer 2 (link layer) even if the last one is a logical interface.

The two layers configuration is managed in two different nodes:

bri-x node

in this node you can configure layer 1

isdn\isdn-bri-x node

instead you have to go to isdn node to configure layer 2.

The only parameter to be configured on bri node is a "Read Only" parameter; its value depends on how the bri port is allocated for.

If, for example, the port is allocated for a VoIP User Terminal, the parameter value will be “NT” that means that the bri port is working like a Network Termination; instead if it is allocated for an ISDN WAN the parameter value will be “TE” and the bri port is working like a Terminal Equipment.

```
ATOSNT\bri1>>show work
Show of ATOSNT bri1
Operation mode: NT

ATOSNT\bri2>>show work
```

```
Show of ATOSNT bri2
Operation mode : TE
```

Table

Syntax	Description
NT|TE	Indicates the operation mode of the BRI port: NT the port is working as a Central Office (Network Termination) side of a connection; in this case an ISDN terminal (ISDN phone, PBX network side) should be connected to the port. This is the tipical working mode when an Integrated Access Device or gateway is connected between the legacy ISDN equipment and the VoIP network; TE the port is working as a Terminal Equipment side of a connection; in this case the port must be connected to a Network Termination (Central Office, PBX user side…). This configuration must be set, for example, when the bri port is used for ISDN data backup or as an ISDN terminal (ISDN TE).

Index

ManBridge

Bridge

The bridge function is used to connect two or more interfaces using a transmission device. A selective action is carried out on traffic.

The bridge has two different functions:

forwarding process

to send packets from the input port to one or more output ports ;

learning process

to learn the hosts connected to the interfaces .

To execute the learning process, the bridge analyses the header of every Ethernet frame received over the interfaces and saves the MAC source address and identifier of the transmitting interface, adding an entry in the forwarding table (*filtering database*).

The information is used to determine the output port/s of the frame during the forwarding process:

The filtering database contains dynamic entries managed by the learning process, they can be added, updated or deleted from the database.

Another functionality of the bridge is the *spanning tree* process. This process periodically converts networks with closed loops into a tree to eliminate circular paths where the bridge does not operate correctly. Broadcast or multicast frames transmitted over networks with loop would be indefinitely transmitted over the network by the bridges.

ATOSNT can work simultaneously as bridge and router just selecting the incoming traffic over the interfaces. Incoming packets havig destination MAC address as device MAC address will be routed.

Bridges – Node

In “Bridges” node it is possibile to create o remove a bridge profile. Moreover it is possible to create a classifier, with several options (STP,VLAN,ARP,OPT) that can be assigned to the bridge profile in order to select specific packets to perform (or not) bridiging.

```
ATOSNT\bridges>>set ?

Nodes not available.
Set command parameters:
 level of log  [loglevel]  Current value: 1
```

Table 1: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the bridge events. Default: 1

```
ATOSNT\bridges>>add ?

add  help :  Add a new BRIDGE or a new LIST or a new ENTRY of a list
add  usage:
 <STP-OPT><name><opt-type>[equal|not-equal]<opt-value>
 <VLAN-OPT><name><opt-type>[equal|not-equal]<opt-value>
 <ARP-OPT><name><opt-type>[equal|not-equal]<opt-value>
 <IP-OPT><name><opt-type>[equal|not-equal]<opt-value>
 <CLASSIFIER><name>[rule-pos]<target>
             [equal|not-equal]<src-mac>
             [equal|not-equal]<dest-mac>[stp-opt-list]
             [equal|not-equal]<protocol>[vlan-opt-list|arp-opt-list|ip-opt-list]
             [equal|not-equal]<pkt-type>]
             [in-port[equal|not-equal]<bridge-port-name>]
             [input[equal|not-equal]<bridge-name>]
             [out-port[equal|not-equal]<bridge-port-name>]
             [output[equal|not-equal]<bridge-name>]
 <BRIDGE>[numeric_suffix_name]

add command parameters:
 STP-OPT
 VLAN-OPT
 ARP-OPT
 IP-OPT
 CLASSIFIER
 BRIDGE

ATOSNT\bridges>>del ?

del  help :  Remove a BRIDGE or a LIST or a ENTRY of a list
```

```
del  usage:
 <STP-OPT><name>[<opt-type>]
 <VLAN-OPT><name>[<opt-type>]
 <ARP-OPT><name>[<opt-type>]
 <IP-OPT><name>[<opt-type>]
 <CLASSIFIER><name>[rule-pos]
 <BRIDGE><name>

del command parameters:
 STP-OPT
 VLAN-OPT
 ARP-OPT
 IP-OPT
 CLASSIFIER
 BRIDGE
```

Creating a STP Option list

An STP Option list can be used as rule for traffic selection in the classifier configuration explained below.

This is the syntax:

```
ATOSNT\bridges>>add STP-OPT <name><opt-type>[equal|not-equal]<opt-value>.
```

Table 2: add STP-OPT

Syntax	Description
STP-OPT	Keyword
name max 16 char	Name of the list
bpdu-type|bpdu-flags|bpdu-root-addr| bpdu-root-prio|bpdu-root-cost|bpdu-sender-addr| bpdu-sender-prio|port|msg-age|max-age| hello-time|forward-delay	Can set to one of the following option type
equal|not-equal	Matches or not the option value. Default: equal
opt-value	config|tcn]) • bpdu-flags (value [0-255|topology-change|topology-change-ack]) • bpdu-root-addr (mac address [aa-bb-cc-dd-ee-ff]) • bpdu-root-prio (value [0-65535]) • bpdu-root-cost (value [0-4294967295]) • bpdu-sender-addr (mac address [aa-bb-cc-dd-ee-ff]) • bpdu-sender-prio (value [0-65535]) • port (value [0-65535]) • msg-age (value [0-65535]) • max-age (value [0-65535]) • hello-time (value [0-65535]) • forward-delay (value [0-65535])

Creating a VLAN Option list

A VLAN Option list can be used as rule for traffic selection in the classifier configuration explained below.

This is the syntax:

```
ATOSNT\bridges>>add VLAN-OPT  <name><opt-type>[equal|not-equal]<opt-value>
```

Table 3: add VLAN-OPT

Syntax	Description
VLAN-OPT	Keyword
name [max 16 char]	Name of the list
vlan-id|priority|eth-type	Can set the option type
equal|not-equal	Matches or not the option value. Default: equal
opt-value	ARP|802.1Q|X25|PPPoE-Discovery|PPPoE-Session]

Creating a ARP Option list

An ARP Option list can be used as rule for traffic selection in the classifier configuration explained below.

This is the syntax:

```
ATOSNT\bridges>>add ARP-OPT <name><opt-type>[equal|not-equal]<opt-value>
```

Table 4: add ARP-OPT

Syntax	Description
ARP-OPT	Keyword
name [max 16 char]	Name of the list
op-code|hw-type|protocol-type|src-ip|dst-ip|src-mac|dst-mac	Can set the option type
equal|not-equal	Matches or not the option value. Default: equal
opt-value	Reply] • hw-type [ethernet] • protocol-type [0-FFFF hex|IPv4|ARP|802.1Q|X25|PPPoE-Discovery|PPPoE-Session] • src-ip (ip address [aa.bb.cc.dd]) • dst-ip (ip address [aa.bb.cc.dd]) • src-mac (mac address [aa-bb-cc-dd-ee-ff]) • dst-mac (mac address [aa-bb-cc-dd-ee-ff])

Creating a IP Option list

An IP Option list can be used as rule for traffic selection in the classifier configuration explained below.

This is the syntax:

```
ATOSNT\bridges>>add ARP-OPT <name><opt-type>[equal|not-equal]<opt-value>
```

Table 5: add IP-OPT

Syntax	Description
IP-OPT	Keyword
name [max 16 char]	Name of the list
protocol|src-ip|dst-ip|src-port|dst-port|tos	Can set the option type
equal|not-equal	Matches or not the option value. Default: equal
opt-value	tcp|udp|dccp|sctp|icmp] • src-ip (ip address [aa.bb.cc.dd]) • dst-ip (ip address [aa.bb.cc.dd]) • src-port [0-65535] • dst-port [0-65535] • tos [0-FF hex]

Creating a Classifier

A classifier is a profile that collects one or more lists described above and then can be assigned to the bridge.

This is the syntax:

```
ATOSNT\bridges>>add CLASSIFIER <name>[rule-pos]<target>
             [equal|not-equal]<src-mac>
             [equal|not-equal]<dest-mac>[stp-opt-list]
             [equal|not-equal]<protocol>[vlan-opt-list|arp-opt-list|ip-opt-list]
             [equal|not-equal]<pkt-type>]
             [in-port[equal|not-equal]<bridge-port-name>]
             [input[equal|not-equal]<bridge-name>]
             [out-port[equal|not-equal]<bridge-port-name>]
             [output[equal|not-equal]<bridge-name>]
```

Table 6: add CLASSIFIER

Syntax	Description
CLASSIFIER	Keyword
name	Name of the classifier
rule-pos [1-32]	Position of the rule in the list.
permit | deny	target
equal|not-equal	Matches or not the rule. Default: equal
src-mac	Sets the source mac type [any|host] and address [aa-bb-cc-dd-ee-ff]. "Host" stands for local address

dest-mac	Sets the destination mac type [any|host|stp] and address [aa-bb-cc-dd-ee-ff]. “Host” stands for local address and “stp” for a stp-opt-list
stp-opt-list	Name of the predefined stp-opt-list. See above
0-FFFF hex | anyprot|IPv4|ARP|802.1Q|X25| PPPoE-Discovery	Sets the protocol type
vlan-opt-list|arp-opt-list|ip-opt-list	Depending on the protocol set a relative list should be configured.
host|broadcast|multicast|otherhost	Sets the packet type. ”Host” stands for local traffic and ”otherhost” for foreign traffic.
in-port [eth0|..]	One of the created RF1483 capable interface .
input [bridge0|..	One of the created bridge.
out-port [eth0|..]	One of the created RF1483 capable interface .
output [bridge0|..	One of the created bridge.

Creating a new bridge

The bellow example shows how to create a new bridge

ATOSNT\bridges>>add BRIDGE ?
add command parameters:
BRIDGE numeric suffix name [max 9 decimal digits]
<cr>

ATOSNT\bridges>>add BRIDGE 1
Command executed

Now, there is a new subnode named “bridge1” available.

```
ATOSNT\bridges\bridge1>>set ?

Available nodes:
                      stp

Set command parameters:
 enable                  [on|off]                  Current value: off
 description             [description]             Current value:
 filtering classifier    [filtering-classifier]    Current value:
 ageing time             [ageingtime]              Current value: 300
 spanning tree protocol  [spanning-tree-protocol]  Current value: off
```

Table 7: set

Syntax	Description
on | off	Enables/disables the bridge
Description [max 100 char]	A short description of the new bridge
filtering-classifier	Predefined classifier described above.
ageingtime [0-1000000]	Ageing time of seen mac-addres Default: 300
spanning-tree-protocol [on|off]	Enables/disables spanning tree protocol Default: off

Adding/Removing an interface to the bridge

With the comands add/del it is possible to add or delete an interface to the bridge.

```
ATOSNT\bridges\bridge1>>add ?

add  help :  Add a new INTERFACE
add  usage:
 <IFC><interface-name>

add command parameters:
 IFC
```

```
ATOSNT\bridges\bridge1>>del ?

del  help :  Remove a INTERFACE
del  usage:
 <IFC><interface-name>

del command parameters:
 IFC
```

Table 8: add

Syntax	Description
IFC	keyword
interface-name [eth0]	Sets the name of the interface to add to the bridge

Table 9: del

Syntax	Description
IFC	keyword
interface-name [empty]	Removes the interface name of the brige

Now there is a new subnode, eth0

```
ATOSNT\bridges\bridge1>>?

Available nodes:
                       stp
                       eth0
Available commands:
up                      Move one step up from the current node
top                     Back to the root of the tree
quit                    Exit from CLI session
set                     Set 'bridge1' options
add                     Add a new INTERFACE
del                     Remove a INTERFACE
conf                    Show the configuration in CLI command format
full-conf               Show full configuration in CLI command format
show                    Show 'bridge0' settings
delete                  Delete statistics
tree                    Show the tree structure of CLI interface
help                    Help of item
info                    Show the system informations
date                    Show or setting system date and time
save                    Save configuration data
restart                 Restart device
telnet                  Open telnet client session
ssh                     Open SSH2 client session
ping                    Send an ICMP ECHO request
atmping                 Send an ATM loopback cells
tracert                 Display a trace of packet
mtrace                  Display a path for a multicast group
resolve                 Resolve a IP address or IP name
log                     Log Management
show-logging-level      Show logged level
banner                  Edit pre and post login banners
```

Under the eth0 subnode it is possible to configure the following parameters:

```
ATOSNT\bridges\bridge1\eth0>>set ?

Nodes not available.
Set command parameters:
 cost           [cost]           Current value: 10
 priority       [priority]       Current value: 128
```

```
ignore status  [ignore-status]  Current value: off
```

Table 10: set

Syntax	Description
cost [1-65535]	Each interface in a bridge could have a different speed and this value is used when deciding which link to use. Faster interfaces should have lower cost. Default: 1000000/IFC_SPEED(Kbit)
priority [0-255]	Sets the port priority. In case of multiple ports with the same cost, it is also possible to apply a priority. Default: 128
ignore-status [on|off]	When the parameter is set: • **off**: the physical status of this interface will be considered to determinate the physical status of the bridge. • **on**: the physical status of this interface will be ignored to determinate the physical status of the bridge. Default: off

STP node

In stp node, it is possible to tuning the spanning-tree protocol

```
ATOSNT\bridges\bridge1\stp>>set ?

Nodes not available.
Set command parameters:
 bridge priority           [bridge-priority]     Current value: 2
 hello time (sec)          [hello-time]          Current value: 2
 forward delay time (sec)  [forward-delay-time]  Current value: 15
 max message age (sec)     [max-age]             Current value: 20
```

Table 11: set

Syntax	Description
bridge-priority	Value [0-65535]. Default :2
hello-time	Value (sec) [1-10]. Default :2
forward-delay-time	Value (sec) [4-30]. Default :15
max-age	Value (sec) [6-40]. Default :220

Index

ManCertificate

Certificate Overview

A digital certificate is generated by a certification entity that associates the identity data to an individual, organization or company confirming the digital identity on the web. The digital certificate is mainly valid for user authentication or website on internet in a way that the assistance of a third party trusted by either party involved in the communication is needed. The name of the trusted entity is **Certificate Authority** (CA) e can be a public body or a company recognized on Internet.

The digital certificate's main function is to authenticate the holder but can also be used to encrypt and sign communications digitally.

One application example is the SSL/TLS authentication process, where the client OpenVPN uses the following files:

- **CA (Certificate Authority) file**

  PEM format is used by most CA;

- **KEY file**

  local client's private key in PEM format;

- **CERT file**

  local client's signed certificate in PEM format duly signed by the certificate authority in the CA file.

Under "certificate" node, ATOSNT allows the user to import different types of file formats like PEM, GADMIN or OVPN:

- **PEM format**

  may consist of a certficate (public key) or a private key.

- **OVPN format**

  defines a file type where multiple certificates are being imported at the same time in one file.

- **GADMIN format**

  is a complete client setup package (tar.gz) for openvpn client (SSL/TLS); the bundle contains also ca, cert and key files.

Once imported, any file will appear in the appropriate list of CERT o CA o KEY files.

Certificate - Commands

```
ATOSNT\certificate>>?

Nodes not available.

Available commands:
up                      Move one step up from the current node
top                     Back to the root of the tree
quit                    Exit from CLI session
set                     Set 'certificate' options
add                     Add a new profile
del                     Remove a profile
conf                    Show configuration in CLI command format
full-conf               Show full configuration in CLI command format
```

```
show                    Show 'certificate' settings
delete                  Delete statistics
tree                    Show the tree structure of CLI interface
help                    Help of item
info                    Show the system informations
date                    Show or setting system date and time
save                    Save configuration data
restart                 Restart device
telnet                  Open telnet client session
ssh                     Open SSH2 client session
ping                    Send an ICMP ECHO request
atmping                 Send an ATM loopback cells
tracert                 Display a trace of packet
mtrace                  Display a path for a multicast group
resolve                 Resolve a IP address or IP name
log                     Log Management
show-logging-level      Show logged level
banner                  Edit pre and post login banners

import                  Import certificate on node ATOSNT\certificate>>
remove                  Remove certificate on node ATOSNT\certificate>>
```

Import command allows to import a certificate on "certificate" node of ATOSNT.
Remove command allows to remove a certificate from "certificate" node of ATOSNT.

```
ATOSNT\certificate>>import ?

import  help :  Import certificate
import  usage:
 <TFTP><remote file name>[server-name]<type>[name]
 <FTP><remote file name>[server-name[:port]]<type>[name]
 <SCP><remote path/file-name>[server-name[:port]]<type>[name]
 <HTTP><[username:password@]URL/file-name[:port]><type>[name]
 <FROM-DISK><local source-file name><type>[name]

import command parameters:
 protocol              [TFTP|FTP|HTTP|SCP|FROM-DISK]
```

Table 1: import

Syntax	Description
TFTP|FTP|HTTP|SCP|FROM-DISK	Protocol type to use for the certificate file importation
remote file name [max 128 char]	Name of the remote file to import
server-name [max 128 char][:port]	Name or IP address and destination port of the host where the TFTP/FTP/HTTP/SCP server is located.
type [pem|gadmin|ovpn]	Sets the type of the file format to import. • PEM format may consist of a certficate (public key) or a private key. • OVPN format defines a file type where multiple certificates are being imported at the same time in one file. • GADMIN format is a complete client setup package (tar.gz) for openvpn client (SSL/TLS); the bundle contains also ca, cert and key files.
name	Sets the local folder name where the imported files will be allocated
remote path/file-name [max 128 char]	Sets the remote path where the file is located and the file name to import.
username:password@]URL/file-name[:port]	Username and password
local source-file name [max 128 char]	Name of the local source file

```
ATOSNT\certificate>>remove ?

remove  help :  Remove certificate
remove  usage:
 <REMOVE>[name]

remove command parameters:
 name      [cert1]
```

Table 2: remove

Syntax	Description
REMOVE	keyword
name [cert1]	Name of the certificate to remove

With **set** command you can configure this parameter:

```
ATOSNT\certificate>>set ?

Nodes not available.
Set command parameters:
 level of log  [loglevel]  Current value: 1
```

Table 3: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOS to log the events of the certificate node, from the less detailed one (0) to the more detailed one (5) [default: 1]

Use **add** command to add a new certificate profile on "certificate" node.

```
ATOSNT\certificate>>add ?

add  help :  Add a new profile
add  usage:
 <PROFILE><type>[name]

add command parameters:
 PROFILE

ATOSNT\certificate>>add PROFILE ?

add command parameters:
 type     [openvpn]

ATOSNT\certificate>>add PROFILE openvpn
Command executed
```

Table 4: add a new PROFILE

Syntax	Description
PROFILE	Keyword
type	Sets the profile type to be choosed from a current list; at the moment openvpn type is only available
name	Sets the profile name

This the result:

```
ATOSNT\certificate>>tree
certificate             profile0
```

A new subnode named "profile0" appears under "certificate" node.

In a profile of "OpenVPN" type, they must be defined the files to be used, available in ATOSNT after using the "import" command performed under the "certificate" node. For more details look at "How to import .....".

The files to be used are:

- the client's certificate (cert);
- the client's private key (private-key);
- the CA certificate (ca-cert).

```
ATOSNT\certificate\profile0>>set ?

Nodes not available.
Set command parameters:
```

```
 certificate authority  [ca-cert]      Current value:
 certificate            [cert]         Current value:
 private key            [private-key]  Current value:
```

Example of how to create a certificate profile importing the certificate file(s) from a remote server

Suppose that for the files importation you will use:

- TFTP Protocol
- gadmin-openvpn-client-data-linux.tar.gz

  is the certificate file name to import
- 192.168.111.33

  is the remote server IP address where the certificate file is located
- gadmin

  is the type of the file format
- cert1

  is the local folder name where the imported files will be allocated

Now, you should use **import** command with the following syntax:

```
ATOSNT\certificate>>import TFTP gadmin-openvpn-client-data-linux.tar.gz 192.168.111.33 gadmin cert1
```

ATOSNT will start the file importation and will show this message:

```
Starting...
Downloading 'gadmin-openvpn-client-data-linux.tar.gz' using TFTP protocol
gadmin-openvpn-clien 100% |*******************************|  3980   0:00:00 ETA

Writing File! Do Not turn off!
3980 bytes written
Command executed
```

As a result, the imported files will be now located in a local folder named "cert1" and on "certificate" node will appear a subnode named "profile0" where you must comfigured all three parameters, see below, in order that "profile0" could be used by the "OpenVPN client" interface type available on **Service-Vpn for OpenVPN – Commands** in **Interfaces** node.

```
ATOSNT\certificate\profile0>>set ?

Nodes not available.
Set command parameters:
 certificate authority  [ca-cert]      Current value:
 certificate            [cert]         Current value:
 private key            [private-key]  Current value:
```

Note that ATOSNT will present the parameters to be configured with the folder name where the imported files are allocated, followed by the parameter's name, as described below.

```
ATOSNT\certificate\profile0>>set ca-cert ?

 certificate authority  [<cr>|cert1/cacert.pem]
```

```
 Current value:
 Default fw value:

ATOSNT\certificate\profile0>>set ca-cert cert1/cacert.pem
Command executed


ATOSNT\certificate\profile0>>set cert ?

 certificate  [<cr>|cert1/cert.pem]

 Current value:
 Default fw value:

ATOSNT\certificate\profile0>>set cert cert1/cert.pem
Command executed


ATOSNT\certificate\profile0>>set private-key ?

 private key  [<cr>|cert1/key.pem]

 Current value:
 Default fw value:

ATOSNT\certificate\profile0>>set private-key cert1/key.pem
Command executed
```

At this point, an "OpenVPN client" interface could use the certificate profile "profile0" configuring the "certificate-profile" parameter defined in **Service-Vpn for OpenVPN – Commands** in **Interfaces** node.

Look at a short summary of the configuration commands at "certificate" and "service-vpn for OpenVPN" nodes:

```
ATOSNT\certificate>>show work
Show of ATOSNT certificate
Level of log : 1

Show of ATOSNT certificate profile0
Certificate authority : cert1/cacert.pem
Certificate           : cert1/cert.pem
Private key           : cert1/key.pem

Command executed
------------------------------
ATOSNT\interfaces\tun10\service-vpn>>show conf
Show of ATOSNT interfaces tun10 service-vpn
Level of log                : 1
Protocol                    : udp
```

```
Server                        :
Local address or ifc name     : none
Protocol port                 : 1194
Address from server           : off
Certificate profile name      : profile0
Cipher algorithm              : BF_CBC
keep alive timeout            : 10
keep alive not reply timeout : 30
```

Command executed

ManClassifierMap

Classifier Map Overview

A Classifier Map is a set of rules specifying access right or permissions to users or system processes. Each rule includes a matching condition and an action to be taken; matching condition is based on the packet properties, the action instead specifies whether the packet is permit or not (deny). The specific action depends upon the requested service or application that uses the classifier map.

Classifier maps are utilized in the following services or applications:

- QoS, to differentiate services (action: marking packets);
- Routing policy, static advanced route traffic control (action: marking packets);
- Firewall (action: accept/discard packets).

When configuring classifiers, parameters can be straight specified in the rule, otherwise they can be settled by creating a classifier map profile that also includes stateful parameters; a such profile should thereby included in a single rule of a classifier map.

ATOSNT provides a powerful, flexible mechanism to protect the LAN from intrusions and external attacks and manage the access rights of individual hosts to external services.

For example, you can decide which stations can use e-mail, navigate on the Internet, access programming, etc.

Especially if using the CLI, the configuration of the firewall functions requests the specific knowledge of network protocols and is reserved to expert users.

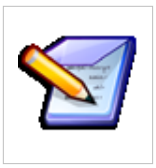
Classifier maps are based on the rules formulation to filter incoming and outgoing traffic. The rules are contained in one or more lists, defined as classifier-maps.

Each rule contains a permission **permit** or negation **deny** clause. Three situations are possible:

- the packet does not meet the conditions of the rule: the packet is subjected to the next rule in the classifier-map
- the packet meets the conditions of the rule and the rule is a **deny** rule: the packet is discarded immediately or it will not suffer the requested action (depending on the application)
- the packet meets the conditions of the rule and the rule is a **permit** rule: the packet will suffer the requested action for example it will be transmitted to the routing function that routes the packet to the destination interface,

without additional checks.

If it does not meet any rule in the list, the packet is discarded or will not suffer the requested action



It is recommended to consider all hosts in the LAN when you create classifier-maps.

Creation and Management of Classifier Maps

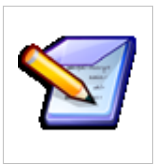
The configuration process of the classifier-maps can include two steps:

- you create one or more classifier-maps with a sequence of rule for every classifier-map
- every classifier-map can include a classmap profile

You can define up to 64 lists, with max of 64 rules for every list

To create a classifier-map you must go to the **classifier-map** node and use the add command. The same command can be used to add rules to an already existing classifier-map.

The order used to include the rules in the list is important because the rules are applied to the same order they are created.



When creating or modifying a classifier-map, you have only to save modifications without restarting the device. Moreover, you cannot use add/del commands on an classifier-map if they have been already used by any application

Classifier Map - Commands

On **classifier-map** node you can set, del and add the following parameters:

```
ATOSNT\classifier-map>>set ?

Nodes not available.
Set command parameters:
 level of log  [loglevel]  Current value: 1

ATOSNT\classifier-map>>del ?

del  help :  Delete an ENTRY or CLASS MAP
del  usage:
 <name> [rule number]

del command parameters:
 classifier map name      [Empty list]
```

Table 1: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the node events. Default: 1

How to create a Classifier Map and a new rule

add command is used to create a new rule

```
ATOSNT\classifier-map>>add ?

add  help :  Add new ENTRY or CLASS MAP
add  usage:
 <name>[rule num]<right><protocol: TCP|6 ><src-addr><dest-addr>[IP-option]<src port><dest port>
[tcp-flag][src-ifc]
 <name>[rule num]<right><protocol: UDP|17><src-addr><dest-addr>[IP-option]<src port><dest-port>
[src-ifc]
 <name>[rule num]<right><protocol: ICMP|1><src-addr><dest-addr>[IP-option][icmp-type][src-ifc]
 <name>[rule num]<right><protocol:ANYPROT><src-addr><dest-addr>[IP-option][src-ifc]
 <name>[rule num]<right><profile-name>

add command parameters:
 classifier map name      [Any value(max 32 char)]
```

for packets with TCP payload

```
<name>[rule num]<right><protocol: TCP|6 ><src-addr><dest-addr>[IP-option]<src port><dest port>
[tcp-flag][src-ifc]
```

for packets with UDP payload

```
<name>[rule num]<right><protocol: UDP|17><src-addr><dest-addr>[IP-option]<src port><dest-port>
[src-ifc]
```

for packets with ICMP payload

```
<name>[rule num]<right><protocol: ICMP|1><src-addr><dest-addr>[IP-option][icmp-type][src-ifc]
```

for packets with a different protocol

```
<name>[rule num]<right><protocol:ANYPROT><src-addr><dest-addr>[IP-option][src-ifc]
```

for packets with a Profile

A Classifier Map can also be configured using a **Profile** which should have been previously defined in the **Classmap Profile** node. The Profile only defines the matching conditions. The action to be taken by the Classifier Map is defined by the **right** value (permit or deny) , as described below.

```
<name>[rule num]<right><profile-name>
```

A Classifier Map with a Profile is used whenever you need to configure a **Stateful firewall** .

Table 2: add classfier-map

Syntax	Description
Name [max 32 characters]	Name of the access list you want to create or add an entry. A new list is created if you enter the add command with the name of a non-existing list. It is recommended to use names that easily identify the type of filter you want to create.
rule num [1 - 32767]	Rule Number that identifies an entry (or a rule) of the list; leaving out this parameter each entry added will have a progressive number.
right [permit|deny]	Access right : permit If permit and the packet meets the rules, the packet is accepted with no additional checks and sent to the routing function. deny If deny, the packet is discarded immediately.
protocol [0-255|tcp|udp|icmp| anyprot]	Type of access protocol
src-addr [aa.bb.cc.dd|host|router|any]	Source address value used to compare to the source address field of the packet IP header. The possible values are: • aa.bb.cc.dd Address field obtained by combining "IP address" and "wild mask" . Value 1 in IP wild mask position indicates that the corresponding bit in IP address must not be checked. • host [aa.bb.cc.dd|string] host identified with a specific IP address or "string" host identified with any of the names assigned/resolved by the DNS service of the router • router Router IP address • any No check is carried out.
dest-addr [aa.bb.cc.dd|host|router|any]	Destination address value used to compare to the destination address field in the packet IP header. The possible values are: • aa.bb.cc.dd Address field obtained by combining "IP address" and "wild mask" . Value 1 in IP wild mask position indicates that the corresponding bit in IP address must not be checked. • host [aa.bb.cc.dd|string] host identified with a specific IP address or "string" host identified with any of the names assigned/resolved by the DNS service of the router • router Router IP address • any No check is carried out.
ip-option [0-255|looserouting|timestamp|recordroute| sourcerouting|routeralert|anyoption]	Value used to check the IP option field of the packet
src-port	Value used to check the source port number of the TCP or UDP packet
dest-port	Value used to check the destination port number of the TCP or UDP packet .
icmp-type	Value used to check the icmp-type field of the ICMP packet.
tcp-flag	Tcp flag value

src-ifc	Sets the source interface name that can be chosen from the list of the interfaces (static or dynamic). In this mode, the filter is applied only to the selected interface.

Adding a new entry (or a new rule) in a position already used cause the slipping of the next pre-existent rules.

ip option

If present, indicates the values in the datagram option field of the IP packet header. The following values can represent multiple simultaneous options:

Table 3: ip-option

Syntax	Description
looserouting	LSR - Loose Source Routing option (131) - [RFC791,JBP]
timestamp	TS - Internet Timestamp option (68) - [RFC791,JBP]
recordroute	RR - Record Route option (07) - [RFC791,JBP]
routeralert	SID - Router Alert option - [RFC791,JBP]
strictrouting	SSR - Strict Source Routing option (137) - [RFC791,JBP]
sourcerouting	LSRand SSR-Loose and Strict Source Routing option (131 – 137) - [RFC791,JBP]
any option	Match packets with ANY Option
0 -255	Match packets with Option

scr-port and **dest-port** are used for TCP and UDP packets. They indicate the value of the source or destination port field in the header of the TCP or UDP packet.

Table 4: scr-port and dest-port

Syntax	Description
port	**Equivalent Port** match only packets on a given port number. The value ports are listed in the bellow table
range [0-65535]	Match only packets in the range of port numbers
anyport	Any port.

The mnemonic values used with EQUARE

Table 5: EQU mnemonic values

Syntax	Description
dns	Domain Name Service (53).
ftp	File Transfer Protocol (21).
ftp-data	FTP data connections (20).
pop2	Post Office Protocol v2 (109).
pop3	Post Office Protocol v3 (110).
smtp	Simple Mail Transport Protocol (25).
snmptrap	SNMP Traps (162).
telnet	Telnet (23).
http	World Wide Web (http, 80).
tftp	Trivial File Transfer Protocol (69).

icmp-type is an optional parameter. If present, it indicates the values of the type field in the ICMP header.

Table 6: icmp-type

Syntax	Description
echo-request	Echo request ICMP packet (icmp-type = 08).
echo-reply	Echo reply packet (icmp-type = 00).
timestamp-request	sets the timestamp request ICMP packet (icmp-type = 13)
timestamp-reply	Sets the timestamp reply ICMP packet (icmp-type = 14).

tcp-flag is an optional parameter. If present, it indicates the values of the flag field of the TCP header.

Table 7: flag

Syntax	Description
flag-value [0-65535]	Value of the flag field
flag-wildmask [0-65535]	Indicates the flag-value bits to be included in the comparison (digit 1 in any position indicates that the corresponding bit in flag-value is not checked).

The flag weight for the two fields is:

ACK 16 SYN 2

PSH 8 FIN 1

How to delete a Classifier Map

The following command is used to delete an entry of the Classifier-map or the whole Classifier-map:

```
ATOSNT\classifier-map>>del ?

del  help :  Delete an ENTRY or CLASS MAP
del  usage:
 <name> [rule number]
```

```
del command parameters:
 classifier map name
```

Table 8: del

Syntax	Description
name	Classifier-map name
rule number	Allows to delete only an entry of the classifier-map, identified by its position number. Leaving out this parameter the classifier-map is removed with all its entries

Examples: how to block e-mails

To prevent host 192.168.118.70 from using e-mail service, both incoming and outgoing, you can create a classifier-map with the following rules:

ATOSNT\classfier-map>>add nomail deny tcp host 192.168.118.70 any anyport equ smtp

Command executed

ATOSNT\classfier-map>>add nomail deny tcp host 192.168.118.70 any anyport equ pop3

Command executed

ATOSNT\classfier-map>> add nomail permit anyprot any any

Command executed

ATOSNT\classifier-map>>show conf

Show of ATOSNT classifier-map

Level of log : 1

CLASSIFIER MAP

CLASSIFIER MAP nomail RULE N.1

Access right and protocol .. deny tcp

Source/dest address ..... <host 192.168.118.70><any>

IP option ..... none

Source/dest port ..... <anyport><equ smtp>

TCP flag (value/wildmask) .. none

CLASSIFIER MAP nomail RULE N.2

Access right and protocol .. deny tcp

Source/dest address ..... host 192.168.118.70><any>

IP option ..... none

Source/dest port ..... <anyport><equ pop3>

TCP flag (value/wildmask) .. none

CLASSIFIER MAP nomail RULE N.3

Access right and protocol .. permit anyprot

Source/dest address ..... <any><any>

IP option ..... none

The first command creates the “nomail” Classifier-map and defines the following rule:

discard **deny** packets that:

use the tcp protocol;

have 192.168.118.70 as source address;

have any value as destination address;

have any value as source port;

have the port reserved to the SMTP service as destination port.

The second command adds a second rule to the nomail list:

discard **deny** packets that:

use the tcp protocol;

have 192.168.118.70 as source address;

have any value as destination address;

have any value as source port;

have the port reserved to the POP3 service as destination port.

The last rule permits the transmission of packets that:

use any protocol;

have any value as source address;

have any value as destination address.

The last rule is essential for the correct routing of packets that are not used for e-mail. The packets are discarded if this rule is not present.

Infact, the rule:

ATOSNT\classfier-map>>add list-name permit anyprot any any

added in the last position of the list permits the transmission of all packets that do not correspond to any of the above rules.

How to check a Classifier Map

Once you have created the “nomail” classifier-map you can check it with the **show conf** command:

ATOSNT\classfier-map>>**show conf**

Show of ATOSNT classifier-map

Level of log : 1

CLASSIFIER MAP

CLASSIFIER MAP nomail RULE N.1

Access right and protocol .. deny tcp

Source/dest address ..... <host 192.168.118.70><any>

IP option ..... none

Source/dest port ..... <anyport><anyport>

TCP flag (value/wildmask) .. none

CLASSIFIER MAP nomail RULE N.2

Access right and protocol .. deny tcp

Source/dest address ..... <host 192.168.118.70><any>

IP option ..... none

Source/dest port ..... <anyport><equ pop3>

TCP flag (value/wildmask) .. none

CLASSIFIER MAP nomail RULE N.3

Access right and protocol .. permit anyprot

Source/dest address ..... <any><any>

IP option ..... none

go to the **firewall** node to associate and active the “NOMAIL” classifier-map using the following command:

ATOSNT\firewall >>add PACKET-FILTER nomail IFC eth0 in

Command executed

You can show the configuration with the **show conf**

LIST OF PACKET FILTERS

CLASSIFIER MAP	IFC TYPE	INTERFACE NAME	DIRECTION	DISCARD MODE
nomail	IFC	eth0	IN	

How to block Internet access

To prevent hosts 192.168.118.70 and 192.168.118.71 from using the Internet, you can create a classifier-map with the following commands:

```
ATOSNT\classifier-map>>add NOINTERNET deny tcp 192.168.118.70 0.0.0.1 any anyport equ http
Command executed
ATOSNT\classifier-map>>add NOINTERNET permit anyprot 192.168.118.70 0.0.0.1 any
Command executed
```

You can show the configuration with the **show conf** command:

```
CLASSIFIER MAP NOINTERNET RULE N.1
Access right and protocol .. deny tcp
Source/dest address ..... <192.168.118.70 0.0.0.1><any>
IP option ..... none
Source/dest port ..... <anyport><equ http>
TCP flag (value/wildmask) .. none
CLASSIFIER MAP NOINTERNET RULE N.2
Access right and protocol .. permit anyprot
Source/dest address ..... <192.168.118.70 0.0.0.1><any>
IP option ..... none
```

go to the **firewall** node to associate and activate the “NOINTERNET” classifier-map using the following command:

```
ATOSNT\firewall >>add PACKET-FILTER nointernet IFC eth0 in
Command executed
```

You can show the configuration with the **show conf** command:

LIST OF PACKET FILTERS

CLASSIFIER MAP	IFC TYPE	INTERFACE NAME	DIRECTION	DISCARD MODE
NOINTERNET	IFC	eth0	IN	

How to block ATOSNT management

To prevent management from LAN (Web and Telnet configuration) of host “PC_1” you can create an Classifier-map with the following commands:

```
ATOSNT\classifier-map>>add NOMANAGEMENT deny tcp host pc_1 any anyport equ http
Command executed
ATOSNT\classifier-map>>add NOMANAGEMENT deny tcp host pc_1 any anyport equ telnet
Command executed
```

You can show the configuration with the **show conf** command:

```
CLASSIFIER MAP NOMANAGEMENT RULE N.1
Access right and protocol .. deny tcp
Source/dest address ..... <host pc_1><any>
IP option ..... none
Source/dest port ..... <anyport><equ http>
TCP flag (value/wildmask) .. none
CLASSIFIER MAP NOMANAGEMENT RULE N.2
Access right and protocol .. deny tcp
Source/dest address ..... <host pc_1><any>
IP option ..... none
Source/dest port ..... <anyport><equ telnet>
TCP flag (value/wildmask) .. none
CLASSIFIER MAP NOMANAGEMENT RULE N.3
Access right and protocol .. permit anyprot
Source/dest address ..... <any><any>
IP option ..... none
```

go to the **firewall** node to associate and activate the “NOMANAGEMENT” classifier-map using the following command:

```
ATOSNT\firewall >>add PACKET-FILTER nomanagement ROUTER in
Command executed
```

You can show the configuration with the **show conf** command:

LIST OF PACKET FILTERS

CLASSIFIER MAP	IFC TYPE	INTERFACE NAME	DIRECTION	DISCARD MODE
NOMANAGEMENT	ROUTER		IN	

Index

ManClassifierIpv6

Classifier IPv6 - Overview

classifier-ipv6 node allows to classify the traffic.
Classifiers are used in combination with the rules in services such as QoS, Firewall, advanced routing, classifier map and so on.

Calssifier IPv6 - Commands

In **classifier-ipv6** node you can configure the following parameters

```
ATOSNT\classifier-ipv6>>set ?

Nodes not available.
Set command parameters:
 level of log  [loglevel]  Current value: 1
```

Table 1: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the Classifier IPv6 events. Default: 1

To add a new Rule or IPv6 Classifier, you should use **add** command

```
ATOSNT\classifier-ipv6>>add ?

add  help :  Add new RULE or IPV6 CLASSIFIER
add  usage:
 <CLASSIFIER><name>[rule-number]<target>
             [prot[not]<value>]
             [src[not]<addr[/prefix]>]
             [dst[not]<addr[/prefix]>]
             [in-ifc[not]<name>]
             [out-ifc[not]<name>]
             [recent[check|update]<time><count>]
             [limit[hour|second|minute|day]<rate><burst>]

add command parameters:
 CLASSIFIER
```

Table 2: add

Syntax	Description
CLASSIFIER	Keyword
name [Any value(max 32 char)]	Sets the classifier's name
rule-number [1-64]	Sets the rule number to apply to IPv6 packets
target [deny|permit]	Specifies the target of the rule
src|dst|in-ifc|out-ifc| recent|limit]	Sets one of the following option parameters that make up the rule specification: • prot the protocol of the rule or of the packet to check

	• protocol match [not] when set to "not" it allows to classify the traffic that is different to the one to which the rule is being applied. • protocol [0-255|tcp|udp|vrrp|icmpv6|ipv6route|ipv6frag] the specified protocol can be a number (0-255) or one of tcp, udp, vrrp, icmpv6, ipv6route or ipv6frag. • src source specification • source match [not] when set to "not" it allows to classify the traffic that is different to the one to which the rule is being applied. • source [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/0-128] specifies IPv6 source address and prefix • dst destination specification • destination match [not] the specified rule is applied each time the traffic daoes not match the destination address • destination [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/0-128] specifies IPv6 destination address and prefix • in-ifc Specifies the name of the interface via which the packet is received • in match [not] when set to "not" it allows to classify the traffic that is different to the one to which the rule is being applied. • in [router|loopback0|eth0|eth1|dlci100] Sets one of the configured interfaces • out-ifc Specifies the name of an interface via which a packet is going to be sent • out match [not] when set to "not" it allows to classify the traffic that is different to the one to which the rule is being applied. • out [router|loopback0|eth0|eth1|dlci100] Sets the name of an interface via which a packet is going to be sent • recent [check|update] Sets the recent check or update mode • recent time [1-4294967295|none] Sets the recent time in sec • limit [hour|second|minute|day] Sets the maximum average matching rate specified as hour, second, minute or day. • limit rate [1-4294967295] Sets the maximum average matching rate specified as a packet number • limit burst [1-4294967295] Sets the maximum initial number of packets to match: this number gets recharged by one every time the limit specified above is not reached, up to this number

To delete a rule or an IPv6 Classifier, you should use **del** command

```
ATOSNT\classifier-ipv6>>del ?

del  help :  Delete a RULE or IPV6 CLASSIFIER
```

```
del  usage:
 <CLASSIFIER><name>[rule-number]

del command parameters:
 CLASSIFIER
```

Table 3: del

Syntax	Description
CLASSIFIER	Keyword
name	Name of the classifier to be deleted
rule-number	Number of the rule in which the classifier is being used

ManClassmapProfile

Classmap Profile Configuration

Classmap profile defines the match conditions of a profile without setting any action to take.

Classmap profile works very closed to the **Classifier Map**. Classmap profile contains additional parameters with respect the Classifier map, useful for example for the **firewall** configuration.

Classmap Profile - Node

In the **classmap-profile** node you can configure a profile for a packet classification

Classmap Profile - Commands

In the classmap-profile node, the following parameters can be set and add:

```
ATOSNT\classmap-profile>>set ?

Nodes not available.

ATOSNT\classmap-profile>>add ?

add  help :  Add a MATCH PROFILE
add  usage:
 <MATCH-COND><name>

add command parameters:
 MATCH-COND

ATOSNT\classmap-profile>>add MATCH-COND newprof
Command executed
```

Table 1:**add MATCH-COND**

Syntax	Description
MATCH-COND	Keyword Specifies the match conditions of the profile
name	Specifies the profile's name

```
ATOSNT\classmap-profile>>set ?

Available nodes:
                      newprof

ATOSNT\classmap-profile>>newprof
ATOSNT\classmap-profile\newprof>>set ?

Nodes not available.
Set command parameters:
 description        [description]             Current value:
 protocol           [protocol]                Current value: udp
 source addr/name   [source-ip-address]       Current value: 192.168.110.75
  source wildmask   [src-wildmask]            Current value: 0.0.0.0
 dest addr/name     [destination-ip-address]  Current value: router
 dest wildmask      [dest-wildmask]           Current value: 0.0.0.0
 ip option          [ip-option]               Current value: 0
 source min port    [src-min-port]            Current value: http
 source max port    [src-max-port]            Current value: any
 dest min port      [dest-min-port]           Current value: any
 dest max port      [dest-max-port]           Current value: any
 tcp flag           [tcp-flag]                Current value: 00
 tcp flag wildmask  [tcp-flag-wildmask]       Current value: 00
 icmp type          [icmp-type]               Current value: none
 source ifc         [src-ifc]                 Current value: eth0
 policy             [policy]                  Current value: none
 limit rate value   [limit-rate-value]        Current value: 0 *
 limit rate unit    [limit-rate-unit]         Current value: second *
 limit bursts       [limit-bursts]            Current value: 0 *
 recent time (sec)  [recent-time]             Current value: 0 *
 recent count       [recent-count]            Current value: 0 *
 fragment option    [fragmentation]           Current value: unspecified *
 conn state         [conn-state]              Current value: Established *

* Stateful Firewall setting commands
```

Table 2:**set**

Syntax	Description
description [max 100 char]	Specifies a brief descrition for the profile set
protocol [0-256|tcp|udp| icmp|any]	Specifies the access protocol type Default: any
source-ip-address [Any value(0-100 char)|router|any]	Specifies the source IP address Default: any
src-wildmask [aa.bb.cc.dd]	Specifies the source wildmask Default: 0
destination-ip-address [Any value(0-100 char)|router|any]	Specifies the destination IP address Default: any
dest-wildmask [aa.bb.cc.dd]	Specifies the destination wildmask Default: 0
ip-option [0-255|loosero uting| timestamp|recordroute| strictrouting|sourcerouting| routeralert|anyoption]	Specifies the IP option Default: 0
src-min-port [0-65535|any| dns|ftp|ftpdata|pop2|pop3| smtp|snmptrap|telnet|http|tftp	Specifies the source minimum port number Default: any
src-max-port [0-65535|any| dns|ftp|ftpdata|pop2| pop3|smtp|snmptrap| telnet|http|tftp]	Specifies the source maximum port number Default: any
tcp-flag [0-3F hex]	Specifies the tcp flag Default: unspecified
tcp-flag-wildmask [0-3F hex]	Specifies the tcp flag wildmask Default: 0
icmp-type [echorequest|echoreply|none]	Specifies the icmp type Default: none
src-ifc [eth0|loopback0]	Specifies the source interface Default: empty
policy [none|ipsec]	Specifies the policy Default: none
limit-rate-value [0-65535]	Specifies the rate-limit of specific incoming packets Default: 0
limit-rate-unit [unspecified|second| minute|hour|day]	Specifies the rate-limit of the incoming packets for an specific time period Default: unspecified
limit-bursts [0-65535]	Specifies the admited short bursts in excess of the limit rate Default: 0
recent-time (sec) [0-65535]	Specifies the limit of the incoming (for instance SSH) connection attempts from an external host to an specific number (count) within a time interval in sec. Default: 0
recent count [0-65535]	Specifies the limit of the incoming (for instance SSH) connection attempts from an external host to an specific number (count) within a time interval in sec. Default: 0
fragmentation [unspecified|2nd+further|headonly]	Specifies matching for fragmented packets Default: unspecified
conn-state [none|Invalid|Established| New|Related|E+N|E+R|N+R|I+N| I+E|I+R|I+E+N|E+N+R|I+E+R| I+N+R|I+E+N+R]	Specifies the matching conditions with packets in different states Default: none

Classmap Profile Configuration Example

ATOSNT\classmap-profile\newprofile>>**show conf**

Show of ATOSNT classmap-profile newprofile

Description :

Protocol : tcp

Source addr/name : 192.168.110.75

Source wildmask : 0.0.0.0

Dest addr/name : any

Dest wildmask : 0.0.0.0

Ip option : 0

Source min port : any

Source max port : any

Dest min port : any

Dest max port : any

Tcp flag : 0

Tcp flag wildmask : 0

Icmp type : none

Source ifc :

Policy : none

Limit rate value : 0

Limit rate unit : unspecified

Limit bursts : 0

Recent time (sec) : 0

Recent count : 0

Fragment option : unspecified

Conn State : Established

Index

ManConnectivityMonitor

Connectivity Monitor Configuration

Connectivity Monitor is the feature that allows to monitor different services such as VOIP or BACKUP service. Several probes can be set up using different probe names. The probes allow to monitor all protocols stack levels and to report any state change (UP / DOWN).
At the moment only PING probe type has been implemented.
A PING probe, informs about a status change when a reachable destination IP address becomes unreachable and vice versa.

The main scope of the probe is to declare if the destination IP address is reachable (**UP**) or unreachable (**DOWN**).

Connectivity Monitor - Commands

Connectivity Monitor feature is available on **connectivity-monitor** node. You can use set, add and del commands to configure the available parameters at this node.

```
ATOSNT\connectivity-monitor>>set ?

Nodes not available.
Set command parameters:
 level of log  [loglevel]  Current value: 1
```

Table 1: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the node events . Default: 1

```
ATOSNT\connectivity-monitor>>add ?

add  help :  Add a new connectivity monitor probe
add  usage:
 <PROBE>[name][type]

add command parameters:
 PROBE
```

*Table 2:***add**

Table 2: add

Syntax	Description
PROBE	Keyword
name	It is the probe name. If the name is unspecified a probe called "probeidx" is created, “idx” is a progressive index starting from 0.
type	Defines the probe type. At the moment only “PING” type is available.

```
ATOSNT\connectivity-monitor>>del ?

del  help :  Remove a connectivity monitor probe
del  usage:
 <PROBE>[name][type]

del command parameters:
 PROBE
```

Table 3: del

Syntax	Description
PROBE	Keyword
name	It is the probe name. If the name is unspecified a probe called "probeidx" is created,“idx” is a progressive index starting from 0.

The node "name" contains a set of configuration parameters. The configuration parameters of PING probe are the following:

```
ATOSNT\connectivity-monitor\probe0>>set ?

Nodes not available.
Set command parameters:
 level of log                     [loglevel]              Current value: 1
 initial delay (sec)              [initial-delay]         Current value: 100
 ip address                       [address]               Current value: 0.0.0.0
 local ip address                 [local-ip-address]      Current value: 0.0.0.0
 timeout (msec)                   [timeout]               Current value: 200
 packet size                      [packet-size]           Current value: 32
 burst size                       [burst-size]            Current value: 5
 burst loss threshold (percent)   [burst-loss-threshold]  Current value: 20
 inter burst time (sec)           [inter-burst-time]      Current value: 4
 ok burst number                  [ok-burst-number]       Current value: 3
 ko burst number                  [ko-burst-number]       Current value: 1
 window burst number              [window-burst-number]   Current value: 3
 inter window time (sec)          [inter-window-time]     Current value: 4
 ip tos code (hex)                [tos]                   Current value: B8
```

Table 4: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOS to log the events of the probe, from the less detailed one (0) to the more detailed one (5) [Default: 1]
initial-delay [0-300]	Waiting time before the probe activation. Range:0-300 sec [Default: 100 sec]
address	Sets the destination address of ping request [Default: 0.0.0.0.]
local-ip-address	To configure the source address used for ping request probe The address must be present on one of the interface available, created before (i.e. loopback or logic interface) If this parameter is set to 0.0.0.0 means that source for ping probe packets will be the address assigned to the interface according to the routing table [Default: 0.0.0.0]
timeout [20-2000]	Timeout for ping response [Default: 200 msec]
packet-size [16-1024]	Size of ping request packet [Default: 32 bytes]
burst-size [1-255]	Number of ping request sent for each burst. [Default: 5]
burst-loss-threshold [1-100]	Maximum percentage of packets lost per burst of ping to declare success (burst OK) [Default: 20 percent]
inter-burst-time [1-255]	Time period in seconds between bursts of ping [Default: 4sec]
ok-burst-num [1-255]	Number of consecutive successful bursts to declare the probe in the UP state [Default: 3]
ko-burst-num [1-255]	Number of consecutive failed bursts to declare the probe in the DOWN state [Default: 1]
window-burst-number [value]	Number of bursts in the observation window. This parameter can be used to limit the traffic generated by the connectivity monitor. Range:Max (ok-burst-num, ko-burst-num)-255 [Default: 3]
inter-window-time [value]	Time period in seconds between two observation windows. This parameter can be used to limit the traffic generated by the connectivity monitor. Range: inter-burst-time - 255 [Default: 4]
ip-tos-code [0-0xFF]	TOS of ping request packet [Default: 0xB8]

PROBE Status - UP/DOWN

Show Status command shows any status change (UP or DOWN) based on the reachability of the destination IP address

In the configuration process, you should follow these steps:

1. define the remote destination IP address you want to reach and monitor
2. associate the probe PING test to one CPE's interface

for more details look at the following example.

PING Configuration example

This is an example of PING configuration. The PING probe0 is associated to eth0 interface to monitor a remote IP address **192.168.119.200** that is reachable.

With **show status** command, you can see **up** status.

Look at the commands to use:

ATOSNT\connectivity-monitor\probe0>>**show status**

probe0 status: **up**

LIST OF probe0 RUNNING USERS

eth0

Command executed

ATOSNT\connectivity-monitor>>**conf**

add connectivity-monitor PROBE probe0

set connectivity-monitor probe0 address 192.168.119.200

add interfaces IFC eth0 eth0

set interfaces eth0 conn-mon-probe probe0

set interfaces eth0 ip address 192.168.1.1/24

set interfaces eth0 ip dhcp-client on

add ip route 0.0.0.0 0.0.0.0 192.168.1.1 1

ATOSNT\connectivity-monitor>>**show work**

Show of ATOSNT connectivity-monitor

Level of log : 1

Show of ATOSNT connectivity-monitor probe0

Level of log : 1

Initial delay (sec) : 100

Ip address : **192.168.119.200**

Local IP Address : 0.0.0.0

Timeout (msec) : 200

Packet size : 32

Burst size : 5

Burst loss threshold (percent) : 20

Inter burst time (sec) : 4

OK burst number : 3

KO burst number : 1

Window burst number : 3

Inter window time (sec) : 4

Ip TOS code (Hex) : B8

Command executed

ATOSNT\interfaces>>**show work**

Show of ATOSNT interfaces

Level of log : 1

Show of ATOSNT interfaces loopback0

Level of log : 1

Description :

Show of ATOSNT interfaces loopback0 ip

Level of log : 1

IP address : 127.0.0.1
Netmask : 255.255.255.255
MTU value : 1500
Show of ATOSNT interfaces eth0
Level of log : 1
Description :
Enable : on
Mean rate window (sec) : 0
Network group :
Network group disable time (sec) : 0
Connectivity monitor probe : **probe0**
Probe fault action : **none**
Use basic MAC address : false
Mirror to :
Encapsulation : 802.3
Show of ATOSNT interfaces eth0 ip
Level of log : 1
IP address : 192.168.119.49
Netmask : 255.255.255.0
Default router : 192.168.119.1
MTU value : 1500
DHCP client : on
Unnumbered from :
TCP MSS adjustment : path-mtu
Tx queue len : 1000
Show of ATOSNT interfaces eth0 service-8023
Tag insertion : off
Default VID : 1
Default priority : 0
Priority translation : off
Tag removal : off
Use ingress priority : false
LIST OF TOS TO PRIORITY
Empty list
LIST OF POLICY MARKER TO PRIORITY
Empty list
Command executed

Look at the status changing to "down" when the destination IP address 192.168.119.200 is not reachable.

ATOSNT\connectivity-monitor\probe0>>set address 192.168.119.200
ATOSNT\connectivity-monitor\probe0>>**show status**
probe0 status: **down**
LIST OF probe0 RUNNING USERS eth0
Command executed

When probe status is "down", in "interfaces" node, eth0 subnode, two possible actions can be chosen in "probe-fault-action" parameter configuration.

Look at the below commands to use

ATOSNT\interfaces\eth0>>set **probe-fault-action** ?

probe fault action [none|disconnect]

Current value: none

Default fw value: none

ATOSNT\interfaces\eth0>>set probe-fault-action **disconnect**

Command executed

ATOSNT\interfaces\eth0>>**show work**

Show of ATOSNT interfaces eth0

Level of log : 1

Description :

Enable : on

Mean rate window (sec) : 0

Network group :

Network group disable time (sec) : 0

Connectivity monitor probe : **probe0**

Probe fault action : **disconnect**

Use basic MAC address : false

Mirror to :

Encapsulation : 802.3

PROBE Status DOWN

In case the connectivity monitor PROBE status has changed to **down** because the destination IP address is not reachable any more, “probe-fault-action” parameter ("interfaces" node, eth0 subnode), can be configured with one of the two options:

- **None**

  eth0 interface will not remove the local static route but it will declare that it has lost its own IP address.

- **Disconnect**

  eth0 interface will remove the local static route; it will declare that it has lost its own IP address and it will try to renegotiate to get a new IP address.

In both cases, the loss IP address declaration means, that any static route configured on that interface will be removed from the working routing table.

Warning

Please note that if the new working routing table does not allow the reachability of the IP address monitored by the probe, the probe will always remain in **DOWN** state.

So in conclusion, the recommendation is to choose option:

- None

  if the address to be monitored by the probe, is inside the same subnet of the CPE or Router

- Disconnect

  if the probe is reachable via a different interface from eth0.

Index

ManConfTelnetSsh

Configuration via Telnet or SSH

ATOSNT provides **Telnet** and **SSH servers** services. With that services it is possible to access to the CLI of the remote device from any network reachable through a Telnet or SSH client.

To access via Telnet from a linux terminal:

```
user@linuxhost:~$ telnet 192.168.110.135
Trying 192.168.110.135...
Connected to 192.168.110.135.
Escape character is '^]'.
```

Then ATOSNT device asks for login:

```
login as: user
password: ****

ATOSNT Remote CLI

CTRL+d to exit

Init Command Line Interface...
ATOS Version: 5.4.0.rc2 (67@cwjnegs/egtmuqq)
ATOS Date: 02/09/2011 14:09
ATOS License: ETH1+TR069+AdvancedPlus
Hardware: BG1242FW - 2363B
Product Code: 708190270
Serial Number: 000098
eth0 MAC Address: 00:D0:D6:48:6D:0A
Wireless manager: 2.0.0
Wireless card: Atheros Communications, Inc. - AR5007G
AVDSL Driver version: 2.1.0

User name:user
Password:****
<user> logged at Administrator level
ATOSNT>>
```

The same thing when you use an SSH client, with the difference that depending on the used client, it is possible to configure a secure key:

```
user@linuxhost:~$ ssh 192.168.110.135

Entering character mode
Escape character is '^]'.

login as: user
password: ****
```

```
ATOSNT Remote CLI

CTRL+d to exit

Init Command Line Interface...
ATOS Version: 5.4.0.rc2 (67@cwjnegs/egtmuqq)
ATOS Date: 02/09/2011 14:09
ATOS License: ETH1+TR069+AdvancedPlus
Hardware: BG1242FW - 2363B
Product Code: 708190270
Serial Number: 000098
eth0 MAC Address: 00:D0:D6:48:6D:0A
Wireless manager: 2.0.0
Wireless card: Atheros Communications, Inc. - AR5007G
AVDSL Driver version: 2.1.0

User name:mario
Password:****
<mario> logged at Administrator level
ATOSNT>>
```

Index

ManDect

DECT

Some CPE models like BG8542 and BG7420 have integrated in the gateway a **DECT /CAT-iq™** base station that allows to work with any certified CAT-iq™ handset.

DECT stands for **Digital Enhanced Cordless Technology**.

A **DECT system** consists of a portable part (**DECT handset**) and a fixed part (**DECT base**).

There are 2 possible mechanisms to connect a portable part (DECT handset) to the fixed part (DECT base)

1. GAP
2. CAT-iq™

GAP stands for **Generic Access Profile** and has been defined to allow third party handsets to connect to a DECT base with limited functionality. No standardized power saving mechanisms are supported by this profile.

CAT-iq™ stands for **Cordless Advanced Technology, Internet and Quality** and has been defined to ensure interoperability between handsets and bases from different manufacturers. The level of interoperability is defined in dedicated **profiles** (1.0, 2.0, 2.1, 3.0, 4.0). A standardized **no emission mode** is included in the 2.0 profile, as an optional feature.

DECT - Commands

In the root node, there is the **dect** subnode, where you can configure the following parameters with set command

```
ATOSNT\dect>>set ?

Available nodes:
                        base0

Set command parameters:
 level of log  [loglevel]  Current value: 1
```

Notice that there is an available node, named **base0**. Actually the **dect** node automatically generates the **base0** node associated to it.

Table 1: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the DECT events. Default: 1

To add a new DECT base, you should use **add** command

Table 2: add a DECT

Syntax	Description
BASE	keyword
name [max 3 decimal digits]	Name of the DECT base to add

With **tree** command, you can see all the DECT bases.

```
ATOSNT\dect>>tree
dect                    base0
                        base1
```

To delete an existing DECT base, you should use **del** command

```
ATOSNT\dect>>del ?

del  help :  Delete a DECT
del  usage:
 <BASE><Name>

del command parameters:
 BASE
```

Table 3: del a DECT

Syntax	Description
BASE	keyword
name [max 3 decimal digits]	Name of the DECT base to delete

DECT Node - Configuration

dect Node automatically generates a subnode named **base0**.

If you go to **base0** node, you can configure the following parameters:

```
ATOSNT\dect\base0>>set ?

Nodes not available.
Set command parameters:
 enable              [on|off]             Current value: on
 level of log        [loglevel]           Current value: 1
 description         [description]        Current value:
 pin code            [pin-code]           Current value: 1234
 nemo support        [NEMO-Support]       Current value: off
 encryption enable   [encryption-enable]  Current value: off
 rf enable           [RF-enable]          Current value: off
```

Table 4: set

Syntax	Description
on|off	Enables/disables the DECT base functionality
loglevel [0-5]	Sets the level of log. Default: 1
description [max 100 char]	Sets a brief description of the DECT base
pin-code [max 8 char]	Sets a **pin code** for the handsets registration. The "pin code" is a password (max 8 characters, in the above example is "1234") to be used by the handsets during the registration to the base station. Notice that many handsets allow a pin code of 4 characters as maximum. The DECT base integrated in the CPE, can manage up to 6 DECT handsets.
NEMO-Support [on|off]	Enables/disables the **"no emission"** mode. **Nemo** mode means completely deactivating all the transmitters when the system is idle. The main focus of this mode is to minimize the emitted radiated power of the system. The power consumption in the handset increases as it has to listen more often for the beacon signal. This mode is standardized, so it is interoperable between different vendors. All handsets which are attached to the CPE need to support this mode before it can be enabled. It is an optional feature of CAT-iq^{TM} 2.0. Default: off
encryption-enable [on|off]	Set on means that the data transmission between the base and the handset is encrypted Default: off
RF-enable [on|off]	Activates/deactivates the RF transceiver of the DECT base Default: off

Note: Notice that by default the "RF-enable" parameter is off and you must set on as well as "enable [on|off]" parameter. After setting both parameters, the DECT base works properly and the DECT LED on the front panel is turn on.

Show Work

You need to assign a pin code to each DECT base station you will use. In this case, only one base station has been used, **base0** and the **pin code** assigned is **1234**. See bellow.

```
ATOSNT\dect\base0>>show work
Show of ATOSNT dect base0
Enable            : on
Level of log      : 1
Description       :
Base type         : on-board
Pin Code          : 1234
NEMO Support      : on
Encryption enable : off
RF enable         : on

Command executed
```

Show Status

```
ATOSNT\dect\base0>>show status

base0 Info
 Firmware Info
 Max registrable handsets: 6
 Registered handsets: none
```

Note that the maximum number of handsets supported by base0 station is 6.

DECT Node - Operating Commands

In **base0** node there are the following operating commands:

```
ATOSNT\dect\base0>>?

Nodes not available.

Available commands:

register                Enable registration on node ATOSNT\dect\base0>>
de-register             Delete registration on node ATOSNT\dect\base0>>
page                    Paging on node ATOSNT\dect\base0>>
call-test               Make a call test on node ATOSNT\dect\base0>>
```

Lets see in detail each one of them

DECT Handsets Registration

The are two ways to register the handsets to the DECT base station, one is using the CLI **register** command, the other one is using the **DECT button** placed at the CPE rear panel.

Warning: Before starting the handsets registration, the "pin-code" parameter of the base station must be configured.

Example of Handset Registration with Register Command

To register the handset using CLI **register** command, you should perform these steps:

1. Take the handset or cordless telephone
2. With the help of the terminal menu, enter in the "Portable" configuration page
3. Enter as "pin code" "1234" that is the same used in the DECT base
4. Choose "Register" function from the terminal menu

Now you should type **"register"** , see below for more details.

```
ATOSNT\dect\base0>>register?

register  help :  Enable registration
register  usage:
 no parameters

register command parameters:
 <cr>
ATOSNT\dect\base0>>register

Waiting for handset registration (60 sec)
Command executed
```

Notice that the base station is now waiting for the request of the handset registration for 1 minute period.

After this period, the two units, the base and the handset can "see" each other and the handset will be registered to the main base.

For this example we have taken two cordless terminals from the market, one is branded Siemens (handset1), the other one is Alcatel (handset2).

With **show Status** command, you will see this info:

```
ATOSNT\dect\base0>>show status

base0 Info
 Firmware Info
 Max registrable handsets: 6
 Registered handsets: handset1,handset2
   Handset1 codecs: G.722, G.726
   Handset2 codecs: G.726
 Attached handsets: handset1,handset2
```

Notice that the terminal registration order nominates the terminal number, so the first terminal registered is named "handset1" and so on.

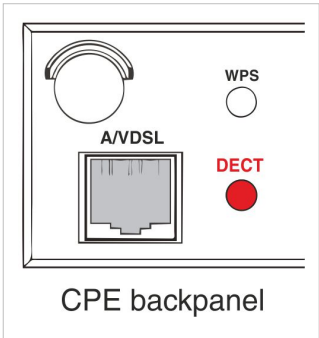
Example of Handset Registration with DECT Button

Before starting the handsets registration, check that "enable" and "RF-enable" parameters are set on and the DECT LED at the CPE front panel is fixed on (the base station is working properly).

This is the starting point. Note that 6 is the maximum number of handsets to be registered the the base0 station.

```
ATOSNT\dect\base0>>show work
Show of ATOSNT dect base0
Enable             : on
Level of log       : 1
Description        :
Base type          : on-board
Pin Code           : 1234
NEMO Support       : on
Encryption enable  : off
RF enable          : on

Command executed

ATOSNT\dect\base0>>show status

base0 Info
 Firmware Info
 Max registrable handsets: 6
 Registered handsets: none

Command executed
```

At the CPE backpanel there are two buttons, as you can see in the below picture.



CPE backpanel

To register the handset using DECT button, you should perform these steps:

1. Take the handset or cordless telephone
2. With the help of the terminal menu, enter the "Portable" configuration page
3. Enter "pin code" "1234" that is the same used in the DECT base
4. Choose from the terminal menu "Register the Portable"

At this point, press DECT button for more than 5". The DECT LED starts flashing for 60 seconds, actually the LED is on for 500 ms and then is off for another 500 ms. During this period, the base station is listening the terminals requests for registration.

At last with **show status** you can see the two handsets registration.

```
ATOSNT\dect\base0>>show status

base0 Info
 Firmware Info
 Max registrable handsets: 6
 Registered handsets: handset1,handset2
   Handset1 codecs: G.722, G.726
   Handset2 codecs: G.726
 Attached handsets: handset1,handset2
```

```
Command executed
```

Call-test

Call-test command allows to make a call test to a handset at a time. This useful tool allows the administrator network to rapidly identify where the handset is and to decide in which area of office or home to place it.

```
ATOSNT\dect\base0>>call-test ?

call-test  help :  Make a call test
call-test  usage:
 <choice handset>

call-test command parameters:
 handset            [handset1|handset2]

ATOSNT\dect\base0>>call-test handset2

Making test call on handset2
Command executed

ATOSNT\dect\base0>>call-test handset1

Making test call on handset1
Command executed
```

De-register

De-register command allows to delete the handsets registration.

The administrator has multiple choices to delete the handset registration, he can delete the registration of all handsets or one specific handset at a time (handset1 or handset2).

See below how the command works.

```
ATOSNT\dect\base0>>de-register ?

de-register  help :  Delete registration
de-register  usage:
 <choice handset>

de-register command parameters:
 handset            [all-handset|handset1|handset2]
```

Example of how to delete the handsets registration

In this example the de-registration of all handsets to the DECT base is performed

ATOSNT\dect\base0>>de-register all-handset

De-registering all-handset

Command executed

At last, you can verify the result with **show status** command

ATOSNT\dect\base0>>**show status**

base0 Info

Firmware Info

Max registrable handsets: 6

Registered handsets: none

Paging Functionality - Command

With **page** command, the base station sends an audible and/or alert signal to all handsets indicating that the base wants to know where the handsets are placed.

See below for more details.

```
ATOSNT\dect\base0>>page ?

page  help :  Paging
page  usage:
 no parameters

page command parameters:
 <cr>
```

Example of how paging the handsets associated to the base

Start typing **page** command as described in the above paragraph. As a result, all handsets are ringing at the same time.

```
ATOSNT\dect\base0>>page

Paging on Handset1
Paging on Handset2
Command executed
```

Intercom - Making Internal Calls

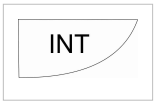
Intercom is short for intercommunication.

For communications within a building, at the office or home, you can use the **Intercom** mode that allows to make internal calls, **free of charge**, to other DECT handsets registered to the same base station. The base station integrated in the CPE supports up to 6 handsets that can be placed in different areas of the office or home.

Calling other handsets

Suppose that two DECT handsets hace been registered to the base in this order of registration, first handset1 and then handset2, and that handset1 wants to make a call to handset2.

To start the internal call, take **handset1**



Press **INT** button

Enter number **2** that corrisponds to the receiving handset. Then **handset2** is called.

Ending a call

To end the call, press the **end call** button.

Making and Receiving External Calls

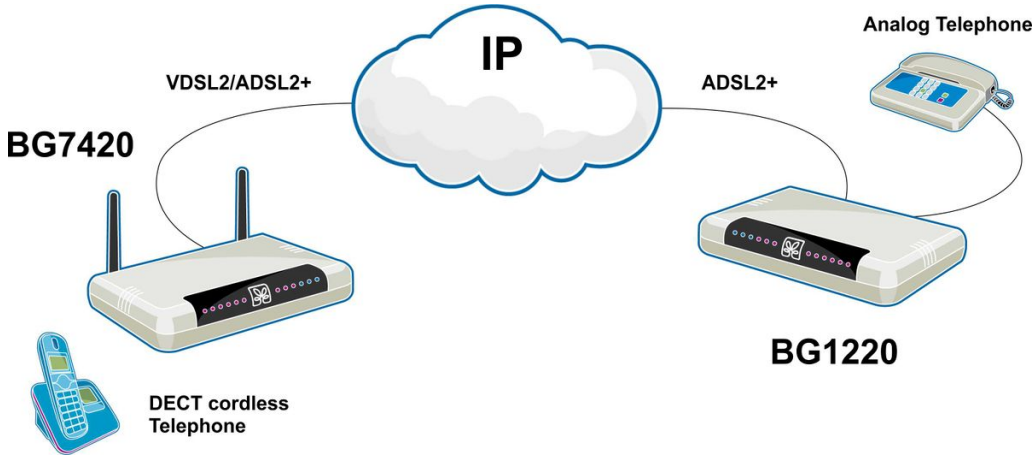
In order to make and receive calls from outside, you should go to section **Call-mng – Commands** at the **VoIP** node and configure the parameters of **INBOUND** and **OUTBOUND** functionalities

Example of DECT Configuration

Application Scenario

At the local site there is a CPE **BG7420** with a **DECT cordless telephone** connected and at the remote site, there is another CPE **BG1220** with an **Analog telephone (POTS)** connected to it.

BG7420 and BG1220 are business VoIP gateways with router functionalities.



Suppose that a user at the local site, wants to make and receive calls from the Analog Telefone connected to BG1220.

DECT cordless telephone is registered to the base station **DECT base0** with username "9202".
DECT base0 is the base station integrated into the **BG7420**
The number asigned to the remote Analog Telefone is "9201".

The example shows how to configure BG7420 to make and receive external calls using a DECT handset

ATOSNT>>**show conf**

set wlan0 RF-mode b-g-n

set wlan0 ssid ATOS-NT:wlan0

set wlan0 nick ATOS-NT:wlan0-NICK

set dect base0 pin-code 0000

set dect base0 RF-enable on

add interfaces IFC eth0 eth0

set interfaces eth0 ip address 192.168.1.2/24

set interfaces eth0 ip defaultrouter 192.168.1.1

set interfaces eth0 ip dhcp-client on

add voip user-terminal DECT base0 1

add voip trunk SIP 9202

set voip trunk sip-9202 on

set voip trunk sip-9202 authentication-password 9202

set voip trunk sip-9202 authentication-user-id 9202

set voip trunk sip-9202 user-name 9202

set voip trunk sip-9202 proxy-host 192.168.31.200

set voip trunk sip-9202 registrar-host 192.168.31.200

add voip call-mng OUTBOUND dect-base0.1 ALL-NUMBER 0 NO-PREPEND sip-9202 default

add voip call-mng INBOUND sip-9202 ALL-NUMBER dect-base0.1

ATOSNT>>**show dect status -s**

List of attached DECT devices

Empty list

base0 Info

Firmware Info

Max registrable handsets: 6

Registered handsets: handset1

Handset1 codecs: G.722, G.726

Attached handsets: handset1

Command executed

ATOSNT>>**show voip status -s**

Current Connections = 1 (Max Connections = 8)

Status of Sip

TrunkName	Host	dnsmgr	Username	Refresh State	Reg.Time
9202	192.168.31.200:5060	N	9202	124 Registered	25 March 2014 21:04:06

1 SIP registrations.

Status of dect-base0.1

Configuration status : enable, used into InBoundList, OutBoundList

Status : OUTGOING ACTIVE(9201)

DECT-FP Air Codec : G.726

DSP Resource : ALLOCATED

DSP Media : OPENED

DSP Encoder : CODE-G729_8

DSP Decoder : CODE-G729_8

Echo cancellation : ON

Silence suppression : OFF

Connected to : 192.168.31.240:5100

Status of sip-9202

Configuration status : enable

Current Registrar Host : 192.168.31.200

Current Proxy Host : 192.168.31.200

Secondary Proxy Hosts : None

Interface status : eth0 up

Registration status : Registered (Refresh Time = 123 sec)

Logical status : used into InBoundList,OutBoundList

Message waiting : No

Connections:

UserTerm	Dir	RemoteUser	Codec
dect-0.1	to	9201	G.729a

Command executed

ATOSNT>>**show voip statistics -s**

Statistics of dect-base0.1

	Incoming	Outgoing
Calls :	2	3
Calls Answer :	1	2
Calls Busy :	0	0
Calls No Answer :	0	0
Calls Failed :	1	1

Realtime statistics

VOICE pkts from Line : 12306

VOICE octects from Line : 246120

VOICE pkts to Line : 12310

VOICE octects to Line : 246200

MOS R value : 93.00

MOS calculation time interval : 4

MOS advantage factor : 1

MOS LQE measured : 4.1

VOICE pkts from handset : 24547

VOICE pkts to handset : 24583

VOICE pkts overflow from handset : 2

VOICE pkts underflow from handset : 0

VOICE pkts invalid from handset : 0

PLC pkts from handset : 1

Statistics of sip-9202

	Incoming	Outgoing
Calls :	2	3
Calls Answer :	1	2
Calls Busy :	0	0
Calls No Answer :	0	0
Calls Failed :	1	1

Connections:

Duration	RECV: Pack	Octects	Lost	%	Jitt	SEND: Pack	Octects	Lost	%	Jitt	UserTerm	Dir	RemoteUser
00:04:10	0000012345	0000246900	00000	00%	0000	0000012350	0000247000	00000	00%	0002	dect-0.1	to	9201

Statistics of Call-mng

ID	SOURCE		DESTINATION		START	END	TOTAL	RESULT	ACTIVE
75424.0	dect-base0.1	1	sip-9202	9201	2014-03-25 20:57:04	2014-03-25 20:57:14	10	ACTIVE	7
75473.2	sip-9202	9201	dect-base0.1	9202	2014-03-25 20:57:53	2014-03-25 20:58:06	13	ACTIVE	3
75892.6	sip-9202	9202	dect-base0.1	9202	2014-03-25 21:04:52	2014-03-25 21:04:52	0	NO-ANS	
75891.4	dect-base0.1	1	sip-9202	9202	2014-03-25 21:04:51	2014-03-25 21:04:56	5	FAILED	

ID	RECV: Pack	Octects	Lost	%	Jitt	SEND: Pack	Octects	Lost	%	Jitt
75424.0	0000000350	0000007000	00000	00%	0000	0000000354	0000007080	00000	00%	0000
75473.2	0000000159	0000003180	00000	00%	0000	0000000164	0000003280	00000	00%	0000

Command executed

List of compatible DECT handsets or cordless telephones

This is the list of the DECT cordless telephones tested in our lab and fully compliant with ATOSNT:

- Siemens Gigaset Model AS200

- Siemens Gigaset Model A58H

- Siemens Gigaset Model C610

- ALCATEL Versatis F250

- ALCATEL Versatis E100

ManDhcp

DHCP

DHCP stands for "Dynamic Host Control Protocol" and enables to automatically assign (**DHCP Server**) or to get (**DHCP Client**) TCP/IP configuration.

This functionality provides easy network management for administrators, because the same configuration can be used for all devices, without the need to manually assign the TCP/IP parameters to every PC.

ATOSNT implements both DHCP Server and DHCP Client features.

DHCP Server – Commands

In case you want to use DHCP Server function, you have to go to the subnode **dhcpserver** in the root node:

```
ATOSNT\dhcpserver>>set?

Set command parameters:
 enable                 [on|off]          Current value: off
 level of log           [loglevel]        Current value: 1
 timeout server (msec)  [server-timeout]  Current value: 0
```

Table 1: set

Syntax	Description
on | off	Enables/disables the DHCP server [default: off]
loglevel [0-5]	Sets the detail level used by ATOSNT to record the events of the DHCP server operations [default: 1]
server-timeout (msec) [0-30000]	Configures, in milliseconds, the time after that the device replies to a DHCP request if none DHCP server has already replied to [default: 1000]

```
ATOSNT\dhcpserver>>add ?

add  help :  Add a new pool
add  usage:
 <IFC><Interface name>[manual-binding]

add command parameters:
 IFC
```

Example of how to built a new dhcp pool on ETH0 interface:

```
ATOSNT\dhcpserver>>add iFC eth0
```

Table 2: add

Syntax	Description
IFC	Keyword.
Interface name	String that identifies the interface you want to use (e.g. ETH0, ETH1, ETH0:0, VCC0..).
manual-binding | Normal	If “MANUAL-BINDING” option is specified, the created pool will be manual binding type where it is possible to release for a specific client (the pool is built only for one client), a specific IP Address. The association is identified through the client Id or “HW Address” (such as the client MAC ADDRESS). In addition, all other DHCP parameters are offered in the “Offered DHCP" phase.

```
ATOSNT\dhcpserver>>del ?

del  help :  Delete pool
del  usage:
 <IFC><Pool name>

del command parameters:
  IFC
```

Table 3: del

Syntax	Description
IFC	Keyword.
Pool Name	String that identifies the pool name you want to delete (e.g. ETH0, ETH1, ETH0:0, VCC0, …).

DHCP Server – Nodes

Once a DHCP pool has been created, a new subnode with the used interface name appears.

“Interface” pool – Commands

```
ATOSNT\dhcpserver\eth0>>set ?

Available nodes:
                      relay

Set command parameters:
 enable                        [on|off]          Current value: on
 description                   [description]     Current value:
 first address of pool         [startaddress]    Current value: 192.168.110.136
 last  address of pool         [endaddress]      Current value: 192.168.110.254
 netmask                       [netmask]         Current value: 255.255.255.0
 address default router        [defaultrouter]   Current value: 192.168.110.135
 address primary dns           [dns1]            Current value: 192.168.110.135
```

```
address secondary dns          [dns2]            Current value: 0.0.0.0
address primary wins           [wins1]           Current value: 0.0.0.0
address secondary wins         [wins2]           Current value: 0.0.0.0
lease time (sec) (0=disable)   [leasetime]       Current value: 86400
host name                      [hostname]        Current value: PC_0
domain name                    [domainname]      Current value: LocalDomain
tftp server name               [server-name]     Current value:
boot file name                 [boot-file-name]  Current value:
file name                      [boot-file]       Current value:
next server ip                 [next-server]     Current value: 0.0.0.0
```

Table 4: set

Syntax	Description
Learning-ifc	Associates the DHCP learning mode to the selected interface (e.g. vcc0-ppp0).
startaddress [aa.bb.cc.dd]	Indicates the first address that the DHCP server can use for assignment to hosts in the ETH0 (default: 192.168.1.2, i.e. the IP address after the default address assigned to the device over ETH0).
endaddress [aa.bb.cc.dd]	Indicates the last address that the DHCP server can use for assignment to hosts in the ETH0 (default: 192.168.1.254).
defaultrouter [aa.bb.cc.dd]	Default router address. The information is included in the configuration assigned by the DHCP server to the hosts in the ETH0 (default: 0.0.0.0).
dns1 [aa.bb.cc.dd]	Primary DNS address (default: 0.0.0.0). The information is included in the configuration assigned by the DHCP server to the hosts in the ETH0.
dns2 [aa.bb.cc.dd]	Secondary DNS address (default: 0.0.0.0). The information is included in the configuration assigned by the DHCP server to the hosts in the LAN.
wins1 [aa.bb.cc.dd]	WINS address (default: 0.0.0.0). The information is included in the configuration assigned by the DHCP server to the hosts in the ETH0.
wins2 [aa.bb.cc.dd]	Secondary WINS address (default: 0.0.0.0). The information is included in the configuration assigned by the DHCP server to the hosts in the ETH0.
leasetime (sec) (0=disable) [(0)-(2147483647)]	Time in seconds during which the use of the assigned address is guaranteed to the host, default: 86400.
hostname [max 24 char]	Basic name assigned to the hosts (0-20 characters, default: PC_ . Hosts are assigned a name made up of the basic name followed by two decimals (i.e. PC_01, PC_02).
domainname [max 240 char]	Domain name assigned to the hosts with 0-23 characters, default: DomName.
server-name [max 64 char]	Sets the TFTP server name (option 66). The information is included in the configuration assigned by the DHCP server to the hosts in the ETH0.
boot-file-name [max 32 char]	Sets the Boot file name name (option 67). The information is included in the configuration assigned by the DHCP server to the hosts in the ETH0.
boot-file	Sets a Boot file string. It is refered to the “file” field header of the DHCP ACK packet (RFC2131)
next-server	Specifies the TFTP server IP address usually used by IP Phone to download the “boot file”

You can activate the DHCP learning when you operate with PPP encapsulation. During the initial negotiation the remote PPP server releases a pool of addresses (one IP address and one subnet mask defining the number of usable addresses). The PPP client dynamically overwrites the DHCP fields with the new values that remain valid until the connection is active. The DHCP distributes these values to the hosts in the local network that request them. This mode allows the network administrator to configure both WAN and LAN addresses dynamically from remote.

The addresses of the pool used by the DHCP server must be compatible with the address assigned to the device over the ETH0.

Dynamic “IFC_pool” node allows to define:

- a static association between the host mac address and the IP address that a DHCP server releases to that host;
- a list of hosts, each identified by its mac address, that cannot accept an IP address released by a DHCP server .

```
ATOSNT\dhcpserver\eth0>>add ?

Available nodes:
                       relay
add  help :  Add static association or excluded host or option

add  usage:
 <STATIC-ASSOCIATION><ip addr><mac-address:aa-bb-cc-dd-ee-ff> to STATIC-ASSOCIATION LIST
 <EXCLUDED-HOST><mac-address:aa-bb-cc-dd-ee-ff>               to EXCLUDED-HOST LIST
 <EXCLUDED-ADDRESS><start-ip-addr>[end-ip-addr]               to EXCLUDED-ADDRESS LIST
 <OPTION><option-code><option-type><option value..>           to OPTION LIST

add command parameters:
 STATIC-ASSOCIATION
 EXCLUDED-HOST
 EXCLUDED-ADDRESS
 OPTION
```

Table 5: add/del

Syntax	Description
STATIC-ASSOCIATION <ip addr><mac addr>	Associates a device mac address to an IP address released by a DHCP server. Up to 128 entries can be added.
EXCLUDED-HOST <mac addr>	Indicates, by the mac address, the host that cannot have an IP address from a DHCP server. Up to 128 entries can be added.
EXCLUDED-ADDRESS	Allows to exclude an IP address contained in a DHCP pool addresses. If “end-address is specified a whole range can be excluded. If the DHCP pool is active, every changed is performed immediately. If the DHCP is not active, that means no restart is done after creating the new pool, every add/del entry will be active after a restart. Up to 128 excluded host range can be defined. The following warning or error can be showN when a wrong command is typed: **End address must be greater than start address** - if start address is greater than end address, **Excluded addresses must be inside pool** - if it is defined a range out of the pool , **Excluded addresses already defined**" - if an excluded range is already defined, **List of excluded address full** - if 128 excluded ranges are just defined **Warning some excluded ip address are already in use** - if one or more IP address are excluded, and those IP are just in use, it is recommended to perform a restart to right manage the DHCP client request.
OPTION <option-code>	Specifies the DHCP option code (from 1 to 255) **OPTION Type:** **HEX** indicates that the option value is expressed by a sequence of bytes in hexadecimal annotation, separated by “space. Each number can express up to 4 bytes, depending of the hexadecimal digits written: 1 or 2 hexadecimal digits express 1 byte 3 or 4 hexadecimal digits express 2 bytes 5 or 6 hexadecimal digits express 4 bytes 7 or 8 hexadecimal digits express 4 bytes. **ASCII** indicates that the option value is referred to ASCII string. It cannot be separated by “space The option ascii value is 64 characters maximum **IP** indicates that the option value is expressed as a punctual dotted IP address. To define several IP address “space must be used from an IP address value and the other.

	Up to 16 option-code for each type of expression used can be created. The maximum value length is 64 bytes. Examples: Add option 128 hex 0F indicates that the option 128 has 1 byte, the decimal value is 15 and it will be coded in DHCP packet 0x80 0x01 0x0F Add option 128 hex 000F indicates that the option 128 has 2 bytes, the decimal value are 0 and 15 and it will be coded in DHCP packet 0x80 0x02 0x 00 0x0F Add option 128 hex 0B0AF1 indicates that the option 128 has 3 bytes, the decimal value are 11, 10 and 241 and it will be coded in DHCP packet 0x80 0x03 0x0B 0x0A 0xF1 Add option 128 ip 192.168.0.1 indicates that the option 128 has as value an IP address 192.168.0.1 and it will be coded in DHCP packet 0x80 0x04 0xC0 0xA8 0x00 0x01 Add option 128 ip 192.168.0.1 192.168.0.2 indicates that the option 128 has 2 ip address value: 192.168.0.1 and 192.168.0.2. It will be coded in DHCP packet 0x80 0x08 0xC0 0xA8 0x00 0x01 0xC0 0xA8 0x00 0x02 Add option 128 ascii abcde indicates that the option 128 has abcdee as string value and it will be coded in DHCP packet 0x80 0x05 0x61 0x62 0x63 0x64 0x65

“Interface” pool – Configuration Example

ATOSNT\dhcpserver\eth0>>**show conf**
Show of ATOSNT dhcpserver eth0
Learning interface : ----
First address of pool : 192.168.1.2
Last address of pool : 192.168.1.254
Netmask : 255.255.255.0
Address default router : 192.168.1.1
Address primary DNS : 192.168.1.1
Address secondary DNS : 0.0.0.0
Address primary WINS : 0.0.0.0
Address secondary WINS : 0.0.0.0
Lease Time (sec) (0=Disable) : 7200
Host name : PC_0
Domain name : LocalDomain
TFTP server name :
Boot file name :
File name :
Next server ip : 0.0.0.0
LIST OF STATIC ASSOCIATION
IP Address MAC Address
192.168.1.102 00-18-F3-07-33-79
192.168.1.101 00-18-F3-07-33-78
192.168.1.100 00-18-F3-07-33-77
LIST OF EXCLUDED HOST
MAC Address
00-18-F3-07-33-73
00-0B-AC-38-F4-82
00-C0-02-E0-E0-BE
LIST OF EXCLUDED ADDRESS
START ADDRESS END ADDRESS
192.168.1.3 192.168.1.3
192.168.1.5 192.168.1.25
LIST OF OPTION
Empty list
Show of ATOSNT dhcpserver eth0 relay
Enable : off
LIST OF DHCP SERVER
Empty
Command executed

In the following example is shown a simple DHCP server configuration procedure on the ETH0 interface:

```
interfaces
add IFC eth0 802.3 eth0
top
set interfaces eth0 on
set interfaces eth0 ip address 192.168.1.1
set interfaces eth0 ip netmask 255.255.255.0
set dhcpserver on
dhcpserver
add ifc eth0
top
set dhcpserver eth0 startaddress 192.168.1.2
set dhcpserver eth0 endaddress 192.168.1.254
set dhcpserver eth0 netmask 255.255.255.0
set dhcpserver eth0 defaultrouter 192.168.1.1
set dhcpserver eth0 dns1 192.168.1.1
set dhcpserver eth0 leasetime 0
set dhcpserver eth0 hostname PC_0
set dhcpserver eth0 domainname LocalDomain
```

To trace the DHCP Server events, the following command can be used:

```
set dhcpserver loglevel 5 -s
log start
L1: U 08/01/2010 14:16:32:430 OFDhcp: Receive DISCOVER
L2: U 08/01/2010 14:16:32:430 OFDhcp: Interface=eth0 option: ciaddr=0.0.0.0 yiaddr=0.0.0.0 Host name=roberto-laptop Parameter request list=1 28 2 3 15 6 119 12 44 47 26 121 42
L1: U 08/01/2010 14:16:32:430 OFDhcp: Send OFFER
L2: U 08/01/2010 14:16:32:430 OFDhcp: Interface=eth0 option: ciaddr=0.0.0.0 yiaddr=192.168.1.2 Net mask=255.255.255.0 Lease time=-1 Default router=192.168.1.1 Domain name=LocalDomain DNS=192.168.1.1 Host name=roberto-laptop Server Addres=192.168.1.1
L1: U 08/01/2010 14:16:32:430 OFDhcp: Receive REQUEST
L2: U 08/01/2010 14:16:32:430 OFDhcp: Interface=eth0 option: ciaddr=0.0.0.0 yiaddr=0.0.0.0 Server Addres=192.168.1.1 Addres=192.168.1.2 Host name=roberto-laptop Parameter request list=1 28 2 3 15 6 119 12 44 47 26 121 42
L1: U 08/01/2010 14:16:32:430 OFDhcp: Send ACK
L2: U 08/01/2010 14:16:32:430 OFDhcp: Interface=eth0 option: ciaddr=0.0.0.0 yiaddr=192.168.1.2 Net mask=255.255.255.0 Lease time=-1 Default router=192.168.1.1 Domain name=LocalDomain DNS=192.168.1.1 Host name=roberto-laptop Server Addres=192.168.1.1
```

Pool-manual-binding– Commands

When the “MANUAL-BINDING” option is selected a manual binding DHCP server pool will be created, where for a certain client (pool for a unique client), identified by a “client id” or a “HW address”, it is possible to release a specific IP address and other DHCP parameters.

```
ATOSNT\dhcpserver>>add iFC eth0 manual-binding
```

In the “eth0_mb0” node, all DHCP parameters managed by ATOSNT can be configured. Moreover, in this case, two additional settings can be done:

```
ATOSNT\dhcpserver\eth0_mb0>>set ?

Nodes not available.
Set command parameters:
 enable                          [on|off]          Current value: on
 client id (hex format)          [client-id]       Current value:
 client hw address               [hw-address]      Current value: 00-00-00-00-00-00
 ip address                      [address]         Current value: 0.0.0.0
 netmask                         [netmask]         Current value: 255.255.255.0
 address default router          [defaultrouter]   Current value: 192.168.110.135
 address primary dns             [dns1]            Current value: 192.168.110.135
 address secondary dns           [dns2]            Current value: 0.0.0.0
 address primary wins            [wins1]           Current value: 0.0.0.0
 address secondary wins          [wins2]           Current value: 0.0.0.0
 lease time (sec) (0=disable)    [leasetime]       Current value: 86400
 host name                       [hostname]        Current value: PC_1
 domain name                     [domainname]      Current value:
 tftp server name                [server-name]     Current value:
 boot file name                  [boot-file-name]  Current value:
 file name                       [boot-file]       Current value:
 next server ip                  [next-server]     Current value: 0.0.0.0
```

Table 6: set

Syntax	Description
client-id <string hex value>	Identifies the client-id parameter to assign the unique IP address released by the DHCP server pool. The string value must be in “dotted hexadecimal notation” format (eg. 00.1.03.A.0B.CC.DD.EE.FF.41.01). If client-id string is configured, no hw-address string mac address must be present.
hw-address <string mac address>	Identifies the HW address parameter (typically the MAC ADDRESS) to assign the unique IP address released by the DHCP server pool. The string value must be in “dotted hexadecimal notation” format (eg. 01.02.0A.0B.0C.0D) If hw-address mac address string is configured, no client-id string must be present.
address <ip addr>	Configures the unique ip address released by DHCP server for this pool. The selected address must not be present in any other pool

As in the “normal” pool, in the Manual binding pool it is possible to specify DHCP option code (from 1 to 255), using the following command:

```
ATOSNT\dhcpserver\eth0_mb0>>add ?

add  help :  Add option

add  usage:
 <OPTION><value>

add command parameters:
 OPTION
```

```
ATOSNT\dhcpserver\eth0_mb0>>del ?

del  help :  Delete option

del  usage:
 <OPTION><value>

del command parameters:
 OPTION
```

Pool Nodes

Relay – Commands

```
ATOSNT\dhcpserver\eth0\relay>>add ?

add  help :  Add a new DHCP server
add  usage:
 <DHCP-SERVER><ip addr server DHCP>

add command parameters:
 DHCP-SERVER

ATOSNT\dhcpserver\eth0\relay>>del ?

del  help :  Delete a DHCP server
del  usage:
 <DHCP-SERVER><ip addr server DHCP>

del command parameters:
 DHCP-SERVER
```

Table 7: add/del

Syntax	Description
dhcp-server <ip addr server DHCP>	Indicates, with DHCP relay mode enabled, a DHCP server in the net for DHCP request forwarding.

```
ATOSNT\dhcpserver\eth0\relay>>set ?

Nodes not available.
Set command parameters:
 enable  [on|off]  Current value: off
```

Table 8: set

Syntax	Description
onloff	Enables/disables a DHCP request forwarding to a DHCP server in the net already configured with add command.

DHCP Client - Commands

The **dhcpclient** node allows to configure the loglevel and the vendor-id information.

It is possible to associate the DHPC client functionality to any interface that requires an IP address.

```
ATOSNT\dhcpclient>>set ?

Nodes not available.
Set command parameters:
 level of log       [loglevel]   Current value: 1
 vendor identifier  [vendor-id]  Current value: off
```

Table 9: set

Syntax	Description
Loglevel <1-5>	Sets the detail level used by ATOSNT to record the events of the DHCP client operations. [default: 1].
vendor-id <onloff>	Enables/Disables transmission of Vendor Id information at BOOTP phase (option 43, 60, 125): • Option 43: Vendor-Specific Information (25 bytes) • Option 125: Unassigned (30 bytes) • Option 60: Vendor class identifier = "dslforum.org"(Default off)

```
ATOSNT\dhcpclient>>add ?

add  help :  Add Client id

add  usage:
 <CLIENT-ID><ifc-name><ASCII|HEX><option>

add command parameters:
 CLIENT-ID
```

Table 10: set

Syntax	Description
CLIENT-ID	Keyword
ifc-name	the interface name
ASCII | HEX	the Client-id type
option	the Client-id value • ASCII: max 32 char length string • HEX: max 32 Hexadecimal value

In the following example the device will require an IP address for its interface to the network (ETH0 side):

interfaces

add IFC eth0 802.3 eth0

top

set interfaces eth0 on

set interfaces eth0 ip dhcp-client on

To trace the DHCP Client events, the following command can be used:

set dhcpclient loglevel 5

log start

L1: U 08/01/2010 11:12:30:170 OFDhcpCli: frame DISCOVER transmitted on interface eth0

L1: U 08/01/2010 11:12:30:230 OFDhcpCli: Process frame OFFER received on interface eth0

L1: U 08/01/2010 11:12:30:230 OFDhcpCli: frame REQUEST transmitted on interface eth0

L1: U 08/01/2010 11:12:30:290 OFDhcpCli: Process frame ACK received on interface eth0

L1: U 08/01/2010 11:12:30:290 OFDhcpCli: parameters obtained on interface eth0.

L1: U 08/01/2010 11:12:30:290 OFDhcpCli:

Specific ip address : 192.168.110.163

Net mask : 255.255.255.0

Address gateway : 192.168.110.1

DNS : 192.168.111.131

DHCP server address : 192.168.111.132

Leased time : 14400 sec

Index

ManDhcp6client

DHCP6CLIENT

dhcp6client node allows you to create and manage profiles for dhcp6 clients

DHCP6CLIENT – Commands

Set command permits to configure global parameters of dhcp6client node.

```
ATOSNT\dhcp6client>>set ?

Nodes not available.
Set command parameters:
 level of log  [loglevel]  Current value: 1
```

Table 1: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOS to record dhcp6 clients events.

ManDhcp6server

DHCP6server

"Dynamic Host Configuration Protocol for IPv6" (further **DHCPv6**) enables DHCP servers to pass configuration parameters such as IPv6 network addresses to IPv6 nodes (Routers and Hosts).

DHCPv6 is the "stateful address autoconfiguration protocol" and is specified in RFC 3315.

DHCPv6 offers the capability of automatic allocation of reusable network addresses and additional configuration flexibility (e.g. DNS server, NTP server,etc.).

DHCPv6 Protocol Options

Options are used to carry additional information and parameters in DHCPv6 messages. Every option shares a common base format. Some options apply to the client, some are specific to an IA (Identity Association), and some are specific to the addresses within an IA.

Rapid Commit Option

Is an available option. When a client includes a Rapid Commit option in a Solicit message, if the client is prepared to perform the Solicit-Reply (two) message exchange, the server will respond with a Reply message that includes the Rapid Commit option and will commit the assigned addresses in the Reply message to the client.

In the following paragraphs you can find three basic modes to configure a DHCPv6 server. The user can try other configurations just making combinations of them.

- **Stateless mode**

  DHCP server releases only options (and not addresses)

- **Stateful mode**

  DPCPv6 server releases a pool of IPv6 addresses

- **Prefix Delegation**

DHCPv6 server is delegating a prefix, that is a pool of IPv6 addresses (and not options)

DHCP6server – Commands

Set command permits to configure global parameters in the dhcp6server node.

```
ATOSNT\dhcp6server>>set?

Set command parameters:
 enable                 [on|off]             Current value: off
 level of log           [loglevel]           Current value: 1
```

Table 1:set

Syntax	Description
enable [on|off]	Activates/deactivates all dhcp6 pools. A pool is a range of IPv6 addresses assigned by the DHCPv6 server Default: on
loglevel [0-5]	Sets the detail level used by ATOSNT to record dhcp6 server events. Default: 1

Clear command permits to reset all addresses lists and restart all dhcp6 servers.

```
ATOSNT\dhcp6server>>clear?

clear  help :  Clear all entry
clear  usage:
 no parameters

clear command parameters:
 <cr>
```

Table 2:clear

Syntax	Description
clear	It clears all entry

Add command allows to configure a pool for an existing interface. **Del** command deletes an existing pool.

```
ATOSNT\dhcp6server>>add ?

add  help :  Add a new dhcp6 pool
add  usage:
 <IFC><Interface name>

add command parameters:
 IFC

ATOSNT\dhcp6server>>add IFC ?

add command parameters:
 interface name[eth0]
ATOSNT\dhcp6server>>add IFC eth0
```

```
Command executed
```

```
ATOSNT\dhcp6server>>del ?

Available nodes:
                        eth1
del  help :  Delete dhcp6 pool
del  usage:
 <IFC><Pool name>

del command parameters:
 IFC
```

Table 3:add/del

Syntax	Description
IFC	Keyword
Interface name	String that identifies the associated interface (e.g. ETH0, ETH1, ETH0:0, VCC0, …).

DHCP6server Pool – Commands

Set command permits to configure dhcp6 server pool.

```
ATOSNT\dhcp6server\eth1>>set ?

Available nodes:
                      pd

Set command parameters:
 enable                    [on|off]              Current value: on
 description               [description]         Current value:
 pool                      [pool]                Current value: none
 t1 timer (sec)            [t1-timer]            Current value: 3600
 t2 timer (sec)            [t2-timer]            Current value: 5400
 preferred lifetime (sec)  [preferred-lifetime]  Current value: 86400
 valid lifetime (sec)      [valid-lifetime]      Current value: 86400
 option lifetime (sec)     [option-lifetime]     Current value: 86400
 rapid commit              [rapid-commit]        Current value: off
```

Table 4: set

Syntax	Description
enable [on|off]	Activates/deactivates the DHCP6 pool [default: off].
description	Description for DHCP6 pool.
pool [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/0-128|none]	Sets the IPv6 addresses pool. [Default: none]
t1-timer [1-2147483647|infinity]	T1 is the time expressed in units of seconds at which a client contacts the server from which the addresses were obtained to extend the lifetimes of the addresses assigned. The value 0xffffffff is taken to mean "infinity" when used as a lifetime or a value for T1 or T2. [Default: 3600]
t2-timer [1-2147483647|infinity]	T2 is the time expressed in units of seconds at which the client contacts any available server to extend the lifetimes of the addresses assigned to the IA_NA. The value 0xffffffff is taken to mean "infinity" when used as a lifetime or a value for T1 or T2. [Default: 5400]
preferred-lifetime [1-2147483647|infinity]	It is the time in seconds that a valid address is preferred (i.e., the time until deprecation). When the preferred lifetime expires, the address becomes deprecated. Preferred lifetime must not be larger than valid lifetime. You should configure word INFINITY for infinity time. [Default: 86400]
valid-lifetime [1-2147483647|infinity]	It is the time in seconds that an address remains in the valid state (i.e., the time until invalidation). The valid lifetime must be greater than or equal to the preferred lifetime. When the valid lifetime expires, the address becomes invalid. [Default: 86400]
option-lifetime [600-2147483647]	It is the time in seconds that a client should wait before refreshing the information retrieved from DHCPv6 server. It must be greater than 600 seconds. This option is used with stateless DHCPv6 because there are no addresses or other entities with lifetimes that can tell the client when to contact the DHCPv6 server to refresh its configuration. [Default: 86400]
rapid-commit [on|off]	Activates/deactivates the DHCPv6 Rapid Commit Option. The Rapid Commit option is used to signal the use of the two message exchange for address assignment.

Add command allows to configure in the DHCPv6 server network parameters to release to the clients like DNS or NTP server addresses.

```
ATOSNT\dhcp6server\eth0>>add ?

add  help :  Add a new OPTION
add  usage:
 <OPTION><type><value>

 add command parameters:
 OPTION

ATOSNT\dhcp6server\eth0>>add OPTION ?

add command parameters:
 Type [DNS-SERVER|DOMAIN-NAME|NTP-SERVER|SIP-SERVER|SIP-DOMAIN|
```

```
        NIS-SERVER|NIS-DOMAIN|NIS+SERVER|NIS+DOMAIN]
```

Table 5: set

Syntax	Description
OPTION	Keyword
DOMAIN-NAME| NTP-SERVER|SIP-SERVER| SIP-DOMAIN|NIS-SERVER| NIS-DOMAIN|NIS+SERVER| NIS+DOMAIN]	Selects the option type to configure in the DHCPv6 server
DNS-SERVER [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]	Specifies the IPv6 address of a Domain Name System (DNS) server available to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client.
DOMAIN-NAME [max 253 char]	Configures a Domain Name for a DHCP for IPv6 client
NTP-SERVER [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]	Specifies the IPv6 address of a Network Time Protocol (NTP) server available to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client.
SIP-SERVER [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]	Specifies the IPv6 address of a SIP server available to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client.
SIP-DOMAIN [max 253 char]	Configures a SIP Domain Name available to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client.
NIS-SERVER [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]	Specifies the IPv6 address of a network information service (NIS) server available to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client. DHCPv6 for stateless configuration allows a DHCPv6 client to export configuration parameters like DHCPv6 options to a local DHCPv6 server. The local DHCPv6 server can then provide the imported configuration parameters to other DHCPv6 clients.
NIS-DOMAIN [max 253 char]	Configures a NIS Domain Name available to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client.
NIS+SERVER [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]	NIS+ server option provides a list of IPv6 addresses of NIS+ servers available to send to the client.
NIS+DOMAIN [max 253 char]	Enables a DHCPv6 server to export a client's NIS+ domain name information to the DHCPv6 client.

DHCP6server Prefix Delegation mode

In Prefix Delegation mode, the DHCPv6 server is delegating a prefix, that is a pool of IPv6 addresses. It does not release options.

The Prefix Delegation mode provides a mechanism for automated delegation of IPv6 prefixes using the Dynamic Host Configuration Protocol (DHCP). This mechanism is intended for delegating a long-lived prefix from a delegating router to a requesting router. It is appropriate for situations in which the delegating router does not have knowledge about the topology of the networks to which the requesting router is attached, and the delegating router does not require other information aside from the identity of the requesting router to choose a prefix for delegation.
For example, these options would be used by a service provider to assign a prefix to a Customer Premise Equipment (CPE) device acting as a router between the subscriber's internal network and the service provider's core network.
The requesting router subnets the delegated prefix and assigns the longer prefixes to links in the subscriber's network. In a typical scenario, the requesting router subnets a single delegated /48 prefix into /64 prefixes and assigns one /64 prefix to each of the links in the subscriber network.

```
ATOSNT\dhcp6server\eth1\pd>>set ?

Nodes not available.
```

```
Set command parameters:
 enable                        [on|off]              Current value: off
 pd pool                       [pool]                Current value: none
 pd length                     [pd-length]           Current value: unspecified
 pd t1 timer (sec)             [t1-timer]            Current value: 3600
 pd t2 timer (sec)             [t2-timer]            Current value: 5400
 pd preferred lifetime (sec)   [preferred-lifetime]  Current value: 86400
 pd valid lifetime (sec)       [valid-lifetime]      Current value: 86400
```

Table 6: set

Syntax	Description
enable [on | off]	Enables/disables the DHCPv6 prefix delegation. Default: off.
pd-pool [prefix/plen | none]	Specifies the Prefix Delegation pool. Default: none.
pd-lenght [1-128 | unspecified]	Configures the Prefix Delegation lenght. Default: unspecified.
t1-timer [1-2147483647|infinity]	T1 is the time expressed in units of seconds at which a client contacts the server from which the addresses were obtained to extend the lifetimes of the addresses assigned. The value 0xffffffff is taken to mean "infinity" when used as a lifetime or a value for T1 or T2. Default: 3600.
t2-timer [1-2147483647|infinity]	T2 is the time expressed in units of seconds at which the client contacts any available server to extend the lifetimes of the addresses assigned to the IA_NA. The value 0xffffffff is taken to mean "infinity" when used as a lifetime or a value for T1 or T2. Default: 5400.
preferred-lifetime [1-2147483647|infinity]	Length of time that a valid address is preferred, when expires, the address becomes deprecated. Time in seconds, must not be larger than valid lifetime. Configure word INFINITY for infinity time. Default: 86400.
valid-lifetime [1-2147483647|infinity]	Length of time an address remains in the valid state, when expires, the address becomes invalid. Time in seconds, must be greater than or equal to the preferred lifetime. Configure word INFINITY for infinity time. Default: 86400.

DHCP6server Stateful mode - Configuration Example

In Stateful mode, the DHCP6 server releases a pool of IPv6 addresses

ATOSNT\dhcp6server\eth1>>**conf**

add dhcp6server IFC eth1

add dhcp6server eth1 OPTION DNS-SERVER 2001:4860:4860::8888

add dhcp6server eth1 OPTION DNS-SERVER 2001:4860:4860::8844

set dhcp6server eth1 pool 2015:15::/64

ATOSNT\dhcp6server\eth1>>**show work**

Show of ATOSNT dhcp6server eth1

Enable : on

Description :

Pool : 2015:15::/64

T1 timer (sec) : 3600

T2 timer (sec) : 5400

Preferred lifetime (sec) : 86400

Valid lifetime (sec) : 86400

Option lifetime (sec) : 86400

Rapid commit : off

LIST OF OPTIONS

TYPE	OPTION-VALUE
DNS-SERVER	2001:4860:4860::8888
DNS-SERVER	2001:4860:4860::8844

Show of ATOSNT dhcp6server eth1 pd

Enable : off

PD pool : none

PD length : unspecified

PD T1 timer (sec) : 3600

PD T2 timer (sec) : 5400

PD Preferred lifetime (sec) : 86400

PD Valid lifetime (sec) : 86400

Command executed

ManDdns

DDNS

ATOSNT delivers a Dinamyc DNS (**DDNS**) client feature. That is, it maintains the IP address of a host name. It periodically checks whether the IP address stored by the DNS server is the real current address of the device that is running. Several DDNS services can be configured.

DDNS – Commands

```
ATOSNT\ddns>>add ?

add help : Add a new DDNS profile

add usage:

<DDNS-CLIENT>[name]

add command parameters:

DDNS-CLIENT
```

Table 1: add

Syntax	Description
DDNS-Client	Keyword. If no name is configured, after adding a DDNS client a new subnode will be created by using DDNS-Client-n name, where “n” is the number of the entry created.
name	Optionally, you can customize the subnode name that will be created. If no name is specified, a name will automatically be assigned as :ddns-client-x where x is a progressive number.

Example: Configuration of a DDNS service using DynDNS.org:

ATOSNT\ddns>>add DDNS-Client myddns

Command executed

```
ATOSNT\ddns>>del ?

del  help :  Remove a DDNS profile
del  usage:
 <DDNS-CLIENT><name>

del command parameters:
 DDNS-CLIENT
```

Table 2: del

Syntax	Description
DDNS-CLIENT	Keyword.
name	Name of the DDNS client you want to delete.

Example:

ATOSNT\ddns>>del DDNS-Client myddns

Command executed

DDNS – Nodes

As soon as a new DDNS client is added, the corresponding subnode will be created.

```
ATOSNT\ddns\ddns-client-1>>set ?

Nodes not available.

Set command parameters:
level of log [loglevel] Current value: 1
description [description] Current value:
enable [on|off] Current value: on
local ip address [local-ipaddress] Current value: 0.0.0.0
update period (sec)  [update-period] Current value: 60
username [username] Current value: myusername
password [password] Current value: mypw
DDNS system [ddns-system] Current value: dyndns@dyndns.org
Alias [alias] Current value: myhost@dyndns.org</pre>
```

Table 3: set

Syntax	Description
loglevel	Configures the detail level used by ATOSNT to record the DDNS events: 0 no type of anomalous event is saved; 1 errors (i.e. protocol errors); 2 errors and first level warnings; 3 errors and second level warnings; 4 errors, first and second level warnings, first level signaling; 5 errors, first and second level warnings, first and second level signaling.
Description	Up to 100 characters can be used to write a description of the DDNS clinet service (default null).
enable [on |off]	Enables/disables the selected DDNS client (default on)
local-ipaddress	Configures the DDNS client IP address (default 0.0.0.0).

update-period	Configures how often the IP is checked. The period is in seconds. Default is 60 seconds.
username	Change member name (username) configuration used by the DDNS client (provided by the DDNS Service Provider)
password	Change password configuration used by the DDNS client (provided by the DDNS Service Provider)
DDNS-system	Change DDNS system name (e.g. dyndns@dyndns.org [1]default@no-ip.com [2], statdns@dyndns.org)
alias	Change Host name you have chosen for the DDNS service

Index

References

[1] mailto:dyndns@dyndns.org
[2] mailto:default@no-ip.com

ManDns

DNS

ATOSNT delivers **DNS server** and **forwarder** functionalities to make easier PC's configuration and installation over the LAN. When DNS server/forwarder functionalities are active, the queries of a host name can be addressed directly to ATOSNT.

To avoid using one or more external DNS servers, you only need to configure the IP address of the Aethra device over the ETH as DNS primary server.

Queries for local host name are resolved by ATOSNT. Queries for remote host name are returned by ATOSNT to one or more external DNS, whose addresses are configured in a list of servers. ATOSNT supports recursive queries.

Once the final answer has been obtained, the answer is transmitted to the PC over the local network that has released the query and is saved on a local cache, in order to be used to resolve the next queries with the same name locally.

The DNS cache is contained in a volatile memory. The information contained in the DNS cache is lost when the device is switched off.

DNS – Commands

```
ATOSNT\dns>>set ?

Available nodes:
                        host

Set command parameters:
 enable                  [on|off]           Current value: on
 level of log            [loglevel]         Current value: 5
 max retries             [maxretries]       Current value: 3
 timeout retries (sec)   [timeout]          Current value: 20
 defaults host ifc       [defaulthost-ifc]  Current value:
```

Table 1: set

Syntax	Description
on|off	Activates/deactivates DNS server/forwarder functionalities. Default: on.
loglevel [0-5]	Set the detail level used by ATOSNT to record events in the DNS node. Default: 1.
maxretries [1-255]	Sets the maximum number of attempts to the same server. Default: 3.
timeout (sec) [0-65535]	Sets the maximum waiting time of the answer to a query. Default: 20 sec/10.
defaulthost [<cr>|eth0]	Activates/deactivates the system name resolution (configurable in ATOSNT\System>>node of the device in the specified interface. If enabled, ATOSNT internal services (Telnet, WEB server) can be invoked from a PC in the LAN, by simply referring to the name assigned to the device. Default: <cr> (disabled).

You can create a list of external DNS servers used by ATOSNT to address queries on unknown host names, with the following commands/options:

```
ATOSNT\dns>>add ?

Available nodes:
                        host
add  help :  Add a new DNS server
add  usage:
   <SERVER><domain/host-name><primary-ip>[secondary-ip] [src-ip/mask] [prio]
   <SERVER><domain/host-name><ifc-name> [primary-ip] [secondary-ip] [src-ip/mask] [prio]

add command parameters:
  SERVER
```

Table 2: add

Syntax	Description
SERVER	Keyword. .
domain/host-name [Any value(max 100 char)|anydomain]	Specifies the DNS domain or single hostname to resolve. If “anyDomain” is used as domain name, it is intended to resolve all domains with this entry.
primary-ip [aa.bb.cc.dd] secondary-ip [aa.bb.cc.dd]	Indicate the addresses of the two DNS servers for the domain name (primary and possibly secondary).
ifc-name	Indicates the interface where one DNS server for all domains can be found. It is searched on the selected ifc interface (ifc name) configured with PPP or PPPoE encapsulation. The DNS server is advised by the access server (with string domain name domain) during the IPCP negotiation. The same address is deleted at the end of the PPP or PPPoE session.
src-ip/mask	Optional: if configured this entry, it is only applied for requests coming from that source ip/net
prio	Optional: this parameter gives a priority to this entry in order to have the possibility to chose preferred servers for a certain domain.

Example: configuration of one primary and secondary DNS from the default configuration.

ATOSNT>>add dns SERVER anyDomain vcc0-ppp0

ATOSNT\dns>>**show conf**

Show of ATOS dns

Enable: on

Level of log: 1

Max retries: 3

Timeout retries (sec/10): 20

Defaults host: on

LIST OF DNS SERVICE

DOMAIN NAME PRIMARY ADDRESS SECONDARY ADDRESS IFC

anyDomain vcc0-ppp0

Or:

ATOSNT**>>**add dns server anyDomain 1.1.1.1 2.2.2.2

LIST OF DNS SERVICE

DOMAIN NAME PRIMARY ADDRESS SECONDARY ADDRESS IFC

anyDomain 1.1.1.1 2.2.2.2

```
ATOSNT\dns>>del ?

Available nodes:
                        host
del  help :  Delete a DNS server
del  usage:
   <SERVER><domain/host-name><primary-ip>[secondary-ip]
   <SERVER><domain/host-name><ifc-name> [primary-ip] [secondary-ip]

del command parameters:
 SERVER
```

Table 3: del

Syntax	Description
SERVER	Keyword.
domain name	Deletes the entry from the list of DNS servers with *domain name*.

DNS – Nodes

Host

The DNS node contains a subnode that is used to add the resolutions of specific hosts.

```
ATOSNT\dns\host>>add ?

add  help :  Add a new host
```

```
add  usage:
 <host name><ip add>

add command parameters:
 host name        [max 100 char]
```

Table 4: add

Syntax	Description
host name [max 100 char]	Adds a static resolution of the host
ip add [aa.bb.cc.dd]	Host IP address

```
ATOSNT\dns\host>>del ?

del  help :  Delete a new host
del  usage:
 <host name>

del command parameters:
 host name        [max 100 char]
```

Table 5: del

Syntax	Description
host name	Deletes the static resolution with *host name* host value.

Index

ManEthxPhy

ETHx Physical Interfaces

ETH0, ETH1 and so on identify the node where pysical ethernet parameters can be managed.

One or multiple ETH interfaces are defined depending on the specific hardware model (usually referred to as ETH0, ETH1, etc.).

Depending on the model, if an ethernet switch is present, it is named ETH0 and a number of port subnodes allows the ethernet ports configuration.

Logical interfaces are abstract interfaces built on top an ETH interface (for more details see “Interfaces” paragraph)

ETHx – Commands

In case of ethernet switch in ETH0:

```
ATOSNT\eth0>>set ?

Available nodes:
                        port1
                        port2
                        port3
                        port4

Set command parameters:
 send buffer (bytes)   [send-buffer]           Current value: auto
 null vid replacement  [null-vid-replacement]  Current value: off
```

Table 1: set

Syntax	Description
send-buffer (bytes) [1-256000|auto]	Send buffer is a parameter that allows to dimension the size of a buffer developed to adapt the fast internal data transfer speed to the slower physical link and thus to reduce the latency [default auto]
null-vid-replacement [on|off]	Enables/disables the retagging action with the default port specific VID1to ingress frames with a null VID (a null VID may still carry 802.1p bits). [default: off]

```
ATOSNT\eth0>>add ?

add  help :  Add new VLAN
add  usage:
  <VLAN><VID value><port value (n-m,k,l)>[regular|native]

add command parameters:
 VLAN
```

Table 2: add VLAN

Syntax	Description
VLAN	Keyword
VID [1-4094]	802.1Q VLAN Identifier
port [n-m,a,b,c (1-4)]	Identify ports associated to VLAN ID. Ports can be configured one to one, using a comma to separate them, or as a range.
regular|native	*Only available on some CPE models* • regular: normal default behaviour • native: frames are transmitted untagged even if tag-removal is set to off. Allowed for a single vid only

Example: How to create a VLAN with VLAN ID 100 on port 1 and 2

ATOSNT\eth0>>add VLAN 100 1-2

Command executed

ATOSNT\eth0>>show conf

Show of ATOSNT eth0

Send buffer (bytes) : auto

Null vid replacement : off

LIST OF VLANS

VID Port

100 1,2

In case of single ethernet port in ETH0 (or ETHx) the following parameters can be managed:

```
ATOSNT\eth1>>set?


Nodes not available.


Set command parameters:

link mode [link-mode] Current value: auto

wiring mode [wiring-mode] Current value: auto
```

Table 3: set link-mode

Syntax	Description
Auto	Configure port in automatic mode (default), according to the 802.3 IEEE stardard.
10-half	Configure port in 10 half duplex transmission mode.
10-full	Configure port in 10 full duplex transmission mode.
100-half	Configure port in 100 half duplex transmission mode.
100-full	Configure port in 100 full duplex transmission mode.

Table 4: set wiring-mode

Syntax	Description
Auto	Configure wiring connection of the ethernet port in automatic mode (default).
MDIX	Configure wiring connection of the ethernet port in “Media Dependent Interface with Crossover” mode.
MDI	Configure wiring connection of the ethernet port in “Media Dependent Interface” mode.

Example to configure the ETH1 fix to 100 full duplex and MDI:

```
ATOSNT>>set eth1 link-mode 100-full

Command executed
```

```
ATOSNT>>set eth1 wiring-mode mDI
Command executed
```

```
ATOSNT>>show eth1 status

Status of port single

Wiring Status: MDI

Link Status: Up/100Mbps/Full-Duplex
```

ETHx – Nodes

Portx subnode

```
ATOSNT>>set eth0 port1?

Nodes not available.

Set command parameters:

link mode [link-mode] Current value: auto

wiring mode [wiring-mode] Current value: auto

default vid [default-vid] Current value: 1

default priority [default-priority] Current value: 0

tag removal [tag-removal] Current value: on
```

Table 5: set

Syntax	Description
link-mode <auto| 10-half| 10-full| 100-half| 100-full>	Configure the Ethernet port transmission in automatic mode (default), according to the 802.3 IEEE stardard.; in 10 half duplex mode, in 10 full duplex mode; in 100 half duplex mode; in 100 full duplex mode.
wiring-mode auto|MDIX|MDI	Configure wiring connection of the ethernet port. Auto: automatic mode (default). MDIX: “Media Dependent Interface with Crossover” mode. MDI: “Media Dependent Interface” mode.
default-vid value	Define the default vid applied to untagged ingress frames (range: 1 – 4094, default 0).
default-priority value	Define the default priority applied to untagged ingress frames (range: 0 – 7, default 0).
tag-removal on|off	Enable/disable 802.1Q and 8021.p tag removal from the frames transmitted from portX. [default: on]

Vlan packets (802.1q) coming from the local network are dropped when their VID value is different from the one already configured on one of the switch ports. Ethernet packets (802.3) coming from the local network become vlan packets with the default VID value.

ETHx – Status

Example to show the ETH0 ports status when at least one physical port is UP (only models with ethernet switch):

```
ATOSNT>>show eth0 status

Filtering Data Base of n.0 switch contents

List of dynamic entries

 N Age MAC Port

0000 2 00:00:AA:92:38:08 1
0001 3 00:02:B3:0A:A2:8F 1
0002 3 00:09:6B:85:68:75 1
0003 3 00:0B:AC:38:F4:82 1
0004 3 00:0C:29:00:85:87 1
0005 3 00:0C:29:37:19:A4 1
0006 3 00:0C:29:58:01:7A 1
0007 3 00:0C:29:85:AA:40 1
0008 3 00:0C:29:96:D3:AF 1
0009 3 00:0C:29:AE:59:17 1
```

```
0010 3 00:0F:20:9A:69:00 1
0011 3 00:0F:20:9A:69:27 1
0012 3 00:15:C5:1D:7A:36 1
0013 3 00:15:C5:1D:7C:32 1
0014 3 00:18:F3:07:1F:DA 1
0015 3 00:1A:C1:DA:67:4D 1
0016 3 00:1B:77:B6:DC:AA 1

Status of port 1

Wiring Status: MDI

Auto Negotiation: Completed

Link Status: Up/100Mbps/Full-Duplex

Partner Abilities: 100Full/100Half/10Full/10Half/Flow-Ctrl

Status of port 2
Link Status: Down

Status of port 3
Link Status: Down

Status of port 4
Link Status: Down
```

Example to show the ETH0 ports status when all physical ports are DOWN (only models with ethernet switch):

```
ATOSNT>>show eth0 status


Filtering Data Base of n.0 switch contents


List of dynamic entries

Empty



Status of port 1
Link Status: Down

Status of port 2
Link Status: Down

Status of port 3
```

```
Link Status: Down

Status of port 4
Link Status: Down
```

Example to show the ETH1 status when it is UP:

```
ATOSNT>>show eth1 status


Status of port single

Wiring Status: MDI

Auto Negotiation: Completed

Link Status: Up/100Mbps/Full-Duplex

Partner Abilities: 100Full/100Half/10Full/10Half/Flow-Ctrl
```

Example to show the ETH1 status when it is DOWN:

```
ATOSNT>>show eth1 status


Status of port single

Link Status: Down
```

Note 1 The default port VID parameter is configured on each portX subnode.

Index

ManEthernetCFM

Ethernet-CFM Overview

Link-layer OAM allows detection of faults on an Ethernet First Mile (EFM) link.

Ethernet-CFM or **Ethernet Service OAM** allows to monitor a customer's end-to-end Ethernet service. This monitoring ability is agnostic to the layers supporting the service, which may be EFM (i.e. DSL or native Ethernet fiber), but may also be other services such as SONET, ATM, or MPLS ("Ethernet pseudowires").

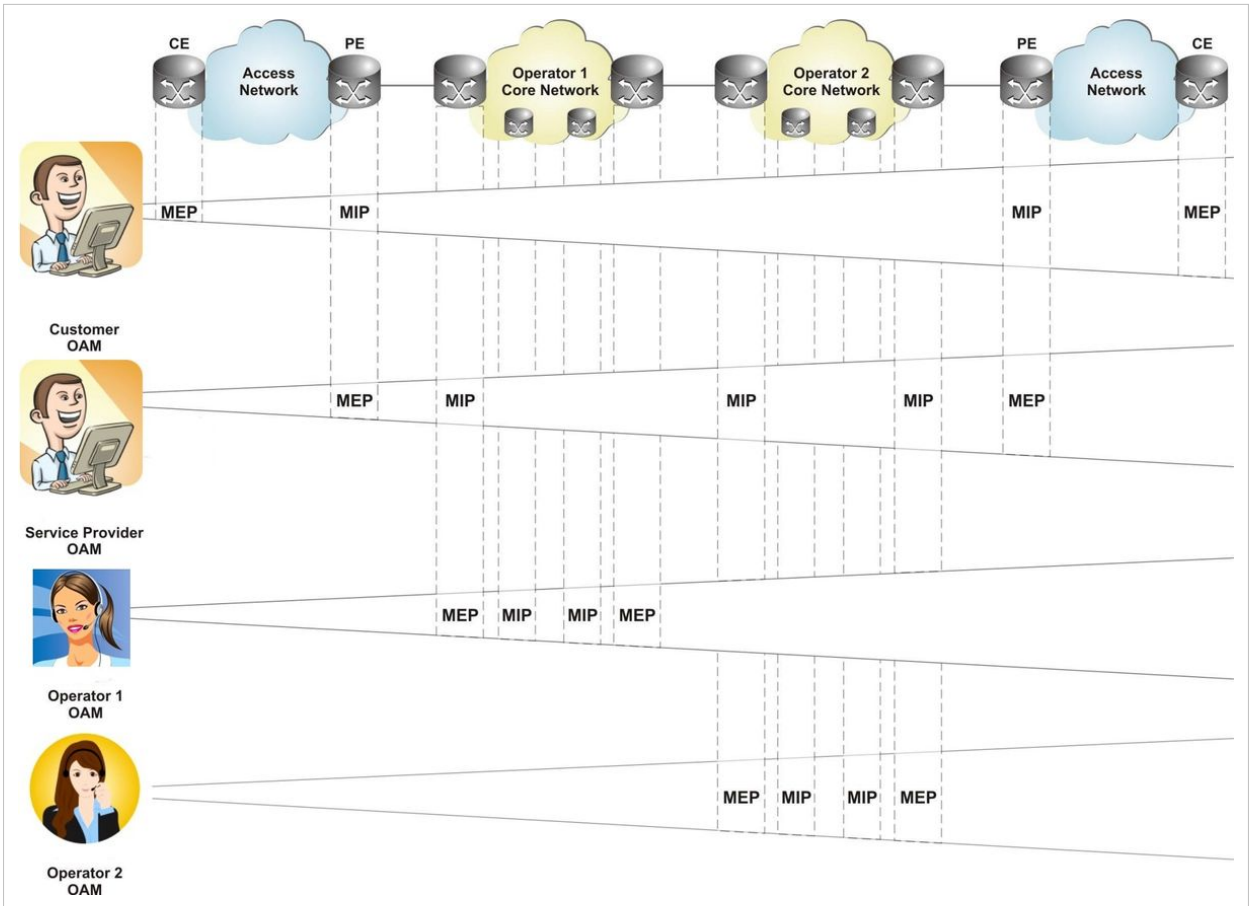
Several service providers and/or network operators could be involved in providing the service and each one needs to separately monitor the layer for which it is responsible.

When an Ethernet service is first initiated, the end-to-end path integrity must be verified. If some failure is detected, the service provider needs to identify the customers that are affected, and what rerouting can be performed.

Ethernet Service OAM is based on **IEEE Standard 802.1ag**[1] and **ITU-T Y.1731** [2]. IEEE 802.1ag is also termed **"Connectivity Fault Management (CFM)"**.

Both standards are similar in that it divides a network into maintenance domains in the form of hierarchy levels, which are allocated to users, service providers and operators. CFM then assigns **maintenance end points (MEPs)** to the edges of each domain and **maintenance intermediate points (MIPs)** to ports within domains. This helps define the relationships between all entities from a maintenance perspective, to allow each entity to monitor the layers under its responsibility and easily localize problems.

Y.1731 defines a **maintenance entity (ME)** that requires management. MEs are grouped into ME groups (MEGs, referred to as **Maintenance Associations or MAs** in IEEE language). In order to enable detection of incorrect connectivity, each MEG is given a unique ID, and OAM messages specify the **MEG ID** for which the message is intended. At the ends of managed entities we find MEG End Points **(MEPs)**, which are the functions that generate and process OAM frames to monitor and maintain the ME. There may also be MEG Intermediate Points **(MIPs)** that can respond to OAM messages, but cannot originate them. For point-to-point MEGs, a MEP has a single peer MEP, but in between there may be many MIPs. Hence a MEP can send **CC messages** to its peer MEP, or direct **non-intrusive LB** messages towards the peer MEP or to any MIP. It is the responsibility of the MEP to prevent OAM messages from leaking out of the administrative domain to which they belong, or entering another domain. However, MEPs transparently pass OAM frames from other domains when they belong to a higher OAM level, thus enabling end-to-end management of customer connectivity



Service CFM MEPs and MIPs

Ethernet-CFM - Configuration

In the **ethernet-cfm** node, the following parameters can be set, add or del:

```
ATOSNT\ethernet-cfm>>set ?

Nodes not available.
Set command parameters:
 enable        [on|off]    Current value: on
 level of log  [loglevel]  Current value: 1
```

Table 1: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the ethernet-cfm events. Default: 1
on|off	Enables/Disables Ethernet Connectivity Fault Management (CFM) globally. Default: off.

```
ATOS\ethernet-cfm>>add ?

add help : Add a new service or MIP
```

```
add usage:
<SERVICE><level><mdid><short-name>
<MIP><level><interface>

add command parameters:
SERVICE
MIP
```

To activate the CFM protocol on intermediate points, a MIP will be created.

Table 2: add MIP

Syntax	Description
level [0-7]	Integer that identifies the maintenance level.
interface	A string that identifies an 802.3 interface configured as a maintenance point (MP) at a specified maintenance domain.

To activate the CFM protocol on endpoints, a maintenance association will be created associated to a maintenance domain at a given level. We name *service* such association.

Table 3: add SERVICE

Syntax	Description
level [0-7]	Integer that identifies the maintenance level.
mdid	String of a maximum of 43 characters that identifies the maintenance domain (MDID) in continuity check messages.
short-name	String of a maximum of 43 characters that identifies a service (i.e. maintenance association – MA). This is the Short MA name. Default: null string (“”).

```
ATOS\ethernet-cfm>>del ?

del help : Delete a service or MIP

del usage:
<SERVICE><service_name>
<MIP><mip_name>

del command parameters:

SERVICE
MIP
```

Table 4: del MIP

Syntax	Description
MIP-name	A string that identifies an existing MIP.

Table 5: del SERVICE

Syntax	Description
service-name	A string that identifies an existing service, i.e. a maintenance association within a maintenance domain at a given level.

Ethernet-CFM - MIP - Configuration

```
ATOSNT\ethernet-cfm\mip-5-eth0>>show work
Show of ATOSNT ethernet-cfm mip-5-eth0
Maintenance level : 5
Interface         : eth0
Enable            : on

ATOSNT\ethernet-cfm\mip-5-eth0>>set ?

Nodes not available.
Set command parameters:
 enable             [on|off]  Current value: on
```

Table 6: set MIP

Syntax	Description
on|off	Enables/Disables this maintenance intermediate point (MIP). Default: on.

Ethernet-CFM SERVICE - Configuration

```
ATOSNT\ethernet-cfm>>add SERVICE ?

add command parameters:
 MD level       [0-7]
ATOSNT\ethernet-cfm>>add SERVICE 3 ?
add command parameters:
 MDID           [max 43 char]
ATOSNT\ethernet-cfm>>add SERVICE 3 md ?
 add command parameters:
 Short MA name  [max 43 char]
ATOSNT\ethernet-cfm>>add SERVICE 3 md MA ?
 Command complete (enter cr)
ATOSNT\ethernet-cfm>>add SERVICE 3 md MA
Command executed
```

```
ATOSNT\ethernet-cfm>>set ?

Available nodes:
                        3-ma
ATOS\ethernet-cfm\3-ma>>show conf

Set command parameters:
cc interval [cc-interval] Current value: 1s
```

Table 7: set

Syntax	Description
cc-interval [3.3ms|10ms|100ms|1s|10s|1m|10m]	Configures the time period between message transmissions. Default: 1s

```
ATOSNT\ethernet-cfm\3-ma>>add ?

add  help :  Add a MEP or a remote MP within MA/MD
add  usage:
 <MEP><ifc-name><mpid>[direction]
 <REMOTE><mpid>[mac-address]

add command parameters:
 MEP
 REMOTE
```

To activate a CFM maintenance endpoint (MEP) within a MA, a new interface will be created.

Table 8: add MEP

Syntax	Description
ifc-name	A string that identifies an 802.3 interface that can act as a maintenance point (MP) at a specified maintenance domain (MD).
mpid	Integer from 1 to 8191 that identifies the MEP.
direction	(optional) Indicates the direction of CFM packets: inward (up MEP) or outward (down MEP). Enumeration [up|down]. Default: up.

To add remote MEPs within MA, REMOTE table will be populated.

Table 9: add REMOTE

Syntax	Description
mpid	Integer from 1 to 8191 that identifies the MEP.
mac-address	MAC address of the peer MP

```
ATOSNT\ethernet-cfm\3-ma>>del ?

del  help :  Delete a MEP or a remote MP within MA/MD
del  usage:
 <MEP><mep-name>
```

```
 <REMOTE><mpid>

del command parameters:
 MEP
 REMOTE
```

Table 10: del MEP

Syntax	Description
MEP-name	A string that identifies an existing MEP.

Table 11: del REMOTE

Syntax	Description
mpid	Integer from 1 to 8191 that identifies the remote MEP.

Ethernet-CFM SERVICE MEP - Configuration

```
ATOSNT\ethernet-cfm\3-ma>>add MEP ?

add command parameters:
 interface   [eth0|loopback0]
ATOSNT\ethernet-cfm\3-ma>>add MEP eth0 ?
 add command parameters:
 mpid        [1-8191]
ATOSNT\ethernet-cfm\3-ma>>add MEP eth0 5 ?
 add command parameters:
 direction   [up|down]
 <cr>
ATOSNT\ethernet-cfm\3-ma>>add MEP eth0 5 down
Command executed

ATOSNT\ethernet-cfm\3-ma>>set ?

Available nodes:
                      eth0-5
Set command parameters:
 cc interval        [cc-interval]  Current value: 1s

ATOSNT\ethernet-cfm\3-ma\eth0-5>>show conf
Show of ATOSNT ethernet-cfm 3-ma eth0-5
Enable            : off
Interface         : eth0
MPID              : 5
Direction         : down
Continuity check  : on
Lowest alarm      : DefRDICCM
```

```
Alarm time (msec) : 2500
Reset time (msec) : 10000
CCM Loss measure  : off
AIS               : off
AIS level         : auto
AIS interval      : 1-second
LCK               : off
LCK level         : auto
LCK interval      : 1-second

ATOSNT\ethernet-cfm\3-ma\eth0-5>>set ?

Set command parameters:
 enable            [on|off]                 Current value: off
 continuity check  [continuity-check]       Current value: on
 lowest alarm      [lowest-alarm-priority]  Current value: DefRDICCM
 alarm time (msec) [alarm-time]             Current value: 2500
 reset time (msec) [reset-time]             Current value: 10000
 ccm loss measure  [ccm-loss-measure]       Current value: off
 ais               [ais]                    Current value: off
 ais level         [ais-level]              Current value: auto
 ais interval      [ais-interval]           Current value: 1-second
 lck               [lck]                    Current value: off
 lck level         [lck-level]              Current value: auto
 lck interval      [lck-interval]           Current value: 1-second
```

Table 12: set

Syntax	Description
on|off	Enables/Disables this maintenance endpoint (MEP). Default: off.
continuity-check [on|off]	See [1] (§20.10.1, §12.14.7.1.3g). Default: on
lowest-alarm-priority [DefRDICCM|DefMACstatus|DefRemoteCCM| DefErrorCCM|DefXconCCM|none]	An integer value (1~6) indicating the lowest defect priority that can trigger the generation of a Fault Alarm. See [1] (§12.14.7.1.3, §20.1.2, §20.9.5).Default: DefRDICCM
alarm-time [0-4294967295]	The time (in msec) that defects must be present before a Fault Alarm is issued. See [1] (§20.33.3 and §12.14.7.1.3l).Default: 2500
reset-time [0-4294967295]	The time (in msec) that defects must be absent before resetting a Fault Alarm. See [1] (§20.33.4 and §12.14.7.1.3m). Default: 10000ms.
ccm-loss-measure [on|off]	Enables or disables loss measure for Continuity Check (CC) frames. Default: off.
ais [off|auto|forced]	Status of the Alarm Indication Signal (AIS) function for MA of this interface.Default: off.
ais-level [0|1|2|3|4|5|6|7|auto]	Maintenance level where AIS frames will be sent. If set to “auto”, it will be that of the first higher level MP (if present).Default: auto.

ais-interval [1-second|1-minute]	AIS transmission period (interval between two consecutive AIS frames).Default: 1-second.
lck [off|auto|forced]	Enables the Lock frame (LCK).Default: off
lck-level [0|1|2|3|4|5|6|7|auto]	Maintenance level where LCK frames will be sent. If set to “auto”, it will be that of the first higher level MP (if present).Default:auto.
lck-interval [1-second|1-minute]	LCK transmission period (interval between two consecutive LCK frames).Default: 1-second.

Ethernet-CFM SERVICE REMOTE - Configuration

```
ATOSNT\ethernet-cfm\3-ma>>add REMOTE ?
add command parameters:
 mpid        [1-8191]
ATOSNT\ethernet-cfm\3-ma>>add REMOTE 7 ?
add command parameters:
 MAC address [aa-bb-cc-dd-ee-ff]
 <cr>
ATOSNT\ethernet-cfm\3-ma>>add REMOTE 7 ?
add command parameters:
 MAC address [aa-bb-cc-dd-ee-ff]
 <cr>
ATOSNT\ethernet-cfm\3-ma>>add REMOTE 7
Command executed
ATOSNT\ethernet-cfm\3-ma>>add REMOTE 11 ?
add command parameters:
 MAC address [aa-bb-cc-dd-ee-ff]
 <cr>
ATOSNT\ethernet-cfm\3-ma>>add REMOTE 11
Command executed
ATOSNT\ethernet-cfm\3-ma>>set ?
Available nodes:
                      eth0-5
Set command parameters:
 cc interval        [cc-interval]  Current value: 1s

ATOSNT\ethernet-cfm\3-ma>>show work
Show of ATOSNT ethernet-cfm 3-ma
Maintenance level : 3
Domain identifier : md
Short MA name     : MA
CC interval       : 1s

LIST OF REMOTES
MPID MAC ADDRESS
7    00-00-00-00-00-00
11   00-00-00-00-00-00

Show of ATOSNT ethernet-cfm 3-ma eth0-5
```

```
Enable            : off
Interface         : eth0
MPID              : 5
Direction         : down
Continuity check  : on
Lowest alarm      : DefRDICCM
Alarm time (msec) : 2500
Reset time (msec) : 10000
CCM Loss measure  : off
AIS               : off
AIS level         : 4
AIS interval      : 1-second
LCK               : off
LCK level         : 4
LCK interval      : 1-second

LIST OF REMOTES
MPID MAC ADDRESS         CCM defect  Last RDI  Port  IFC Sender

ATOSNT\ethernet-cfm\3-ma\eth0-5>>show work
Show of ATOSNT ethernet-cfm 3-ma eth0-5
Enable            : off
Interface         : eth0
MPID              : 5
Direction         : down
Continuity check  : on
Lowest alarm      : DefRDICCM
Alarm time (msec) : 2500
Reset time (msec) : 10000
CCM Loss measure  : off
AIS               : off
AIS level         : 4
AIS interval      : 1-second
LCK               : off
LCK level         : 4
LCK interval      : 1-second

LIST OF REMOTES
MPID MAC ADDRESS         CCM defect  Last RDI  Port  IFC Sender
7    00-00-00-00-00-00   false       false     0     0   0
11   00-00-00-00-00-00   false       false     0     0   0
```

Syntax	Description
mac-address	MAC address of the remote MEP 20.19.7 and 12.14.7.6.3d
mac-address	MAC address of the remote MEP 20.19.7 and 12.14.7.6.3d
mpid	Maintenance point identifier of the remote MEP.
CCM defect	Reports the state of the remote MEP. When true, no CCM has been received from the remote MEP for a specific time. See [1] (§20.19.1)
Last RDI	Boolean flag. Contains the RDI flag from the last-received CCM. See [1] (§20.19.2 and 12.14.7.6.3e)
Port	Enumerated value. Contains the value obtained from the Port Status TLV (21.5.4) of the last-received CCM or a value indicating that the last-received CCM contained no Port Status TLV. See [1] (§20.19.3 and 12.14.7.6.3f)
IF Status	Enumerated value. Contains the value obtained from the Interface Status TLV (21.5.5) of the last-received CCM or a value indicating that the last-received CCM contained no Interface Status TLV. See [1] (§20.19.4 and 12.14.7.6.3g)
Sender ID	Enumerated value. Contains the value obtained from the Sender ID TLV (21.5.3) of the last-received CCM or a value indicating that the last-received CCM contained no Sender ID TLV. See [1] (§20.19.5 and 12.14.7.6.3g)

Ethernet-CFM SERVICE MEP - Information

```
ATOSNT\ethernet-cfm\3-ma\eth0-5\information>>show work
Show of ATOSNT ethernet-cfm 3-ma eth0-5 information
Index                   : 1
Interface MAC address   : 00-D0-D6-48-87-E7
Bridge name             :
Bridge MAC address      : 00-00-00-00-00-00
VID                     : 0
Priority                : 0
CCM sent                : 1
DefXconCCM              : false
DefErrorCCM             : false
DefRemoteCCM            : false
DefMACstatus            : false
DefRDICCM               : false
Highest defect priority : none
FNG state               : 0
CCM sequence errors     : 0
LBM to send             : 0
Next LBM trans ID       : 1
LBR in order            : 0
LBR out of order        : 0
LBR no match            : 0
LBR transmitted         : 0
LBM period (msec)       : 1000
LBM timeout (sec)       : 5
LBM response count      : 0
Next LTM trans ID       : 1
LTR unexpected          : 0
LTM TTL                 : 64
LTM flag                : 0
```

```
LTM timeout (sec)       : 5
TX counter              : 0
RX counter              : 0
AIS TX                  : off
AIS RX                  : off
LCK TX                  : off
LCK RX                  : off
Alarm suppressed        : false
```

Syntax	Description
Bridge name	Bridge name, or interface name if it does not belong to any bridge
CCM sent	Number of sent CCM frames. See [1] (§20.10.2 and §12.14.7.1.3w)
DefXconCCM	A boolean flag set and cleared by the MEP Cross Connect state machine to indicate that one or more cross connect CCMs has been received, and that 3.5 times of at least one of those CCMs' transmission interval has not yet expired. See [1] (§20.23.3 and §12.14.7.1.3s)
DefErrorCCM	A boolean flag set and cleared by the Remote MEP Error state machine to indicate that one or more invalid CCMs has been received, and that 3.5 times that CCM's transmission interval has not yet expired. See [1] (§20.21.3 and §12.14.7.1.3r)
DefRemoteCCM	A Boolean indicating the aggregate state of the Remote MEP state machines. True indicates that at least one of the Remote MEP state machines is not receiving valid CCMs from its remote MEP, and false that allRemote MEP state machines are receiving valid CCMs. someRMEPCCMdefect is the logical OR of all of the rMEPCCMdefect variables for all of the Remote MEP state machines on this MEP. See [1] (§20.33.5 and §12.14.7.1.3q)
DefMACstatus	A Boolean indicating that one or more of the remote MEPs is reporting a failure in its Port Status TLV (21.5.4) or Interface Status TLV (21.5.5). It is true if either some remote MEP is reporting that its interface is not isUp (i.e., at least one remote MEP's interface is unavailable), or if all remote MEPs are reporting a Port Status TLV that contains some value other than psUp (i.e., all remote MEPs' Bridge Ports are not forwarding data). It is thus the logical OR of the following two terms: a)The logical AND, across all remote MEPs, of the rMEPportStatusDefect variable; OR b) The logical OR, across all remote MEPs, of the rMEPinterfaceStatusDefect variable. See [1] (§20.33.6 and §12.14.7.1.3p)
DefRDICCM	A Boolean indicating the aggregate health of the remote MEPs. True indicates that at least one of the Remote MEP state machines is receiving valid CCMs from its remote MEP that has the RDI bit set, and false that no Remote MEP state machines are receiving valid CCMs with the RDI bit set. someRDIdefect is the logical OR of all of the rMEPlastRDI variables for all of the Remote MEP state machines on this MEP. See [1] (§20.33.7 and §12.14.7.1.3o)
Highest defect priority	An enumerated value indicating the highest priority defect among the variables xconCCMdefect (§20.23.3), errorCCMdefect (§20.21.3), someRMEPCCMdefect (§20.33.5), someMACstatusDefect (§20.33.6), and someRDIdefect (§20.33.7), as limited by lowestAlarmPri (§20.9.5). See [1] (§20.33.9 and 12.14.7.7.2c)
FNG state	Statues of MEP Fault Notification Generator state machine See [1] (§20.35 and §12.14.7.1.3f)
CCM sequence errors	The total number of out-of-sequence CCMs received from all remote MEPs. See [1] (§20.16.12 and §12.14.7.1.3v)
LBM to send	The integer number of LBMs that the MEP Loopback Initiator transmit state machine is to transmit. See [1] (§20.28.1 and §12.14.7.3.2c)
Next LBM trans ID	The value to place in the Loopback Transaction Identifier field of the next LBM transmitted by xmitLBM(). nextLBMtransID is incremented by 1 by the MEP Loopback Initiator transmit state machine with each transmission. See [1] (§20.28.2 and §12.14.7.1.3x)
LBR in order	The total number of valid, in-order LBRs received See [1] (§20.31.1c1 and §12.14.7.1.3y)
LBR out of order	The total number of valid, out-of-order LBRs received. See [1] (§20.31.1c2 and §12.14.7.1.3z)
LBR no match	The total number of LBRs received whose mac_service_data_unit did not match (except for the OpCode) that of the corresponding LBM. See [1] (§20.31.1c3 and §12.14.7.1.3aa)
LBR transmitted	The total number of LBRs transmitted. See [1] (§20.26.2 and §12.14.7.1.3ad)

LBM rate	LBM transmission rate
LBM timeout	LBM timeout
LBM response count	Counter of LBM responses
Next LTM trans ID	The next LTM Transaction Identifier to be sent in an LTM. See [1] (§20.36.1 and §12.14.7.1.3ab)
LTR unexpected	The total number of unexpected LTRs received. See [1] (§20.39.1c and §12.14.7.1.3ac)
LTM TTL	An initial value for the LTM TTL field (§21.8.4). Default value, if not specified, is 64. See [1] (§20.37.1g and §12.14.7.4.2d)
LTM flag	The Flags field for LTMs transmitted by the MEP See [1] (§20.37.1h and §12.14.7.4.2b)
LTM timeout	LTM timeout
TX counter	Number of transmitted frames
RX counter	Number of received frames
AIS TX	Boolean value indicating if AIS frames are being transmitted.
AIS RX	Boolean value indicating if AIS frames are being received.
LCK TX	Boolean value indicating if LCK frames are being transmitted.
LCK RX	Boolean value indicating if LCK frames are being received.
Alarm suppressed	Boolean value indicating if alarms have become suppressed due to the reception of AIS frames.

Ethernet-CFM SERVICE MEP – Performance

```
ATOSNT\ethernet-cfm\3-ma\eth0-5\performance>>show work
Show of ATOSNT ethernet-cfm 3-ma eth0-5 performance
Loss measure                 : single-ended
LMM period (msec)            : 0
LMM to send                  : 0
Delay measure                : none
DMM period (msec)            : 0
DMM to send                  : 0
TST period (msec)            : 0
TST to send                  : 0
TST nest seqID               : 0
LMM Current Near End         : 0
LMM Current Far End          : 0
LMM Accumulated Near End     : 0
LMM Accumulated Far End      : 0
LMM Ratio Near End           : 0
LMM Ratio Far End            : 0
DMM last delay (msec)        : 0
DMM last variation (msec)    : 0
DMM average delay (msec)     : 0
DMM average variation (msec) : 0
DMM delay samples            : 0
```

Syntax	Description
Loss measure	Loss measure mode, enumeration of Off|Single-Ended|Dual-Ended.
LMM period	LMM transmission period.
LMM to send	The integer number of LMM frames that the MEP is to transmit.
Delay measure	Delay measure mode, enumeration of Off|One-Way|Two-Way.
DMM period	DMM transmission period.
DMM to send	The integer number of DMM frames that the MEP is to transmit.
TST period	TST transmission period.
TST to send	The integer number of TST frames that the MEP is to transmit.
TST next seqID	Sequence ID of the next TST frame to transmit.
LMM Current Near End	Current LM near-end value.
LMM Current Far End	Current LM far-end value.
LMM Accumulated Near End	Accumulated LM near-end value.
LMM Accumulated Far End	Accumulated LM far-end value.
LMM Ratio Near End	LM near-end ratio.
LMM Ratio Far End	LM far-end ratio.
DMM last delay	Last DM delay value.
DMM last variation	Last DM delay variation value.
DMM average delay	Average DM delay value.
DMM average variation	Average DM delay variation value.
DMM delay samples	Number of delay samples.

Ethernet-CFM SERVICE MEP – Commands

loopback

To send Ethernet connectivity fault management (CFM) loopback messages to a destination maintenance endpoint (MEP) and maintenance intermediate point (MIP), use the loopback command.

```
ATOSNT\ethernet-cfm\3-ma\eth0-5>>loopback ?

loopback  help :  Send a loop-back message (ETH-LB)
loopback  usage:
 <mac address>[tries][period][timeout][pattern type][pattern size]

loopback command parameters:
 MAC address  [aa-bb-cc-dd-ee-ff]
```

Syntax	Description
mac-address	MAC address of the destination MP
tries	Number of sent ETH-LB messages. Default: 10.
period	ETH-LB transmission period. Default: 1 sec
timeout	Timeout for ETH-LB response. Default: 12 sec
pattern type	Test pattern type . Enumerated value: null-no-CRC|null-with-CRC|PRBS-no-CRC|PRBS-with-CRC. See [2] (§9.3.2)
pattern size	Size (octets number) of ETH-LB optional test TLV. See [2] (§9.3.2)

linktrace

To send Ethernet connectivity fault management (CFM) linktrace messages to a destination maintenance endpoint (MEP), use the linktrace command.

```
ATOSNT\ethernet-cfm\3-ma\eth0-5>>link-trace ?

link-trace  help :  Perform a link-trace transaction (ETH-LT)
link-trace  usage:
 <mac address>[timeout]

link-trace command parameters:
 MAC address [aa-bb-cc-dd-ee-ff]
```

linktrace command parameters:

Syntax	Description
mac-address	MAC address of the destination MEP
timeout	Timeout for ETH-LB response. Default: 12 sec

loss-measure

Single-ended ETH-LM is used for on-demand loss measurement. In this case, a MEP sends frames with ETH-LM request information to its peer MEP and receives frames with ETH-LM reply information from its peer MEP to carry out loss measurements.

```
ATOSNT\ethernet-cfm\3-ma\eth0-5>>loss-measure ?

loss-measure  help :  Perform a loss measurement (ETH-LM, single-ended only)
loss-measure  usage:
 <mac address>[tries][period]

loss-measure command parameters:
 MAC address [aa-bb-cc-dd-ee-ff]
```

loss-measure command parameters:

Syntax	Description
mac-address	MAC address of the peer MEP
tries	Number of sent ETH-LM messages. Default: 10.
period	ETH-LM transmission period. Default: 1s

delay-measure

One-way or two-way ETH-DM frames are used for on-demand measure of delay and delay variation. In this case, a MEP sends DMM frames with ETH-DM information to its peer MEP and receiving DMR frames with ETH-DM information from the peer MEP during the diagnostic interval.

```
ATOSNT\ethernet-cfm\3-ma\eth0-5>>delay-measure ?

delay-measure  help :  Perform a delay measurement (one-way or two-way)
delay-measure  usage:
 <one-way|two-way><mac address>[tries][period]

delay-measure command parameters:
 Mode        [none|one-way|two-way]
```

loss-measure command parameters:

Syntax	Description
mode	[one-vay|two-way]. Default: two-way
mac-address	MAC address of the peer MEP
tries	Number of sent ETH-DM messages. Default: 10.
period	ETH-DM transmission period. Default: 1s

ethernet-test

Ethernet Test Signal function (ETH-Test) is used to perform one-way on-demand in-service or out-of-service diagnostics tests. This includes verifying bandwidth throughput, frame loss, bit errors, etc.

```
ATOSNT\ethernet-cfm\3-ma\eth0-5>>ethernet-test ?

ethernet-test  help :  Perform a performance measurement using ETH-TST
ethernet-test  usage:
  <mac address>[tries][period][pattern size][pattern type]

ethernet-test command parameters:
 MAC address  [aa-bb-cc-dd-ee-ff]
```

Ethernet-test command parameters:

Syntax	Description
mac-address	MAC address of the destination MP
tries	Number of sent ETH-TST messages. Default: 10.
period	ETH-TST transmission period. Default: 1s
pattern type	null-with-CRC|PRBS-no-CRC|PRBS-with-CRC. See [2] (§9.3.2)
pattern size	ize (octets number) of ETH-TST optional test TLV. See [2] (§9.3.2)

References

1 IEEE 802.1ag - IEEE Standard for Local and Metropolitan Area Networks Virtual Bridged Local Area Networks Amendment 5: Connectivity Fault Management

2 ITU-T Recommendation Y.1731 - OAM functions and mechansims for Ethernet based networks

ManEthernetOAM

Ethernet-OAM Overview

Ethernet Operations, Administration, and Maintenance (OAM) is a protocol for installing, monitoring and troubleshooting Ethernet metropolitan-area networks (MANs) and Ethernet WANs.

It relies on a new, optional sublayer in the data link layer of the OSI model. Ethernet OAM can be implemented on any full-duplex point-to-point or emulated point-to-point Ethernet link.

A system-wide implementation is not required; OAM can be deployed for part of a system; that is, on particular interfaces.

Normal link operation does not require Ethernet OAM. OAM frames, called OAM protocol data units (PDUs), use the slow protocol destination MAC address 0180.c200.0002. They are intercepted by the MAC sublayer and cannot propagate beyond a single hop within an Ethernet network.

Ethernet OAM is a relatively slow protocol with modest bandwidth requirements. The frame transmission rate is limited to a maximum of 10 frames per second; therefore, the impact of OAM on normal operations is negligible.

The functional requirements that Ethernet OAM is required to meet are:

- Discovery: a procedure to detect if the remote endpoint supports OAM.
- Remote Fault Indication and Link Monitoring
- Remote Loopback: to activate a loopback state in the remote endpoint, where all the received frames (except OAM frames) are returned to the local endpoint
- Variable polling: to query the remote endpoint for its MIB variables

A DTE is configured to have either an ACTIVE or a PASSIVE role.

Only an ACTIVE DTE can:

- initiate the discovery process
- send Remote Loopback commands
- send Variable Requests.

Remote loopback

Only a DTE in the ACTIVE role can initiate and terminate a remote loopback. An OAM entity can put its remote entity into loopback mode using a loopback control OAMPDU. This helps you ensure the quality of links during installation or when troubleshooting. In loopback mode, every frame received is transmitted back on that same port

except for OAMPDUs and pause frames. The periodic exchange of OAMPDUs must continue during loopback state to maintain the OAM session. The loopback command is acknowledged by responding with an Information OAMPDU with the loopback state indicated in the state field. This allows you, for instance,to estimate if a network segment can satisfy an SLA. You can test delay, jitter and throughput (implementations for these tests will be vendor specific).

Ethernet-OAM - Configurations

```
ATOSNT\ethernet-oam>>show conf
Show of ATOSNT ethernet-oam
Level of log : 1
Enable       : on

ATOSNT\ethernet-oam>>set ?

Nodes not available.

Set command parameters:
 level of log  [loglevel]  Current value: 1
 enable        [on|off]    Current value: on
```

Table 1: set

Syntax	Description
loglevel [0-5]	Set level of log. Default 1.
on|off	Enables/Disables the Ethernet OAM protocol support. Default: on.

To activate the link layer OAM protocol a node associated with an ethernet interface will be created.

```
ATOSNT\ethernet-oam>>add ?

add  help :  Add a new interface
add  usage:
 <IFC><interface_name>

add command parameters:
 IFC
```

Table 2: add interface

Syntax	Description
Name	A string that contains an ATOSNT interface.

```
ATOSNT\ethernet-oam>>del ?
del help: Delete an interface in the Ethernet OAM profile

del usage:
 IFCname

del command parameters:
 IFC
```

Table 3: del interface

Syntax	Description
Name	Interface name.

Ethernet-OAM ETH0 – Configurations

```
ATOSNT\ethernet-oam\eth0>>show conf

Available nodes:

 link-monitor

Show of ATOSNT ethernet-oam eth0
Level of log: 1
Enable: on
Mode: active
Link monitoring : supported
Remote loopback: supported
PDU interval (x 100ms): 10
PDU size (bytes) : 1518
Connection timeout (sec): 5
MIB retrieval: on

ATOSNT\ethernet-oam\eth0>>set ?

Set command parameters:
level of log [loglevel] Current value: 1
enable [on|off] Current value: on
mode [active|passive] Current value: active
link monitoring[supported|not-supported] Current value: supported
remote loopback [supported|not-supported] Current value: supported
PDU interval [pdu-interval]  Current value: 10
PDU size [pdu-size]  Current value: 1518
```

```
connection timeout [connection-timeout] Current value: 5
mib-retrieval [mib-retrieval] Current value: on
```

Table 4: set

Syntax	Description
loglevel [0-5]	Set level of log. Default 1.
on|off	Enables/Disables the Ethernet OAM protocol on interface. Default: on.
mode [active|passive]	Configure the DTE role. Default: active.
link-monitoring [supported|not-supported]	Configure the link monitoring support. Link monitoring operations start automatically when support is enabled. Default: supported.
remote-loopback [supported|not-supported]	Configure the remote loopback support. Default: supported.
pdu-interval (x 100ms) [1-10]	Interval between two PDU in unit of 100 ms. Default: 10 (1 PDU per seconds).
pdu-size (bytes) [64-1518]	Configure the maximum size of a OAM PDU. Range 64~1518, default: 1518.
connection-timeout (sec) [2-30]	Configure the timeout value (in seconds) for an Ethernet OAM session. After establishing a session if you don't receive PDUs in this time interval, the session will be restarted. Default:5.
mib-retrieval [on|off]	Enables/disables MIB retrieval on an Ethernet OAM session. Default: on.

Ethernet-OAM ETH0 – Show Status

```
ATOSNT\ethernet-oam\eth0>>show status
*********************************
status of local eth0 OAM node
*********************************
mac address: 00:D0:D6:08:CA:53
admin state: enabled
operational status: operational
loopback status: not active
OAM PDU max size: 1518
config revision: 1
local state: parser action = FWD, multiplexer action = FWD
mode: active
functions: no unidirection support,loopback support,event support,variable support

*********************************
status of peer eth0 OAM node
*********************************
mac address: 00:D0:D6:08:CA:54
admin state: enabled
operational status: operational
vendor OUI: D0D6
vendor SPI: 7745
OAM PDU max size: 1518
config revision: 1
local state: parser action = FWD, multiplexer action = FWD
```

```
mode: active
functions: no unidirection support,loopback support,event support,variable support
symbol error config: window=1000(symbols), threshold=1(errored symbols)
frame error config: window=10(100 ms), threshold=1(errored frames)
frame period error config: window=20000(frames), threshold=1(errored frames)
frame seconds error config: window=600(100 ms), threshold=1(errored frame seconds)
Command executed
```

Ethernet-OAM ETH0 – Show Statistics

```
ATOSNT\ethernet-oam\eth0>>show statistics
*********************************
statistics of local eth0 OAM PDU
*********************************
*******upstream direction *******
unsupported codes: 0
information: 515
unique event: 0
duplicate event: 0
loopback control: 0
organization specific: 0
variables request: 62
variables response: 0
******downstream direction ******
unsupported codes: 0
information: 510
unique event: 0
duplicate event: 0
loopback control: 0
organization specific: 0
variables request: 0
variables response: 62
| Timestamp | Event type | Location | Window | Threshold | Error count | Running total | Event total |
|53096 |LINK FAULT |LOCAL | | | |1 |1 |

*********************************
statistics of peer eth0 OAM PDU
*********************************
*****peer upstream direction *****
unsupported codes: 0
information: 1
unique event: 0
duplicate event: 0
loopback control: 0
organization specific: 0
variables request: 0
variables response: 45
****peer downstream direction ****
```

```
unsupported codes: 0
information: 254
unique event: 0
duplicate event: 0
loopback control: 0
organization specific: 0
variables request: 62
variables response: 0
Command executed
```

Link-Monitor – Configurations

In **Link-Monitor** node, you can use set, add and del commands to configure the following parameters:

```
ATOSNT\ethernet-oam\eth0\link-monitor>>show conf
Show of ATOS ethernet-oam eth0 link-monitor
Symbol period window (symbols) : 1000
Symbol period threshold (errored symbols): 1
Symbol period event enable: on
Frame window (sec): 1
Frame threshold (frames): 1
Frame event enable: on
Frame period window (frames): 1000
Frame period threshold (frames): 1
Frame period event enable: on
Frame seconds window (sec): 60
Frame seconds threshold (errored frame seconds): 1
Frame seconds event enable: on
Dying gasp event enable: on
Critical event enable: on

LIST OF DATABASES
Empty list

ATOSNT\ethernet-oam\eth0\link-monitor>>set?
Set command parameters:
symbol period window (symbols)             [symbol-period-window]             Current value: 1000
symbol period threshold (errored symbols)       [symbol-period-threshold]       Current value: 1
symbol period event enable                   [symbol-period-event]             Current value: on
frame window (sec)                          [frame-window]                   Current value: 1
frame threshold (frames)                    [frame-threshold]             Current value: 1
frame event enable                          [frame-event]                   Current value: on
frame period window (frames)                    [frame-period-window]             Current value: 1000
frame period threshold (frames)             [frame-period-threshold]       Current value: 1
frame period event enable                   [frame-period-event]             Current value: on
frame seconds window (sec)                    [frame-seconds-period]             Current value: 60
frame seconds threshold (errored frame seconds)[frame-seconds-threshold]       Current value: 1
frame seconds event enable                    [frame-seconds-event]             Current value: on
dying gasp event enable                    [dying-gasp-event]             Current value: on
```

```
critical event enable                          [critical-event]            Current value: on
```

Table 5: set

Syntax	Description
symbol-period-window (symbols) [1000-1000]	Configure the window size (in symbols) for an Ethernet OAM errored symbol period event. Default 1000.
symbol-period-threshold (errored symbols) [0-60000000]	Configure the threshold (in symbols) that trigger an Ethernet OAM errored symbol period event. Default: 1.
symbol-period-event-enable [on|off]	Enables/Disables the Ethernet OAM errored symbol event generation on interface. Default: on.
frame-window (sec) [1-60]	Configure the window size (x 100ms) for an Ethernet OAM errored frame event. Default 10.
frame-threshold (frames) [0-60000000]	Configure the threshold (in frames) that trigger an Ethernet OAM errored frame event. Default: 1.
frame-event-enable [on|off]	Enables/Disables the Ethernet OAM errored frame event generation on interface. Default: on.
frame-period-window (frames) [100-60000]	Configure the window size (in frames) for an Ethernet OAM errored frame period event. Default 1000.
frame-period-threshold (frames) [0-1000000]	Configure the threshold (in frames) that trigger an Ethernet OAM errored frame period event. Default: 1.
frame-period-event-enable [on|off]	Enables/Disables the Ethernet OAM errored frame period event generation on interface. Default: on.
frame-seconds-window [100-9000]	Configures the window size (x 100ms) for an Ethernet OAM frame-seconds error event. Default: 6000.
frame-seconds-threshold [0-900]	Configures the threshold (in frames) that trigger an Ethernet OAM frame-seconds error event. Default: 1.
frame-seconds-event-enable [on|off]	Enables/Disables the Ethernet OAM errored frame seconds event generation on interface. Default: on.
dying-gasp-event-enable [on|off]	Enable/Disable the Ethernet OAM dying gasp event generation on interface. Default: on.
critical-event-enable [on|off]	Enable/Disable the Ethernet OAM critical event generation on interface. Default: on.

```
ATOSNT\ethernet-oam\eth0\link-monitor>>add ?
add help: Add a new database
add usage:
  <DATABASE><window(hours)><period(minutes)>
add command parameters:
  DATABASE



ATOSNT\ethernet-oam\eth0\link-monitor>>del ?
del help: Remove a database
del usage:
  <DATABASE><window(hours)><period(minutes)>
del command parameters:
  DATABASE
```

Table 6: add/del DATABASE

Syntax	Description
Window	Observation window in hours.
Period	Observation timeout in minutes.

```
ATOSNT\ethernet-oam\eth0\link-monitor>>show statistics
statistics of eth0 databases
************************************************************
window:1(hours)-period:1(minutes) database
************************************************************
| | Timestamp | Event type | Location | Window | Threshold | Error count | Running total | Event total
| 2~3 | 3400 | FRAME ERROR | LOCAL | 10 | 1 | 2 | 2 | 1
| | 3400 | FRAME ERROR | REMOTE | 10 | 1 | 2 | 2 | 1
| | 8060 | SECONDS ERROR | LOCAL | 600 | 1 | 1 | 1 | 1
| | 8060 | SECONDS ERROR | REMOTE | 600 | 1 | 1 | 1 | 1
| 1~2 | 10288 | FRAME ERROR | LOCAL | 10 | 1 | 2 | 4 | 2
| | 10288 | FRAME ERROR | REMOTE | 10 | 1 | 2 | 4 | 2
| | 10795 | FRAME ERROR | LOCAL | 10 | 1 | 2 | 6 | 3
| | 10795 | FRAME ERROR | REMOTE | 10 | 1 | 2 | 6 | 3
| | 14138 | SECONDS ERROR | LOCAL | 600 | 1 | 2 | 3 | 2
| | 14138 | SECONDS ERROR | REMOTE | 600 | 1 | 2 | 3 | 2
| 0~1 | 16063 | FRAME ERROR | LOCAL | 10 | 1 | 4 | 10 | 4
| | 16063 | FRAME ERROR | REMOTE | 10 | 1 | 4 | 10 | 4
| | 16164 | FRAME ERROR | LOCAL | 10 | 1 | 2 | 12 | 5
| | 16164 | FRAME ERROR | REMOTE | 10 | 1 | 2 | 12 | 5
| | 20216 | SECONDS ERROR | LOCAL | 600 | 1 | 2 | 5 | 3
| | 20216 | SECONDS ERROR | REMOTE | 600 | 1 | 2 | 5 | 3
************************************************************
window:1(hours)-period:15(minutes) database
************************************************************
| | Timestamp | Event type | Location | Window | Threshold | Error count | Running total | Event total
| | 3400 | FRAME ERROR | REMOTE | 10 | 1 | 2 | 2 | 1
| | 8060 | SECONDS ERROR | LOCAL | 600 | 1 | 1 | 1 | 1
| | 8060 | SECONDS ERROR | REMOTE | 600 | 1 | 1 | 1 | 1
| | 10288 | FRAME ERROR | LOCAL | 10 | 1 | 2 | 4 | 2
| | 10288 | FRAME ERROR | REMOTE | 10 | 1 | 2 | 4 | 2
| | 10795 | FRAME ERROR | LOCAL | 10 | 1 | 2 | 6 | 3
| | 10795 | FRAME ERROR | REMOTE | 10 | 1 | 2 | 6 | 3
| | 14138 | SECONDS ERROR | LOCAL | 600 | 1 | 2 | 3 | 2
| | 14138 | SECONDS ERROR | REMOTE | 600 | 1 | 2 | 3 | 2
| | 16063 | FRAME ERROR | LOCAL | 10 | 1 | 4 | 10 | 4
| | 16063 | FRAME ERROR | REMOTE | 10 | 1 | 4 | 10 | 4
| | 16164 | FRAME ERROR | LOCAL | 10 | 1 | 2 | 12 | 5
| | 16164 | FRAME ERROR | REMOTE | 10 | 1 | 2 | 12 | 5
| | 20216 | SECONDS ERROR | LOCAL | 600 | 1 | 2 | 5 | 3
| | 20216 | SECONDS ERROR | REMOTE | 600 | 1 | 2 | 5 | 3
```

```
Command executed
```

Ethernet-OAM ETH0 – Commands

```
ATOSNT\ethernet-oam\profile0\eth0>>remote-loopback ?

remote-loopback help: Start/Stop a remote loopback

remote-loopback usage:

<ON|OFF>

remote-loopback command parameters:

Mode [on|off]
```

Index

ManFirewall

Firewall

Firewall functionality analyzes and filters IP packets between network interfaces. The most common application of the firewall is to protect traffic between the hosts in the LAN and the Internet.

The firewall allows to filter packets based on the IP packet header and/or on the connection state information and performs actions on packets that match the rules. To use the firewall feature, you should follow two steps:

1. You define a firewall rule and save it under a name in the **Classifier Map** node. You can also define a **Classmap Profile** in the classmap-profile node where you define the profile match conditions.
2. After defining the rules, you apply the classifier-map to an interface as a packet filter specifying the traffic direction (inlout).

Firewall rules specify the match conditions for traffic and the action to be taken if the match conditions are satisfied. Rules are executed in sequence, according to the rule number. If the traffic matches the characteristics specified by the rule, the rule's action is executed; if not, the system "falls through" to the next rule.

The action can be one of these:

- **Permit**. Traffic is allowed and forwarded
- **Deny**. Traffic is silently discarded
- **Discard**. Traffic is discarded with error messages

ATOSNT support two types of firewall:

- Stateless firewall
- Stateful firewall

Stateless Firewall

In a stateless firewall, a **packet filter** application operating at network layer, examines each packet header and based on a specific set of rules it decides to prevent it from passing (Deny, for packets to be silently discarded, or Discard, for packets to have error messages as response, or to allow it to pass Permit).

The single packet is inspected and handled based only on the information contained in the packet itself.

Stateful Firewall

Unlike stateless firewalls, stateful firewalls track the state of network connections and traffic flows and allow or restrict traffic based on whether its connection state is known and authorized. In a stateful firewall a **stateful packet inspection** is performed, paying attention to “memory” of the connections; in order to have this information, the firewall application must be able to maintain a table holding attributes of the open connections.
The action is taken based on a set of rules related to the specific state of connections or time attributes of the single sessions.

The default stateful settings can be modified using the **conntrack-table-size, conntrack-tcp-loose and conntrack-hash-size** commands.

Stateful parameters are available to be settled in the **classmap -profile** node ; classmap profiles are profiles of matching condition that, combined with permission, allow user to obtain a classifier map rule .When configuring the firewall you should set the classifier map which defines the set of rules and the action to be taken (deny, permit or discard) if the match conditions are satisfied. The rules definition are based on the information contained in the IP packet header or on the connection state information .

Firewall - Node

Firewall feature is available at the **firewall** node.

Firewall - Commands

At the **firewall** node, the following parameters can be set:

```
ATOS \firewall>>set ?


Nodes not available.
Set command parameters:
 disable all ping replies          [ping-disable-all]        Current value: off
 disable broadcast ping replies    [ping-disable-broadcast]  Current value: on
 accept source routing ip options  [source-route-ip-option]  Current value: off
 log pkts with invalid addresses   [log-martians]            Current value: off
 accept icmp redirect pkts         [icmp-redirect-accept]    Current value: off
 send icmp redirect pkts           [icmp-redirect-send]      Current value: on
 source validation policy          [source-validation]       Current value: disable
 use tcp syn cookies               [syn-cookies]             Current value: off
 conntrack table size              [conntrack-table-size]    Current value: default *
 conntrack tcp loose               [conntrack-tcp-loose]     Current value: off   *
 conntrack hash size               [conntrack-hash-size]     Current value: default  *
 level of log                      [loglevel]                Current value: 1


* Default Stateful Firewall settings
```

*Table 1:***set**

Syntax	Description
ping-disable-all <on|off>	Disable/enable ICMP echo requests incoming.Default: off.
Ping-disable-broadcast <on|off>	Disable/enable broadcast ICMP echo requests incoming.Default: on.
Source-route-ip-option<on|off>	Enable/disable accepting source routing ip option. Default: off.
Log-martians <on|off>	Enable/disable logging packets with invalid addresses. Default: off.
Icmp-redirect-accept <on|off>	Enable/disable accepting ICMP redirect packets. Default: off.
Icmp-redirect-send <on|off>	Enable/disable sending ICMP redirect packets. Default: on.
Source-validation <disable|strict|loose>	Activate /deactivate source validation policy. Default: disable.
Syn-cookies <on|off>	Enable/disable using TCP SYN cookies. Default: off.
Conntrack-table-size < 128-32768|default>	Set the maximum size of the connection tracking table. Default: Default (the value depends on the Kernel version)
Conntrack-tcp-loose <on|off>	Specifies whether previously established connections are to be tracked for stateful traffic filtering. Default: on.
Conntrack-hash-size < 128-32768|default>	Set the size of the hash table associated with the connection tracking table. Default: Default (the value depends on the Kernel version)
Loglevel <value>	Set level of log. Default: 1.

In an **stateless firewall**, to add a new **Packet Filter**, you should use the **add** command.

```
ATOSNT\firewall>>add ?

add  help :  Add a IPv4 or IPv6 PACKET FILTER to list
add  usage:
 <PACKET-FILTER><classifier><ALL-IFC><direction>[discard-mode]
 <PACKET-FILTER><classifier><IFC><ifc-name><direction>[discard-mode]
 <PACKET-FILTER><classifier><ROUTER><direction>[discard-mode]
 <PACKET-FILTER><classifier><VRRP-IFC><vrrp-instance-name><direction>[discard-mode]
 <PACKET-FILTER-IPV6><classifier><ALL-IFC><direction>[discard-mode]
 <PACKET-FILTER-IPV6><classifier><IFC><ifc-name><direction>[discard-mode]
 <PACKET-FILTER-IPV6><classifier><ROUTER><direction>[discard-mode]
 <PACKET-FILTER-IPV6><classifier><VRRP-IFC><vrrp-instance-name><direction>[discard-mode]

add command parameters:
 PACKET-FILTER
 PACKET-FILTER-IPV6
```

*Table 2:***add PACKET-FILTER**

Syntax	Description
PACKET-FILTER or PACKET-FILTER-IPV6	Keyword Specify the set of rules for IPv4 or IPv6 packet filtering action
classifier-map-name [Any value(max 32 char)]	Specify the classifier map's name
ALL-IFC	Specify the interface(s) type where the filter is active on. The firewall will filter packets destined to all interfaces
IFC	The firewall will filter packets destined to a selected IFC.
ifc name	The interface's name to which the firewall will filter packets
ROUTER	The firewall will filter packets to / from the Router interface
VRRP-IFC	The firewall will filter packets destined to a virtual interface configured in vrrp node
vrrp-instance-name [vrrp0|vrrp1]	Sets the name of the VRRP instance choosen from the list of the vrrp instances configured in vrrp node
in|out	Specify the direction of packets to filter. Mandatory. • **in** the firewall will filter packets entering the interface and traversing the device. You can apply one **in** packet filter • **out** the firewall will filter packets leaving the interface. You can apply one **out** packet filter
discard mode <silently |icmp-net-unreach |icmp-host-unreach | icmp-port-unreach |icmp-proto-unreach |icmp-net-prohib | icmp-host-prohib |icmp-admin-prohib |tcp-reset>	Specify if deny has to be resolved as silently or discard with error messages (all other values). Optional. Default: silently.

Firewall Configuration Example

This is an example of **Stateless firewall**.

It defines a firewall rule that filters on source IP address and destination protocol. This rule allows TCP packets originating from the host with IP address 192.168.110.75 and destined for the Telnet port of the Router through eth0 interface.

ATOSNT\firewall>>show conf
Show of ATOSNT firewall
Disable all ping replies : off
Disable broadcast ping replies : on
Accept source routing IP options : off
Log pkts with invalid addresses : off
Accept ICMP redirect pkts : off
Send ICMP redirect pkts : on
Source validation policy : disable
Use TCP SYN cookies : off
Conntrack table size : default
Conntrack tcp loose : on
Conntrack hash size : default
Level of log : 1
LIST OF PACKET FILTERS

CLASSIFIER MAP	IFC TYPE	INTERFACE NAME	DIRECTION	DISCARD MODE
fwfilter	ROUTER		IN	

LIST OF CLASSIFIER MAPS
Classifier map name : fwfilter
RULE N. : 1
Right : permit
Protocol/profile : tcp
Source address : 192.168.110.75
Source wild mask : 0.0.0.0
Dest address : router
Source port : anyport
Dest port : equ
Max dest port : telnet
Source ifc : eth0

This is an example of **Stateful firewall**.
The rule is to accept a limited rate of two incoming ICMP echo request packets (pings) per second allowing bursts of 5 packets without dropping the packets.

ATOSNT\firewall>>add PACKET-FILTER Ratelimit ROUTER IN

Show of ATOSNT classmap-profile newprofile

Description :

Protocol : icmp

Source addr/name : any

Source wildmask : 0.0.0.0

Dest addr/name : any

Dest wildmask : 0.0.0.0

Ip option : 0

Source min port : any

Source max port : any

Dest min port : any

Dest max port : any

Tcp flag : 00

Tcp flag wildmask : 00

Icmp type : echorequest

Source ifc :

Policy : none

Limit rate value : 2

Limit rate unit : second

Limit bursts : 5

Recent time (sec) : 0

Recent count : 0

Fragment option : unspecified

Conn State : Established

LIST OF CLASSIFIER MAPS

Classifier map name : Ratelimit

RULE N. : 1

Right : permit

Protocol/profile : NewProfile

Firewall Statistics Example

In the example a classifier-map was first defined with the action to discard the ICMP packets coming from a host with an ip source address 192.168.110.88, then a packet-filter firewall was configured to apply the rule on the router eth0 interface to the incoming packets.

After a few seconds of sending ping packets by the host with ip address 192.168.110.88 to the eth0 interface, you can see how the statistics counters change.

ATOSNT>>add classifier-map noping 1 deny icmp 192.168.110.88 0.0.0.0 any

Command executed

ATOSNT>>add classifier-map noping 2 permit anyprot any any

Command executed

ATOSNT>>show classifier-map conf

Show of ATOSNT classifier-map

Level of log : 1

Classifier map name : noping

RULE N. : 1

Right : deny

Protocol/profile : icmp

Source address : 192.168.110.88

Source wild mask : 0.0.0.0

Dest address : any

Classifier map name : noping

RULE N. : 2

Right : permit

Protocol/profile : anyprot

Source address : any

Dest address : any

Command executed

ATOSNT\firewall>>add PACKET-FILTER noping iFC eth0 in

Command executed

ATOSNT\firewall>>show statistics -s

Statistics of packet filter:

noping on interface eth0 direction IN counters:

Rule n.1 counters:

permitted packet ... 0

permitted bytes 0

denied packet 19

denied bytes 1596

Rule n.2 counters:

permitted packet ... 184

permitted bytes 24417

denied packet 0

denied bytes 0

Command executed

ATOSNT\firewall>>show statistics

Statistics of packet filter:

noping on interface eth0 direction IN counters:

Rule n.1 counters:

permitted packet ... 0

permitted bytes 0

denied packet 40

denied bytes 3360

Rule n.2 counters:

permitted packet ... 738

permitted bytes 98652

denied packet 0

denied bytes 0

Command executed

ManFrameRelay

Frame Relay Service Configuration

Frame Relay is a service available over the serial multiprotocol VX interface when it is used as a WAN interface.

Routed and/or bridging traffic packets from/to LAN interface, can be transported by the serial VX interface, through a Frame Relay network.

Frame Relay service is available on the **fr** node.

fr - Commands

At “fr” node it’s possible to **set** the following parameters:

```
ATOSNT\fr>>set ?

Available nodes:
                        fr-port0
                        dlci0
                        dlci1
                        dlci2
                        dlci3

Set command parameters:
 level of log  [loglevel]  Current value: 5
```

Table 1:**set**

Syntax	Description
loglevel <0-5>	Set the level detail used by ATOS to log the events on the fr node [default: 1]

To add a new Frame Relay port or DLCI, you should use **add** command:

```
ATOSNT\fr>>add ?

add  help :  Add a FR-port or DLCI
add  usage:
 <PORT><phy-ifc>
 <DLCI>[numeric_suffix_name][fr_port]

add command parameters:
 port
 dlci

ATOSNT\fr>>add port ?

add command parameters:
 HDLC Port                [Empty list]
 <cr>
```

```
ATOSNT\fr>>add dlci ?

add command parameters:
 FR Port                   [fr-port0]
 DLCI numeric suffix name [max 3 decimal digits]
 <cr>
```

Table 2:**add PORT**

Syntax	Description
PORT	Keyword. Set the port to built-in the Frame Relay service
phy-ifc	This is the physical interface associated to the port for the Frame Relay service. At the moment there is only one physical interface that supports Frame Relay service, and this is the serial VX interface identified and available on the rooth menu as Serial0

Table 3:**add DLCI**

Syntax	Description
DLCI	Keyword. Stands for *Data Link Connection Identifier*. Data traffic is sent through a Frame Relay network using a data link connection identifier (DLCI), which specifies the frame's destination
numeric_suffix_name	Optionaly, up to 3 digital digits can be used to name the dlci. If name is not defined a progressive number will be added to dlci name (e.g. the first dlci name will be dlci0, the second dlci1 and so on)
fr_port	The port to which the dlci is associated

fr - Node

To show the structure of the "fr" node you should use the **tree** command:

```
ATOSNT\fr>>tree
fr                      fr-port0                lmi
                        dlci0
                        dlci1
                        dlci2
                        dlci3
```

fr-port0 - Commands

At the fr-port0 subnode, you can **set** the following parameters:

```
ATOSNT\fr\fr-port0>>set ?

Available nodes:
                        lmi

Set command parameters:
 level of log  [loglevel]  Current value: 5
```

Table 4:**set**

Syntax	Description

loglevel <0-5>	Set the level detail used by ATOS to log the events on the fr-port0 node [default: 1]

lmi - Commands

At the lmi subnode, you can **set** the following parameters:

```
ATOSNT\fr\fr-port0\lmi>>set ?

Nodes not available.
Set command parameters:
 level of log                                    [loglevel]  Current value: 1
 lmi type                                        [type]      Current value: ANSI
 lmi mode                                        [mode]      Current value: USER
 n391 (full status polling counter)              [n391]      Current value: 6
 n392 (error threshold)                          [n392]      Current value: 3
 n393 (monitored events count)                   [n393]      Current value: 4
 t391 (link integrity verification polling time) [t391]      Current value: 10
 t392 (polling verification time)                [t392]      Current value: 15
```

Table 5:**set**

Syntax	Description
loglevel <0-5>	Sets the level detail used by ATOS to log the events on the lmi subnode [default: 1]
type [DISABLED|ITU|ANSI|CISCO]	Sets the LMI specification that can be configured as disabled or compliant to ITU, ANSI or Cisco standard. [default: DISABLED]
mode [USER|NETWORK]	Set LMI mode: • USER : the device will act as a "user" LMI entity • NETWORK : the device will act as a "network" LMI entity [default: USER]
n391 [1-255]	Defines the STATUS ENQUIRE number after which to ask for logic single frame-relay connection status (FULL STATUS ENQUIRE trasmission) [default: 6]
n392 [1-10]	Defines the number of event errors (checked in a n393 event window) after which the frame-relay connection is stated as DOWN [default: 3]
n393 [1-10]	Defines the window for monitor events [default: 4]
t391 [5-30]	Defines the number of seconds after which to check the frame-relay connection integrity (STATUS ENQUIRE trasmission) [default: 10]
t392 [5-30]	Defines the number of seconds to wait for a STATUS ENQUIRE before noticing an event error [default: 15]

fr-port0 Configuration example

ATOSNT\fr\fr-port0>>show conf
Show of ATOSNT fr fr-port0
Level of log : 5
HDLC Port : serial0
Show of ATOSNT fr fr-port0 lmi
Level of log : 1
LMI type : ANSI
LMI mode : USER
N391 (Full status polling counter) : 6
N392 (Error Threshold) : 3
N393 (Monitored events count) : 4
T391 (Link integrity verification polling time) : 10
T392 (Polling verification time) : 15

fr-port0 Status and Statistics

ATOSNT\fr\fr-port0>>**show status**
status of FR port fr-port0
state : Up
Command executed
ATOSNT\fr\fr-port0>>**show statistics**
statistics of FR port fr-port0
******* upstream direction *******
bytes : 1818026
packets : 89922
requeues : 0
queue full : 0
****** downstream direction ******
bytes : 1611652
packets : 89534
errors : 0
drops : 0

dlci0 - Commands

At the dlci0 subnode you can **set** the following parameters:

```
ATOSNT\fr\dlci0>>set ?

Nodes not available.
Set command parameters:
 level of log    [loglevel]  Current value: 5
 fr port         [fr-ifc]    Current value: fr-port0
 dlci            [dlci]      Current value: 102
 cir (kbit/sec)  [cir]       Current value: 2048
 bc (bytes)      [bc]        Current value: 2000
```

```
be (bytes)      [be]        Current value: 0
```

Table 6:**set**

Syntax	Description
loglevel <0-5>	Sets the level detail used by ATOS to log the events on the dlci0 subnode [default: 1]
fr-ifc [fr-port0]	Sets the port to built-in the Frame relay service [default: fr-port0]
dlci [1-1022]	Sets the dlci value associated to the fr-port0 [default: 16]
cir [8-2048]	Sets in kbit per second, the guaranteed frame-relay data transmission rate. [default: 2048]
bc [2000-65535]	Sets in bytes, the guaranteed frame-relay data transmission peak in Tc time (Tc = BC*8/CIR) [default: 2000]
be [0-65535]	A possible value for this parameter allows to calculate the PIR1 = CIR*(1+BE/BC) [default: 0]

dlci0 - Configuration example

ATOSNT\fr\dlci0>>show conf

Show of ATOSNT fr dlci0

Level of log : 5

FR Port : fr-port0

DLCI : 102

CIR (Kbit/sec) : 2048

Bc (bytes) : 2000

Be (bytes) : 0

dlci0 - Status and Statistics

ATOSNT\fr\dlci0>>**show status**

status of frame-relay circuit dlci0

state: Up

ATOSNT\fr\dlci0>>**show statistics**

statistics of frame-relay circuit dlci0

******* upstream direction *******

bytes: 16380

packets: 390

errors: 0

****** downstream direction ******

bytes: 0

packets: 0

errors: 0

drops: 0

ManFXO

FXO Overview

FXO stands for Foreign Exchange Office. FXO is the physical interface that generates the off-hook and on-hook indications to the Foreign Exchange Subscribers (FXS) interfaces.
The node allows the incoming and/or outgoing calls management.

fxo - Commands

In **fxo** node you can configure the following parameters:

```
ATOSNT\fxo1>>set ?

Nodes not available.
Set command parameters:
 level of log                    [loglevel]              Current value: 1
 caller id type                  [cid-type]              Current value: fsk-v23
 hook flash time (msec)          [hookflash-time]        Current value: 200
 digit play time (msec)          [digit-play-time]       Current value: 100
 interdigit play time (msec)     [interdigit-play-time]  Current value: 100
```

Table 1: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the FXO events. Default: 1
fsk-v23|dtmf]	Sets the Caller ID type. Caller ID caller identification CID is the telephone service that sends information such as caller's number and name before callee's hooking off. ATOSNT supports the following standards Bellcore FSK,ETSI FSK V23 and DTMF. FSK signal is first detected on PSTN and then is generated to the POTS interfaces to which the call is forwarded. • fsk-bell202 Bellcore FSK • fsk-v23 ETSI FSK • dtmf Default: fsk-v23
hookflash-time [50-1000]	Sets the time in msec of hookflash. A hookflash is a brief interruption in the loop current that is not interpreted as a call disconnect. When the PBX or PSTN senses the hookflash, it puts the current call on hold and provides a secondary dial tone or access to other features such as transfer or call waiting access. Default: 200
digit-play-time [50-127]	Sets the time duration in msec of each digit. FXO interface generates and sends the digits to the network. Default: 100
interdigit-play-time [50-127]	Sets the time interval in msec between digits Default: 100

```
ATOSNT\fxo1>>show work
Show of ATOSNT fxo1
```

```
Level of log                    : 1
Operation mode                  : FXO
Caller ID Type                  : fsk-v23
Hook Flash Time (msec)          : 200
Digit Play Time (msec)          : 100
```

Interdigit Play Time (msec) : 100

ManInterfaces

Interfaces

ATOSNT permits the configuration of multiple data connections. There are many different types of interfaces. The connection type depends on the physical and logical interface. If you have subscribed multiple ATM virtual circuits with the service provider, you can establish simultaneous connections to different destination/service, each destination identified with VPI/VCI value.

This section deals with defining configuration for all logical interfaces such as Ethernet, WLAN, PPP, VLAN, etc.

The main node to add logical interface is “Interfaces”. Starting from this node the following commands are available:

Interfaces – Commands

```
ATOSNT\interfaces>>set ?
Nodes available:
                  loopback0
                  eth0
                  bridge0
                  wlan0
                  w3g0-ppp0
                  wlan0
                  vcc0
                  vcc0-ppp0
                  isdn-bri1-ppp0
                  ml-ppp0
                  vpn-ppp0
                  vpn0
                  vpn-gre0
                  pptp-server0
                  tun10
                  tap10
                  dlci0
                  dlci0-ppp0

Set command parameters:
  level of log  [loglevel]  Current value: 1
```

Table 1: set

Syntax	Description
Loglevel [0-5]	Sets the detail level used by ATOS to log the events of the interfaces, from the less detailed one (0) to the more detailed one (5). Adding the [- s] option, this command will be extended to all subnodes. [default: 1]

```
ATOSNT\interfaces>>add ?

add  help :  Add an Interface
add  usage:
 <IFC><parent_ifc>[ip/netmask][option[vid]][ifc name]

add command parameters:
 IFC

ATOSNT\interfaces>>add IFC ?

add command parameters:
 parent ifc name [isdn-bri1isdn-bri2
```

eth0|eth1|wlan0|ptm0|loopback|vpn|pptp-server|ml|openvpn]

```
Syntax  Description
IFC Keyword
parent_ifc Parent ifc name previously created. That string identifies
the “physical” interface you want to use (e.g. eth0, eth1, ptm0,
eth0:0, vcc0, dlci0, loopback, vpn, pptp-server, openvpn, w3g, vlan,
etc.). Using the “help” command you can see the available parent
interfaces .
 ip/netmask [aa.bb.cc.dd[/0-32]] Optionally you can configure at
creation phase the IP address and Netmask of the logical interface. If
no IP/netmask are specified, the logical interface will be created
using 0.0.0.0 as IP address and netmask.
 option [vid]Depending on the parent ifc used, option field can assume
the following values:
If ETH or WLAN parent ifc:
802.3 - to configure IEEE 802.3 standard interface;
802.1QP - to configure a Virtual Lan (VLAN) interface. In this case,
vid option value can be specified;
802.3-PPPoE - to configure a point to point over ethernet interface;
802.1QP-PPPoE - to configure a Virtual Lan (VLAN) interface over a
PPPoE connection. In this case, vid option value can be specified.
If VCC parent ifc:
IP - to configure an IPoA connection (RFC2684/RFC2864 standard);
802.3 - to configure IEEE 802.3 standard interface RFC2684;
802.1QP - to configure a Virtual Lan (VLAN) interface. In this case,
vid option value can be specified;
PPP - to configure a PPPoA connection (RFC2364 standard);
802.3-PPPoE - to configure a point to point over ethernet interface;
```

```
802.1QP-PPPoE - to configure a Virtual Lan (VLAN) interface over a
PPPoE connection. In this case, vid option value can be specified.
If VPN parent ifc:
PPTP  - to configure a PPTP VPN client
IP-in-IP - to configure an IP-in-IP VPN
IP6-in-IP - to configure a IP6-in-IP VPN
IP-in-IP6 - to configure a IP-in-IP6 VPN
IP6-in-IP6 - to configure a IP6-in-IP6 VPN
GRE - to configure a GRE VPN
IP6GRE - to configure a IP6 GRE VPN
6RD - to configure a 6RD VPN
If OpenVPN parent ifc:
IP   - to configure a TUN connection
802.3  - to configure a TAP connection
For PPTP Server parent ifc:
local - to identify the interface that has invoked the service
no local - to identify any interface
For DLCI parent ifc:
IP - to configure an IP over Frame Relay connection (RFC2427);
802.3 - to configure Bridge over Frame Relay (RFC2427);
802.1QP - to configure a Virtual Lan (VLAN) interface. In this case,
vidoption value can be specified;
PPP - to configure a PPP over Frame Relay (RFC1973);
802.3-PPPoE - to configure a point to point over ethernet interface;
802.1QP-PPPoE - to configure a Virtual Lan (VLAN) interface over a
PPPoE connection. In this case, vid option value can be specified.
 ifc nameOptionally, a string can be used to better identify the new
Interface. If name is not defined the interface name will be assigned
automatically by the firmware using the parent ifc name.
```

isdn-bri2

```
isdn-bri2
```

These are some examples of added interfaces:

```
isdn-bri2
```

Add a vpn interface

```
isdn-bri2
```

ATOSNT\interfaces>>add IFC vpn ? add command parameters: ip/netmask [aa.bb.cc.dd[/0-32

```
isdn-bri2
 encapsulation          [PPTP|IP-in-IP|IP6-in-IP|IP-in-IP6|IP6-in-IP6|GRE|IP6GRE|L2TP|IP6L2TP|6RD]
 ifc name               [max 15 char]
 <cr>
```

Suppose you want to add a vpn PPTP

```
ATOSNT\interfaces>>add IFC vpn PPTP
<cr>
```

As a result a new subnode named vpn-ppp0 appears.

```
ATOSNT\interfaces>>tree
interfaces              loopback0              ip
                                               ipv6
                        eth0                   ip
                                               ipv6                    slaac
                                                                       dhcp
                                                                       nd                      ra
                                               service-8023
                        vpn-ppp0               ip
                                               service-vpn
                                               service-ppp
```

In the below table there is a summary of the possible created subnodes when a new vpn interface is added

add IFC	Encap. type	subnode
vpn	PPTP	vpn-ppp0
vpn	IP-in-IP	vpn-ipip0
vpn	IP6-in-IP	vpn-ip6ip0
vpn	IP-in-IP6	vpn-ipip60
vpn	IP6-in-IP6	vpn-ip6ip60
vpn	GRE	vpn-gre0
vpn	IP6GRE	vpn-ip6gre0
vpn	6RD	vpn-6rd0

To delete an interface, the following command must be used:

```
ATOSNT\interfaces>>del?

del help: Delete an Interface
del usage:
 <IFC><ifc name>

del command parameters:
IFC

ATOSNT\interfaces>>del IFC?

del command parameters:
ifc name [eth0|ptm0|w3g0-ppp0|wlan0|vcc0|vcc0-ppp0|vpn-ipip0|vpn-ppp0|vpn-ip6ip0|vpn-ipip60|vpn-ip6ip60]
```

Table 3: del

Syntax	Description
IFC	Keyword
ifc name	Existing interface name to be deleted.

Interfaces – Nodes

Once an interface has been created a new subnode appears. Dependig of the interface type, each interface can have different tree. Here you can find an example of the most common used interfaces:

```
ATOSNT\interfaces>>tree

interfaces
loopback0    ip
             ipv6
eth0         ip
             ipv6      slaac
                       dhcp
                       nd      ra
             service-8023
bridge0      ip
             ipv6      slaac
                       dhcp
                       nd      ra
             service-8023
ptm0         ip
w3g0-ppp0    ip
             ipv6      slaac
                       dhcp
                       nd      ra
             service-ppp
wlan0        ip
             ipv6      slaac
                       dhcp
                       nd      ra
             service-8023
vcc0         ip
             ipv6      slaac
                       dhcp
                       nd      ra
             service-8023
             service-atm
vcc0-ppp0    ip
             ipv6      slaac
                       dhcp
                       nd      ra
             service-atm
```

```
             service-ppp
dlci0        ip
             service-8023
dlci0-ppp0   ip
             service-ppp
vpn-ppp0     ip
             service-vpn
             service-ppp
vpn-ipip60   ip
             service-vpn
vpn-ip6ip0   ipv6      slaac
                       dhcp
                       nd      ra
              service-vpn
vpn-gre0     ip
             ipv6      slaac
                       dhcp
                       nd      ra
             service-vpn
vpn-ip6gre0  ipv6      slaac
                       dhcp
                       nd      ra
             service-vpn
tun10        ip
             ipv6     slaac
                      dhcp
                      nd            ra
             service-vpn
tap10        ip
             ipv6     slaac
                      dhcp
                      nd            ra
             service-vpn
             service-8023
vpn-6rd0     ipv6     slaac
                      dhcp
                      nd            ra
pptp-server0 ip
             service-vpn
             service- ppp
ml-ppp0      ip
             ipv6     slaac
                      dhcp
                      nd            ra
             bod
             service-ppp
eth0:0       ip
```

```
eth0.100      ip
              ipv6      slaac
                        dhcp
                        nd            ra
              service-8023
              service-8021q

isdn-bri1-ppp0    ip
                  ipv6      slaac
                            dhcp
                            nd            ra
                  service-dialer
                  service-ppp
```

“Interface” subnode – Operating and Configuration Commands

For each “subinterface” the following operating commands are available:

```
connect                 Opens a session on node ATOSNT\interfaces\interface name>>
disconnect              Closes a session on node ATOSNT\interfaces\interface name>>
loopeth                 Enables/disables ethernet loop on node ATOSNT\interfaces\interface name>>
no-keepalive            Enables/disables no-keepalive on node ATOSNT\interfaces\interface name>>
```

Configuration Commands :

```
ATOSNT\interfaces>>set <interface name> ?


Available nodes:
                     ip


Set command parameters:
 level of log                     [loglevel]                  Current value: 1
 description                      [description]               Current value:
 enable                           [on|off]                    Current value: on
 opening mode                     [open-mode]                 Current value: on-demand
 mean rate window (sec)           [mean-rate-window]          Current value: 0
 inactivity time (sec)            [inactivitytime]            Current value: 60
 active traffic classifier        [active-traffic]            Current value:
 network group                    [network-group]             Current value:
 network group disable time (sec) [network-group-disable-time] Current value: 0
 connectivity monitor probe       [conn-mon-probe]            Current value: probe0
 probe fault action               [probe-fault-action]        Current value: disconnect
 use basic mac address            [use-basic-mac-addr]        Current value: false
```

Table 4: set

Syntax	Description
loglevel [0-5]	Sets the level detail used by ATOS to log the events [default 1]
Description	Up to 100 characters can be used to describe the node content
on|off	Enables/disables the subinterface
open-mode [always-on|on-demand|network-group-tracking]	*Only available on the PPP subinterface* Configure the PPP subinterface session modes: • **Always-on** the session is always opened • **On-demand** the session is opened and closed either on traffic over the subinterface or with the connect and disconnect commands. • **Network-group-tracking** the session is opened if NETWORK-GROUP goes down and closed if NETWORK-GROUP goes up Default values depend on the PPP subinterface type. Typically W3G subinterfaces are “on-demand”, VCC PPP subinterfaces are “always-on”.
mean-rate-window (sec) [0- 60]	Sets the rate window size. [default 0]
inactivitytime [0 – 65535]	*Only available on the PPP subinterface* Indicates the time after which the PPP session is cleared in case of no data packet transmission. The timer is not active if the value is 0. This means that the connection is “always-on” , i.e. it is active as long as the physical level is active. If the value is not 0, the connection is “on-demand” , i.e. it activates with data traffic and remains active until the set timer expires. [default 0]
active-traffic <string>	*Only available on the PPP subinterface* Classifier name created in the classifier-map node to be associated to the ingress traffic that actives the interface.
network-group <string>	Name of the “network-group” created in the “ip\networkgroup” node to be associated to the interface
network-group-disable-time <value>	Time to delay the interface disconnection when a network-group up state is received (e.g. the “main interface” recovers)
conn-mon-probe <string>	Sets the probe name configured in "connectivity-monitor" node to be associated to the interface. In case of connectivity monitor PING probe, the IP address should be the default gateway of the interface or an IP address located on the same subnet mask of the interface. For more details go to Connectivity Monitor - Commands
probe-fault-action [none|disconnect]	Sets the two possible actions that can be undertaken by the interface in case the connectivity monitor PROBE status is "down" (unreachable destination IP address). For more details go to Connectivity Monitor - PROBE Status DOWN : • **none** the interface will not remove the local static route but it will declare that it has lost its own IP address. • **disconnect** the interface will remove the local static route; it will declare that it has lost its own IP address and it will try to renegotiate to get a new IP address. For more details, go to

use-basic-mac-addr [true|false]	• **false** The Mac address is built-in just changing the most significant byte (00) in the product's Mac address 00:D0:D6:xx:xx • **true** It means that the Mac address used is the same than the product's Mac address 00:D0:D6:xx:xx
mirror-to	*Only available on Ethernet type interfaces (eth0, vlan, ptm, vcc 802.3, vcc PPPoE...* it means that it makes a copy of all packets sent and received over the ethernet interface

“Interface” IP subnode – Commands

Each subinterface added has an IP subnode where you can configure the relevant IP parameters:

```
ATOSNT\interfaces\eth0>>set ip?


Nodes not available.

Set command parameters:

 level of log        [loglevel]        Current value: 1

 ip address          [address]         Current value: 30.30.5.40

 netmask             [netmask]         Current value: 255.255.255.0

 default router      [defaultrouter]   Current value: 30.30.5.4

 mtu value           [mtu]             Current value: 1500

 dhcp client         [dhcp-client]     Current value: on

 auto provisioning   [auto-provisioning]  Current value: off

 unnumbered from     [unnumbered-from]  Current value:

 tcp mss adjustment  [tcp-mss-adjust]  Current value: path-mtu

 tx queue len        [tx-queue-len]    Current value: 1000</pre>
```

Table 5: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOS to log the events of the IP subinterface, from the less detailed one (0) to the more detailed one (5) [default: 1]
address [aa.bb.cc.dd]	Sets the IP address of the subinterface. [default: 0.0.0.0]
netmask [aa.bb.cc.dd]	Sets the subinterface netmask [default: 0.0.0.0] for all subinterfaces unless for PPP subinterface [default: 255.255.255.255] only for PPP subinterface *Note for PPP subinterfaces:* As referred above the netmask parameter default value for PPP subinterfaces is 255.255.255.255. • If netmask value is left set to 0.0.0.0 automatically it forces the use of the "natural" netmask associated to the address class assigned by PPP negotiation. • Instead, if netmask parameter is configured to a different value, this will be used regardless of the address class assigned by PPP unless it would be "larger" than the "natural" address; in this case the netmask to use will be the "natural" one.
defaultrouter [aa.bb.cc.dd]	Sets the default gateway IP address of the subinterface. [default: 0.0.0.0]

mtu [256 - 2048]	Configures the MTU (Maximum Transmission Unit) parameter. [default: 1500].
dhcp-client [on|off]	Enables/disables dhcp-client on the subinterface. [default: off]
auto-provisioning <off|fast-provisioning>	Enables/disables the IP autoconfiguration mode. off autoconfiguration mode is disabled fast-provisioning Enables the IP autoconfiguration mode.The auto provisioning procedure follows this scheme: 1. The CPE will receive all packets coming from the network. 2. All packets different from ICMP will be dropped. 3. If the IP destination address of the ICMP packet is different from the IP source address + 1, the packet will be dropped. 4. The CPE configures its address with the packet IP destination address that is the IP source address +1. 5. The autoprovisioning procedure ends up. [default: off]
unnumbered-from [<cr>|eth0|loopback0]	Sets the same IP address of the interface specified in "unnumbered-from" parameter.
tcp-mss-adjust [none|path-mtu|500–1460]	Configures the TCP MSS Adjustment value in terms of maximum segment size (MSS) of packets flow that travelling through an interface. none no MSS adjust is used path-mtu configures the MSS adjust as the MTU value for the same subinterface 500 – 1460 specifies a value of Maximum Segment Size [default path-mtu]
tx-queue-len	This parameter is only involved if QoS is not used over the interface. It indicates the packets length of the interface transmission queue. This queue is not related to the behaviour of the interface driver but it is implemented on the upper level. This means that if the interface driver ends the space on the own queue, the kernel will use “tx-queue-len” as additional space, waiting for the queue driver will have free space. This queue allows to manage exceeding traffic burst. This mechanism also manages traffic priorization based on the queued packets ToS field. Each interface has three queues with different priority (0=high, 1=mid, 2=low). Patckets to send to the driver are scheduled with prority order (first packets with priority 0, then 1 and last 2). **Mapping table between ToS and tx-queue priority:**

ToS	Description	Queue-priority
0	Normal Service	1
1	Minimize Monetary Cost	2
2	Maximize Reliability	1
3	Minimize Monetary Cost + Maximize Reliability	1
4	Maximize Throughput	2
6	Minimize Monetary Cost + Maximize Throughput	2
7	Minimize Monetary Cost + Maximize Reliability + Maximize Throughput	2
8	Minimize Delay	0
9	Minimize Monetary Cost + Minimize Delay	0
10	Maximize Reliability + Minimize Delay	0
11	Minimize Monetary Cost + Maximize Reliability + Minimize Delay	0
12	Maximize Throughput + Minimize Delay	1
13	Minimize Monetary Cost + Maximize Throughput + Minimize Delay	1
14	Maximize Reliability + Maximize Throughput + Minimize Delay	1
15	Minimize Monetary Cost + Maximize Reliability + Maximize Throughput + Minimize Delay	1

tx-queue-len default value:

ETH interface = 1000

VLAN interface = 256

VCC interface = 256

PPP interface = 3

“Interface” IPv6 subnode – Commands

Each subinterface added has an IPv6 subnode where you can configure the relevant IPv6 parameters:

Example of eth0\ipv6 interface

```
ATOSNT\interfaces\eth0\ipv6>>set ?

Available nodes:
                      slaac
                      dhcp
                      nd

Set command parameters:
 level of log         [loglevel]    Current value: 1
 enable               [on|off]      Current value: off
 hop limit            [hop-limit]   Current value: 64
 autoconfiguration    [autoconfig]  Current value: disabled
```

Table 6: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to log the events of the IPV6 network interface, from the less detailed one (0) to the more detailed one (5) [default: 1]
on|off	Enables/disables IPV6 on the network interface. [default: off]
hop-limit [1-255|unspecified]	Sets the hop limit value for IPv6 header. Hop limit is a substitute for IPv4 time to live. It is a 8-bit unsigned integer. Decremented by 1 by each node that forwards the packet. The packet is discarded if Hop Limit is decremented to zero. [default: 64]
autoconfig [disabled|slaac|slaac+dhcp|dhcp]	Sets the autoconfiguration mode on interface. [default: disabled]

Example of eth0-ppp0\ipv6 interface

```
ATOSNT\interfaces\eth0-ppp0\ipv6>>set ?

Available nodes:
                      slaac
                      dhcp
                      nd

Set command parameters:
 level of log         [loglevel]    Current value: 1
 enable               [on|off]      Current value: off
 hop limit            [hop-limit]   Current value: 64
 autoconfiguration    [autoconfig]  Current value: disabled
 local interface id   [local-id]    Current value: ::
 remote interface id  [remote-id]   Current value: ::
```

Table 7: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to log the events of the IPV6 network interface, from the less detailed one (0) to the more detailed one (5) [default: 1]
on|off	Enables/disables IPV6 on the network interface. [default: off]
hop-limit [1-255|unspecified]	Sets the hop limit value for IPv6 header. Hop limit is a substitute for IPv4 time to live. It is a 8-bit unsigned integer. Decremented by 1 by each node that forwards the packet. The packet is discarded if Hop Limit is decremented to zero. [default: 64]
autoconfig [disabled|slaac|slaac+dhcp|dhcp]	Sets the autoconfiguration mode on interface. [default: disabled]
local-id [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]	Sets the local identifier for PPP negotiation on network interface. [default: ::]
remote-id [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]	Sets the remote identifier for PPP negotiation on network interface. [default: ::]

```
ATOSNT\interfaces\eth0\ipv6>>add ?
```

```
Available nodes:
                        nd
add  help :  Add a new ADDRESS or PREFIX DELEGATION
add  usage:
 <NETWORK><address[/prefix-length]>[type]
 <PD><interface>

add command parameters:
 NETWORK
 PD
```

Add a new NETWORK address

```
ATOSNT\interfaces\eth0\ipv6>>add NETWORK 2001:123::1/32 ?

add command parameters:
 type                   [link-local|global|anycast|eui-64]
 <cr>
```

Table 8: add NETWORK address

Syntax	Description
NETWORK	Keyword.
address/prefix-length	The address and prefix to be assigned to the network interface. [default prefix length: 64]
type <link-local|global|anycast|eui64>	Specifying the address type **eui-64** the command configures global addresses with an interface identifier (ID) in the low-order 64 bits of the IPv6 address. Only the 64-bit network prefix for the address needs to be specified, the last 64 bits are automatically computed from the interface ID. Specifying the address type **link-local** the command configures a link-local address on the interface that is used instead of the link-local address that is automatically configured when IPv6 is enabled on the interface. Specifying the address type **anycast** the command adds an IPv6 anycast address. If the type isn't specified the command adds an IPv6 global address. [default: not specified]

Add Prefix Delegation

```
ATOSNT\interfaces\eth0\ipv6>>add PD ?

add command parameters:
 interface [eth0|eth1]
```

Table 9: add Prefix Delegation

Syntax	Description
PD	Keyword.
interface	Interface from which acquire the prefix to be assigned to the network interface.

Interface IPV6 slaac subnode – Commands

One of the most interesting addressing features in IPv6 is the feature called **IPv6 Stateless Address Autoconfiguration** which allows a device (further node) on an IPv6 network to automatically configure its own IP address. The feature also defines a method whereby the IP address can be renumbered.

IPv6 Stateless Address Autoconfiguration is specified in RFC 4862

The autoconfiguration process includes generating a link-local address, multicasting, the Neighbor Discovery (ND) protocol, and the ability to generate the interface identifier of an address from the underlying data link layer address.

The method consists of :

- Link-Local Address Generation: The device generates a link-local address derived from the data link layer (MAC) address
- Link-Local Address Uniqueness Test: The device tests to ensure that the address isn't already in use on the LAN (Neighbor Solicitation message and Neighbor Advertisement responses)
- Link-Local Address Assignment: Assuming the uniqueness of the address, the device assigns the link-local address to its IP interface.
- Router Contact: The device attempts to contact a local router to get more information to continue the configuration (Router Advertisement messages and Router Solicitation)
- Router Direction: The router provides direction to the node on how to proceed with the autoconfiguration. It may tell the node that on this network “stateful” autoconfiguration is in use, and tell it the address of a DHCP server to use. Alternately, it will tell the host how to determine its global Internet address.
- Global Address Configuration: Assuming that stateless autoconfiguration is in use on the network, the host will configure itself with its globally-unique Internet address. This address is generally formed from a network prefix provided to the host by the router, combined with the device's identifier as generated in the first step.

Using IPv6 Router Solicitations and Router Advertisements, hosts on the network can learn what network they are connected to, and once they do, they can automatically configure a host ID on that network and use the router as a default gateway.

Link local addresses are for connectivity inside the local network and are not reachable outside of the local network they are connected to.

```
ATOSNT\interfaces\eth0\ipv6\slaac>>set ?

Nodes not available.
Set command parameters:
 default router            [default-router]      Current value: off
 default route preference  [default-route-pref]  Current value: on
```

Table 10: set

Syntax	Description
default-router [on|off]	Enables/disables default router learning in Router Advertisement. [default: off]
default-route-pref [on|off]	If Enabled (ON), the default route PREFERENCE specified in "router advertisement" message will be used in the default route installation.[default: on]

Interface IPV6 dhcp subnode – Commands

The parameters you can configure in this subnode are related to **DHCPv6 Options**.

DHCP for IPv6 (further DHCPv6) is the "stateful address autoconfiguration protocol" specified in RFC 3315.

The Dynamic Host Configuration Protocol for IPv6 enables DHCP servers to pass configuration parameters such as IPv6 network addresses to IPv6 nodes (Routers and Hosts).

DHCPv6 offers the capability of automatic allocation of reusable network addresses and additional configuration flexibility (e.g. DNS server, NTP server, etc.).

DHCPv6 Options

Options are used to carry additional information and parameters in DHCPv6 messages. Every option shares a common base format. Some options apply to the client, some are specific to an IA (Identity Association).

Identity Association for Non-temporary Addresses Option

The Identity Association for Non-temporary Addresses option (IA_NA) is used to carry an IA_NA, the parmeters associated with the IA_NA, and the non-temporary addresses associated with the IA_NA.

Addresses appering in an IA_NA-options field are not temporary addresses

Terminology:

- Identity Association (IA)

  is a collection of addresses assigned to a client. Each IA has an associated IAID. A client may have more than one IA assigned to it; for example, one for each of its interfaces.Each IA holds one type of address; for example, an identity association for temporary addresses (IA_TA) holds temporary addresses

- Identity association identifier (IAID)

  An identifier for an IA, chosen by the client. Each IA has an IAID, which is chosen to be unique among all IAIDs for IAs belonging to that client.

- Identity association for non-temporary addresses (IA_NA)

  An IA that carries assigned addresses that are not temporary addresses

- Identity association for temporary addresses (IA_TA)

  An IA that carries temporary addresses

DHCPv6 options - Prefix Delegation

The specification RFC 3633 **IPv6 Prefix Options for DHCPv6** describes new options for DHCPv6, between them, it describes the mechanism for automated delegation of IPv6 prefixes.

This mechanism is intended for delegating a long-lived prefix from a delegating router to a requesting router and is appropriate for situations in which the delegating router does not have knowledge about the topology of the networks to which the requesting router is attached, and the delegating router does not require other information aside from the identity of the requesting router to choose a prefix for delegation.

For example, these options would be used by a service provider (ISP) to assign a prefix to a Customer Premise Equipment (CPE) device acting as a router between the subscriber's internal network and the service provider's core network. Thanks to this mechanism the DHCPv6-PD client (the CPE device) will be allowed to segment the received address IPv6 address space, and assign it dynamically to its IPv6 enabled interfaces.

Terminology:

- requesting router

  is the router that acts as a DHCPv6 client and is requesting prefix(es) to be assigned

- delegating router

  is the router that acts as a DHCPv6 server and is responding to the prefix request

- Identity Association for prefix Delegation (IA_PD)

  is a collection of prefixes assigned to the requesting router. Each IA_PD has an associated IAID. A requesting router may have more than one IA_PD assigned to it; for example, one for each of its interfaces.

Rapid Commit Option

When a client includes a Rapid Commit Option in a Solicit message, the server must responde with a Rapid Commit option and commit the assigned addresses in the Replay message sent in response to the Solicit message during the Solicit-reply message exchange.

```
ATOSNT\interfaces\eth0\ipv6\dhcp>>set ?

Nodes not available.
Set command parameters:
 request ia for non-temporary address  [ia-na]         Current value: on
 request ia for prefix delegation      [ia-pd]         Current value: off
 rapid commit                          [rapid-commit]  Current value: off
```

Table 11: set

Syntax	Description
ia-na [onloff]	If enabled, dhcp sends a request for an IA_NA (identity association for non-temporary address). [default: on]
ia-pd [onloff]	If enabled, dhcp sends a request for an IA_PD (identity association for prefix delegation). [default: off]
rapid-commit	If enabled, dhcp will include a rapid-commit option in solicit messages and will expect a reply message that includes a rapid commit option in response.[default: off]

Interface IPV6 nd subnode – Commands

IPv6 Neighbor Discovery (ND) is a new protocol for IPv6.
IPv6 nodes on the same link use Neighbor Discovery to discover each other's presence, to determine each other's link-layer addresses, to find routers, and to maintain reachability information about the paths to active neighbors.

```
ATOSNT\interfaces\eth0\ipv6\nd>>set ?

Available nodes:
                      ra

Set command parameters:
 level of log                            [loglevel]          Current value: 1
 neighbour solicitation interval (msec)  [ns-interval]       Current value: 1000
 neighbour reachable time (msec)         [reachable-time]    Current value: 30000
 neighbour solicitation max number       [ns-mcast-max-num]  Current value: 3
 dad attempts                            [dad-attempts]      Current value: 1
```

Table 12: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOS to record the events of the interface nd operations. [default: 1]
ns-interval [500-3600000]	Sets the time in milliseconds between retransmitted Neighbor Solicitation messages. [default: 1000].
reachable-time [100-3600000]	Sets the time in milliseconds that a node assumes a neighbor is reachable after having received a reachability configuration. [default: 30000]
ns-mcast-max-num [1-255]	The maximum number of attempts (Neighbour Solicitation) to resolve an address before marking the entry as unreachable. [default:3]
dad-attemps [0-600]	Sets the number of attempts for ipv6 duplicate address detection. [default:1]

"Interface IPV6 nd" ra subnode – Commands

```
ATOSNT\interfaces\eth0\ipv6\nd\ra>>set ?

Nodes not available.
Set command parameters:
 sending of router advertisements  [sending-ra]        Current value: on
 max ra interval (sec)             [max-ra-interval]   Current value: 600
 min ra interval (sec)             [min-ra-interval]   Current value: 200
 managed address configuration     [managed-addr-cfg]  Current value: off
 other configuration               [other-cfg]         Current value: off
 default router preference         [def-rtr-pref]      Current value: medium
 default router lifetime (sec)     [def-rtr-lifetime]  Current value: 1800
 hop limit                         [hop-limit]         Current value: unspecified
 reachable time                    [reachable-time]    Current value: unspecified
 retrans time                      [ns-interval]       Current value: unspecified
 link mtu                          [mtu]               Current value: unspecified
```

Table 13: set

Syntax	Description
sending-ra [on|off]	Enables/disables the router advertisement sending. [default: on]
max-ra-interval [4-1800]	The maximum time in seconds allowed between sending unsolicited multicast router advertisements from the interface. [default: 600 seconds]
min-ra-interval [3-(0.75*max-ra-interval)]	The minimum time in seconds allowed between sending unsolicited multicast router advertisements from the interface. [default: 200 seconds]
managed-addr-cfg [on|off]	When enabled, it indicates that addresses are available via Dynamic Host Configuration Protocol [DHCPv6].[default: off]
other-cfg [on|off]	When enabled, it indicates that other configuration information is available via DHCPv6. Examples of such information are DNS-related information or information on other servers within the network.[default: off]
def-rtr-pref [medium|high|low]	Is the preference associated with the default router.[default: medium]
def-rtr-lifetime [0-9000]	The lifetime in seconds associated with the default router. The field can contain values up to 9000 seconds. A Lifetime of 0 indicates that the router is not a default router and SHOULD NOT appear on the default router list.[default: 1800]

hop-limit [unspecified|specified]	Sets the hop limit value for IPv6 header.
reachable-time [unspecified|specified]	The time, in milliseconds, that a node assumes a neighbor is reachable after having received a reachability confirmation. Used by the Neighbor Unreachability Detection algorithm (see Section 7.3 of RFC 4861). A value of zero means unspecified (by this router). Must be no greater than 3,600,000 milliseconds (1 hour).[default: 0]
ns-interval [unspecified|specified]	Sets the time in milliseconds between retransmitted Neighbor Solicitation messages.
mtu [unspecified|specified]	Enables/Disables the MTU option in router advertisement. The MTU option is used in router advertisement messages to ensure that all nodes use the same MTU value on links lacking a well-defined MTU. If true the option use the specified MTU value. This value must not be smaller than 1280 and not greater than the maximum MTU allowed for this. [default: 0 (option not included)]

Add a new PREFIX

PREFIX parameter allows to configure which IPv6 prefixes are included in IPv6 router advertisements.
The prefix advertisement can be used by neighboring devices to autoconfigure their interface addresses.
Stateless autoconfiguration uses IPv6 prefixes provided in router advertisement messages to create the global unicast address from the link-local address.

```
ATOSNT\interfaces\eth0\ipv6\nd\ra>>add ?

add  help :  Add a new PREFIX
add  usage:
 <PREFIX><address/prefix-length|default>[no-advertise]
 <PREFIX><address/prefix-length|default>
         [valid-lifetime <value|infinite>]
         [preferred-lifetime <value|infinite>]
         [no-autoconfig]
         [off-link]
         [no-rtr-address]

add command parameters:
 PREFIX

ATOSNT\interfaces\eth0\ipv6\nd\ra>>add PREFIX ?

add command parameters:
 prefix                  [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/0-128|default]

ATOSNT\interfaces\eth0\ipv6\nd\ra>>add PREFIX 2001:33::/64 ?

add command parameters:
 option                  [no-advertise|valid-lifetime|preferred-lifetime|
                         no-autoconfig|off-link|no-rtr-address]
 <cr>
```

Table 14: set

Syntax	Description
PREFIX	Keyword.
type	Specifying **address/prefix-length** you configure the network address to include in Router Advertisement. Specifying **default** you configure the default values used in all unspecified prefixes included in Router Advertisement .
no-advertise	The optional "no-advertise" keyword indicates that the specified prefix is not included in Router Advertisement.
valid-lifetime [0-4294967295|infinite]	Specifies the time in seconds that the specified IPv6 prefix is advertised as being valid. The maximum value represents infinite, which can also be specified with infinite. [default: 2592000 (30 days)]
preferred-lifetime [0-4294967295|infinite]	Specifies the time in seconds that the specified IPv6 prefix is advertised as being preferred. The maximum value represents infinite, which can also be specified with infinite. [default: 604800 (7 days)]
no-autoconfig	The optional no-autoconfig keyword indicates to hosts on the local link that the specified prefix cannot be used for IPv6 autoconfiguration.
off-link	The optional off-link keyword indicates that the specified prefix is not used for on-link determination.

Interface IPv6 nd ra - Configuration Example

ATOSNT\interfaces\eth0\ipv6\nd>>**show conf**

Show of ATOSNT interfaces eth0 ipv6 nd

Level of log : 1

Neighbour solicitation interval (msec) : 1000

Neighbour reachable time (msec) : 30000

Neighbour solicitation max number : 3

DAD attempts : 1

Show of ATOSNT interfaces eth0 ipv6 nd ra

sending of router advertisements : on

max ra interval (sec) : 600

min ra interval (sec) : 200

managed address configuration : off

other configuration : off

default router preference : medium

default router lifetime (sec) : 1800

Hop limit : unspecified

Reachable time : unspecified

Retrans time : unspecified

link MTU : unspecified

LIST OF PREFIXES

PREFIX	ADVERTISE	V-LIFETIME	P-LIFETIME	AUTOCONF	LINK	RTR-ADDR
2001:32::/64	yes	2592000	604800	no	on	yes

Command executed

"Interface" Multilink PPP subnode - Commands

MLPPP bundle functionality is used with ISDN ports when these are configured as TE (terminal Equipment).
It provides a total duplex bandwidth of 128 kbit/s with 1 BRI ISDN or up to 256 kb/s with 2 BRI ISDN depending on the product model. For instance for a bundle of 256 kb/s, the user should set up B1 and B2 channels from the two BRI ISDN accesses.

When used the MLPPP feature, during the call set up, there will be as many calls as there are the bearer channels used to get the remote end-point.

ml-ppp0 Subnode allows to set the folowing parameters:

```
ATOSNT\interfaces\ml-ppp0>>set ?

Available nodes:
                       ip
                       bod
                       service-ppp

Set command parameters:
 level of log                      [loglevel]                    Current value: 1
 description                       [description]                 Current value:
 enable                            [on|off]                      Current value: on
 opening mode                      [open-mode]                   Current value: on-demand
 inactivity time (sec)             [inactivitytime]              Current value: 60
 active traffic classifier         [active-traffic]              Current value:
 network group                     [network-group]               Current value:
 network group disable time (sec)  [network-group-disable-time]  Current value: 0
```

To add a link (B channel) to the multilink interface, you should use add command:

```
ATOSNT\interfaces\ml-ppp0>>add ?

add  help :  Add a link in a multilink interface
add  usage:
 <LINK><ifc name>[priority]

add command parameters:
 LINK
ATOSNT\interfaces\ml-ppp0>>add LINK ?

add command parameters:
 ifc name  [isdn-bri1-ppp0|isdn-bri1-ppp1|isdn-bri2-ppp0|isdn-bri2-ppp1]

ATOSNT\interfaces\ml-ppp0>>add LINK isdn-bri1-ppp0 ?

add command parameters:
  priority  [0-255]
 <cr>
ATOSNT\interfaces\ml-ppp0>>add LINK isdn-bri1-ppp0
Command executed
```

```
ATOSNT\interfaces\ml-ppp0>>add LINK isdn-bri1-ppp1
Command executed
ATOSNT\interfaces\ml-ppp0>>add LINK isdn-bri2-ppp0
Command executed
ATOSNT\interfaces\ml-ppp0>>add LINK isdn-bri2-ppp1
Command executed

The multilink interface will be operational after setting:
- PPP profile
- MLPPP profile

Command executed
```

Table 15: add LINK

Syntax	Description
LINK	Keyword
ifc name	This is the list of the available ISDN interfaces (the number depends on the product model) to built-in the Multilink interface. At the moment Multilink PPP interface only works with ISDN.
priority [0-255]	Optional value to set the link priority; it defines the order in which you add the link in the bundle. Set to 255 means maximum priority; instead if not specified, it remains the order in which they were added.

"Interface" Multilink PPP BOD subnode - Commands

Bandwith-On-Demand (BOD) refers to the ability of a system to dynamically change the bandwith of a multilink bundle by establishing and removing links.

BOD subnode is used to configure the Bandwith on Demand service.

A link will be added if in "add-time" will occur that traffic exceeds the threshold calculated as follows:

traffic rate = (((rate of last link added) *(“add threshold/100”)) + rate of other link added)

A link will be dropped if in "drop-time" will occur that traffic not exceed the threshold calculated as follows:

traffic rate = (((rate of last link added) *(“drop threshold/100”)) + rate of other link added)

At BOD subnode, the following parameters can be configured:

```
ATOSNT\interfaces\ml-ppp0>>set bod ?

Nodes not available.
Set command parameters:
 level of log             [loglevel]             Current value: 1
 enable                   [on|off]               Current value: off
 add link time (sec)      [add-link-time]        Current value: 20
 add link threshold (%)   [add-link-threshold]   Current value: 80
 drop link time (sec)     [drop-link-time]       Current value: 40
 drop link threshold (%)  [drop-link-threshold]  Current value: 70
```

Table 16: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOS to log the events from the less detailed one (0) to the more detailed one (5). [Default: 1]
on|off	Enables/disables Bandwith-On-Demand feature
add-link-time [1-3600]	Sets the add-time in seconds [Default: 20]
add-link-threshold (%) [1-100]	Sets the add-threshold in percentage [Default: 80]
drop-link-time (sec) [1-3600]	Sets drop-time in sec [Default: 40]
drop-link-threshold (%) [1-100]	Sets drop-threshold in percentage [Default: 70]

"Interface" Service-802.3 subnode – Commands

Each added Ethernet subinterface has a Service-8023 subnode where you can configure the relevant parameters with set, add and del commands:

```
ATOSNT\interfaces\eth0>>set service-8023?

Nodes not available.
Set command parameters:
 tag insertion         [tag-insertion]     Current value: off
 default vid           [default-vid]       Current value: 1
 default priority      [default-priority]  Current value: 0
 priority translation  [prio-translation]  Current value: off
 tag removal           [tag-removal]       Current value: off
 use ingress priority  [use-ingress-prio]  Current value: false
```

Table 17: set

Syntax	Description
off]	Activates/deactivates the tagging insertion in the incoming untagged ethernet frames. [default: off].
default-vid [1 – max-vid]	Defines the default vid applied to the untagged ingress frames [default: 0]. Max-vid depends on the CPE hardware platform and can be 4094 or 4092.
default-priority [0 – 7|from -tos]	Defines the default priority applied to the untagged ingress frames [default: 0].
prio-translation [off|0 – 7|from-policy-marker]	Defines and activates the priority translation applied to all ingress frames [default: off).
tag-removal [1-4094|off|all-vid]	Enables/disables 802.1Q and 8021.p tag removal from the frames transmitted [default: off].
use-ingress-prio [true|false]	Enables/disables use of 8021.p priority [default: false].

To add a translation rule from TOS or POLICY MARKER to PRIORITY, you should use add command

```
ATOSNT\interfaces\eth0\service-8023>>add ?

add  help :  Add a translation rule from TOS or POLICY MARKER to PRIORITY
add  usage:
 <TOS-TO-PRIO><tos><mask><priority>
```

```
 <POLICY-MARKER-TO-PRIO><policy-marker><action><priority>

add command parameters:
 TOS-TO-PRIO
 POLICY-MARKER-TO-PRIO
```

Table 18: add TOS-TO-PRIO

Syntax	Description
TOS-TO-PRIO	Keyword
tos [0-FF hex]	Sets Ipv4 TOS or Ipv6 TRAFFIC CLASS value
mask [0-FF hex]	Sets the the Bitmask value
priority [0-7]	Defines the Priority 802.1p value

Table 19: add POLICY-MARKER-TO-PRIO

Syntax	Description
POLICY-MARKER-TO-PRIO	Keyword
policy-marker [1-256]	Identifies a policy marker configured in QoS node for an ingress policy (POLICY POLICING).
action [assign|decrement|increment]	Specifies the action to do in the priority field.
priority [0-7]	Sets the Priority 802.1p value or delta .

To delete a translation rule from TOS or POLICY MARKER to PRIORITY, you should use del command

```
ATOSNT\interfaces\eth0\service-8023>>del ?

del  help :  Delete a translation rule from TOS or POLICY MARKER to PRIORITY
del  usage:
 <TOS-TO-PRIO><tos>
 <POLICY-MARKER-TO-PRIO><policy-marker>

del command parameters:
 TOS-TO-PRIO
 POLICY-MARKER-TO-PRIO
```

Table 20: del TOS-TO-PRIO

Syntax	Description
TOS-TO-PRIO	Keyword
tos [0-FF hex]	Deletes Ipv4 TOS or Ipv6 TRAFFIC CLASS value

Table 21: del POLICY-MARKER-TO-PRIO

Syntax	Description
POLICY-MARKER-TO-PRIO	Keyword
policy-marker [0-65535]	Deletes a policy marker configured in the QoS node for an ingress policy.

“Interface” Service-Atm subnode – Commands

Each added VCC subinterface has a Service-Atm subnode where you can configure the relevant parameters:

```
ATOSNT\interfaces>>set vcc0 service-atm?

Nodes not available.

Set command parameters:
encapsulation  llc-snap [llcsnap]   Current value: on
crc preserved [fcspreserved] Current value: off
```

Table 22: set

Syntax	Description
llcsnap [on|off]	You can include a header indicating the encapsulation mode of the payload when you transmit data packets. The parameter value must be selected according to the operating mode of the server connected to the device. If you change to on, the encapsulation mode is added to the payload. [default on].
fcspreserved [on|off]	Activates/deactivates the "Preserved CRC" option. This option maintains the error detection code (CRC-32) of the Ethernet frames in incoming and outgoing packets. [default: off].

“Interface” Service-Ppp subnode – Commands

Each added PPP subinterface has a Service-Ppp subnode where you can configure the relevant parameters:

Service PPP

```
ATOSNT\interfaces>>set isdn-bri1-ppp0 service-ppp ?

Nodes not available.
Set command parameters:
 level of log   [loglevel]       Current value: 1
 ppp profile    [ppp-profile]    Current value: ppp0
```

Table 23: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOS to log the events of the service PPP subnode, from the less detailed one (0) to the more detailed one (5) [default: 1]
ppp-profile	Selects the PPP profile, previously added on the “point-to-point” node, to use on the PPP subinterface.

Service PPPoE

```
ATOSNT\interfaces>>set vcc0-ppp0 service-ppp?

Nodes not available.

Set command parameters:
level of log [loglevel] Current value: 1

ppp profile [ppp-profile] Current value: ppp0
pppoe profile [pppoe-profile] Current value: pppoe0
```

Table 24: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOS to log the events of the service PPP subnode, from the less detailed one (0) to the more detailed one (5) [default: 1]
ppp-profile	Selects the PPP profile, previously added on the “point-to-point” node, to use on the PPP subinterface.
pppoe-profile	Select the PPPoE profile, previously added on the “point-to-point” node, to use on the PPPoE subinterface.

Service MLPPP

```
ATOSNT\interfaces\ml-ppp0>>set service-ppp ?

Nodes not available.
Set command parameters:
 level of log   [loglevel]       Current value: 1
 ppp profile    [ppp-profile]    Current value: ppp0
 mlppp profile  [mlppp-profile]  Current value: mlppp0
```

Table 25: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOS to log the events of the service PPP subnode, from the less detailed one (0) to the more detailed one (5) [default: 1]
ppp-profile	Selects the PPP profile, previously added on the “point-to-point” node, to use on the PPP subinterface.
mlppp-profile	Selects the MLPPP profile, previously added on the “point-to-point” node, to use on the PPP subinterface.

“Interface” Service-802.1Q subnode – Commands

Each added VLAN subinterface has a Service-8021Q subnode where you can configure the relevant parameters:

```
ATOSNT\interfaces\eth0.1\service-8021q>>set ?

Nodes not available.
Set command parameters:
 egress priority      [priority]             Current value: 0
 ingress priority     [ingress-priority]     Current value: 0
 egress priority map  [egress-priority-map]  Current value: 0 1 2 3 4 5 6 7
```

Table 26: set

Syntax	Description
priority [0-7|from-ingress|from-map]	Sets the egress priority applied to egress frames: • 0-7 from 802.1p bits • from-ingress means it uses the same priority that the incoming packet • from-map means it uses the mapping configured in the "egress-priority-map" [default 0]
ingress-priority [0–7|trasparent]	Defines the mapping from 802.1p bits in ingress frames and the priority : • 0-7 from 802.1p bits • trasparent means that the priority is the same as the received packet. [default 0]
egress-priority-map [list of 8 values (0-7)]	Defines the 802.1p bits mapping applied to egress frames when the “priority” parameter value is from-map Default: 0 1 2 3 4 5 6 7

“Interface” Service-Vpn subnode

Each added VPN subinterface has a service-vpn subnode where you can configure the relevant parameters

Service-Vpn for PPTP VPN client - Commands

```
ATOSNT\interfaces>>set vpn-ppp0 service-vpn ?
Nodes not available.
Set command parameters:
 remote peer                      [remote-peer]                Current value:
 pptp echo request timeout (sec)  [pptp-echo-req-timeout]      Current value: 60
 pptp echo reply timeout (sec)    [pptp-echo-reply-timeout]    Current value: 60
```

Table 27: set

Syntax	Description
remote-peer [max 16 char]	To configure the remote peer. [default empty]
pptp-echo-req-timeout (sec) [0-255]	To configure the echo request timeout. [default 60]
pptp-echo-reply-timeout (sec) [0-255]	To configure the echo reply timeout. [default 60]

Service-Vpn for IP-in-IP VPN - Commands

```
ATOSNT\interfaces\vpn-ipip0\service-vpn>>set ?

Nodes not available.
Set command parameters:
 remote ip address          [remote-address]             Current value: 0.0.0.0
 local address or ifc name  [local-address-or-ifc-name]  Current value: none
```

Table 28: set

Syntax	Description
remote-address [aa.bb.cc.dd]	To configure the remote ip address [default 0.0.0.0]
local-address-or-ifc-name [aa.bb.cc.dd|none|loopback0|eth0|vpn-ipip0]	To configure the local address or local interface [default none]

Service-Vpn for IP6-in-IP VPN - Commands

```
ATOSNT\interfaces\vpn-ip6ip0\service-vpn>>set ?

Nodes not available.
Set command parameters:
 remote ip address          [remote-address]             Current value: 0.0.0.0
 local address or ifc name  [local-address-or-ifc-name]  Current value: none
```

Table 29: set

Syntax	Description
remote-address [aa.bb.cc.dd]	To configure the remote ip address [default 0.0.0.0]
local-address-or-ifc-name [aa.bb.cc.dd|none|loopback0|eth0|vpn-ipip0]	To configure the local address or local interface [default none]

Service-Vpn for IP-in-IP6 – Commands

```
ATOSNT\interfaces\vpn-ipip60\service-vpn>>set ?

Nodes not available.
Set command parameters:
 remote ip address          [remote-address]             Current value: ::
 local address or ifc name  [local-address-or-ifc-name]  Current value: none
```

Table 30: set

Syntax	Description
remote-address [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]	To configure the remote ip address [default ::]
local-address-or-ifc-name [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx|none| loopback0|eth0|vpn-ipip0|vpn-ppp0|vpn-ip6ip0|vpn-ipip60|vpn-ip6ip60]	To configure the local address or local interface [default none]

Service-Vpn for IP6-in-IP6 VPN – Commands

```
ATOSNT\interfaces\vpn-ip6ip60\service-vpn>>set ?

Nodes not available.
Set command parameters:
 remote ip address          [remote-address]             Current value: ::
 local address or ifc name  [local-address-or-ifc-name]  Current value: none
```

Table 31: set

Syntax	Description
remote-address [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]	To configure the remote ip address [default ::]
local-address-or-ifc-name [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx|none| loopback0|eth0|vpn-ipip0|vpn-ppp0|vpn-ip6ip0|vpn-ipip60|vpn-ip6ip60]	To configure the local address or local interface [default none]

Service-Vpn for GRE VPN - Commands

```
ATOSNT\interfaces\vpn-gre0\service-vpn>>set ?

Nodes not available.
Set command parameters:
 remote ip address                [remote-address]             Current value: 0.0.0.0
 local address or ifc name        [local-address-or-ifc-name]  Current value: 0.0.0.0
```

```
 tx sequence number              [seq-num-tx-enable]          Current value: off
 rx sequence number              [seq-num-rx-enable]          Current value: off
 tx checksum                     [checksum-tx-enable]         Current value: off
 rx checksum                     [checksum-rx-enable]         Current value: off
 tx key value                    [key-tx-value]               Current value: none
 rx key value                    [key-rx-value]               Current value: none
```

Table 32: set

Syntax	Description
remote-address [aa.bb.cc.dd]	Sets the public remote ip address [default 0.0.0.0]
local-address-or-ifc-name [aa.bb.cc.dd|none|loopback0|eth0|vpn-ipip0|vpn-ppp0| vpn-ip6ip0|vpn-ipip60|vpn-ip6ip60|vpn-gre0]	Sets the public local ip address or ifc name. [default 0.0.0.0]
Seq-num-tx-enable [on|off]	If enabled, adds a sequence number to the gre header tx packet. [default off]
Seq-num rx-enable [on|off]	If enabled, the receiver evaluates the received gre header sequence number and drops packets arriving out of order. [default off]
Checksum-tx-enable [on|off]	If enabled, the checksum is calculated for each outgoing GRE packet and stored in GRE header. The checksum bit is set in GRE header. Tunnel checksum is used to verify the integrity of packets. [default off]
Checksum-rx-enable [on|off]	If enabled, a packet with an incorrect checksum is dropped. [default off]
Key-tx-value [1-FFFFFFFF hex|none]	Configures the tx key for the gre tunnel .The two ends of a tunnel must have the same key or have no key at the same time. [default none]
Key-rx-value [1-FFFFFFFF hex|none]	Configures the rx key for the gre tunnel. A matching tunnel key value must be used on both ends of the tunnel or received packets are discarded. [default none]

Service-Vpn for IP6GRE VPN - Commands

IP6GRE VPN is only available on some CPEs like SV6044E

```
ATOSNT\interfaces\vpn-ip6gre0>>set service-vpn ?

Nodes not available.
Set command parameters:
 remote ip address               [remote-address]               Current value: ::
 local address or ifc name       [local-address-or-ifc-name]    Current value: none
 tx sequence number              [seq-num-tx-enable]            Current value: off
 rx sequence number              [seq-num-rx-enable]            Current value: off
 tx checksum                     [checksum-tx-enable]           Current value: off
 rx checksum                     [checksum-rx-enable]           Current value: off
 tx key value                    [key-tx-value]                 Current value: none
 rx key value                    [key-rx-value]                 Current value: none
```

Table 33 : set

Syntax	Description
remote-address [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]	Sets the public remote ip address [default ::]
local-address-or-ifc-name [aa.bb.cc.ddlnonelloopback0leth0lvpn-ipip0lvpn-ppp0lvpn-ip6ip0lvpn-ipip60lvpn-ip6ip60lvpn-gre0]	Sets the public local ip address or ifc name. [default none]
Seq-num-tx-enable [on|off]	If enabled, adds a sequence number to the gre header tx packet. [default off]
Seq-num rx-enable [on|off]	If enabled, the receiver evaluates the received gre header sequence number and drops packets arriving out of order. [default off]
Checksum-tx-enable [on|off]	If enabled, the checksum is calculated for each outgoing GRE packet and stored in GRE header. The checksum bit is set in GRE header. Tunnel checksum is used to verify the integrity of packets. [default off]
Checksum-rx-enable [on|off]	If enabled, a packet with an incorrect checksum is dropped. [default off]
Key-tx-value [1-FFFFFFFF hex|none]	Configures the tx key for the gre tunnel .The two ends of a tunnel must have the same key or have no key at the same time. [default none]
Key-rx-value [1-FFFFFFFF hex|none]	Configures the rx key for the gre tunnel. A matching tunnel key value must be used on both ends of the tunnel or received packets are discarded. [default none]

Service-Vpn for 6RD VPN – Commands

6rd is the mechanism to facilitate the rapid deployment of IPv6 across existing IPv4 infrastructures of Internet service providers (ISPs).

6rd, like 6to4, utilizes stateless IPv6 in IPv4 encapsulation. It requires to use one of its own IP prefixes. The delegated prefix is constructed by appending the ISP-assigned IPv4 address to the 6RD prefix.

6to4 is an Internet transition mechanism for migrating from IPv4 to IPv6, a system that allows IPv6 packets to be transmitted over an IPv4 network without the need to configure explicit tunnels. Special relay servers are also in place that allow 6to4 networks to communicate with native IPv6 networks.

```
ATOSNT\interfaces\vpn-6rd0\service-vpn>>set ?

Nodes not available.
Set command parameters:
 local address or ifc name  [local-address-or-ifc-name]  Current value: none
 ipv6 prefix 6rd            [ipv6-prefix]                Current value: 2002::/16
 ipv4 common prefix 6rd     [ipv4-common-prefix]         Current value: 0.0.0.0/0
```

Table 34: set

Syntax	Description
local-address-or-ifc-name [aa.bb.cc.dd|none|loopback0|eth0|vpn-ppp0|vpn-6rd0]	Sets the public local ip address or ifc name. [default none]
ipv6-prefix [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/0-128]	Sets the 6RD prefix [default 2002::/16]
ipv4-common-prefix [aa.bb.cc.dd/0-32]	All routers in the 6rd domain can share a common ipv4 prefix for their ipv4 address blocks. This common prefix is provisioned to all nodes and it doesn't need to be carried in the ipv6 destination . [defualt 0.0.0.0/0]

Service-Vpn for PPTP Server - Commands

```
ATOSNT\interfaces>>set pptp-server0 service-vpn ?
Nodes not available.

Set command parameters:
 local address or ifc name        [local-address-or-ifc-name]  Current value: 0.0.0.0
```

Table 35: set

Syntax	Description
local-address-or-ifc-name	To configure the local address or local interface [default empty]

Service-Vpn for OpenVPN – Commands

```
ATOSNT\interfaces>>set tun10 service-vpn ?

Nodes not available.
Set command parameters:
 level of log                  [loglevel]                    Current value: 1
 protocol                      [protocol]                    Current value: udp
 server                        [server]                      Current value:
 local address or ifc name     [local-address-or-ifc-name]   Current value: none
 protocol port                 [port]                        Current value: 1194
 address from server           [address-from-server]         Current value: off
 certificate profile name      [certificate-profile]         Current value: profile0
 cipher algorithm              [cipher-alg]                  Current value: BF_CBC
 keep alive timeout            [keep-alive-timeout]          Current value: 10
 keep alive not reply timeout  [keep-alive-no-reply-timeout] Current value: 30
```

Table 36: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOS to log the events of the OpenVPN service, from the less detailed (0) to the more detailed one (5) [default: 1]
protocol [udp|tcp|udp6|tcp6]	Sets the protocol to be used for the communications with the remote server. [default: udp]
port [1-65535]	Sets the TCP/UDP port number for both the local client and the remote server. [default: 1194]
address-from-server [on|off]	If enabled, OpenVPN client should accept option (ip address,..) pushed by the remote server. [default: off]
local-address-or-ifc-name [aa.bb.cc.dd| xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx| eth0]	Local ip address or ifc name for bind. If unspecified, openVPN will bind to all interfaces. [default: none]
server [max 100 char]	Sets the remote server name or ip/ipv6 address. [default --]
certificate-profile [<cr>|profile0]	Sets the name of the certificate profile, used during the client authentication, defined under **Certificate** node. For more details click on and go to "certificate" node. [default --]
cipher-alg [none|BF_CBC|AES_128_CBC |AES_192_CBC|AES_256_CBC]	Sets the cipher algorithm for the packets encryption. [default BF-CBC]
keep-alive-timeout (sec) [1-3600]	Enables to send a ping to the remote server over tcp/udp control channel if no packets have been sent for at least n seconds. [default: 10]
keep-alive-no-reply-timeout (sec) [1-3600]	It causes openVPN to restart after n seconds pass without reception of a ping or other packet from remote [default: 30]

"Interface" Service-Dialer subnode - Commands

Service - Dialer subnode allows to setup the ISDN Number of the remote end-point in the outgoing call.

Previously, the user should have configured the ISDN ports as TE (Terminal Equipment) ISDN.

Under this subnode, set and add commands can be used:

```
ATOSNT\interfaces\isdn-bri1-ppp0>>set ?

Available nodes:
                      ip
                      service-dialer
                      service-ppp

Set command parameters:
 level of log                     [loglevel]                   Current value: 1
 description                      [description]                Current value:
 enable                           [on|off]                     Current value: on
 opening mode                     [open-mode]                  Current value: on-demand
 mean rate window (sec)           [mean-rate-window]           Current value: 0
 inactivity time (sec)            [inactivitytime]             Current value: 60
 active traffic classifier        [active-traffic]             Current value:
 network group                    [network-group]              Current value:
 network group disable time (sec) [network-group-disable-time] Current value: 0
 connectivity monitor probe       [conn-mon-probe]             Current value:
```

```
 probe fault action                [probe-fault-action]          Current value: none
```

```
ATOSNT\interfaces\isdn-bri1-ppp0>>add ?

Available nodes:
                        service-dialer

ATOSNT\interfaces\isdn-bri1-ppp0>>add service-dialer ?

add  help :  Add an ISDN called number
add  usage:
 [NUMBER>[called-number>[called-subaddress]

add command parameters:
 NUMBER

ATOSNT\interfaces\isdn-bri1-ppp0>>add service-dialer NUMBER ?
add command parameters:
 Called number          [1-20 decimal digits may be preceded by +]

ATOSNT\interfaces\isdn-bri1-ppp0>>add service-dialer NUMBER +390712506541
```

Table 37: add NUMBER

Syntax	Description
NUMBER	Keyword
called-number [1-20 decimal digits may be preceded by +]	Set Called party number information element to identify the called party of a call.
called-subaddress	Set Called party subaddress information element to identify the subaddress of the called party of the call.

Configuration Examples

ETHx configuration example

Here an example about how to create a new 802.3 ETH subinterface setting IP address 192.168.1.1 and mask 255.255.255.0

add interfaces ifC eth0 192.168.1.1/24

The result is the following:

ATOSNT>>show interfaces eth0 conf

Show of ATOSNT interfaces eth0

Level of log: 1

Description:

Enable: on

Encapsulation: 802.3

Show of ATOSNT interfaces eth0 ip

Level of log: 1

IP address: 192.168.1.1

Netmask: 255.255.255.0

Default router: 0.0.0.0

MTU value: 1500

DHCP client: off

TCP MSS adjustment: path-mtu

Tx queue len: 1000

Another 802.3 ETH subinterface is created with IP address 192.168.4.1/24

add interfaces ifC eth0 192.168.4.1/24

ATOSNT\interfaces>>tree

interfaces loopback0 ip

eth0 ip

eth0:0 ip

ATOSNT>>show interfaces eth0:0 conf

Show of ATOSNT interfaces eth0

Level of log: 1

Description:

Enable: on

Encapsulation: 802.3

Show of ATOSNT interfaces eth0:0 ip

Level of log: 1

IP address: 192.168.4.1

Netmask: 255.255.255.0

Default router: 0.0.0.0

MTU value: 1500

DHCP client: off

TCP MSS adjustment: path-mtu

Tx queue len: 1000

VLAN configuration example on ETH0 interface

Here an example to create a new 802.3QP VLAN subinterface, setting IP address 192.168.6.1, mask 255.255.255.0, VLAN id 100

add interfaces ifC eth0 192.168.6.1 802.1QP 100

ATOSNT\interfaces>>tree

interfaces loopback0 ip

eth0 ip

eth0.100 ip

service-8021q

The result is the following:

ATOSNT>>show interfaces eth0.100 conf

Show of ATOSNT interfaces eth0.100

Level of log: 1

Description:

Enable: on

Encapsulation: 802.1QP

Show of ATOSNT interfaces eth0.100 ip

Level of log: 1

IP address: 192.168.6.1

Netmask: 255.255.255.0

Default router: 0.0.0.0

MTU value: 1500

DHCP client: off

TCP MSS adjustment: path-mtu

Tx queue len: 256

Show of ATOSNT interfaces eth0.100 service-8021q

VID: 100

Default priority: 0

VCCx configuration example – IPoA encapsulation

Here an example to create a new VCC subinterface in IpoA encapsulation mode, setting IP address 1.2.3.4, netmask 255.255.255.248 named “dati”, over VCC0 channel

add interfaces ifC vcc0 1.2.3.4/29 ip dati

The result is the following:

ATOSNT>>show interfaces dati conf
Show of ATOSNT interfaces dati
Level of log: 1
Description:
Enable: on
Encapsulation: IP
Show of ATOSNT interfaces dati ip
Level of log: 1
IP address: 1.2.3.4
Netmask: 255.255.255.248
Remote IP address: 0.0.0.0
MTU value: 1500
Show of ATOSNT interfaces dati service-atm
Encapsulation LLC-SNAP: on
CRC preserved: off

VCCx configuration example – IPoE encapsulation, fix IP address

Here an example to create a new VCC subinterface in IPoE encapsulation mode, setting IP address 4.3.2.1, netmask 255.255.255.252 named "dati_IPoE over VCC2 channel"

add interfaces ifC vcc2 4.3.2.1/30 802.3 dati_IpoE

set interfaces dati_ipoe ip defaultrouter 4.3.2.2

The result is the following:

ATOSNT>>show interfaces dati_ipoe conf
Show of ATOSNT interfaces dati_ipoe
Level of log: 1
Description:
Enable: on
Encapsulation: 802.3
Show of ATOSNT interfaces dati_ipoe ip
Level of log: 1
IP address: 4.3.2.1
Netmask: 255.255.255.252
Default router: 4.3.2.2
MTU value: 1500
DHCP client: off
TCP MSS adjustment: path-mtu
Tx queue len: 256
Show of ATOSNT interfaces dati_ipoe service-atm
Encapsulation LLC-SNAP: on
CRC preserved: off

VCCx configuration example – IPoE encapsulation, dynamic IP address

Here an example to create a new VCC subinterface in IPoE encapsulation, using “dhcp client” mode to receive dynamic IP address, named “dati_dhcpclient”over VCC1 channel

add interfaces ifC vcc1 dati_dhcpclient

The result is the following:

ATOSNT>>show interfaces dati_ipoe conf

Show of ATOSNT interfaces dati_ipoe

Level of log: 1

Description:

Enable: on

Encapsulation: 802.3

Show of ATOSNT interfaces dati_ipoe ip

Level of log: 1

IP address: 4.3.2.1

Netmask: 255.255.255.252

Default router: 4.3.2.2

MTU value: 1500

DHCP client: off

TCP MSS adjustment: path-mtu

Tx queue len: 256

Show of ATOSNT interfaces dati_ipoe service-atm

Encapsulation LLC-SNAP: on

CRC preserved: off

PPTP VPN configuration example

ATOSNT\interfaces\vpn-ppp0>>**show conf**

Show of ATOSNT interfaces vpn-ppp0

Level of log : 1

Description :

Enable : on

Opening mode : on-demand

Mean rate window (sec) : 0

Inactivity time (sec) : 60

Active traffic classifier :

Network group :

Network group disable time (sec) : 0

Connectivity monitor probe :

Probe fault action : none

Encapsulation : PPTP

Show of ATOSNT interfaces vpn-ppp0 ip

Level of log : 1

IP address : 0.0.0.0

Netmask : 0.0.0.0

Remote IP address : 0.0.0.0

MTU value : 1500

TCP MSS adjustment : path-mtu

Tx queue len : 256

Show of ATOSNT interfaces vpn-ppp0 service-vpn

Remote peer :

PPTP echo request timeout (sec) : 60

PPTP echo reply timeout (sec) : 60

Show of ATOSNT interfaces vpn-ppp0 service-ppp

Level of log : 1

PPP Profile :

IP-in-IP VPN configuration example

ATOSNT\interfaces\vpn0>>**show conf**

Show of ATOSNT interfaces vpn0
Level of log : 1
Description :
Enable : on
Mean rate window (sec) : 0
Network group :
Network group disable time (sec) : 0
Connectivity monitor probe :
Probe fault action : none
Encapsulation : IP-in-IP
Show of ATOSNT interfaces vpn0 ip
Level of log : 1
IP address : 0.0.0.0
Netmask : 0.0.0.0
Remote IP address : 0.0.0.0
MTU value : 1400
TCP MSS adjustment : path-mtu
Tx queue len : 1000
Show of ATOSNT interfaces vpn0 service-vpn
Remote IP address : 0.0.0.0
Local address or ifc name : 0.0.0.0

GRE VPN configuration example

ATOSNT\interfaces\vpn-gre0>>**show conf**

Show of ATOSNT interfaces vpn-gre0

Level of log : 1

Description :

Enable : on

Mean rate window (sec) : 0

Network group :

Network group disable time (sec) : 0

Connectivity monitor probe :

Probe fault action : none

Encapsulation : GRE

Show of ATOSNT interfaces vpn-gre0 ip

Level of log : 1

IP address : 0.0.0.0

Netmask : 0.0.0.0

Remote IP address : 0.0.0.0

MTU value : 1400

TCP MSS adjustment : path-mtu

Tx queue len : 1000

Show of ATOSNT interfaces vpn-gre0 service-vpn

Remote IP address : 0.0.0.0

Local address or ifc name : 0.0.0.0

TUN OpenVPN configuration example using a certificate profile defined in "certificate" node

ATOSNT\interfaces\tun10>>**show conf**

Show of ATOSNT interfaces tun10

Level of log : 1

Description :

Enable : on

Opening mode : always-on

Mean rate window (sec) : 0

Network group :

Network group disable time (sec) : 0

Connectivity monitor probe :

Probe fault action : none

Encapsulation : IP

Show of ATOSNT interfaces tun10 ip

Level of log : 1

IP address : 0.0.0.0

Netmask : 0.0.0.0

Remote IP address : 0.0.0.0

MTU value : 1400

TCP MSS adjustment : path-mtu

Tx queue len : 1000

Show of ATOSNT interfaces tun10 ipv6

Level of log : 1

Enable : off

Hop limit : 64

Autoconfiguration : disabled

LIST OF NETWORKS

Empty list

LIST OF PREFIX DELEGATIONS

Empty list

Show of ATOSNT interfaces tun10 ipv6 slaac

Default router : off

Default route preference : on

Show of ATOSNT interfaces tun10 ipv6 dhcp

Request ia for non-temporary address : on

Request ia for prefix delegation : off

Rapid commit : off

Show of ATOSNT interfaces tun10 ipv6 nd

Level of log : 1

Neighbour solicitation interval (msec) : 1000

Neighbour reachable time (msec) : 30000

Neighbour solicitation max number : 3

DAD attempts : 1

Show of ATOSNT interfaces tun10 ipv6 nd ra

sending of router advertisements : on

max ra interval (sec) : 600

min ra interval (sec) : 200

managed address configuration : off

other configuration : off

default router preference : medium

default router lifetime (sec) : 1800

Hop limit : unspecified

Reachable time : unspecified

Retrans time : unspecified

link MTU : unspecified

LIST OF PREFIXES

Empty list

Show of ATOSNT interfaces tun10 service-vpn

Level of log : 1

Protocol : udp

Server :

Local address or ifc name : none

Protocol port : 1194

Address from server : off

Certificate profile name : profile0

Cipher algorithm : BF_CBC

keep alive timeout : 10

keep alive not reply timeout : 30

Command executed

TAP OpenVPN configuration example using a certificate profile defined in "certificate" node

ATOSNT\interfaces\tap10>>**show conf**

ATOSNT\interfaces\tap10>>show conf

Show of ATOSNT interfaces tap10

Level of log : 1

Description :

Enable : on

Opening mode : always-on

Mean rate window (sec) : 0

Network group :

Network group disable time (sec) : 0

Connectivity monitor probe :

Probe fault action : none

Use basic MAC address : false

Mirror to :

Encapsulation : 802.3

Show of ATOSNT interfaces tap10 ip

Level of log : 1

IP address : 0.0.0.0

Netmask : 0.0.0.0

Default router : 0.0.0.0

MTU value : 1400

Auto provisioning : off

TCP MSS adjustment : path-mtu

Tx queue len : 1000

Show of ATOSNT interfaces tap10 ipv6

Level of log : 1

Enable : off

Hop limit : 64

Autoconfiguration : disabled

LIST OF NETWORKS Empty list

LIST OF PREFIX DELEGATIONS Empty list

Show of ATOSNT interfaces tap10 ipv6 slaac

Default router : off

Default route preference : on

Show of ATOSNT interfaces tap10 ipv6 dhcp

Request ia for non-temporary address : on

Request ia for prefix delegation : off

Rapid commit : off

Show of ATOSNT interfaces tap10 ipv6 nd

Level of log : 1

Neighbour solicitation interval (msec) : 1000

Neighbour reachable time (msec) : 30000

Neighbour solicitation max number : 3

DAD attempts : 1

Show of ATOSNT interfaces tap10 ipv6 nd ra

sending of router advertisements : on

max ra interval (sec) : 600

min ra interval (sec) : 200

managed address configuration : off

other configuration : off

default router preference : medium

default router lifetime (sec) : 1800

Hop limit : unspecified

Reachable time : unspecified

Retrans time : unspecified

link MTU : unspecified

LIST OF PREFIXES

Empty list

Show of ATOSNT interfaces tap10 service-vpn

Level of log : 1

Protocol : udp

Server :

Local address or ifc name : none

Protocol port : 1194

Address from server : off

Certificate profile name : profile0

Cipher algorithm : BF_CBC

keep alive timeout : 10

keep alive not reply timeout : 30

Show of ATOSNT interfaces tap10 service-8023

Tag insertion : off

Default VID : 1

Default priority : 0

Priority translation : off

Tag removal : off

Use ingress priority : false

LIST OF TOS TO PRIORITY

Empty list

LIST OF POLICY MARKER TO PRIORITY

Empty list

Command executed

Service-Vpn for PPTP Server configuration example

The example shows to the user how to configure a Router or CPE located at the Headquarters, to work in server mode and to provide vpn services to the mobile clients outside the organization, through a public network (i.e Internet) establishing secure VPNs tunnels communications.

- **AAA node**

1. Start defining a profile "Staff" in AAA node.
2. Define a RAC-ACCOUNT named "Members" with user id "mobile" and password "123" for the vpn clients.
3. Set a RAC-ADDRESS with a pool of addresses named pool-rac-server
4. Set the association between "Staff" profile and "Member" RAC-ACCOUNT.

Use "conf" and "show work" commands to see how to configure the parameters and the result.

ATOSNT\aaa>>**conf**

add aaa PROFILE Staff

add aaa RAC-ACCOUNT Members mobile 1234 any

add aaa RAC-ADDRESS pool-rac-server 1.1.1.2 1.1.1.10

set aaa staff account-group members

ATOSNT\aaa>>**show work**

Show of ATOSNT aaa

Level of log : 1

Local IP Address : 0.0.0.0

LIST OF RAC-ACCOUNTS

GROUP	USERNAME	PASSWORD
Members	mobile	1234

LIST OF RAC-ADDRESS

NAME	START ADDRESS	END ADDRESS
pool-rac-server	1.1.1.2	1.1.1.10

Show of ATOSNT aaa staff

Account name : members

NAS identifier :

AAA Server timeout (sec) : 5

AAA Server retries : 4

AAA Authorization : off

AAA Accounting : off

Command executed

- **Point-to-Point node**

Mobile users will reach the CPE at the HQ using PPP links with username and password defined in "Staff" profile under "aaa" node.

1. Set a PPP profile named ppp0
2. In ppp0 node, switch from ppp-client to ppp-server mode
3. Set on ccp and in mppe node, set on key 40 and key 128 (encryption keys for secure communications)
4. In server node, enables aaa-profile "Staff" and as pool address name, "pool-rac-server" just defined in aaa node RAC-ADDRESS
5. Set dns1, dns2, wins1 and wins2 server parameters

These are the commands.

ATOSNT\point-to-point\ppp0\server>>**conf**

add point-to-point PROFILE PPP ppp0

set point-to-point ppp0 type ppp-server

set point-to-point ppp0 ccp mppe key40 on

set point-to-point ppp0 ccp mppe key128 on

set point-to-point ppp0 server aaa-profile Staff

set point-to-point ppp0 server pool-name pool-rac-server

set point-to-point ppp0 server primary-dns 8.8.8.8

set point-to-point ppp0 server secondary-dns 8.8.4.4

set point-to-point ppp0 server primary-wins 192.168.110.8

set point-to-point ppp0 server secondary-wins 192.168.29.1

ATOSNT\point-to-point\ppp0\server>>**show work**

Show of ATOSNT point-to-point ppp0 server

AAA profile name : Staff

Address pool name : pool-rac-server

Primary DNS : 8.8.8.8

Secondary DNS : 8.8.4.4

Primary WINS : 192.168.110.8

Secondary WINS : 192.168.29.1

Command executed

- **Interfaces node**

1. Add a pptp-server interface named pptp-server0 and eth1 interface, such as the physical interface to provide the requested vpn services by the mobile clients
2. Assign to the pptp-server0 interface an IP address belonging to the same subnet than the pool of addresses of pool-rac-server, in this case 1.1.1.1/24
3. Associate to the pptp-server0 interface, the vpn service and eth1
4. Associate to the pptp-server0 interface, PPP services to be provided to the mobile clients with PPP profile defined in ppp0, the subnode of "Point-to-Point" node
5. Enable dhcp client and napt on eth1 interface

These are the commands.

ATOSNT\interfaces>>**conf**

add interfaces IFC pptp-server pptp-server0

add interfaces IFC eth1 eth1

set interfaces pptp-server0 ip address 1.1.1.1/24

set interfaces pptp-server0 service-vpn local-address-or-ifc-name eth1

set interfaces pptp-server0 service-ppp ppp-profile ppp0

set interfaces eth1 ip dhcp-client on

add napt IFC eth1

set napt eth1 on

add ip route 0.0.0.0 0.0.0.0 192.168.1.1 1

ATOSNT\interfaces>>**show work**

Show of ATOSNT interfaces

Level of log : 1

Show of ATOSNT interfaces pptp-server0

Level of log : 1

Description :

Enable : off

Network group :

Network group disable time (sec) : 0

Encapsulation : PPTP-SERVER

Show of ATOSNT interfaces pptp-server0 ip

more...[y][n]? y

Level of log : 1

IP address : 0.0.0.0

Netmask : 0.0.0.0

MTU value : 1400

Show of ATOSNT interfaces pptp-server0 service-vpn

Local address or ifc name : eth1

Show of ATOSNT interfaces pptp-server0 service-ppp

Level of log : 1

PPP Profile : ppp0

Show of ATOSNT interfaces eth1

Level of log : 1

Description :

Enable : on

Mean rate window (sec) : 0

Network group :

Network group disable time (sec) : 0

Connectivity monitor probe :

Probe fault action : none

Use basic MAC address : false

Mirror to :

Encapsulation : 802.3

Show of ATOSNT interfaces eth1 ip

Level of log : 1

IP address : 0.0.0.0

Netmask : 0.0.0.0

Default router : 0.0.0.0

more...[y][n]? y

MTU value : 1500

DHCP client : off

Unnumbered from :

TCP MSS adjustment : path-mtu

Tx queue len : 1000

Show of ATOSNT interfaces eth1 service-8023

Tag insertion : off

Default VID : 1

Default priority : 0

Priority translation : off

Tag removal : off

Use ingress priority : false

LIST OF TOS TO PRIORITY

Empty list

LIST OF POLICY MARKER TO PRIORITY

Empty list

Command executed

DLCIx configuration example - IPoFR encapsulation

ATOSNT\interfaces>>**show dati conf**

Show of ATOSNT interfaces dati

Level of log : 1

Description :

Enable : on

Mean rate window (sec) : 0

Network group:

Network group disable time (sec): 0

Connectivity monitor probe :

Probe fault action : none

Encapsulation : IP

Show of ATOSNT interfaces dati ip

Level of log : 1

IP address : 1.2.3.4

Netmask : 255.255.255.0

Remote IP address : 0.0.0.0

MTU value: 1500

DHCP client: off

TCP MSS adjustment: path-mtu

Tx queue len: 1000

DLCIx configuration example – IPoE encapsulation, fix IP address

ATOSNT\interfaces>>**show dati_ipoE conf**

Show of ATOSNT interfaces dati_ipoe

Level of log : 1

Description :

Enable : on

Mean rate window (sec) : 0

Network group :

Network group disable time (sec) : 0

Connectivity monitor probe :

Probe fault action : none

Use basic MAC address : false

Encapsulation : 802.3

Show of ATOSNT interfaces dati_ipoe ip

Level of log : 1

IP address : 1.2.3.4

Netmask : 255.255.255.0

Default router : 1.2.3.5

MTU value : 1500

DHCP client : off

TCP MSS adjustment : path-mtu

Tx queue len : 1000

Show of ATOSNT interfaces dati_ipoe service-8023

Tag insertion : off

Default VID : 1

Default priority : 0

Priority translation : off

Tag removal : off

Use ingress priority : false

LIST OF TOS TO PRIORITY

Empty list

LIST OF POLICY MARKER TO PRIORITY

Empty list

DLCIx - PPPy configuration example – PPPoFR encapsulation

ATOSNT\interfaces>>**show dati conf**

Show of ATOSNT interfaces dati

Level of log : 1

Description :

Enable : on

Opening mode : always-on

Mean rate window (sec) : 0

Inactivity time (sec) : 0

Active traffic classifier :

Network group :

Network group disable time (sec) : 0

Connectivity monitor probe :

Probe fault action : none

Encapsulation : PPP

Show of ATOSNT interfaces dati ip

Level of log : 1

IP address : 0.0.0.0

Netmask : 0.0.0.0

Remote IP address : 0.0.0.0

MTU value : 1496

TCP MSS adjustment : path-mtu

Tx queue len : 256

Show of ATOSNT interfaces dati service-ppp

Level of log : 1

PPP Profile : ppp0

Ml-ppp0 configuration example at 128 kb/s with ISDN BR1 port

In this example a Multilink PPP interface has been created allocating B1 and B2 channels of the ISDN BRI1 access in a single link with a total throughput of 128 kb/s

ATOSNT\interfaces\ml-ppp0>>**show work**

Show of ATOSNT interfaces ml-ppp0

Level of log : 1

Description :

Enable : on

Opening mode : on-demand

Inactivity time (sec) : 60

Active traffic classifier :

Network group :

Network group disable time (sec) : 0

Encapsulation : PPP

LIST OF LINKS

INTERFACE PRIORITY

isdn-bri1-ppp0 0

isdn-bri1-ppp1 0

Show of ATOSNT interfaces ml-ppp0 ip

Level of log : 1

IP address : 10.64.64.76

Netmask : 255.255.255.255

Remote IP address : 10.112.112.124

MTU value : 1500

TCP MSS adjustment : path-mtu

Tx queue len : 3

Show of ATOSNT interfaces ml-ppp0 bod

Level of log : 1

Enable : off

Add link time (sec) : 20

Add link threshold (%) : 80

Drop link time (sec) : 40

Drop link threshold (%) : 70

Show of ATOSNT interfaces ml-ppp0 service-ppp

Level of log : 1

PPP Profile : ppp0

MLPPP Profile : mlppp0

ATOSNT\interfaces**isdn-bri1-ppp0**>>show work

Show of ATOSNT interfaces isdn-bri1-ppp0

Level of log : 1

Description :

Enable : on

Opening mode : on-demand

Mean rate window (sec) : 0

Inactivity time (sec) : 60

Active traffic classifier :

Network group :

Network group disable time (sec) : 0

Connectivity monitor probe :

Probe fault action : none

Encapsulation : PPP

Show of ATOSNT interfaces isdn-bri1-ppp0 ip

Level of log : 1

IP address : 0.0.0.0

Netmask : 0.0.0.0

Remote IP address : 0.0.0.0

MTU value : 1500

TCP MSS adjustment : path-mtu

Tx queue len : 256

Show of ATOSNT interfaces isdn-bri1-ppp0 service-dialer

Level of log : 1

Incoming call : disable

LIST OF CALLED NUMBERS

+39071250681

Show of ATOSNT interfaces isdn-bri1-ppp0 service-ppp

Level of log : 1

PPP Profile : ppp0

ATOSNT\interfaces**isdn-bri1-ppp1**>>show work

Show of ATOSNT interfaces isdn-bri1-ppp1

Level of log : 1

Description :

Enable : on

Opening mode : on-demand

Mean rate window (sec) : 0

Inactivity time (sec) : 60

Active traffic classifier :

Network group :

Network group disable time (sec) : 0

Connectivity monitor probe :

Probe fault action : none

Encapsulation : PPP

Show of ATOSNT interfaces isdn-bri1-ppp1 ip

Level of log : 1

IP address : 0.0.0.0

Netmask : 0.0.0.0

Remote IP address : 0.0.0.0

MTU value : 1500

TCP MSS adjustment : path-mtu

Tx queue len : 256

Show of ATOSNT interfaces isdn-bri1-ppp1 service-dialer

Level of log : 1

Incoming call : disable

LIST OF CALLED NUMBERS

+39071250681

Show of ATOSNT interfaces isdn-bri1-ppp1 service-ppp

Level of log : 1

PPP Profile : ppp1

Interfaces Status

Here un example of status for some configured interfaces:

ATOSNT>>**show interfaces status -s**

status of loopback0 interface

state: opened

status of ip on loopback0 interface

state: opened

mtu: 1500

tx queue len: 0

local address: 127.0.0.1

netmask: 255.255.255.255

status of eth0 interface

state: operational/not running

hierarchy: eth0 on phy ifc eth0

status of ip on eth0 interface

state: closed

status of w3g0-ppp0 interface

state: operational/not running

hierarchy: w3g0-ppp0 on phy ifc w3g0

status of ip on w3g0-ppp0 interface

state: closed

status of wlan0 interface

state: opened

hierarchy: wlan0 on phy ifc wlan0

status of ip on wlan0 interface

state: opened

mtu: 1500

tx queue len: 1000

local address: 192.168.2.1

netmask: 255.255.255.0

mac address: 00:60:B3:3A:85:D8

status of vcc0 interface

state: operational/running/ip address not assigned

hierarchy: vcc0 on phy ifc vcc0

status of ip on vcc0 interface

state: closed

status of vcc0-ppp0 interface

state: opened

hierarchy: vcc0-ppp0<-->vcc0 on phy ifc vcc0

status of ip on vcc0-ppp0 interface

state: opened

mtu: 1492

tx queue len: 3

local address: 79.23.70.27

netmask: 255.255.255.255

remote address: 192.168.100.1

dns1: 85.37.17.57

dns2: 85.38.28.80

mac address: 12:D0:D6:08:AA:FF

DLCIx - IP over Frame Relay encapsulation

ATOSNT>>**show interfaces status -s**

status of dlci0 interface

state: opened

hierarchy: dlci0 on phy ifc dlci0

mac address: 00:66:30:33:2F:C8

status of ip on dlci0 interface

state: opened

mtu: 1500

tx queue len: 1000

local address: 1.2.3.4

netmask: 255.255.255.0

remote address: 1.2.3.4

DLCIx - PPP over Frame Relay encapsulation

status of dlci2-ppp0 interface

state: opened

hierarchy: dlci2-ppp0<-->dlci2 on phy ifc dlci2

status of ip on dlci2-ppp0 interface

state: opened

mtu: 1496

tx queue len: 256

local address: 2.2.2.2

netmask: 255.255.255.255

remote address: 192.168.80.1

dns1: 192.168.29.1

IP-in-IP VPN

status of vpn0 interface

state: opened

mac address: 00:00:00:00:2f:78

status of ip on vpn0 interface

state: opened

mtu: 1400

tx queue len: 1000

local address: 10.10.10.1

netmask: 255.255.255.0

remote address: 10.10.10.1

GRE VPN

status of vpn-gre0 interface

state: opened

mac address: 00:00:00:00:31:90

status of ip on vpn-gre0 interface

state: opened

mtu: 1476

local address: 20.20.20.1

netmask: 255.255.255.0

remote address: 20.20.20.1

PPTP VPN

status of vpn-ppp0 interface

state: opened

status of ip on vpn-ppp0 interface

state: opened

mtu: 1496

tx queue len: 256

local address: 30.30.30.2

netmask: 255.255.255.255

remote address: 30.30.30.1

PPTP-Server VPN

status of pptp-server0 interface

state: opened

there is a client associated

status of ip on pptp-server0 interface

state: opened

mtu: 1400

local address: 30.30.30.1

netmask: 255.255.255.0

associated clients list

device ppp0 opened from 192.168.31.140

client address: 30.30.30.2

server address: 30.30.30.1

username: cayman

Multilink PPP with ISDN BR1 port

ATOSNT\interfaces\ml-ppp0>>show status

status of ml-ppp0 interface state: opened status of links:

- isdn-bri1-ppp0 link added
- isdn-bri1-ppp1 link added

hierarchy: ml-ppp0 on phy ifc ml

Interfaces Statistics

ATOSNT>>**show interfaces statistics -s**

statistics of loopback0 interface

******* upstream direction *******

packets: 140606

bytes: 10144343

errors: 0

dropped: 0

overruns: 0

requeues: 0

queue full: 0

****** downstream direction ******

packets: 140606

bytes: 10144343

multicast: 0

errors: 0

dropped: 0

overruns: 0

statistics of eth0 interface

******* upstream direction *******

packets: 0

bytes: 0

errors: 0

dropped: 0

overruns: 0

requeues: 0

queue full: 0

****** downstream direction ******

packets: 0

bytes: 0

multicast: 0

errors: 0

dropped: 0

overruns: 0

statistics of w3g0-ppp0 interface

nothing to show

statistics of wlan0 interface

******* upstream direction *******

packets: 616087

bytes: 112503143

errors: 0

dropped: 16

overruns: 0

requeues: 0

queue full: 0

****** downstream direction ******

packets: 705267

bytes: 38142279

multicast: 0

errors: 0

dropped: 0

overruns: 0

statistics of vcc0 interface

******* upstream direction *******

packets: 630135

bytes: 53998629

errors: 0

dropped: 0

overruns: 0

requeues: 0

queue full: 0

****** downstream direction ******

packets: 639530

bytes: 110545692

multicast: 0

errors: 0

dropped: 0

overruns: 0

statistics of vcc0-ppp0 interface

******* upstream direction *******

packets: 617017

bytes: 28648809

errors: 0

dropped: 0

overruns: 0

requeues: 0

queue full: 293

****** downstream direction ******

packets: 626412

bytes: 104930773

multicast: 0

errors: 0

dropped: 0

overruns: 0

DLCIx - IP over Frame Relay

statistics of dlci0 interface

******* upstream direction *******

packets: 48

bytes: 5736

errors: 0

dropped: 0

overruns: 0

requeues: 0

queue full: 0

****** downstream direction ******

packets: 4

bytes: 240

multicast: 0

errors: 0

dropped: 0

overruns: 0

DLCIx - PPP over Frame Relay

statistics of dlci2-ppp0 interface

******* upstream direction *******

packets: 4

bytes: 70

errors: 0

dropped: 0

overruns: 0

requeues: 0

queue full: 0

****** downstream direction ******

packets: 4

bytes: 52

multicast: 0

errors: 0

dropped: 0

overruns: 0

IP-in-IP VPN

statistics of vpn0 interface

********* upstream direction *******

packets: 6

bytes: 480

errors: 0

dropped: 0

overruns: 0

requeues: 0

queue full: 0

********* downstream direction *******

packets: 6

bytes: 360

multicast: 0

errors: 0

dropped: 0

overruns: 0

GRE VPN

statistics of vpn-gre0 interface

********* upstream direction *******

packets: 9

bytes: 756

errors: 0

dropped: 0

overruns: 0

requeues: 0

queue full: 0

********* downstream direction *******

packets: 9

bytes: 540

multicast: 0

errors: 0

dropped: 0

overruns: 0

PPTP VPN

statistics of vpn-ppp0 interface

******* upstream direction *******

packets: 8

bytes: 116

errors: 0

dropped: 0

overruns: 0

requeues: 0

queue full: 0

****** downstream direction ******

packets: 8

bytes: 98

multicast: 0

errors: 0

dropped: 0

overruns: 0

PPTP Server VPN

statistics of pptp-server0 interface

******* upstream direction *******

packets: 8

bytes: 98

errors: 0

dropped: 0

overruns: 0

requeues: 0

queue full: 0

****** downstream direction ******

packets: 8

bytes: 116

multicast: 0

errors: 0

dropped: 0

overruns: 0

statistics of ppp0 client device

******* upstream direction *******

packets: 8

bytes: 98

errors: 0

dropped: 0

overruns: 0

requeues: 0

queue full: 0

****** downstream direction ******

packets: 8

bytes: 116

multicast: 0

errors: 0

dropped: 0

overruns: 0

Index

ManIp

IP

The main function of the routers is to indicate to the IP packets proceeding from the different interfaces (LAN, WAN), the route to follow to the final destination. This is achieved based on the information contained in the routing tables, on the information received from the other routers connected over the WAN or LAN network, and also on the information provided by the network administrator with a specific configuration.

ATOSNT uses:

- **advanced routes**

  entries of the routing table, based on complex rules (policy routing) that may have or not priority over traditional routes, as local or static ones, based on a configuration parameter;

- **static routes**

  to reach a network which is different from the network directly connected or from the ones announced by the routing protocols (e.g. RIP) over the WAN, manually configured inside ATOSNT;

- **RIP, OSPF, BGP**

  to share the contents of the routing table to the other routers and update the routing table with the contents of the received RIP,OSPF,BGP packets.

- **IGMP**

  for multicast routing information.

Routing information carried by routing protocols can be filtered configuring distribution lists.

IP - Commands

```
ATOSNT\ip>>set ?

Available nodes:
                        classifier
                        network-groups
                        route
                        routemap
                        rip
                        ospf
                        bgp
                        multicast

Set command parameters:
 level of log  [loglevel]     Current value: 1
 subnet-zero   [Subnet-zero]  Current value: off
```

Table 1: set

Syntax	Description
subnet-zero	Enabling this command subnet zero can be used on interfaces and on routing updates. If subnet zero parameter is off each network that ends with “0” is allowed only if it has a “natural” netmask (/24, /16 e /8), e.g. network 134.180.1.0/30 is not allowed while network 134.180.1.4/30 is allowed.
loglevel <value>	Set the detail level used by ATOSNT to log the routing events.

IP – Nodes

```
ATOSNT\ip>>?

Available nodes:
                        classifier
                        network-groups
                        route
                        routemap
                        rip
                        ospf
                        bgp
                        multicast
```

Classifier – Node

In this node a packet classifier can be defined in two ways: either incapsulating a classifier map defined in “classifier-map” node or defining a single rule.

Typical, but not exclusive, use of these objects is to define advanced route entries in ip\route node.

Notice that if Classifiers are used for advanced routing of router generated traffic (like SIP or other internal services), the Classifiers cannot be built using classifier map, in this case only Classifiers constructed by single rules can be used.

```
ATOSNT\ip\classifier>>add ?

add  help :  Add a new classifier for policy routing or forwarding
add  usage:
 <IP-CLASS><name><CLASSMAP><classifier-map-name>
 <IP-CLASS><name><RULE><from-address/mask><to-address/mask><tos-value>[<ifc-name>]

add command parameters:
 IP-CLASS
```

```
ATOSNT\ip\classifier>>del ?

del  help :  Delete a classifier for policy routing or forwarding
del  usage:
 <IP-CLASS><name>

del command parameters:
```

```
IP-CLASS
```

Table 2: add

Syntax	Description
<IP_CLASS>	Keyword: IP Classifier
<name> [max 16 char]	Name of the classifier to create in this node.
<CLASSMAP>	Keyword: a classifier map will follow
<classifier-map-name>	One of the classifier maps defined in “classifier-map” node. The classifier “name” will use all rules defined in classifier map to classify traffic.
<RULE>	Keyword: rule for the classifier “name” created in this node will follow.
<from-address/mask>	Source-address/mask-length
<to-address/mask>	Destination-address/mask-length
<tos-value> [maximize-reliability | maximize-throughput | minimize-delay | mt+mr | md+mr | md+mt | md+mt+mr | any-tos]	Selected value of TOS.
<ifc-name> optional [local-traffic|eth0…]	Source interface (where packets come from). Only proposed values can be selected.

Table 3: del

Syntax	Description
<IP_CLASS>	Keyword: IP Classifier
<name> [max 16 char]	Name of the classifier to be deleted.

Example of adding a classifier using a classifier map:

ATOSNT\ip\classifier>>add ip-CLASS Voip_IP_class cLASSMAP voip_class_map

Command executed

Example of adding a classifier using single rule:

ATOSNT\ip\classifier>>add ip-CLASS rule_ip_class rULE 10.0.0.5/32 any any-tos

Command executed

Example of resulting configuration:

ATOSNT\ip\classifier>>show conf

Show of ATOSNT ip classifier

LIST OF IP CLASSIFIERS

NAME TYPE CLASSIFIER-MAP FROM ADDRESS/MASK TO ADDRESS/MASK TOS-BITS(...dtr..) SRC IFC

Voip_IP_class CLASSMAP Voip_class_map

rule_ip_class RULE 10.0.0.5/32 any maximize-reliability

Command executed

Network groups – Node

The use of network groups allows to have a kind of backup method. Configuring a static route into backup interface with administrative distance greaten then the dynamic or local route.

The mechanism of routes installation guarantee that the network group static route doesn't operate until the router can acquire either a dynamic or local route more convenient.

When the "convenient" route (dynamic or local) is loss, the network group static route is installed and data traffic can flow into backup interface.

If the "convenient" route is local, the static route into backup interface is installed only if the transport protocol or the physique layer of the primary interface is DOWN, while if the "convenient" route is acquired y dynamic routing protocol, the backup activation is performed even the primary interface is UP but the watched network is unreachable.

In the IP\Network-Group subnode the following command are available:

```
ATOSNT\ip\network-groups>>add ?

add  help :  Add a new GROUP
add  usage:
 <GROUP>[numeric_suffix_name]

add command parameters:
 GROUP
```

```
ATOSNT\ip\network-groups>>del ?

del  help :  Remove a GROUP
del  usage:
  <GROUP><name>

del command parameters:
 GROUP
```

Table 4: add/del group

Syntax	Description
GROUP	KEYWORD
numeric_suffix_name	Optonal 3 numeric digit

The example below show how to add a network-group.

ATOSNT\ip\route\network-groups>>add GROUP 1

Command executed

After the use of the “add group” command a new dynamic subnode is created where it is possible to set several parameters:

```
ATOSNT\ip\network-groups\group1>>set ?

Nodes not available.
Set command parameters:
 level of log                          [loglevel]                  Current value: 1
 route down announcement delay (sec)   [route-down-delay]          Current value: 0
 route up announcement delay (sec)     [route-up-delay]            Current value: 0
 route check initial delay (sec)       [route-check-initial-delay] Current value: 60
```

Table 5: set

Syntax	Description
Loglevel <value>	Set the detail level used by ATOS to log the events of the selected network group.
route-down-delay <value>	Announcement delay of the DOWN state for the routes of the group. Range: 0-2147493 (seconds), default: 0 (disable).
route-up-delay <value>	Announcement delay of the UP state for the routes of the group. Range: 0-2147493 (seconds), default: 0 (disable).
route-check-initial-delay <value>	Set the waiting time in the start up phase of the router, after which the check of the watched route state is performed. Range: 0-2147493 (seconds), default: 0 (disable).

To add/delete the network to watch, the following command are available:

```
ATOSNT\Ip\network-groups\group1>>add ?

 add  help :  Add a new network

add  usage:

  <NETWORK><address>[netmask|/value]
```

```
ATOSNT\Ip\network-group\group1>>del ?



del  help :  Remove network

del  usage:

  <NETWORK><address><netmask>
```

Table 6: **add / del**

Syntax	Description
Network	Keyword
Address	Add / delete an IP address into list of the group
Netmask	Set the mask of the network added. If no mask is specified a “natural” mask is used.

Examples of How to use "network groups" for Backup Services

In the following examples, you can see how "network groups" work with backup services when the outgoing principal interface (i.e. xDSL interface) does not work at all.

The first mechanism is referred to **"IP Route"**.
An static route and a default gateway interface are configured as alternative to the main interface when this fails.

Suppose the destination network to be monitorized is **192.168.40.0/24**.

Start configuring **group0** under network-group node and adding 192.168.40.0/24 as a destination network IP address

```
ATOSNT\ip\network-groups\group0>>add ?

add  help :  Add a new network
add  usage:
 <NETWORK><address>[netmask|/value]

add command parameters:
 NETWORK

ATOSNT\ip\network-groups\group0>>add NETWORK 192.168.40.0/24
Command executed

ATOSNT\ip\network-groups\group1>>show work
Show of ATOSNT ip network-groups group1
Level of log                        : 1
Route down announcement delay (sec) : 0
Route up announcement delay (sec)   : 0
Route check initial delay (sec)     : 60

LIST OF NETWORKS
192.168.40.0        255.255.255.0
```

Let's see the LIST OF ROUTES:

```
ATOSNT\ip\route>>show work
Show of ATOSNT ip route
ARP update period (sec) : off

LIST OF ROUTES
 DESTINATION         NETMASK             GATEWAY ADDR        INTERFACE      DISTANCE    TYPE
 0.0.0.0             0.0.0.0             0.0.0.0             vcc3-ppp0      1           STATIC
 10.0.0.244          255.255.255.252     192.168.29.2        bridge0        1           STATIC
 127.0.0.1           255.255.255.255     0.0.0.0             loopback0      0           LOCAL
 192.85.1.0          255.255.255.0       0.0.0.0             vlan-85        0           LOCAL
 192.167.0.0         255.255.0.0         192.168.29.2        bridge0        1           STATIC
 192.168.29.0        255.255.255.0       0.0.0.0             bridge0        0           LOCAL
 192.168.31.0        255.255.255.0       192.168.29.2        bridge0        1           STATIC
 192.168.39.0        255.255.255.0       192.168.29.2        bridge0        1           STATIC
 192.168.40.0        255.255.255.0       192.168.29.2        bridge0        1           STATIC
 192.168.43.0        255.255.255.0       192.168.29.2        bridge0        1           STATIC
 192.168.53.0        255.255.255.0       192.168.29.2        bridge0        1           STATIC
 192.168.61.0        255.255.255.0       192.168.29.2        bridge0        1           STATIC
 192.168.62.0        255.255.255.0       192.168.29.2        bridge0        1           STATIC
 192.168.79.0        255.255.255.0       192.168.29.2        bridge0        1           STATIC
 192.168.80.0        255.255.255.0       192.168.29.2        bridge0        1           STATIC
 192.168.90.0        255.255.255.0       192.168.29.2        bridge0        1           STATIC
 192.168.91.81       255.255.255.255     192.168.29.2        bridge0        1           STATIC
 192.168.100.1       255.255.255.255     0.0.0.0             vcc3-ppp0      0           LOCAL
 192.168.110.0       255.255.255.0       192.168.29.2        bridge0        1           STATIC
 192.168.111.0       255.255.255.0       192.168.29.2        bridge0        1           STATIC
 192.168.119.0       255.255.255.0       192.168.29.2        bridge0        1           STATIC

LIST OF ADVANCED ROUTES
Empty list

LIST OF ALTERNATIVE NEXT HOP
Empty list

Command executed
```

Sets the alternative static route **192.168.200.0** and associate this to the network destination 192.168.40.0 using the network-group **group0**

```
ATOSNT\ip\route>>add ?

add  help :  Add a new static route
add  usage:
 <default><gw-ip-add>[distance|group-id]
 <dest-ip-address><mask><gw-ip-address>[distance|group-id]
 <dest-ip-address><mask><ifc-name>[distance|group-id]
 <ip-classifier-name><gw-ip-add>[priority][precedence-over-main-table]
```

```
 <ip-classifier-name><ifc-name>[priority][precedence-over-main-table]

add command parameters:
 Dest ip address                    [aa.bb.cc.dd|default]
 IP Classifier name                 [Empty list]

ATOSNT\ip\route>>add 192.168.200.0 255.255.255.0 vcc3-ppp0 ?

add command parameters:
 Distance                           [1-254]
 Group name                         [group0]
 <cr>

ATOSNT\ip\route>>add 192.168.200.0 255.255.255.0 vcc3-ppp0 group0
Command executed
```

Use **show conf** command to see the list of alternative next hop.

```
ATOSNT\ip\route>>show conf
Show of ATOSNT ip route
ARP update period (sec) : off

LIST OF ROUTES
 DESTINATION         NETMASK             GATEWAY ADDR        INTERFACE      DISTANCE    TYPE
 192.168.110.0       255.255.255.0       192.168.29.2                       1           STATIC
 192.168.39.0        255.255.255.0       192.168.29.2                       1           STATIC
 192.168.40.0        255.255.255.0       192.168.29.2                       1           STATIC
 192.168.31.0        255.255.255.0       192.168.29.2                       1           STATIC
 192.168.111.0       255.255.255.0       192.168.29.2                       1           STATIC
 192.168.80.0        255.255.255.0       192.168.29.2                       1           STATIC
 192.168.53.0        255.255.255.0       192.168.29.2                       1           STATIC
 192.168.43.0        255.255.255.0       192.168.29.2                       1           STATIC
 192.167.0.0         255.255.0.0         192.168.29.2                       1           STATIC
 192.168.90.0        255.255.255.0       192.168.29.2                       1           STATIC
 0.0.0.0             0.0.0.0                                 vcc3-ppp0      1           STATIC
 192.168.61.0        255.255.255.0       192.168.29.2                       1           STATIC
 10.0.0.244          255.255.255.252     192.168.29.2                       1           STATIC
 192.168.79.0        255.255.255.0       192.168.29.2                       1           STATIC
 192.168.91.81       255.255.255.255     192.168.29.2                       1           STATIC
 192.168.62.0        255.255.255.0       192.168.29.2                       1           STATIC
 192.168.119.0       255.255.255.0       192.168.29.2                       1           STATIC

LIST OF ADVANCED ROUTES
Empty list

LIST OF ALTERNATIVE NEXT HOP
 DESTINATION         NETMASK             GATEWAY ADDR        INTERFACE      NET GROUP
 192.168.200.0       255.255.255.0       0.0.0.0             vcc3-ppp0      group0
```

```
Command executed
```

Second example is referred to the **WAN ISDN**.
In this case, when the xDSL network is not available, the backup service is provided on behalf of one of the ISDN interfaces available on the CPE, in particular the isdn bri1.

Start setting isdn bri1 as the right interface for the backup.

```
ATOSNT\interfaces>>add IFC isdn-bri1
The isdn interface will be operational after setting:
- PPP profile
- Called number
Command executed

ATOSNT\interfaces>>isdn-bri1-ppp0
ATOSNT\interfaces\isdn-bri1-ppp0>>set ?

Available nodes:
                      ip
                      service-dialer
                      service-ppp

Set command parameters:
 level of log                      [loglevel]                    Current value: 1
 description                       [description]                 Current value:
 enable                            [on|off]                      Current value: on
 opening mode                      [open-mode]                   Current value: on-demand
 mean rate window (sec)            [mean-rate-window]            Current value: 0
 inactivity time (sec)             [inactivitytime]              Current value: 60
 active traffic classifier         [active-traffic]              Current value:
 network group                     [network-group]               Current value:
 network group disable time (sec)  [network-group-disable-time]  Current value: 0
 connectivity monitor probe        [conn-mon-probe]              Current value:
 probe fault action                [probe-fault-action]          Current value: none
```

Then you should associate isdn bri1 interface to the network destination 192.168.40.0 using the network-group **group0**

```
ATOSNT\interfaces\isdn-bri1-ppp0>>set network-group ?

 network group  [<cr>|group0]

 Current value:
 Default fw value:

ATOSNT\interfaces\isdn-bri1-ppp0>>set network-group group0
Command executed
```

On demand, when the xDSL link fails, the isdn bri1 will switch the traffic to the network destination defined in group0, see below

```
ATOSNT\interfaces\isdn-bri1-ppp0>>show work
Show of ATOSNT interfaces isdn-bri1-ppp0
Level of log                     : 1
Description                      :
Enable                           : off
Opening mode                     : on-demand
Mean rate window (sec)           : 0
Inactivity time (sec)            : 60
Active traffic classifier        :
Network group                    : group0
Network group disable time (sec) : 0
Connectivity monitor probe       :
Probe fault action               : none
Encapsulation                    : PPP

Show of ATOSNT interfaces isdn-bri1-ppp0 ip
Level of log       : 1
IP address         : 0.0.0.0
Netmask            : 0.0.0.0
Remote IP address  : 0.0.0.0
MTU value          : 1500
Unnumbered from    :
TCP MSS adjustment : path-mtu
Tx queue len       : 256

Show of ATOSNT interfaces isdn-bri1-ppp0 service-dialer
Level of log  : 1
Incoming call : disable

LIST OF CALLED NUMBERS
Empty list

Show of ATOSNT interfaces isdn-bri1-ppp0 service-ppp
Level of log  : 1
PPP Profile   :

Command executed
```

Third example is referred to **VRRP**.
Network groups can be used as a trigger mechanism for the change of status of a VRRP instance. When the network group announces the status of DOWN, if our router is the MASTER, it must lower its priority to allow the election of a new master. When the network group announces the UP state, our router must restore its priority (configuration value) to allow a new master router election.

Start adding a new VRRP instance

```
ATOSNT\vrrp>>add ?

add  help :  Add a new VRRP instance
add  usage:
 <INSTANCE>[VRRP-name[id-value]]

add command parameters:
 INSTANCE
ATOSNT\vrrp>>add INSTANCE ?

add command parameters:
 VRRP Name  [max 16 char]
 <cr>

ATOSNT\vrrp>>add INSTANCE
Command executed
ATOSNT\vrrp>>tree
vrrp                    vrrp0                   authentication

ATOSNT\vrrp>>vrrp0
ATOSNT\vrrp\vrrp0>>set ?

Available nodes:
                       authentication

Set command parameters:
 enable                                [on|off]                      Current value: off
 vrrp interface                        [vrrp-interface]              Current value:
 local address or ifc name             [local-address-or-ifc-name]   Current value: 0.0.0.0
 vrid                                  [vrid]                        Current value: 1
 priority                              [priority]                    Current value: 100
 preemption                            [preemption]                  Current value: true
 startup delay until preemption (sec)  [delay-until-preemption]      Current value: 0
 handle virtual mac address            [handle-virtual-mac-address]  Current value: true
 advertisement interval (sec)          [advertisement-interval]      Current value: 1
 gratuitous arp delay (sec)            [gratuitous-arp-delay]        Current value: 5
 gateway interface                     [gateway-interface]           Current value:
 network group                         [network-group]               Current value:
 priority decrement                    [priority-decrement]          Current value: 0
```

Then you should associate VRRP instance to the network destination 192.168.40.0 using the network-group **group0**

```
ATOSNT\vrrp\vrrp0>>set network-group group0
Command executed
```

At last, use **show work** command, to check the result

```
ATOSNT\vrrp\vrrp0>>show work
Show of ATOSNT vrrp vrrp0
```

```
Enable                                : off
VRRP interface                        :
Local address or ifc name             : 0.0.0.0
VRId                                  : 1
Priority                              : 100
Preemption                            : true
Startup delay until preemption (sec) : 0
Handle virtual MAC address            : true
Advertisement interval (sec)          : 1
Gratuitous arp delay (sec)            : 5
Gateway interface                     :
Network group                         : group0
Priority decrement                    : 0

LIST OF ADDRESSES
Empty list

Show of ATOSNT vrrp vrrp0 authentication
Type     : no

Command executed
```

Route – Node

In route node it is possible to visualize all the local routes the device creates on each active interface and add static or advanced routes to forward traffic according to

- the destination network,
- an IP Classifier previously created.

In the latter case, that can be defined as ‘advanced routing’, the system uses not only destination network parameters but any parameter configurable in IP Classifier too (source network, protocol, …).

```
ATOSNT\ip\route>>set ?

Nodes not available.
Set command parameters:
 arp update period (sec)  [arp-upd-period]  Current value: 0
```

Table 7: set

Syntax	Description
arp update period (sec) [0-33554431|offlone-shot]	• **off**:disable • **one-shot**: the installation of every single route (static or advanced) depends on the successful response of the ARP command checking reachability of its gateway configured or default gateway. In case of failure related route will not be installed • **0-33554431**: the same operation as above is repeated with the schedule established by this time period and in case of failures related routes will not be installed. Default : off.

```
ATOSNT\ip\route>>add ?

add  help :  Add a new static route
add  usage:
 <default><gw-ip-add>[distance|group-id]
 <dest-ip-address><mask><gw-ip-address>[distance|group-id]
 <dest-ip-address><mask><ifc-name>[distance|group-id]
 <ip-classifier-name><gw-ip-add>[priority][precedence-over-main-table]
 <ip-classifier-name><ifc-name>[priority][precedence-over-main-table]

add command parameters:
 Dest ip address                    [aa.bb.cc.dd|default]
 IP Classifier name                 [Empty list]
```

Table 8:add

default	Default route
dest-ip-add	Ip Address value of the destination network.
mask	Subnet Mask value of the destination network.
gw-ip-add	Next-hop IP address
distance	Indicates Administrative Distance, not mandatory
classifier-name	Name of the IP Classifier analyzed as forwarding rule. The classifier-name must be previously configured on ip/classifier node.
ifc-name	Defines the outbound interface
priority	Defines the priority when you have a multiple advanced routes (policy based rule)
precedence-over-main-table	Defines the precedence in the routing table

The following command is used to delete a static route:

```
ATOSNT\ip\route>>del ?

del  help:  Delete a static route
del  usage:
 <default>[gw-ip-add]
 <dest-ip-add><mask>[gw-ip-add]
 <dest-ip-add><mask>[ifc-name]
 <ip-classifier-name>
```

```
del command parameters:
 Dest. IP addr                          [aa.bb.cc.dd|default]
 Classifier name                        [Advanced_VOIP]</pre>
```

Table 9: del

Syntax	Description
<default>	Default route
<dest-ip-add>	IP address of the final destination network.
<mask>	Subnet Mask value of the destination network you want to delete.
<classifier-name>	Ip classifier

Following examples show

- how to add a static route via WAN1 interface (second last parameter typed in) to reach the destination network, with 'AD' as 2 (last value typed in);

```
ATOSNT\ip\route>>add 172.168.0.1 255.255.255.0 vcc0 2
Command executed
```

- how to add an advanced route so that traffic defined by classifier Advanced_VOIP must be forwarded on vcc0 interface instead of follow the default static route rules.

```
ATOSNT\ip\route>>add Advanced_VOIP  vcc0 1 high
Command executed
```

IP Route - Show Status Example

ATOSNT>>show ip route status

IP ADDRESS	MASK	GATEWAY	DEVICE	METRIC	TABLE
0.0.0.0	0.0.0.0	0.0.0.0	vcc3-ppp0	1	default
192.168.100.1	255.255.255.255	0.0.0.0	vcc3-ppp0	1	main
2.229.18.238	255.255.255.255	192.168.29.2	bridge0	2	main
192.168.31.200	255.255.255.255	192.168.29.2	bridge0	1	main
2.229.18.239	255.255.255.255	192.168.29.2	bridge0	2	main
106.1.1.1	255.255.255.255	192.168.29.2	bridge0	2	main
2.2.2.0	255.255.255.252	192.168.29.2	bridge0	2	main
192.85.1.0	255.255.255.0	0.0.0.0	vlan-85	1	main
192.168.39.0	255.255.255.0	192.168.29.2	bridge0	1	main
192.168.53.0	255.255.255.0	192.168.29.2	bridge0	1	main
192.168.81.0	255.255.255.0	192.168.29.2	bridge0	2	main
192.168.51.0	255.255.255.0	192.168.29.2	bridge0	2	main
192.168.80.0	255.255.255.0	192.168.29.2	bridge0	1	main
192.168.32.0	255.255.255.0	192.168.29.2	bridge0	2	main
192.168.62.0	255.255.255.0	192.168.29.2	bridge0	2	main
192.168.31.0	255.255.255.0	192.168.29.2	bridge0	1	main
192.168.30.0	255.255.255.0	192.168.29.2	bridge0	2	main
192.168.79.0	255.255.255.0	192.168.29.2	bridge0	2	main
192.168.110.0	255.255.255.0	192.168.29.2	bridge0	1	main
192.168.29.0	255.255.255.0	0.0.0.0	bridge0	1	main
192.168.61.0	255.255.255.0	192.168.29.2	bridge0	1	main
192.168.111.0	255.255.255.0	192.168.29.2	bridge0	1	main
192.168.89.0	255.255.255.0	192.168.29.2	bridge0	2	main
192.168.42.0	255.255.255.0	192.168.29.2	bridge0	2	main
192.168.43.0	255.255.255.0	192.168.29.2	bridge0	1	main
192.168.91.0	255.255.255.0	192.168.29.2	bridge0	2	main
192.168.40.0	255.255.255.0	192.168.29.2	bridge0	1	main
192.168.90.0	255.255.255.0	192.168.29.2	bridge0	1	main
192.167.0.0	255.255.0.0	192.168.29.2	bridge0	1	main
172.16.0.0	255.255.0.0	192.168.29.2	bridge0	2	main
192.85.1.0	255.255.255.255	0.0.0.0	vlan-85	1	local
192.85.1.1	255.255.255.255	0.0.0.0	vlan-85	1	local
192.168.29.0	255.255.255.255	0.0.0.0	bridge0	1	local
192.168.29.1	255.255.255.255	0.0.0.0	bridge0	1	local
192.85.1.255	255.255.255.255	0.0.0.0	vlan-85	1	local
192.168.29.255	255.255.255.255	0.0.0.0	bridge0	1	local
87.3.64.34	255.255.255.255	0.0.0.0	vcc3-ppp0	1	local
127.0.0.1	255.255.255.255	0.0.0.0	loopback0	1	local

IP Route - Show Statistics Example

ATOSNT>>show ip route statistics

```
Route Source          Routes                FIB
connected             4                     4
static                13                    13
rip                   14                    14
------
Totals                31                    31
```

Routemap - Node

To define the conditions for filtering, attribute manipulation changing, redistributing routes from one routing protocol into another, or to enable policy routing, “routemap” node must be used to create the following “containers”:

COMMUNITY-SET - each "community" can contain a list of communities, format: <AS number>:<community number>.

CLASSIFIER – each “classifier” can contain a condition list

MAP - each “map” can contain one or more clauses, marked by sequence numbers, each of whom including one or more classifiers and one or more actions.

CLASSIFIERs and MAPs can be used in the dynamic IP protocol nodes, such as BGP, RIP, OSPF, for the purposes specified above.

```
ATOSNT\ip\routemap>>add ?

add  help :  Add a new COMMUNITY-SET profile, CLASSIFIER or MAP list/element
add  usage:
 <COMMUNITY-SET><name><community>[community..]
 <CLASSIFIER><name><cond-type><param_list>[permission][seq-num]
 <MAP><name><permission><seq-num><CLASSIFIER><name>
 <MAP><name><permission><seq-num><ACTION><action_type><action value>
 <MAP><name><permission><seq-num><PERMIT-ALL-NO-ACTION>

add command parameters:
 COMMUNITY-SET
 CLASSIFIER
 MAP
```

```
ATOSNT\ip\routemap>>del ?

del  help :  Remove COMMUNITY_SET, CLASSIFIER or MAP list/element
del  usage:
 <COMMUNITY-SET><name>
 <CLASSIFIER><name>[seq-num|MATCH_ALL]
 <MAP><name>[permission<seq-num>][<CLASSIFIER><name>]
 <MAP><name>[permission<seq-num>][<ACTION><action_type>]
 <MAP><name>[permission<seq-num>][<PERMIT-ALL-NO-ACTION>]

del command parameters:
 COMMUNITY-SET
 CLASSIFIER
 MAP
```

Creating a new COMMUNITY_SET

A Community Set is a container of community lists that can added using the following format:

Table 10: **add/del a community-set**

Syntax	Description
COMMUNITY-SET	Keyword
community-set name [max 16 char]	Name to assign to the profile
community	<AS value 0-65535>: <community value 1-65535> or well-known community value [local-AS|no-advertise|no-export|internet]

Creating a new CLASSIFIER

A Classifier is a container of conditions that can be added using the following format:

Table 11: **add/del classifier**

Syntax	Description
CLASSIFIER	Keyword
Classifier_name	Name to assign to the Classifier.
Cond_type	Type of rule inserted: - MATCH-IP: execute the match basing on the IP/Netmask address. Optionally the mach is performed basing on the key/mask words configured in “param_list”; - MATCH-NEXTHOP: execute the mach basing on the IP address of the route gateway; - MATCH-METRIC: execute the match basing on the route metric; - MATCH-TAG: execute the match basing on the route tag; - MATCH-COMMUNITY: BGP community-list - MATCH_ALL: this rule can be added to a classifier only if the classifier is homogeneous (all permit or all deny) and if it doesn't contain several conditions of the same type.
param_list	It depends on the cond_type value. **MATCH-IP** <ip-address>, <netmask>, [ge <netmask>] <ip-address>, <netmask>, [le <netmask>] <ip-address>, <netmask>, [ge <netmask> le <netmask>] Note: ip-address and netmask must be expressed by the form a.a.a.a/len ge= greater-than-or-equal-to le=less-than-or-equal-to **MATCH-NEXTHOP** <ip-address> **MATCH-METRIC** <value> (from 0 to 65535) **MATCH-TAG** <value > (from 0 to 65535) **MATCH-COMMUNITY** <COMMUNITY-SET name>

	NOTE: in a classifier matching conditions affecting ip address or next-hop must be consecutive (otherwise its application in routemaps would be ambiguous). With regard to the route-map used in the redistribution of the routes note that: • RIP supports match-tag and set-tag with tag values in the range of 1-65535; • OSPF supports match-tag and set-tag with tag values in the range of 1-4294967295; • BGP supports match-tag, but not set-tag, with tag values in the range of 1-4294967295.
Permission	It can assume the following value: PERMIT (default) DENY
Seq_num	Sequence number. It determines the rule position into classifier. The effect for the final results depends on the rule position. If no sequence number is specified, the system assigns to the rule a sequence number of +10 compared to the last rule sequence number present.

Creating a new MAP

A MAP is a container of CLASSIFIERs and ACTIONs that can be added with the following format:

Table 12: **add/del map**

Syntax	Description
MAP	Keyword
Map_name	Name to assign to the map.
Permission	It can assume the following value: PERMIT DENY It allows to modify the classifier result according to the following table: classifier result permission modified classifier result PERMIT PERMIT PERMIT PERMIT DENY DENY DENY PERMIT DENY DENY DENY DENY
Seq_num	Sequence number. It determines the clause position into the map. The effect for the final results depends on the position of classifiers and actions.
CLASSIFIER	Keyword
Classifier_name	It represents the classifier name, created by the “add classifier ..” command, to associate to a map clause.
ACTION	Keyword

Action type	It indicates the action to execute, associated to the route-map, if its result is PERMIT The available actions are: SET-LOCAL-PREF SET-AS-PATH-PREPEND SET-AS-PATH-EXCLUDE SET-METRIC SET-METRIC-TYPE SET-TAG SET-COMMUNITY **Note** With regard to the route-map used in the redistribution of the routes note that: • RIP supports match-tag and set-tag with tag values in the range of 1-65535; • OSPF supports match-tag and set-tag with tag values in the range of 1-4294967295; • BGP supports match-tag, but not set-tag, with tag values in the range of 1-4294967295.
Action value	Value dependent on the action. SET-LOCAL-PREF: **from 0 to 65535** SET-AS-PATH-PREPEND: up to 8 AS number values (each one **from 0 to 65535**) SET-AS-PATH-EXCLUDE: up to 8 AS number values (each one **from 0 to 65535**) SET-METRIC: **from 0 to 65535** SET-METRIC-TYPE: **<1 | 2>** SET-TAG: **from 0 to 65535** SET-COMMUNITY: **<COMMUNITY-SET name>**

RIP – Node

The Routing Information Protocol (RIP) protocol is mainly defined in RFC 1058 and RFC 2453.

```
ATOSNT\ip\rip>>set ?



Nodes not available.



Set command parameters:

  enable                [on|off]                  Current value: off

  version               [version]                 Current value: 2

  passive interface     [passive-ifc]             Current value: off

  update timer          [update-timer]            Current value: 30

  route timeout timer   [timeout-timer]           Current value: 180

  garbage collect timer [garbage-collect-timer]   Current value: 120

  level of log          [loglevel]                Current value: 1
```

Table 13: **set**

Syntax	Description
Enable [on|off]	Activate/deactivate the RIP on all interfaces (default: OFF).
Version [version]	Enable RIP default version [1 - 2]
Passive Interface [passive-ifc]	Enable/disable the passive interfaces defaults
Update timer [update-timer]	Every update-timer sec, the RIP module send an unsolicited Response message containing the complete routing table to all neighboring RIP routers
Route timeout timer [timeout-timer]	Upon expiration of the timeout-timer, the route is no longer valid; However, it is retained in the routing table for a short time so that neighbors can be notified that the route has been dropped.
Garbage collect timer [garbage-collect-timer]	Upon expiration of the garbage-collect-timer timeout, the route is finally removed from the routing table.
level of log [0 - 5]	Define the loglevel value

```
ATOSNT\ip\rip>>add ?



add  help :  Add a RIP enabled interface or new Redistribute or Filter or Attribute list

add  usage:

  <IFC><interface_name>

  <REDISTRIBUTE><protocol>[map map-name][metric value]

  <FILTER><classifier><name><dir><interface-name>

 add command parameters:

  IFC

  REDISTRIBUTE

  FILTER
```

Table 14: ***add***

Syntax	Description
<IFC><interface_name>	Enable an IFC to partecipate to the RIP routing protocol
<REDISTRIBUTE>><protocol>[<map><map_name>] [metric value]	Redistribute [local|static|default|bgp|ospf] protocol following optional map profile.
<FILTER><classifier><name><dir><interface_name>	Enable a filter for rip packets on given interface and given direction

```
ATOSNT\ip\rip>>del ?

del  help :  Remove interface or Redistribute or Filter or Attribute list

  <IFC><interface_name>

  <REDISTRIBUTE><protocol>[map map-name>]

  <FILTER><classifier><name><dir><interface_name>
```

```
del command parameters:

  IFC

  REDISTRIBUTE

  FILTER
```

Table 15: **del**

Syntax	Description
<IFC><interface_name>	Disable an IFC
<REDISTRIBUTE><protocol>	Delete [local|static|default,bgp|ospf] protocol distribution
<FILTER>><classifier><name><dir><interface_name>	Remove a filter for rip packets from given interface and given direction

RIP interface Node

The example below show how to add interface eth0 to participate to the Rip protocol.

```
ATOSNT\ip\rip>>add IFC eth0
Command executed
```

Then there is a new node available with the same name of the added interface.

```
ATOSNT\ip\rip\eth0>>set ?



Nodes not available.

Set command parameters:
```

```
send version        [send-version]   Current value: 2

rcv version         [rcv-version]    Current value: 2

passive interface   [passive-ifc]    Current value: off

split horizon       [split-horizon]  Current value: on
```

Table 16: **set**

Syntax	Description
send version [send-version]	Version for sending packet (default is the value set on rip node)
rcv version [rcv-version]	Version for receiving packet (default is the value set on rip node)
passive Interface [passive-ifc]	Enable/disable the passive interfaces (default is the value set on rip node)
split horizon [split-horizon]	Enable/disable split-horizon on interface

RIP redistribution and filtering

RIP redistribution

The example below shows how to enable the redistribution of local routes conditioned by predefined given map rule.

```
ATOSNT\ip\rip>>add REDISTRIBUTE local my_map
Command executed
```

Table 17: ***add***

Syntax	Description
REDISTRIBUTE	Keyword
Protocol	Define the protocol that will be redistributed by RIP Local = local routes will be redistributed into RIP Static = static routes will be redistributed into RIP Bgp = routes received by BGP will be redistributed into RIP Ospf = routes received by OSPF will be redistributed into RIP
MAP	Keyword
map_name	Name of the map associated to the redistribution. If no map is specified, all routes belonging to the protocol with the specified METRIC and TAG value will be redistributed. On the contrary, if a map name is specified, METRIC and TAG value to be use in the routes redistribution, must be configured in the “ip\routemap\map_name” command as additional actions for the same map. If in the same protocol more entries are added, only one entry can be use without route_map specified. In this case, it is processed first the entries associated to the route_map, then the entry withoute route_map. To evaluate the entries with route_map specified, the return value from the route_map configuration is used to decide how to manage the routes: · in case of PERMIT the redistribution will be done using the parameters specified in route_map; · in case of DENY the route is not redistribute; · in case of NO_MATCH, the following entry will be checked. If no match is verified after checking all maps, the route is not redistributed.
METRIC	Keyword

Metric value	Configure the metric value of the redistributed route.

RIP filtering

The example below show how to add a filter to a given interface.

```
ATOSNT\ip\rip>>add FILTER classifier my_class in eth0
Command executed
```

Table 18: **add**

Syntax	Description
FILTER	Keyword. In the “del” command, if no other parameters are specified, all filters will be deleted.
CLASSIFIER	Keyword. In the “del” command, if no other parameters are specified, all filters associated to the CLASSIFIERs will be deleted
classifier_name	Name of the CLASSIFIER to associate to the route filtering process. In this context purpose of the CLASSIFIER is to filter the routes so the following rule is applied: if the result of the CLASSIFIER is PERMIT, the route is not filtered; if the result of the CLASSIFIER is DENY, the route is filtered; if the result of the CLASSIFIER is NO_MATCH, the route is filtered.
Dir	Indicate in which direction the filter is applied Dir = IN means that the filter is applied in ingress on the received routes from the RIP protocol; Dir = OUT means that the filter is applied in outgoing direction on the routes sent by RIP protocol.
interface_name	Name of the interface where a RIP connection is present and the filter will be applied to.

OSPF – Node

The Open Shortest Path First (OSPF) protocol, defined in RFC 2328.

OSPF protocol is based on link-state technology which is started from the Bellman-Ford vector based algorithms used in IP routing protocols such as RIP. OSPF has introduced new concepts such as authentication of routing updates, Variable Length Subnet Masks (VLSM), route summarization, etc.

To create an OSPF process the following command is available in the “IP” node[1]:

```
ATOSNT\ip\ospf>>add ?



add  help :  Add a new OSPF instance

add  usage:

  <OSPF><name>
```

```
ATOSNT\ip\ospf>>del ?
```

```
del command parameters:

<OSPF name string>
```

Table 19: **add/del OSPF**

Syntax	**Description**
Ospf	Keyword
<name>	Name to identifier the OSPF process. The new ospf process is identified by the name “ospf-x” where “x” is the name string used in the “add” command. A new “ospf-x” subnode is dynamically created

OSPF-x – Node

In the “ospf-x” subnode, the following commands are available:

```
ATOSNT\ip\ospf\ospf-x>>set ?



Nodes not available.

Set command parameters:

  enable                 [on|off]                 Current value: off

  static router id       [static-router-id]       Current value: 0.0.0.0

  rfc1583 compatibility  [rfc1583-compatibility]  Current value: disable

  distance               [distance]               Current value: 110
```

Table 20: **set**

Syntax	**Description**
Enable <on\off>	Enable/disable the process
static-router-id <ip addr>	It defines the ospf router id. it identifies the router into Autonomous System. If the router-id is changed, to activate the new value a SW reboot must be performed. [default: 0.0.0.0]
rfc1583-compatibility <enable\disable>	In case of multiple routes that announce the same destination, it selects which preference rules must be followed. Enable = RFC1583 preference rules are used; Disable = RFC2328 preference rules are used. [default: disable]
Distance <value>	It defines the distance assigned to the ospf routing protocol. It can assume the value 1 to 254. [default: 110]

```
ATOSNT\ip\ospf\main>>add ?

add  help :  Add new Area or Interface or Redistribution or Filter or Attribute list
add  usage:
```

```
 <AREA><IP address format>
 <IFC><interface_name><area-name>
 <REDISTRIBUTE><protocol>[map map-name>][metric value][metric-type value]
 <FILTER><classifier><name><dir><area-name>
 <SUMMARIZATION><area-name><range ip-addr/mask><advertise|not-advertise>[cost]

add command parameters:
 AREA
 IFC
 REDISTRIBUTE
 FILTER
 SUMMARIZATION
```

```
ATOSNT\ip\ospf\main>>del ?

del  help :  Remove Area or Interface or Redistribution or Filter or Attribute list
del  usage:
 <AREA><area-IP address format>
 <IFC><interface-interface_name>
 <REDISTRIBUTE>[protocol]
 <FILTER>[<classifier><name><dir><area-name>]
 <SUMMARIZATION><area-name><range ip-addr/mask>

del command parameters:
 AREA
 IFC
 REDISTRIBUTE
 FILTER
 SUMMARIZATION
```

OSPF area Node

The example below show how to add an OSPF area.

```
ATOSNT\ip\ospf\ospf1>>add AREA 1.1.1.1
Command executed
```

Table 21: **add**

Syntax	Description
AREA	Keyword
<IP address format>	It defines an area trough the area-id, expressed by an IP address format, where OSPF protocol is active. A new “area-n.n.n.n” subnode is dynamically created. The area-id 0.0.0.0 is reserved to the backbone area.

Table 22: **del**

Syntax	Description
Area-<IP address format>	Delete the selected area.

OSPF area configuration

After creating a new area “1.1.1.1” the following setting are available:

```
ATOS\Ip\ospf-1\area-1.1.1.1>>set  ?



Nodes not available.

Set command parameters:

  external routing capability  [ext-routing-capability]  Current value: no-stub-area

  stub default cost            [stub-default-cost]       Current value: 0

  virtual link                 [virtual-link]            Current value: 0.0.0.0

  authentication type          [authentication-type]     Current value: none
```

Table 23: **set**

Syntax	Description
ext-routing-capability <stub-area|no-stub-area>	It defines if the area is a “stub area” or it isn’t. In case of “stub-area” configuration, the routing to external destination will be based on existence of the default route. [default: no-sub-area]
stub-default-cost <value>	If the area is defines as stub-area and the router is a “area-border” router, this parameter indicates the default route cost that it is annunced into area. [default: 0]
virtual-link <value>	To link not adiacent area
authentication type <none|simple-password|MD5>	Set the authentication procedure to use in the area. This value willl be overridden by the authentication-type parameter of interface node. Default none.

OSPF interface Node

The example below show how to add an interface to participate to OSPF protocol.

```
ATOSNT\ip\ospf\ospf1>>add IFC eth0 area-1.1.1.1
Command executed
```

Table 24: **add**

Syntax	Description
IFC	Keyword
<ifc-name>	Name of existing ifc
<area-name>	Preconfigured ospf area

Table 25: **del**

Syntax	Description
IFC	Keyword
<ifc-name>	Ifc to delete

OSPF interface configuration

After creating a new ospf interface “eth0” the following setting are available:

ATOSNT\ip\ospf\ospf1\eth0>>set ?

Nodes not available.

Set command parameters:

area [area] Current value: area-1.1.1.1

network type [network-type] Current value: unspecified

rxmt interval (sec) [rxmt-interval] Current value: 5

inftrans delay (sec) [inftrans-delay] Current value: 1

hello interval (sec) [hello-interval] Current value: 10

routerdead interval (sec) [router-dead-interval] Current value: 40

ifc output cost [ifc-output-cost] Current value: 10

router priority [router-priority] Current value: 1

network mask [network-mask] Current value: ifc-netmask

authentication type [authentication-type] Current value: none

authentication password [password] Current value:

Table 26: **set**

Syntax	Description
area	It defines the area associated to the interface. A list of available areas will be shown using the help subcommand.
network-type [unspecified|broadcast| non-broadcast |point-to-multipoint| point-to-point]	Typology of network. Default: unspecified.
rxmt-Interval <value>	Time in seconds within retransmission of LSA, between adjacent routers that belong to the interface. This timer is ised also in case of Database Description and Link State Request packet retransmission. [0 - 65535 sec, default 5]
inftrans-Delay <value>	Indicate the time in seconds that is needed to transmit a Link State Update Packet into interface. [0 - 65535 sec, default 1]
hello-Interval <value>	It rappresents the timer in seconds within Hello packets that the router sends into interface. It must be the same for all routers connected to the same network. [0 - 65535 sec, default 10]
router-dead-interval <value>	When this timer has expired, the router declares the neighbor down. The timer is started when the router stops itself to receive Hello packets from the neighbor. [0 - 65535 sec, default 40]
ifc-output-cost <value>	It defines the cost for outgoing packets sent into interface, expressed in link state metric. It will be announced as link cost for the interface, in the router-LSA message. [0 - 255 sec, default 10]
router-priority <value>	It is a 8 bit entire number. It is used during the Designated Router election phase. The router with the higher priority value will be elected as DR. [0 - 255 sec, default 1]
network-mask <aa.bb.cc.dd|ifc-netmask>	Sets a subnet mask to the interface enabled to the OSPF process. Possible parameter values are : • a network mask at your choice in IPv4 address format (eg 255.255.0.0) or • the default value defined by "ifc-netmask" that is the mask value associated to the interface configured in ATOSNT\interfaces\eth0\ip node. Default ifc-netmask
authentication-type <none|simple_password|MD5>	Set the authentication procedure to use in the network. This value must be the same for all router connected in the same network. This value willl override the authentication-type parameter of area node Default none.
authentication-password <string>	Set the password used during the authentication procedure to verify OSPF packets into interface. [max 8 characters]

OSPF redistribution and filtering

OSPF redistribution

The example below show how to enable the redistribution of local routes conditioned by predefined given map rule.

```
ATOSNT\ip\ospf\ospf1>>add REDISTRIBUTE local map mymap metric 10 metric-type 2
Command executed
```

Table 27:***add***

Syntax	Description
REDISTRIBUTE	Keyword
Protocol	It defines the protocol to be redistributed. • local local routes will be redistributed into OSPF • static static routes will be redistributed into OSPF • default default route will be redistributed into OSPF; if keyword ALWAYS is specified, default route will be advertised into the OSPF domain regardless of it is in routing table. • RIP routes received by RIP will be redistributed into OSPF • BGP routes received by BGP will be redistributed into OSPF
MAP	Keyword
map_name	Name of the map associated to the redistribution. If no map is specified, all routes belonging to the protocol with the specified METRIC and TAG value will be redistributed. On the contrary, if a map name is specified, METRIC and TAG value to be use in the routes redistribution, must be configured in the “ip\routemap\map_name” command as additional actions for the same map. If in the same protocol more entries are added, only one entry can be use without route_map specified. In this case, it is processed first the entries associated to the route_map, then the entry withoute route_map. To evaluate the entries with route_map specified, the return value from the route_map configuration is used to decide how to manage the routes: · in case of PERMIT the redistribution will be done using the parameters specified in route_map; · in case of DENY the route is not redistribute; · in case of NO_MATCH, the following entry will be checked. If no match is verified after checking all maps, the route is not redistribute.. Metric
Keyword	
metric value	Value of the metric for the redistributed route.
Metric_type	Keyword
Metric type value	It defines the metric type to use for the redistribution. type 1 = entire path cost type 2 = cost internal AS path

Table 28: **del**

Syntax	Description
REDISTRIBUTE	Keyword. If no other parameters are specified, all redistributions will be deleted.
Protocol	It defines the protocol.

OSPF filtering

The example below show how to add a filter to a given interface.

```
ATOSNT\ip\ospf\ospf1>>add FILTER classifier my_class in area-1.1.1.1
Command executed
```

Table 29: **add/del filter**

Syntax	Description
FILTER	Keyword. In the “del” command, if no other parameters are specified, all filters will be deleted.
CLASSIFIER	Keyword. In the “del” command, if no other parameters are specified, all filters associated to the CLASSIFIERs will be deleted
classifier_name	Name of the CLASSIFIER to associate to the route filtering process. In this context purpose of the CLASSIFIER is to filter the routes so the following rule is applied: if the result of the CLASSIFIER is PERMIT, the route is not filtered; if the result of the CLASSIFIER is DENY, the route is filtered; if the result of the CLASSIFIER is NO_MATCH, the route is filtered.
Dir	Indicate in which direction the filter is applied Dir = IN means that the filter is applied in ingress on the received routes from the OSPF protocol; Dir = OUT means that the filter is applied in outgoing direction on the routes sent by OSPF protocol.
Area-name	Name of the OSPF area the filter is applied to.

OSPF summarization

Syntax	Description
SUMMARIZATION	Keyword
area-name	Preconfigured ospf area.
range [ip-address/netmask]	Network identifying summary route
advertise|not-advertise	Specifies if summary route will be advertised or not-advertised
cost [0-16777215]	Cost for this summary route

BGP – Node

Border Gateway Protocol (BGP), defined in RFC 1105, RFC 1163 and RFC 1267, is a routing protocol operating between close Autonomous systems (AS). ATOSNT implements BGP version 4. AS stands for a logical partition of network with the same administration in routing policies; each AS is identified by an AS Number (ASN).

The main BGP feature is the reliability. BGP protocol is based on TCP transport protocol that manages retransmission in case of packet loss or traffic congestion. TCP allows also to get information about connection status. In an autonomous system BGP configuration deals with ASN and Hold Timer parameters and neighbor BGP routers can be added setting IP address and ASN values.

```
ATOSNT\ip\bgp>>set ?

Nodes not available.
 Set command parameters:
  level of log  [loglevel]  Current value: 1
```

Table 30: **set**

Syntax	**Description**
loglevel <value>	Set the detail level used by ATOSNT to log BGP. [default: 1]

```
ATOSNT\ip\bgp>>add ?

add  help :  Add a new BGP process
 add  usage:
   <BGP><name><AS-number>
```

Table 31: **add**

Syntax	**Description**
BGP	Keyword
<name>	Name of BGP process
<AS-number>	AS-number assigned to the process

Table 32: **del**

Syntax	**Description**
BGP	Keyword
<name>	Name of BGP process

```
ATOSNT\ip\bgp>>clear ?

clear  help :  Clear peer
clear  usage:
 <all>

clear command parameters:
 Peer [all]
 <cr>
```

Syntax	**Description**
Clear [all]	The Clear peer command resets the active BGP sessions

BGP process – Node

The example below show how to add a BGP process with AS-numer=10.

```
ATOSNT\ip\bgp>>add BGP my_bgp 10
Command executed
```

BGP process – Commands

Then in the “my-bgp” subnode, the following commands are available:

```
ATOSNT\ip\bgp\my_bgp>>set ?


Nodes not available.


Set command parameters:

  enable                  [on|off]             Current value: on

  router id               [router-id]          Current value: 0.0.0.0

  hold timer (sec)        [hold-timer]         Current value: 180

  as number               [as-number]          Current value: 1000

  multi exit disc enable  [med-enable]         Current value: off

  distance                [distance]           Current value: 20

  internal distance       [internal-distance]  Current value: 200
```

Table 33: **set**

Syntax	**Description**
on|off	Enable/disable the protocol.
router-id <ip address>	Specify an ip address to identify the router. Default: 0.0.0.0
Hold-timer <value>	Identify max timeout value between *keepalive* and/or *update* messages. After this time the connection should be closed. Default value is 90 sec, configurable range is 0-65535 sec. Keepalive is automatically set at 1/3 of the hold timer value.
as-number <value>	Autonomous system identifier, using values from 0 to 65535. [default: 0]
med-enable <on|off>	Enable/disable multi-exit discriminator (MED) attribute [default: off]
distance <value>	Set the distance for routes received by external Autonomous System [1-254, default: 20]
internal-distance <value>	Set the distance for routes received by the internal Autonomous System [1-254, default: 200]

```
ATOSNT\ip\bgp\my_bgp>>add ?


add  help :  Add new Neighbor or Peer-group or Redistribute or Filter or Attribute or Network list
add  usage:
 <REDISTRIBUTE>[address-family]<protocol>[<map> map-name][<metric> value]
 <REDISTRIBUTE>[address-family]<default><neighbor-ip-address>[<map> map-name]
 <FILTER>[address-family]<classifier><name><dir><neighbor-ip-address|peergroup-name>
```

```
 <ATTRIBUTE-MOD>[address-family]<map-name><dir><neighbor-ip-address|peergroup-name>
 <PEER-GROUP><peer-group-name>
 <NEIGHBOR><neighbor-ip-address><AS-number>
 <NETWORK><ip-address/netmask>[backdoor]
 <NETWORK-IPV6><ipv6-address/netmask>

add command parameters:
 PEER-GROUP
 NEIGHBOR
 REDISTRIBUTE
 FILTER
 ATTRIBUTE-MOD
 NETWORK
 NETWORK-IPV6

ATOSNT\ip\bgp\my_bgp>>del ?

del  help :  Remove Neighbor or Peer-group or Redistribute or Filter or Attribute or Network list
del  usage:
 <REDISTRIBUTE>[address-family]<protocol>[<map> map-name][<metric> value]
 <REDISTRIBUTE>[address-family]<default><neighbor-ip-address>[<map> map-name]
 <FILTER>[address-family]<classifier><name><dir><neighbor-ip-address|peergroup-name>
 <ATTRIBUTE-MOD>[address-family]<map-name><dir><neighbor-ip-address|peergroup-name>
 <PEER-GROUP><peer-group-name>
 <NEIGHBOR><neighbor-ip-address><AS-number>
 <NETWORK><ip-address/netmask>[backdoor]
 <NETWORK-IPV6><ipv6-address/netmask>

add command parameters:
 PEER-GROUP
 NEIGHBOR
 REDISTRIBUTE
 FILTER
 ATTRIBUTE-MOD
 NETWORK
 NETWORK-IPV6
```

BGP redistribution

The example below show how to enable the redistribution of local routes conditioned by predefined given map rule.

```
ATOSNT\ip\bgp\my_bgp>>add REDISTRIBUTE local map mymap metric 10
Command executed
```

Table 34: **add**

Syntax	Description
REDISTRIBUTE	Keyword
address family [inet|inet6]	Specifies the address family of routes to be redistributed. Optional, default: inet.
Protocol	It defines the protocol to be redistributed. Local = local routes will be redistributed into BGP Static = static routes will be redistributed into BGP RIP = routes received by RIP will be redistributed into BGP OSPF = routes received by OSPF will be redistributed into BGP RIPng = routes received by RIPng will be redistributed into BGP (in case of address-family inet6) OSPF6 = routes received by OSPF6 will be redistributed into BGP(in case of address-family inet6)
MAP	Keyword
map_name	Name of the map associated to the redistribution. If no map is specified, all routes belonging to the protocol with the specified METRIC and TAG value will be redistributed. On the contrary, if a map name is specified, METRIC and TAG value to be use in the routes redistribution, must be configured in the “ip\routemap\map_name” command as additional actions for the same map. If in the same protocol more entries are added, only one entry can be used without route_map specified. In this case, it is processed first the entries associated to the route_map, then the entry withoute route_map. To evaluate the entries with route_map specified, the return value from the route_map configuration is used to decide how to manage the routes: · in case of PERMIT the redistribution will be done using the parameters specified in route_map; · in case of DENY the route is not redistribute; · in case of NO_MATCH, the following entry will be checked. If no match is verified after checking all maps, the route is not redistributed.
METRIC	Keyword
metric value	Value of the metric for the redistributed route.

Table 35: **del**

Syntax	Description
REDISTRIBUTE	Keyword. If no other parameters are specified, all redistributions will be deleted.
Protocol	It defines the protocol.

BGP filtering

The example below shows how to add a filter to packets from given neighbor.

```
ATOSNT\ip\bgp\my_bgp>>add FILTER classifier my_class in 27.5.67.89
Command executed
```

Table 36: **add/del filter**

Syntax	Description
FILTER	Keyword. In the “del” command, if no other parameters are specified, all filters will be deleted.
Address-family [inet|inet6]	Specifies the address family the filter applies to. Optional, default: inet.
CLASSIFIER	Keyword. In the “del” command, if no other parameters are specified, all filters associated to the CLASSIFIERSs will be deleted
classifier_name	Name of the CLASSIFIER to associate to the route filtering process. In this context purpose of the CLASSIFIER is to filter the routes so the following rule is applied: if the result of the CLASSIFIER is PERMIT, the route is not filtered; if the result of the CLASSIFIER is DENY, the route is filtered; if the result of the CLASSIFIER is NO_MATCH, the route is filtered.
Dir	Indicate in which direction the filter is applied Dir = IN means that the filter is applied in ingress on the received routes from the BGP protocol; Dir = OUT means that the filter is applied in outgoing direction on the routes sent by BGP protocol.
ip addr neighbor / peergroup name	Neighbor IP address or peer group the filter is applied to.

BGP attribute manipulation

The example below shows how to add an attribute manipulation to packets from given neighbor.

```
ATOSNT\ip\bgp\my_bgp>>add ATTRIBUTE-MOD my_map in 27.5.67.89
Command executed
```

Table 37: **add/del attribute-mod**

Syntax	Description
ATTRIBUTE_MOD	Keyword
Address-family [inet|inet6]	Specifies the address family the attribute modification applies to. Optional, default: inet.
map_name	Name of the MAP to associate to the attribute manipulation process.
Dir	Indicate in which direction the MAP is applied Dir = IN means that the MAP is applied in ingress on the received routes from the RIP protocol; Dir = OUT means that the MAP is applied in outgoing direction on the routes sends by RIP protocol.
ip addr neighbor / peergroup name	Neighbor IP address or peergroup the attribute manipulation will be applied to.

BGP peer-group

A peer-group is a profile that can be assigned to several neighbors.

The example below shows how to add a BGP peer-group.

```
ATOSNT\ip\bgp\my_bgp>>add PEER-GROUP my_peerg
Command executed
```

Then in the “peergroup-my_peerg” subnode, the following commands are available:

```
ATOSNT\ip\bgp\my_bgp\peergroup-my_peerg>>set ?



Nodes not available.

Set command parameters:

  as number                              [as-number]                    Current value: 0

  hold timer (sec)                       [hold-timer]                   Current value: 180

  soft-reconfiguration inbound enable    [soft-reconfiguration-inbound] Current value: off

  send-community enable                  [send-community]               Current value: on

  description                            [description]                  Current value:
```

Table 38: **set**

Syntax	Description
as-number [value]	Value of AS-number for the define peer-group
Hold-timer [value]	Identify max timeout value between *keepalive* and/or *update* messages. After this time the connection should be closed. Default value is 90 sec, configurable range is 0-65535 sec.
soft-reconfiguration-inbound	Soft reconfiguration enables you to generate inbound updates from a neighbor, change and activate BGP policies without clearing the BGP session.. [default: off]
Send-community [on|off]	Enable/disable the send of community [default: on]
description [value]	Peer-group description

BGP neighbor

The example below shows how to add a BGP neighbour with AS-number 5.

```
ATOSNT\ip\bgp\my_bgp>>add NEIGHBOR 56.78.90.7 5
Command executed
```

The below example shows how to add a BGP ipv6 neighbour with AS-number 100.

```
ATOSNT\ip\bgp\my_bgp>>add NEIGHBOR 2001::6a45:1 100
Command executed
```

Then in the “neighbor-56.78.90.7” or “neighbor-2001::6a45:1” subnodes, the following commands are available:

```
ATOSNT\ip\bgp\my_bgp\neighbor-56.78.90.7>>set ?

Nodes not available.
Set command parameters:
 description                          [description]                  Current value:
 remote as number                     [as-number]                    Current value: 5
```

```
ipv4 prefixes advertisement disable     [ipv4-advertisement-disable]    Current value: off
ebgp multihop                           [ebgp-multihop]                 Current value: 1
hold timer (sec)                        [hold-timer]                    Current value: 180
soft-reconfiguration inbound enable     [soft-reconfiguration-inbound]  Current value: off
send-community enable                   [send-community]                Current value: off
peer group name                         [peer-group]                    Current value:
update source ifc                       [update-src-ifc]                Current value:
next-hop-self enable                    [next-hop-self]                 Current value: off
md5 password                            [password]                      Current value:
allow as in as-path (num of instances)  [allow-as-in]                   Current value: 0
local as number                         [local-as-number]               Current value: default
prepend/replace mode                    [prepend-replace-mode]          Current value: prepend
```

Table 39: **set**

Syntax	**Description**
description [max 100 char]	Sets a brief Neighbor description
as-number [value]	Value of AS-number for the define peer-group
ipv4-advertisement-disable [on|off]	Disables/enables ipv4 advertisement [default: off]
ebgp-multihop [1-255]	Allows connections to peers residing in networks not directly connected [default: 1]
hold-timer [value]	Identify max timeout value between *keepalive* and/or *update* messages. After this time the connection should be closed. Default value is 90 sec, configurable range is 0-65535 sec.
soft-reconfiguration-inbound [on/off]	Soft reconfiguration enables you to generate inbound updates from a neighbor, change and activate BGP policies without clearing the BGP session.. [default: off]
send-community [on|off]	Enable/disable the send of community [default: off]
peer group name [value]	Predefined peer-group profile. see above
update source ifc [ifc name]	Allows BGP activation on interface specified (es. any loopback interface configured)
next-hop-self enable [on|off]	Ensures, if active, next-hop reachability without redistributing connected routes. Defult: off (inactive)
password [max 80 char]	Sets MD5 password
allow-as-in [n]	Allows the route advertisement with the local AS in the AS path to be received n times. Default: 0.
local-as-number [0-65535|default]	Allows the router to appear to be a member of another AS, different from its real AS (default of process). Default: 'default'.
prepend-replace-mode [prepend|no-prepend|no-prepend-replace-as]	If no-prepend set, removes private autonomous-system from outbound routing updates for this neighbor and, if no-prepend-replace-as set, replaces it with local-AS specified above. Default: prepend

```
ATOSNT\ip\bgp\my_bgp\neighbor-56.78.90.7\afinet6>>set ?

Nodes not available.
Set command parameters:
 enable                                 [on|off]                        Current value: off
 soft-reconfiguration inbound enable    [soft-reconfiguration-inbound]  Current value: off
 send-community enable                  [send-community]                Current value: off
 peer group name                        [peer-group]                    Current value:
 next-hop-self enable                   [next-hop-self]                 Current value: off
```

```
allow as in as-path (num of instances)  [allow-as-in]                  Current value: 0
```

Table 40: set

Syntax	Description
Enable [on|off]	Enables ipv6 context. Default: off
soft-reconfiguration-inbound [on/off]	Soft reconfiguration enables you to generate inbound updates from a neighbor, change and activate BGP policies without clearing the BGP session. Applies in ipv6 context. [default: off]
send-community [on|off]	Enable/disable the send of community. Applies in ipv6 context [default: off]
peer group name [value]	Predefined peer-group profile. See above Applies in ipv6 context.
update source ifc [ifc name]	Allows BGP activation on interface specified (es. any loopback interface configured). Applies in ipv6 context.
next-hop-self enable [on|off]	Ensures, if active, next-hop reachability without redistributing connected routes. Applies in ipv6 context. Defult: off (inactive)
allow-as-in [n]	Allows the route advertisement with the local AS in the AS path to be received n times. Applies in ipv6 context. Default: 0.

BGP Network

```
ATOSNT\ip\bgp\my_bgp>>add NETWORK ?

add command parameters:
 Address/netmask [aa.bb.cc.dd/0-32]
```

```
ATOSNT\ip\bgp\my_bgp>>add NETWORK-IPV6 ?

add command parameters:
 address/netmask  [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/0-128]
```

The below examples show how to add a BGP network .

```
ATOSNT\ip\bgp\my_bgp>>add NETWORK 56.78.90.0/7
Command executed
```

Table 41: **add/del NETWORK**

Syntax	Description
NETWORK	Keyword
Address/netmask [aa.bb.cc.dd/0-32]	IP address and mask of the network

```
ATOSNT\ip\bgp\my_bgp>>add NETWORK-IPV6 2003::55/128
Command executed
```

Table 42: **add/del NETWORK-IPV6**

Syntax	Description
NETWORK-IPV6	Keyword
Address/netmask [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/0-128]	IPv6 address and mask of the network

Multicast - Node

Overview

Multicast is the delivery of information to a group of destination hosts simultaneously in a single transmission from the source; the copies of messages are created automatically in specific routers (routers supporting multicast, termed mrouters), only when the topology of the network requires it. A group of destination hosts is identified by an IP address of IP Multicast address ranges:

224.0.0.0 - 224.0.0.255	*Well-known multicast addresses, control channels*
224.0.1.0 - 238.255.255.255	*Globally-scoped (Internet-wide) multicast addresses*
239.0.0.0 – 239.255.255.255	*Local multicast addresses*

The implementation of the multicast concept on the IP routing level, where routers create optimal distribution paths for datagrams sent to a multicast destination address, is typically submitted to multicast routing protocols. More specifically, communication protocols host-router (e.g. IGMP) allow receivers to inform the network they are interested in receiving packets for a group, whereas communication protocols router-router (such as MOSPF, DVRMP or PIM protocols) allow the mrouters to construct multicast distribution tree for a group. Static configuration again provides the user to arrange a set of additional tools to complete and/or substitute such multicast routing activity.

In AETHRA IADs it is possible to enable PIM-SM and IGMP protocols. IGMP proxy and snooping features are also available.

IGMP protocol - Node

IGMP (version 2, RFC 2236) is a protocol operating at network layer used by IPv4 systems. IGMP messages are carried in IP datagrams and they can be a query message (request) or a report /leave message (response). The purpose is to establish or release multicast group memberships. Hosts send requests of membership to a group, routers listen for that information and periodically send (Queriers) adjacent hosts subscription queries. IGMP version 3 (RFC 3376) provides also support for “source filtering”.

In order to have an interface IGMP enabled, the user has to add the interface in IGMP configuration node and also to switch “enable” parameter to on. Three operation modes are available, as protocol can be provided also with snooping feature (RFC 4541); snooping feature, on the other hand, can be also the only functionality enabled in case of IP multicast traffic.

IGMP snooping

An IGMP snooping switch, in contrast to normal switch behavior, doesn't forward multicast traffic for a group on all interfaces, but it excludes those segments of the network where nodes are not interested in receiving packet for that group. This is a benefit from the point of view of bandwidth conservation.

IGMP proxying

One of items it is possible to configure on an IGMP-enabled interface is "service": this parameter has to be settled to "proxying" when network topology is a simple tree topology, one connection to the core network and many connections to receivers (RFC 4605). In this case parameter "proxying ifc" must be specified on the interface connected to receivers and there is no need to run a multicast routing protocol, since a proxy device is able to perform the forwarding based on information collected about group memberships. It should be noted that if the proxy device is not the Querier, parameter "only querier forwards" must be set to off, in order to have forwarding granted.

PIM-SM protocol - Node

PIM (Protocol Independent Multicast) is a family of multicast routing protocols for Internet Protocol performing routing over LAN and internet wide-area. Their work is based on unicast routing information supplied by other traditional routing protocol irrespective of which is protocol.

Protocol overview

PIM-SM is the most widely used protocol in PIM family, currently standardized (version 2) in RFC 2117, updated in RFC 2362, later in RFC 4601 and RFC 5059.

PIM-SM is suitable for groups with a very low percentage of subscribers, that is multicast groups members are sparsely distributed over the network, and they explicitly subscribe to a group when interested in receiving traffic for that group. This protocol is based on the construction, for each multicast group, of a shared tree (between multiple sources), ST, having his root in Rendez-vous Point (RP); it optionally can also manage source specific trees (SPT), having their roots in sources.

All PIM routers must know the RP address for all groups they receive subscription request. RP election can be issued by means of static configuration, or instead RP is elected with a dynamic method: the bootstrap mechanism; in this last case a specific router act as BSR (bootstrap router) and must collect and distribute periodically information about RP candidacies and election.

When a multicast source starts to send data, local router directly connected to it (source DR) sends multicast data to RP after having incapsulated them in unicast packets.

Everytime a host asks for a subscription to a group, a PIM JOIN message is sent hop by hop (depending on unicast routing table) from the router directly connected to host (receiver DR), towards the RP; the mrouters reached by this message constitute the shared tree having root in RP and shared among the sources sending data for that group: the RP will multicast data to receivers via the path identified by this distribution tree.

Designated Router

Each router at boot announces itself and learns about adjacent PIM routers with a specific message (HELLO), periodically repeated to destination 224.0.0.13 ("all PIM routers"). The user is allowed to configure the periodicity, the maximum value of random delay of first HELLO message sent (delay is used to avoid simultaneous sending by several routers) and the priority for the election of DR.

The DR, router directly connected to a source or a receiver, multicasts the JOIN/PRUNE messages (receiver DR) or unicasts REGISTER messages (source DR), through its multicast interfaces.

Bootstrap Router

BSR is elected dinamically, depending on priority of each router. The user is allowed to configure a router interface as candidate for BSR election, as well the BSR priority.

Rendezvous Point

A shared tree exists, for each multicast group, rooted in RP: multicast traffic travels from RP towards receivers, along the path identified by this tree.

A PIM router can be configured as RP, or it is configured as candidate for RP election. The user is allowed to configure the static RP addresses for one or several groups or instead a router interface as candidate for one or several groups, as well the priority in case of dynamic election.

Switching to SPT

RP can normally choose to switch to native forwarding, since register encapsulation may result inefficient. It is possible to set some threshold values to decide when the switching to SPT is more convenient.

The user is allowed to configure the minimum rate before the last-hop router switches to SPT and the interval for periodical testing of this rate.

The user is also allowed to configure the minimum rate before the RP switches to the SPT, as well the interval for periodical testing of this rate.

Multicast configuration

“multicast” node configuration

Starting from ip node, “multicast” node occurs, where following actions can be carried out:

1. Adding/deleting a matching condition based classifier profile by **add/del** command ;
2. Modifying parameters by **set** command;
3. Displaying configuration by **show conf** command;

```
ATOSNT\ip\multicast>>set ?

Available nodes:
                        igmp
                        pim

Set command parameters:
  enable        [on|off]    Current value: off
  level of log  [loglevel]  Current value: 1
```

Table 43: **set**

Parameter	Description
enable (on|off)	Enable global multicastconfiguration specified in igmp and pim nodes. Default: off
loglevel <value>	Specify monitoring level for multicast event.Range: 0-5, default: 1.

“igmp” node configuration

Starting from multicast node “igmp” node occurs, where following actions can be carried out

1. Adding/deleting a IGMP enabled interface by **add/del** command ;
2. Displaying configuration by **show conf** command;

```
ATOSNT\ip\multicast\igmp>>add ?


add  help :  Add an IGMP enabled interface


add usage:
  <IFC><interface-name>


ATOSNT\ip\multicast>>show conf


Show of ATOSNT ip multicast


Enable : off


Level of log : 5



Show of ATOSNTbruno ip multicast igmp


Enable : off


Level of log : 5
```

igmp interface node configuration

Starting from igmp node igmp-interface node occurs, where following actions can be carried out:

1. Adding/deleting a static group membership by **add/del** command ;
2. Adding/deleting a static join by **add/del** command;
3. Modifying igmp interface parameters by **set** command;
4. Displaying configuration by **show conf** command;

```
ATOSNT\ip\multicast\igmp\eth0>>add ?


add  help :  Add new IGMP static group membership or IGMP static join group
add  usage:
  <STATIC-MEMBER><group-ip-address>[<source-ip-address>]
  <STATIC-JOIN><group-ip-address>



add command parameters:
```

```
  STATIC-MEMBER
  STATIC-JOIN
ATOSNT\ip\multicast\igmp\eth0>>set ?

Nodes not available.
Set command parameters:
  mode                        [mode]                       Current value: snooping
  protocol version            [protocol-version]           Current value: 2
  robustness variable         [robustness-variable]        Current value: 2
  query interval              [query-interval]             Current value: 125
  query response interval     [query-response-interval]    Current value: 10
  last member query interval  [last-member-query-interval] Current value: 1
  last member query count     [last-member-query-count]    Current value: 2
  association delete timer    [association-delete-timer]   Current value: 80
  service                     [service]                    Current value: routing
  proxying ifc                [proxy-ifc]                  Current value:
  only querier forwards       [only-querier-forwards]      Current value: on

ATOSNT\ip\multicast\igmp\eth0>>show conf
Show of ATOSNT ip multicast igmp eth0
Mode                       : snooping
Protocol version           : 2
Robustness variable        : 2
Query interval             : 125
Query Response interval    : 10
Last member Query interval : 1
Last member Query count    : 2
Association delete timer   : 80
Service                    : routing
Proxying ifc               :
Only Querier forwards      : on

LIST OF STATIC MEMBERS
Empty list

LIST OF STATIC JOINS
Empty list

Command executed
ATOSNT\ip\multicast\igmp\eth0>>
```

Table 44: **add**

Sintassi	Descrizione
mode <snooping|protocol|protocol+snooping]>	Specifica la feature da abilitare nel router, default: snooping.
protocol-version <value>	Versione del protocollo IGMP. Default: 2.
robustness-variable <value>	Definisce la tolleranza della perdita di pacchetti. Valore minimo ammesso: 2. Default: 2.
query-interval <value>	Definisce l'intervallo misurato in secondi fra le General Queries. Default: 125.
query-responseinterval <value>	Definisce l'intervallo di tempo massimo in secondi concesso agli host per inviare la risposta alla General Query. Deve essere minore di query-interval-time.Default: 10.
last-member-query-interval <value>	Definisce sia l'intervallo di invio che il tempo di risposta concesso agli host per le Queries di tipo Group-Specific oppure Group-and-Source-Specific inviate in seguito ad una Leave. Misurato in secondi. Default: 1.
last-member-query-count <value>	Definisce il numero delle Group-Specific e delle Group-and-Source-Specific Queries inviate dal router in seguito ad una Leave. Default: 2.
association-delete-timer <value>	Èil tempo, misurato in millisecondi,di vita residua dell'association dopo un messaggio di leave (multipli di 40). Default: 80.
service <proxying|routing>	Permette al router di avere funzionalità di proxy. Default: routing.
proxying-ifc <name>	Specifica l'interfaccia verso la quale il router svolgerà il ruolo di host IGMP (host interface del proxy device): in questo caso deve essere aggiunta nel nodo igmp anche tale interfaccia con il parametro service configurato al valore proxying Default: none.
only-querier-forwards <on|off>	Permette di forzare il forward anche nel caso il router non sia Querier. Default: on.

"pim" node configuration

Starting from multicast node "pim" node occurs, where following actions can be carried out:

1. Adding/deleting a PIM enabled interface by **add/del** command ;
2. Adding/deleting a STATIC RP entry by **add/del** command ;
3. Adding/deleting a group the router is RP candidate for, by **add/del** command ;
4. Modifying parameters by **set** command;
5. Displaying configuration by **show conf** command

```
ATOSNT\ip\multicast\pim>>add ?


add  help :  Add a PIM enabled interface or static Rendez-vous Point list
add  usage:
  <IFC><interface-name>
  <STATIC-RP><rp-ip-address><group-ip-address>[rp-priority]
  <CAND-RP-GROUP><group-ip-address>



add command parameters:
  IFC
  STATIC-RP
  CAND-RP-GROUP
ATOSNT\ip\multicast\pim>>set ?


Available nodes:
                        eth0
```

```
Set command parameters:
  enable                                [on|off]             Current value: off
  bsr candidate                         [bsr-cand-ifc]       Current value:
  bsr priority                          [bsr-priority]       Current value: 1
  rp candidate                          [rp-cand-ifc]        Current value:
  rp priority                           [rp-priority]        Current value: 1
  rp holdtime                           [rp-cand-hold-time]  Current value: 150
  minimum data rate                     [min-data-rate]      Current value: 50000
  data rate measure interval (sec)      [data-interval]      Current value: 20
  minimum register rate                 [min-register-rate]  Current value: 50000
  register rate measure interval (sec)  [register-interval]  Current value: 20
  level of log                          [loglevel]           Current value: 1

ATOSNT\ip\multicast\pim>>show conf
Show of ATOSNT ip multicast pim
Enable                              : off
BSR Candidate                       :
BSR Priority                        : 1
RP Candidate                        :
RP Priority                         : 1
RP Holdtime                         : 150
Minimum Data Rate                   : 50000
Data Rate Measure Interval (sec)    : 20
Minimum Register Rate               : 50000
Register Rate Measure Interval (sec) : 20
Level of log                        : 1

LIST OF STATIC RPs
Empty list

LIST OF CANDIDATE RP GROUPs
Empty list

Show of ATOSNT ip multicast pim eth0
DR Priority        : 1
Hello Period (sec) : 30
Hello Delay (sec)  : 5

Command executed
ATOSNT\ip\multicast\pim>>
```

“pim” interface node configuration

Starting from pim node pim-interface node occurs, where following actions can be carried out:

1. Modifying pim interface parameters by **set** command;
2. Displaying configuration by **show conf** command;

```
ATOSNT\ip\multicast\pim\eth0>>set ?


Nodes not available.
Set command parameters:
  dr priority         [dr-priority]   Current value: 1
  hello period (sec)  [hello-period]  Current value: 30
  hello delay (sec)   [hello-delay]   Current value: 5


ATOSNT\ip\multicast\pim\eth0>>show conf
Show of ATOSNT ip multicast pim eth0
DR Priority        : 1
Hello Period (sec) : 30
Hello Delay (sec)  : 5


Command executed
```

Table 45: **add**

Sintassi	Descrizione
dr-priority <value>	Specifica la priorità del router come DR. Range: 0-255, default: 1. Elezione in base al valore più alto e, in caso di parità in base al valore dell’ip address più alto.
hello-period <value>	Definisce l’intervallo di tempo in secondi che il router attenderà prima di inviare il successivo messaggio Hello. Range: 0-18724, default:30.
hello-delay <value>	Definisce il tempo massimo in secondi che il router, una volta avviato, attenderà prima di inviare il primo messaggio Hello. Range: 1-255, default: 5.

[1] In ATOS 4.0.x only one OSPF process can be added

Index

ManIpv6

IPv6

Main goal of this node is the Ipv6 traffic routes management.

Routers main function is to indicate the IPv6 packets coming from LAN or WAN interfaces, the route to follow to the final destination. This is achieved based on the information contained in the routing tables, on the information received from other routers connected over the WAN or LAN network, and also on a specific configuration provided by the network administrator.

ATOSNT uses:

- **static routes**

  static routes are defined in the main or basic routing table and allow to reach a different network to which the router is connected or to other networks announced by the routing protocols (e.g. RIPng) over the WAN.

  Static routes are manually configured inside ATOSNT;

- **advanced routes**

  advanced routes are also static routes but they are defined in a separate routing table; the entries of the routing table are based on complex rules (policy routing) and may have or not priority over the traditional routes, as local or basic static ones, defined on the main routing table. One typical application of the advanced routes is in videoconferencing; they allow to separate voice traffic from data and to give high priority to the voice traffic against data.

- **RIPng, OSPFv3, BGP**

  to share the contents of the routing table to other routers and update the routing table with the contents of the received RIPng, OSPFv3, BGP packets.

Routing information carried by routing protocols can be filtered configuring distribution lists.

IPv6 - Commands

In **ipv6** node you should use set command to configure the following parameter.
Notice that in this node there are four subnodes available.

```
ATOSNT\ipv6>>set ?

Available nodes:
                        route
                        routemap
                        ripng
                        ospf6

Set command parameters:
 level of log  [loglevel]  Current value: 1
```

Table 1: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to log the routing events. Default: 1

IPv6 – Nodes

In **IPv6** node you can find these available nodes:

```
ATOSNT\ipv6>>?

Available nodes:
                        route
                        routemap
                        ripng
                        ospf6
```

Route – Node

route node allows to define:

- the route classifiers (keyword is ROUTE-CLS)
- the basic static routes (keyword is ROUTE)
- the advanced routes (keyword is ADV-ROUTE)

The route classifiers can be defined in two ways:

- as a profile defined in **Classifier IPv6** node or
- as a single RULE defined here in this node according to the configuration parameters described below

The basic static routes are configured using the final destination network IPv6 address or the next hop gateway address in addition to the outbound interface and other parameters.

Advanced routes are built in using only classifiers RULE based and not classifiers defined in "Classifier IPv6" node.

In **route** node, it is possible to see all routes with **show work** command. Look at the below example, you can see the local routes the CPE has created on each active interface, the basic static routes, the advanced routes, RIP routes and so on.

```
ATOSNT\ipv6\route>>show work

Show of ATOSNT ipv6 route


LIST OF ROUTES
 ADDRESS/PREFIX-LENGTH                      GATEWAY ADDR                          INTERFACE      DISTANCE    TYPE
 ::/0                                       ::                                    eth0           30          STATIC
 ::1/128                                    ::                                    loopback0      0           LOCAL
 2000:65a2::/64                             fe80::cd0:d6ff:fe60:44ee              eth1           120         RIP
 2001::77/128                               ::                                    eth0           1           STATIC
 2001::88/128                               fe80::cd0:d6ff:fe60:44ee              eth1           120         RIP
 2001:1::/64                                ::                                    eth1           0           LOCAL
 2001:db8::6/128                            ::                                    eth0           1           STATIC
 2001:1111:3333::/64                        ::                                    eth1           0           LOCAL
```

```
2001:3333::/64                          fe80::cd0:d6ff:fe60:44ee                eth1        120         RIP
2001:7777:4444:2222::/64                ::                                      eth1        0           LOCAL
2002:2::/64                             ::                                      eth1        0           LOCAL
2004:db8::/64                           ::                                      eth1        0           LOCAL
2011::99/128                            fe80::cd0:d6ff:fe60:44ee                eth1        120         RIP
3010::/64                               fe80::cd0:d6ff:fe60:44ee                eth1        120         RIP
```

Route - Commands

You should use **add** command to define a route classifier, a basic static route or an advanced route.

```
ATOSNT\ipv6\route>>add ?

add  help :  Add a new route classifier or a static route
add  usage:
 <ROUTE-CLS><name><CLASSIFIER-IPV6><name>
 <ROUTE-CLS><name><RULE><from-addr/prefix-length><to-addr/prefix-length><tos-value>[<ifc-name>]
 <ROUTE><default><gw-ipv6-addr>[distance|group-id]
 <ROUTE><dest-ipv6-addr/prefix-length><gw-ipv6-addr>[distance|group-id]
 <ROUTE><dest-ipv6-addr/prefix-length><ifc-name>[distance|group-id]
 <ADV-ROUTE><route-classifier-name><gw-ipv6-addr>[priority][precedence-over-main-table][group-id]
 <ADV-ROUTE><route-classifier-name><ifc-name>[priority][precedence-over-main-table][group-id]

add command parameters:
 ROUTE-CLS
 ROUTE
 ADV-ROUTE
```

Add a Route Classifier, RULE based

Look at the below example about how to add a route classifier, RULE based

```
ATOSNT\ipv6\route>>add ROUTE-CLS ?

add command parameters:
 Name                  [max 16 char]
ATOSNT\ipv6\route>>add ROUTE-CLS voipcls ?

add command parameters:
 Classifier type       [CLASSIFIER-IPV6|RULE]
ATOSNT\ipv6\route>>add ROUTE-CLS voipcls RULE ?

add command parameters:
 From ipv6 address/prefix length [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/0-128|
                                 any]
ATOSNT\ipv6\route>>add ROUTE-CLS voipcls RULE 2003:55::1/128 ?

add command parameters:
 To ipv6 address/prefix length   [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/0-128|
                                 any]
```

```
ATOSNT\ipv6\route>>add ROUTE-CLS voipcls RULE 2003:55::1/128 any ?

add command parameters:
 Tos bits             [maximize-reliability|maximize-throughput|mt+mr|
                      minimize-delay|md+mr|md+mt|md+mt+mr|any]
ATOSNT\ipv6\route>>add ROUTE-CLS voipcls RULE 2003:55::1/128 any any ?

add command parameters:
 Interface name       [local-traffic|eth0]
 <cr>
ATOSNT\ipv6\route>>add ROUTE-CLS voipcls RULE 2003:55::1/128 any any local-traffic ?
Command complete (enter cr)
```

Table 2: add a Route Classifier

Syntax	Description
ROUTE-CLS	Keyword. IPv6 Route Classifier
name [max 16 char]	Name of the classifier to create in this node.
CLASSIFIER-IPV6|RULE	Sets the classifier type: • CLASSIFIER-IPV6 based or • RULE based CLASSIFIER-IPV6 and RULE are keywords
name [max 16 char]	Name of the classifier defined in “classifier-ipv6” node. The classifier “name” will use all rules defined in classifier-ipv6 node to classify traffic.
RULE	Keyword. It defines the rule for the classifier “name” created in this node.
from-addr/prefix-length [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/0-128|any]	Source-address/prefix-length - it defines the source network address of the traffic
to-addr/prefix-length [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/0-128|any]	Destination-address/prefix-length - it defines the final destination of the traffic
tos-value [maximize-reliability|maximize-throughput| mt+mr|minimize-delay| md+mr|md+mt|md+mt+mr|any]	Selected value of TOS of the marked traffic.
ifc-name optional [local-traffic|eth0…]	It defines the source interface where packets are coming from. Only proposed values can be selected.

Add a **basic Static Route**

```
ATOSNT\ipv6\route>>add ROUTE ?

add command parameters:
 Ipv6 address/prefix-length         [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/0-128|
                                    default]
ATOSNT\ipv6\route>>add ROUTE 2000:33::44/64 ?

add command parameters:
 Gateway ipv6 address               [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]
```

```
 Interface name                      [null0|loopback0|eth0]
```

Table 3: add a basic Static Route

Syntax	Description
<ROUTE>	Keyword: IPv6 static route
<default>	Default route
<dest-ipv6-addr/prefix-length> [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/0-128|default]	Ipv6 address/prefix-length value of the destination network.
<gw-ipv6-add> [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]	Next-hop Gateway IPv6 address
<ifc-name> [null0|loopback0|eth0]	Defines the outbound interface
[distance] [1-254]	Indicates Administrative Distance, not mandatory
[group-id]	Identifier of network-group defined in "network-groups" node

Add an **Advance Route**

```
ATOSNT\ipv6\route>>add ADV-ROUTE ?

add command parameters:
 Name                                [voipclass]
ATOSNT\ipv6\route>>add ADV-ROUTE voipclass ?

add command parameters:
 Gateway ipv6 address                [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]
 Interface name                      [null0|loopback0|eth0]

ATOSNT\ipv6\route>>add ADV-ROUTE voipcls eth0 ?

add command parameters:
 Priority                            [1-16382]
 Precedence over main routing table [high|low]
 Group name                          [Empty list]
 <cr>

ATOSNT\ipv6\route>>add ADV-ROUTE voipcls eth0 1 high
```

Table 4: add an Advanced Route

Syntax	Description
<ADV-ROUTE>	Keyword: IPv6 advanced route
<route-classifier-name>	Name of the IPv6 route classifier defined in "route" node.
<gw-ipv6-addr>	Next-hop gateway IPv6 address
<ifc-name>	Defines the outbound interface
[priority] [1-16382]	Defines the priority when you have multiple advanced routes (policy based rule). Not mandatory, default: 1.
[precedence-over-main-table] [high|low]	Defines the precedence of route over the main routing table. Not mandatory, default: high.
[group-id]	Identifier of network-group defined in "network-groups" node

You should use **del** command to delete a Route Classifier, a basic Static Route or an Advanced Route:

```
ATOSNT\ipv6\route>>del ?

del  help :  Delete a route classifier or a static route
del  usage:
 <ROUTE-CLS><name>
 <ROUTE><default>[gw-ipv6-addr|group-id]
 <ROUTE><dest-ip-address>[gw-ipv6-addr|group-id]
 <ROUTE><dest-ip-address>[ifc-name|group-id]
 <ADV-ROUTE><route-classifier-name><gw-ipv6-addr|group-id>
 <ADV-ROUTE><route-classifier-name><ifc-name|group-id>

del command parameters:
 ROUTE-CLS
 ROUTE
 ADV-ROUTE
```

Table 5: del a Classifier Route

Syntax	Description
<ROUTE-CLS>	Keyword: IPv6 Route Classifier
<name> [max 16 char]	Name of the classifier to be deleted.

Table 6: del a basic Static Route

Syntax	Description
<ROUTE>	Keyword: IPv6 static route
Default	Default route
<dest-ipv6-addr/prefix-length>	IPv6 address/prefix-length of the final destination network.
[gw-ipv6-addr]	Next-hop IPv6 address
[ifc-name]	Define the outbound interface
[group-id]	Identifier of network-group defined in network-groups node

Table 7: del an Advanced Route

Syntax	Description
<ADV-ROUTE>	Keyword: IPv6 advanced route
<route-classifier-name>	Route classifier name defined in ipv6\route node
[gw-ipv6-addr]	Next-hop gateway IPv6 address
[ifc-name]	Define the outbound interface
[group-id]	Identifier of network-group defined in network-groups node

How to add a Route Classifier, RULE based - Configuration Example

"netcls" is the name of the route classifier created to identify or separate all IPv6 traffic coming from 2003:55::/64 netowrk addressed to any network and marked with TOS (minimize-delay+maximize-throughput)

add ipv6 route ROUTE-CLS netcls RULE 2003:55::/64 any md+mt

ATOSNT\ipv6\route>>**show conf**

Show of ATOSNT ipv6 route

LIST OF ROUTE CLASSIFIERS RULE-BASED

NAME	FROM NETWORK	TO NETWORK	TOS BITS	SRC IFC
netcls	2003:55::/64	any	md+mt	

"voipcls" is the name of the route classifier created to identify or separate all IPv6 traffic locally generated with TOS equal to md+mt (minimize-delay+maximize-throughput) value.

ATOSNT\ipv6\route>>add ROUTE-CLS voipcls RULE any any md+mt local-traffic

Command executed

LIST OF ROUTE CLASSIFIERS RULE-BASED

NAME	FROM NETWORK	TO NETWORK	TOS BITS	SRC IFC
voipcls	any	any	md+mt	local-traffic

How to add a Route Classifier, CLASSIFIER-IPV6 based - Configuration Example

"datacls" is the name of the route classifier created to identify all IPv6 traffic coming from 2001 :: 77/128 network. Notice that in this case the rule has been defined in "classifier-ipv6" node

add ipv6 route ROUTE-CLS datacls CLASSIFIER-IPV6 nosrc

ATOSNT\ipv6\route>>**show conf**

Show of ATOSNT ipv6 route

LIST OF ROUTE CLASSIFIERS CLASSIFIER-IPV6-BASED

NAME	CLASSIFIER-IPV6
datacls	nosrc

ATOSNT\classifier-ipv6>>**show work**

Show of ATOSNT classifier-ipv6

Level of log : 1

LIST OF CLASSIFIER

Classifier IPv6 name : nosrc

RULE N. : 1

Target : deny

Source : not 2001::77/128

Command executed

How to add an Static Route - Configuration Example

An Static Route has been created, all IPv6 traffic is forwarded to 30000:: 77/128 network and pass through the gateway with 2001:db8::a503 address

ATOSNT\ipv6\route>>add ROUTE 3000::/64 2001:db8::a503

ATOSNT\ipv6\route>>**show conf**

Show of ATOSNT ipv6 route

LIST OF ROUTES

ADDRESS/PREFIX-LENGTH	GATEWAY ADDR	INTERFACE	DISTANCE	TYPE
3000::/64	2001:db8::a503		1	STATIC

How to add an Advanced Route - Configuration Example

An Advanced Route has been created, all IPv6 traffic identified by the route classifier with voip_cls_2 name, coming from 2010:22::/64 network, will be forwarded to eth0 interface

ATOSNT\ipv6\route>>add ADV-ROUTE voip_cls_2 eth0

ATOSNT\ipv6\route>>**show conf**

Show of ATOSNT ipv6 route

LIST OF ROUTE CLASSIFIERS RULE-BASED

NAME	FROM NETWORK	TO NETWORK	TOS BITS	SRC IFC
voip_cls_2	2010:22::/64	any	any	

LIST OF ADVANCED ROUTES

CLASSIFIER	GATEWAY ADDR	INTERFACE	PRIORITY	PRECEDENCE (over main table)
voip_cls_2		eth0	1	high

IPv6 Route - Show Statistics Example

ATOSNT>>show ipv6 route statistics

Route Source	Routes	FIB
connected	7	7
static	3	3
ripng	1	1
--		
Totals	11	11

Routemap - node

In **routemap** node are defined the conditions for the traffic filtering and for the routes redistribution from one routing protocol into another one.

"routemap" node also allows to define the classifiers which are used inside the routing protocols such as RIPng, BGP and OSPF6 for the traffic redistribution.

To enable the policy routing you shoud create in this node:

- **CLASSIFIER**- each CLASSIFIER contains a condition type or traffic rule
- **MAP** - each MAP can contain one or more clauses, marked by sequence numbers, each of them including one or more classifiers and one or more actions.

The main difference between a MAP and a CLASSIFIER is that the MAP in addition to define the match condition allows to define an action associated to the condition.

Routemap - Commands

In "Routemap" node, you should use **add** and **del** commands to configure the following parameters:

```
ATOSNT\ipv6\routemap>>add ?

add  help :  Add a new CLASSIFIER or MAP list/element
add  usage:
 <CLASSIFIER><name><cond-type><param_list>[permission][seq-num]
 <MAP><name><permission><seq-num><CLASSIFIER><name>
 <MAP><name><permission><seq-num><ACTION><action_type><action value>
 <MAP><name><permission><seq-num><PERMIT-ALL-NO-ACTION>

add command parameters:
 CLASSIFIER
 MAP
```

```
ATOSNT\ipv6\routemap>>del ?

del  help :  Remove CLASSIFIER or MAP list/element
del  usage:
 <CLASSIFIER><name>[seq-num|MATCH_ALL]
 <MAP><name>[permission<seq-num>][<CLASSIFIER><name>]
 <MAP><name>[permission<seq-num>][<ACTION><action_type>]
 <MAP><name>[permission<seq-num>][<PERMIT-ALL-NO-ACTION>]

del command parameters:
 CLASSIFIER
 MAP
```

Add a CLASSIFIER

Table 8: add/del a CLASSIFIER

Syntax	Description
CLASSIFIER	Keyword
Classifier_name	Name to assign to the Classifier.
Cond_type	Type of rule inserted: • **MATCH-IP**: executes the match based on the IPv6 address/prefix length. Optionally the match is performed based on the key/mask words configured in “param_list”; • **MATCH-NEXTHOP**: executes the match based on the IPv6 address of the route gateway; • **MATCH-METRIC**: executes the match based on the route metric; • **MATCH-TAG**: executes the match based on the route tag; • **MATCH-COMMUNITY**: executes the match with one or more BGP communities • **MATCH_ALL**: this rule can be added to a classifier only if the classifier is homogeneous (all permit or all deny) and if it doesn't contain several conditions of the same type.

param_list	It depends on the cond_type value. • **MATCH-IP** <ipv6-address>, <netmask>, [ge <netmask>] <ipv6-address>, <netmask>, [le <netmask>] <ipv6-address>, <netmask>, [ge <netmask> le <netmask>] Notes: ipv6-address and netmask must be expressed by the form x:x:x:x:x:x:x:x/preflen ge = greater or equal to le = less or equal to • **MATCH-NEXTHOP** <ipv6-address> • **MATCH-METRIC** <value> (from 0 to 65535) • **MATCH-TAG** <value > (from 0 to 4294967295) • **MATCH-COMMUNITY** <community-set name> (this profile is defined in ip\routemap node, table of community-set)
Permission	It can assume the following value: PERMIT (default) DENY
Seq_num	Sequence number. It determines the rule position into classifier. The effect for the final results depends on the rule position. If any sequence number is specified, the system assigns to the rule a sequence number of +10 compared to the last rule sequence number present.

Add a MAP

A MAP tipically contains CLASSIFIERs and ACTIONs grouped in clauses.

Table 9: add/del a MAP

Syntax	Description
MAP	Keyword
Map_name	Name to assign to the map.
CLASSIFIER	Keyword
Classifier_name	It represents the classifier name, created by "add classifier" command, to associate to the map.
Permission	It can assume the following value: PERMIT (default) DENY It allows to modify the classifier result according to the following table: classifier result permission modified classifier result PERMIT PERMIT PERMIT PERMIT DENY DENY DENY PERMIT DENY DENY DENY DENY

Seq_num	Sequence number. It determines the classifier position into map. The effect for the final results depends of the classifier position. If any sequence number is inserted, the system assigns to the classifier a sequence number of +10 compared to the last classifier sequence number inserted.
ACTION	Keyword
Action type	It indicates the action to execute, associated to the routemap, if its result is PERMIT The possible actions are: SET-LOCAL-PREF SET-AS-PATH-PREPEND SET-METRIC SET-TAG SET-COMMUNITY SET-MATCH ALL
Action value	Value depends on the action. SET-LOCAL-PREF: **from 0 to 4294967295** SET-AS-PATH-PREPEND: **<AS1 value 0-65535>...<ASn value 0-65535>** SET-METRIC: **from 0 to 4294967295** SET-TAG: **from 0 to 4294967295** SET-COMMUNITY: **<community-set name>** SET- MATCH ALL ????
PERMIT-ALL-NO-ACTION	????.....

RIPng - Node

The Routing Information Protocol for IPv6 (RIPng) is mainly defined in RFC 2080.

RIPng - Commands

You should use set, add and del to configure the node parameters.

```
ATOSNT\ipv6\ripng>>set ?

Nodes not available.
Set command parameters:
 enable                 [on|off]                Current value: on
 passive interface      [passive-ifc]           Current value: on
 update timer           [update-timer]          Current value: 30
 route timeout timer    [timeout-timer]         Current value: 180
 garbage collect timer  [garbage-collect-timer] Current value: 120
 level of log           [loglevel]              Current value: 1
```

Table 10 : set

Syntax	Description
off]	Activates/deactivates the RIPng on all interfaces (default: OFF).
off]	Enables/disables the default passive interfaces
update-timer [5-65535]	Every update-timer sec, the RIPng module sends an unsolicited Response message containing the complete routing table to all neighboring RIPng routers
timeout-timer [5-65535]	Upon expiration of the timeout-timer, the route is no longer valid; however, it is maintained in the routing table for a short time so that neighbors can be notified that the route has been dropped.
garbage-collect-timer [5-65535]	Upon expiration of the garbage-collect-timer timeout, the route is finally removed from the routing table.
loglevel [0 - 5]	Defines the loglevel value

```
ATOSNT\ipv6\ripng>>add ?

add  help :  Add a RIPng enabled interface or new Redistribution or Filtering list
add  usage:
 <IFC><interface_name>
 <REDISTRIBUTE><protocol>[<map> map-name][<metric> value]
 <FILTER><classifier><name><dir><interface-name>

add command parameters:
 IFC
 REDISTRIBUTE
 FILTER
```

```
ATOSNT\ipv6\ripng>>del ?

del  help :  Remove a RIPng enabled interface or Redistribution or Filtering list
del  usage:
 <IFC><interface_name>
 <REDISTRIBUTE><protocol>[<map> map_name][<metric>]
 <FILTER><classifier><name><dir><interface_name>

del command parameters:
 IFC
 REDISTRIBUTE
 FILTER
```

Table 11: add IFC

Syntax	Description
IFC	Keyword. Enables an interface to partecipate to the RIPng routing protocol
interface_name	Name of the interface

Table 12: add REDISTRIBUTE

Syntax	Description
REDISTRIBUTE	Keyword. Allows to redistribute the traffic from one routing protocol into another one
protocol [locallstatic|default|bgp|ospf]	Defines the protocol that will be redistributed by RIPng • Local = local routes will be redistributed into RIPng • Static = static routes will be redistributed into RIPng • Bgp = routes received by BGP will be redistributed into RIPng • Ospf6 = routes received by OSPF6 will be redistributed into RIPng
MAP	Keyword
map_name	Name of the map associated to the redistribution. If no map is specified, all routes belonging to the protocol with the specified METRIC and TAG values will be redistributed. Instead, if a map name is specified, METRIC and TAG values to use in the routes redistribution, must be configured in the “ipv6\routemap\map_name” command as additional actions for the same map. If in the same protocol more entries are added, only one entry can be used without route_map specified. In this case, the entries associated to the route_map will be processed first, then the entry without route_map. To evaluate the entries with route_map specified, the return value from the route_map configuration is used to decide how to manage the routes: • in case of PERMIT the redistribution will be done using the parameters specified in route_map; • in case of DENY the route is not redistributed; • in case of NO_MATCH, the following entry will be checked. If no match is verified after checking all maps, the route is not redistributed.
METRIC	Keyword
Metric value	Configure the metric value of the redistributed route

Table 13: add FILTER

Syntax	Description
FILTER	Keyword. In the “del” command, if no other parameters are specified, all filters will be deleted.
CLASSIFIER	Keyword. In the “del” command, if no other parameters are specified, all filters associated to the CLASSIFIERSs will be deleted
classifier_name	Name of the CLASSIFIER to associate to the route filtering process. Purpose of the CLASSIFIER, in this context, is to filter the routes so the following rule is applied: • if the result of the CLASSIFIER is PERMIT, the route is not filtered; • if the result of the CLASSIFIER is DENY, the route is filtered; • if the result of the CLASSIFIER is NO_MATCH, the route is filtered.

Dir	Indicates the direction the filter is applied to: • Dir = IN means that the filter is applied in ingress on the received routes from the RIPng protocol; • Dir = OUT means that the filter is applied in outgoing direction on the routes sent by RIPng protocol.
interface_name	Name of the interface where a RIPng connection is present and the filter will be applied.

Example of RIPng redistribution and filtering

This example shows how to enable the redistribution of the static and local routes conditioned by a predifined given map rule and to add a filter to a given interface

ATOSNT\ipv6\ripng>>**conf**

add ipv6 ripng REDISTRIBUTE local MAP map1 METRIC 1
add FILTER CLASSIFIER c2 in eth0

ATOSNT\ipv6\ripng>>**show work**

Show of ATOSNT ipv6 ripng

Enable : on

Passive interface : off

Update timer : 30

Route timeout timer : 180

Garbage collect timer : 120

Level of log : 1

LIST OF REDISTRIBUTIONS

PROTOCOL	MAP NAME	METRIC
static	map1	1
local	map1	1

LIST OF FILTERS

TYPE	NAME	DIR	INTERFACE
CLASSIFIER	c1	in	eth0
CLASSIFIER	c2	in	eth0

Show of ATOSNT ipv6 ripng eth0

Passive interface : off

Split Horizon : on

LIST OF IPV6 NETWORKS

Empty list

Command executed

RIPng interface - Node

When you add IFC, as a result, a new subnode appears with the same name of the added interface

```
ATOSNT\ipv6\ripng\eth0>>set ?

Nodes not available.
Set command parameters:
 passive interface  [passive-ifc]    Current value: off
 split horizon      [split-horizon]  Current value: on
```

Table 14:set

Syntax	Description
passive-ifc [on|off]	Enables/disables the passive interface (default is the value set on ripng node)
split-horizon [off|on|poisoned-reverse]	Enables/disables split-horizon on interface with or without poison-reverse. Default: on. If poisoned-reverse is selected, router advertises RIP routes as unreachable over the interface that learned the routes

Example of RIPng interface configuration

The example below shows how to add interface eth0 to participate to the RIPng protocol.

ATOSNT\ipv6\ripng>>add IFC eth0

Command executed

TOSNT\ipv6\ripng>>**show work**

Show of ATOSNT ipv6 ripng

Enable : on

Passive interface : off

Update timer : 30

Route timeout timer : 180

Garbage collect timer : 120

Level of log : 1

Show of ATOSNT ipv6 ripng eth0

Passive interface : off

Split Horizon : on

OSPF for IPv6

OSPF6 – Node

The Open Shortest Path First, version 3 protocol (OSPFv3) for IPv6 is defined in RFC 2740.

In **ospf6** node you should use set, add and del commands to configure the following parameters

```
ATOSNT\ipv6\ospf6>>set ?

Nodes not available.
Set command parameters:
 level of log  [loglevel]  Current value: 1
```

Table 15: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the OSPF6 events. Default: 1

```
ATOSNT\ipv6\ospf6>>add/del ?
add help : Add a new OSPF instance for IPv6
add usage:
  <OSPF><name>

add command parameters:
 OSPF
```

Table 16: add/del

Syntax	Description
OSPF	Keyword
name [max 16 char]	Name to identify the OSPF process for IPv6. The new ospf process is identified by the name configured

OSPF6 process – Node

When you add a new ospf instance, as a result, in "ospf6" node appears a new subnode with the same name of the ospf instance or process just created. In the subnode you can use the following commands:

```
ATOSNT\ipv6\ospf6\ospf1>>set ?

Nodes not available.
Set command parameters:
 enable                  [on|off]                Current value: on
 static router id        [static-router-id]      Current value: 0.0.0.0
```

Table 17: set

Syntax	Description
on|off	Enables/disables the ospf process
static-router-id [aa.bb.cc.dd]	It defines the ospf router id. It identifies the router into Autonomous System. Default: 0.0.0.0 .

```
ATOSNT\ipV6\ospf6\ospf1>>add ?

add  help :  Add new Area or Interface or Redistribution or Filter or Summarization list
add  usage:
 <AREA><IP address format>
 <IFC><interface_name><area-name>
 <REDISTRIBUTE><protocol>[map map-name>][metric value][metric-type value]
 <FILTER><classifier><name><dir><area-name>
 <SUMMARIZATION><area-name><range ipv6-addr/prefix-len><advertise|not-advertise>[cost]
```

```
ATOSNT\ipv6\ospf6\ospf1>>del ?

del  help :  Remove Area or Interface or Redistribution or Filter or Summarization list
del  usage:
 <AREA><area-IP address format>
 <IFC><interface-interface_name>
 <REDISTRIBUTE>[protocol]
 <FILTER>[<classifier><name><dir><area-name>]
 <SUMMARIZATION><area-name><range ipv6-addr/prefix-len>
```

OSPF6 - How to add an AREA

The example below shows how to add an OSPF6 area

```
ATOSNT\ipv6\ospf6\ospf1>>add AREA 1.1.1.1
Command executed
```

Table 18: add AREA

Syntax	Description
AREA	Keyword
<IP address format> [aa.bb.cc.dd]	It defines an area trough the area-id, expressed by an IP address format, where OSPF protocol for IPv6 is active. A new “area-n.n.n.n” subnode is dynamically created. The area-id 0.0.0.0 is reserved to the backbone area.

Table 19: del AREA

Syntax	Description
AREA	Keyword
Area-<IP address format>	Deletes the selected area.

OSPF6 - How to add an IFC

The example below shows how to add an interface to participate to OSPF6 protocol.

```
ATOSNT\ipv6\ospf6\ospf1>>add IFC eth0 area-1.1.1.1
Command executed
```

Table 20: add IFC

Syntax	Description
IFC	Keyword
<ifc-name> [loopback0|eth0]	Name of existing ifc
<area-name>	Preconfigured ospf area

As a result, after creating a new ospf interface, a new subnode appears with the same name of the interface (eth0)

```
ATOSNT\ipv6\ospf6\ospf1>>tree
ospf1                    area-1.1.1.1
                         eth0
```

OSPF interface configuration

In the subnode you can configure the following parameters:

```
ATOSNT\ipv6\ospf6\ospf1\eth0>>set ?

Nodes not available.
Set command parameters:
 area                        [area]                  Current value: area-1.1.1.1
 rxmt interval (sec)         [rxmt-interval]         Current value: 5
 inftrans delay (sec)        [inftrans-delay]        Current value: 1
 hello interval (sec)        [hello-interval]        Current value: 10
 routerdead interval (sec)   [router-dead-interval]  Current value: 40
 ifc output cost             [ifc-output-cost]       Current value: 10
 router priority             [router-priority]       Current value: 1
```

Table 21: set

Syntax	Description
area	It defines the area associated to the interface. A list of available areas will be shown.
rxmt-Interval [0-65535]	Time in seconds within retransmission of LSA, between adjacent routers that belong to the interface.This timer is ised also in case of Database Description and Link State Request packet retransmission.[default 5]
inftrans-Delay [0-65535]	Indicates the time in seconds that is needed to transmit a Link State Update Packet into interface.[default 1]
hello-Interval [0-65535]	It represents the timer in seconds within Hello packets that the router sends into interface. It must be the same for all routers connected to the same network.[default 10]
router-dead-interval [0-65535]	When this timer has expired, the router declares the neighbor down. The timer is started when the router stops itself to receive Hello packets from the neighbor.[default 40]
ifc-output-cost [0-255]	It defines the cost for outgoing packets sent into interface, expressed in link state metric. It will be announced as link cost for the interface, in the router-LSA message.[default 10]
router-priority [0-255]	It is a 8 bit entire number. It is used during the Designated Router election phase. The router with the higher priority value will be elected as DR.[default 1]

OSPF6 - How to REDISTRIBUTE routes

The example below shows how to enable the redistribution of local routes conditioned by predefined given map rule

```
ATOSNT\ipv6\ospf6\ospf1>>add REDISTRIBUTE local map mymap metric 10 metric-type 2
Command executed
```

Table 22: set

Syntax	Description
REDISTRIBUTE	Keyword
Protocol	It defines the protocol to be redistributed. • Local = local routes will be redistributed into OSPF6 • Static = static routes will be redistributed into OSPF6 • RIPng = routes received by RIPng will be redistributed into OSPF6 • BGP = routes received by BGP will be redistributed into OSPF6
MAP	Keyword
map_name	Name of the map associated to the redistribution. If no map is specified, all routes belonging to the protocol with the specified METRIC and TAG value will be redistributed. On the contrary, if a map name is specified, METRIC and TAG value to be used in the routes redistribution, must be configured in the “ipv6\routemap\map_name” command as additional actions for the same map. If in the same protocol more entries are added, only one entry can be use without route_map specified. In this case, it is processed first the entries associated to the route_map, then the entry without route_map. To evaluate the entries with route_map specified, the return value from the route_map configuration is used to decide how to manage the routes: • in case of PERMIT the redistribution will be done using the parameters specified in route_map; • in case of DENY the route is not redistributed; • in case of NO_MATCH, the following entry will be checked. If no match is verified after checking all maps, the route is not redistributed.

Table 23:del

Syntax	Description
REDISTRIBUTE	Keyword. If no other parameters are specified, all redistributions will be deleted.
Protocol	It defines the protocol to be deleted.

OSPF6 - How to add a FILTER

The example below shows how to add a filter to a given interface.

```
ATOSNT\ipv6\ospf6\ospf1>>add FILTER CLASSIFIER my_class in area-1.1.1.1
Command executed
```

Table 24:add/del FILTER

Syntax	Description
FILTER	Keyword. In the “del” command, if no other parameters are specified, all filters will be deleted.
CLASSIFIER	Keyword. Sets the filter type. In the “del” command, if no other parameters are specified, all filters associated to the CLASSIFIERSs will be deleted
classifier_name	Name of the CLASSIFIER to associate to the route filtering process. In this context purpose of the CLASSIFIER is to filter the routes so the following rule is applied: • if the result of the CLASSIFIER is PERMIT, the route is not filtered; • if the result of the CLASSIFIER is DENY, the route is filtered; • if the result of the CLASSIFIER is NO_MATCH, the route is filtered.

Dir	Specifies the direction the filter will be applied to. Dir = IN means that the filter is applied in ingress to the routes received from the OSPF6 protocol; Dir = OUT means that the filter is applied in outgoing direction to the routes sent by OSPF6 protocol.
Area-name	Name of the OSPF area for IPv6 where the filter will be applied to.

OSPF6 - How to add SUMMARIZATION

Look at the below example

```
ATOSNT\ipv6\ospf6\ospf1>>add SUMMARIZATION area-1.1.1.1 2000:22::/64 advertise 345
Command executed
```

Table 25:add/del summarization

Syntax	Description
SUMMARIZATION	Keyword
area-name	Preconfigured ospf6 area.
range [ipv6-address/prefix-length]	Network identifying summary route
advertise|not-advertise	Specifies the option, if summary route will be advertised or not-advertised
cost [0-16777215]	Cost for this summary route

ManISDNData

ISDN Interface Configuration

ISDN physical ports can be configured as **NT** (Network Termination) or **TE** (Terminal Equipment).

When configured as TE, they provide an ISDN WAN interface that can be used for instance, for backup service ensuring continuous network connectivity when the primary xDSL connection fails. Another application that it is used in some countries, is for Internet access. In both cases they work as ISDN FXO.

The TE mode configuration is used whenever the user needs to establish an speech or data communication between two or multiple end-points through the ISDN network.

In Aethra products portfolio there are CPE's that allow to configure 1, 2, 3 and up to 4 **BRI ISDN** and 1 **PRI ISDN**.

BRI is the Basic Rate Interface for ISDN and provides 2 x 64 kbit/s bearer channels ('B' channels) and one 16 kbit/s signaling channel ('D' channel).

Bearer channels may also be multiplexed into what may be considered a single link via a process called B channel BONDING, or via use of Multi-Link PPP "bundling".

B channels or bearer channels are 64 kbit/s digital channels; instead D channel is the delta channel at 64 kbit/s used for signaling/control channel.

In order to use the ISDN ports as TE, it is necessary to configure some ISDN parameters in the outgoing call set up, such as **TEI** (Terminal Equipment Identifier) and the **bearer - capability** . Bearer capability informs the network which kind of information will travel on the B channels or the type of service invoked from the user to the network.

Possible values of bearer capability are: Speech, 3.1 kz and UDI (Unrestricted Digital Information).

PRI ISDN is the Primary Rate Interface and is based on the E-carrier (E1) line in Europe. In North America and japan, the T1 line consists of 24 channels, while an E1 has 32.

In Europe and Australia, PRI consists of 30xB channels + 2xD on an E1 2.048 Mbit/s. One timeslot on the E1 is used for synchronization purposes and is not considered to be a B or D channel.

ISDN parameters are described in more detail in the following paragraphs.

isdn – Node

isdn node allows to access isdn-bri-x and isdn-pri1 subnodes (see below) which are automatically created by the system based on the CPE hardware features.

```
ATOSNT\isdn>>set ?

Available nodes:
                        isdn-bri1
                        isdn-bri2
                        isdn-bri3
                        isdn-bri4
                        isdn-pri1

Set command parameters:
 level of log  [loglevel]  Current value: 1
```

Table 1: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to log the events from the less detailed one (0) to the more detailed one (5). In particular loglevel 4 will only trace layer 3 of the ISDN protocol, while loglevel 5 will trace level 3 +level 2. Default: 1

isdn-bri-x – Commands

In these subnodes, layer 2 of ISDN ports can be configured.

```
ATOSNT\isdn\isdn-bri1>>set ?

Nodes not available.
Set command parameters:
 level of log          [loglevel]              Current value: 1
 tei                   [tei]                   Current value: auto
 calling number        [calling-number]        Current value:
 calling subaddress    [calling-subaddress]    Current value:
 bearer capability     [bearer-capability]     Current value: speech
 type of number        [type-of-number]        Current value: unknown
 sending complete      [sending-complete]      Current value: on
 max voip connections  [max-voip-connections]  Current value: default
```

Table 2: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOS to log the events from the less detailed one (0) to the more detailed one (5). Default: 1
tei [0-63|auto]	Sets in one shot the Point to Point / Point to Multipoint working mode and the TEI value. In fact if a fixed value (from 0 to 63) is selected, layer 2 works in Point to Point mode using the selected TEI value (usually equal to 0). If the “auto” value is selected instead, the Point to Multipoint working mode is selected and the TEI value is dynamically assigned. Default: auto
calling-number [max 20 decimal digits]	Used only if the associated physical port works in TE mode. Sets the calling number to be used in outgoing SETUP.
calling-subaddress [max 4 decimal digits]	Used only if the associated physical port works in TE mode. Sets the calling subaddress in outgoing SETUP.
bearer-capability [speech|3_1khz|UDI]	Sets the bearer capability value in outgoing SETUP. In Voip application it can be overridden WHEN an invite specifying clear-mode is received. In this case a SETUP with UDI bearer capability is generated regardless the value of this parameter. Default: speech
type-of-number [unknown|International|National|Subscriber]	Defines the value to be set in Type Of Number field of Called Number information element in outgoing SETUP messages. Is to be highlighted that the value of this parameter implicitly determines also the value of Numbering Plan field. Specifically: • Type of Number Numbering Plan • Unknown Unknown • National ISDN/Telephony • International ISDN/Telephony • Subscriber Default: unknown
sending-complete [on|off]	Defines if a Sending Complete information element is to be added in outgoing SETUP in order to specify that the given number is complete. Default: on
max-voip-connections [1|default]	Sets the maximum VoIP connections. Default: default. Default means: 4 if call waiting/intermediate call is enabled; otherwise is 2.

isdn-brix - Configuration Examples

This is an example of how to configure **isdn-bri1** port to work as **TE**, TEI parameter set to 0 indicates that the CPE is working with the remote end-point in a Point to Point configuration and the bearer - capability set to UDI indicates the network that it is a data communication (e.g. backup service or a videoconferencing application).

ATOSNT\bri1>>**show work**
Show of ATOSNT bri1
Operation mode : TE
ATOSNT\isdn\isdn-bri1>>**show conf**
Show of ATOSNT isdn isdn-bri1
Level of log : 1
Physical Port : bri1
TEI : 0
Calling number : 071250651
Calling subaddress :
Bearer Capability : UDI
Type of Number : National
Sending Complete : on

In this other example **isdn-bri2** port has been configured as **NT**. ISDN BRI2 port is being used as user terminal for VoIP service. TEI set auto indicates that the working mode is Point to Multipoint and its value is dynamically assigned from the network.

Bearer - capability set to speech indicates that it is a voice communication

ATOSNT\voip>>add user-terminal ISDN isdn-bri2
ATOSNT\bri2>>**show work**
Show of ATOSNT bri2
Operation mode : NT
ATOSNT\isdn\isdn-bri2>>**show conf**
Show of ATOSNT isdn isdn-bri2
Level of log : 1
Physical Port : bri2
TEI : auto
Calling number :
Calling subaddress :
Bearer Capability : speech
Type of Number : unknown
Sending Complete : on

isdn-brix - Status

```
ATOSNT\isdn>>show status -s
Status of isdn-bri1 interface
Layer 1 status = DOWN
Layer 1 up count = 0
Layer 2 status = DOWN
B1 NOT ALLOCATED
B2 NOT ALLOCATED
```

isdn-pri1 – Commands

Based on the CPE hardware, you can have also available one PRI ISDN port that can be configured using the **isdn-pri1** node and the following commands.

```
ATOSNT\isdn\isdn-pri1>>set ?

Nodes not available
Set command parameters:
 level of log                [loglevel]                 Current value: 5
 calling number              [calling-number]           Current value:
 calling subaddress          [calling-subaddress]       Current value:
 bearer capability           [bearer-capability]        Current value: speech
 type of number              [type-of-number]           Current value: unknown
 outgoing b channels         [outgoing-mask]            Current value: 1-15
 outgoing b channels order   [outgoing-order]           Current value: Ascending
 incoming b channels         [incoming-mask]            Current value: 1-15
 incoming b channels order   [incoming-order]           Current value: Descending
 sending complete            [sending-complete]         Current value: on
 drop unrecognized calls     [drop-unrecognized-calls]  Current value: off
```

Table 3: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOS to log the PRI ISDN events from the less detailed one (0) to the more detailed one (5). Default: 1
calling-number [max 20 decimal digits]	Used only if the associated physical port works in TE mode. Sets the calling number in outgoing SETUP.
calling-subaddress [max 4 decimal digits]	Used only if the associated physical port works in TE mode. Sets the calling subaddress in outgoing SETUP.
bearer-capability [speech|3_1khz|UDI]	Sets the bearer capability value in outgoing SETUP. In Voip application it can be overridden WHEN an invite specifying clear-mode is received. In this case a SETUP with UDI bearer capability is generated regardless the value of this parameter. Default: speech

type-of-number [unknown|International|National|Subscriber]	Defines the value to be set in Type Of Number field of Called Number information element in outgoing SETUP messages. Is to be highlighted that the value of this parameter implicitly determines also the value of Numbering Plan field. Specifically: • Type of Number Numbering Plan • Unknown Unknown • National ISDN/Telephony • International ISDN/Telephony • Subscriber Default: unknown
outgoing-mask [n-m,a,b,c (1-31)|all|none]	Allows to create a mask indicating the B channels to be used for outgoing calls. "Outgoing B channels" are the B channels of the outgoing calls addressed to a PRI interface Default: 1-15
outgoing-order [Ascending|Descending]	Allows B channels selection for outgoing calls on a PRI interface. Possible values are: • **Ascending** the first available B channel in ascending order (channel B1) will be chosen. • **Descending** the first available B channel in descending order (channel B30) will be chosen. Default: Ascending
incoming-mask [n-m,a,b,c (1-31)|all|none]	Allows to create a mask indicating the B channels to be used for incoming calls. "Incoming B channels" are the B channels of the incoming calls coming from a PRI interface. Default: 1-15
incoming-order [Ascending|Descending]	Allows B channels selection for incoming calls coming from a PRI interface. Possible values are: • **Ascending** the first available B channel in ascending order (channel B1) will be chosen. • **Descending** the first available B channel in descending order (channel B30) will be chosen. Default: Descending
sending-complete [on|off]	Defines if a Sending Complete Information Element is to be added in outgoing SETUP in order to specify that the given number is complete. Default: on
drop-unrecognized-calls [on|off]	By default this parameter is set to off; instead if set to on and conditioned to the existence of a B CHANNEL ASSIGN LIST, it forces the disconnection of the calls that are coming from - or that are directed to - numbers that do not belong to the numbers list assigned to the B channels. Default: off

It is also possible to configure a list of assigned B channels for outgoing or incoming calls, based on the calling number of the incoming calls or on the called number of the outgoing calls.
You should use **add** command to create the list.

```
ATOSNT\isdn\isdn-pri1>>add ?


add  help :  Add channel assign list
add  usage:
 <CHAN-ASSIGN><OUTGOING|INCOMING><Outgoing-mask><INCOMING|RANGE-NUMBER><Incoming-mask><number><range size>


add command parameters:
 CHAN-ASSIGN
```

Table 4:add

Syntax	Description
CHAN-ASSIGN	Keyword
OUTGOING|INCOMING	Allows to set a list of assigned B channels for outgoing or incoming calls.
Outgoing-mask [n-m,a,b,c (1-31)]	Allows to create a mask indicating the B channels to be used for outgoing calls. "Outgoing B channels" are the B channels of the outgoing calls addressed to a PRI interface Default: 1-15
INCOMING|START-NUMBER	• INCOMING [n-m,a,b,c (1-31)] Allows to create a mask indicating the B channels to be used for incoming calls. "Incoming B channels" are the B channels of the incoming calls coming from a PRI interface. • START-NUMBER [1-20 decimal digits may be preceded by +] is the calling number of incoming calls or the called number of outgoing calls
range size [1-4 decimal digits]	Defines the range size of the called number of the outgoing calls or the range size of the calling number of the incoming calls

To delete a channel assign list, you should use **del** command

```
ATOSNT\isdn\isdn-pri1>>del ?

del  help :  Delete a channel assign list
del  usage:
 <CHAN-ASSIGN><OUTGOING|INCOMING><Outgoing-mask><INCOMING|RANGE-NUMBER><Incoming-mask><number>

del command parameters:
 CHAN-ASSIGN
```

isdn-pri1 - Configuration Example

This is an example of a PRI ISDN port configuration.

- Outgoing calls with called number between +0712506500 and +0712506599 will have chosen B channels 3 or 5 (the first available B channel in ascending order is selected); instead incoming calls with calling number between +0712506500 and +0712506599 will have chosen B channels from 5 to 8 (the first available B channel in descending order is selected).
- Incoming calls with calling number between +0712506600 and +0712506649 will have B channels chosen 1 or 3 (the first available B channel in descending order is selected).
- Outgoing calls with called number between +0712506650 and +0712506699 will have chosen B channels 5 or 7 (the first available B channel in ascending order is selected).

ATOSNT\isdn\isdn-pri1**>>conf**

add isdn pri1

add isdn isdn-pri1 CHAN-ASSIGN OUTGOING 3,5 INCOMING 5-8 +0712506500 99

add isdn isdn-pri1 CHAN-ASSIGN INCOMING 1,3 +0712506600 49

add isdn isdn-pri1 CHAN-ASSIGN OUTGOING 5,7 START-NUMBER +0712506650 49

ATOSNT\isdn\isdn-pri1>>**show work**

Show of ATOSNT isdn isdn-pri1

Level of log : 5

Physical Port : pri1

Calling number :

Calling subaddress :

Bearer Capability : speech

Type of Number : unknown

Outgoing B channels : 1-15

Outgoing B channels order : Ascending

Incoming B channels : 1-15

Incoming B channels order : Descending

Sending Complete : on

Drop Unrecognized Calls : off

LIST OF ASSIGNED-CHANNELS

OUTGOING-MASK	INCOMING-MASK	START-NUMBER	RANGE-SIZE
3,5	5-8	+0712506500	99
Unspecified	1,3	+0712506600	49
5,7	Unspecified	+0712506650	49

Command executed

isdn-pri1 - Status

ATOSNT\isdn\isdn-pri1>>**show status -s**

Status of isdn-pri1 interface

Layer 1 status = UP

Layer 1 up count = 8

Layer 1 up time = 2h 45m 19s

Layer 2 status = UP

Used B Channels: B1 B2 B3 B4 B5 B6 B7 B8 B27 B28 B29 B30 B31

----------RX----------TX----------

LOS Alarm : OFF

AIS Alarm : OFF OFF

LOF Alarm : OFF

RAI Alarm : OFF OFF

BER Alarm : OFF

BER (1sec) : 0.00E+00

Loop : OFF OFF

Command executed

isdn-pri1 - Statistics

ATOSNT\isdn\isdn-pri1>>**show statistics**

Statistics of isdn-pri-line-1

	Incoming	Outgoing
Calls:	15	15
Calls Answer :	15	15
Calls Busy :	0	0
Calls No Answer :	0	0
Calls Failed :	0	0

Command executed

ManLineAux

Line Aux - Overview

The main goal of the auxiliary line is for connecting the CPE to a device, typically an external modem, that can be used for troubleshhoting purposes when the CPE fails.

The CPE is provided with a console port with an RJ-45 interface and allows a serial communication with the device. The console port can be used as a Command Line Interface (CLI) for CPE configuration or as an auxiliary port (Line Aux) for communication with the device.

In the scenario, the PC from the Control Center, will open a Telnet session to access the remote modem while the CPE is transparent and allows to pass the signals transmission to the modem.

Line Aux - Commands

In **line-aux** node you can configure the following parameters:

```
ATOSNT\line-aux>>set ?

Nodes not available.
Set command parameters:
 level of log  [loglevel]  Current value: 1
```

Table 1: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the Line Aux events. Default: 1

To add a new device or terminal, you should use add command

```
ATOSNT\line-aux>>add ?

add  help :  Add a terminal
add  usage:
 <PORT><name>

add command parameters:
 PORT

ATOSNT\line-aux>>add PORT ?

add command parameters:
 port name [console]

ATOSNT\line-aux>>add PORT console ?

Command complete (enter cr)

ATOSNT\line-aux>>add PORT console
Command executed
```

Table 2: add a new device

Syntax	Description
PORT	Keyword
name	sets the port's name

After addying a new port, there is a subnode named "console" where you can configure the following parameters of the serial communication.

```
ATOSNT\line-aux\console>>set ?

Nodes not available.
Set command parameters:
 level of log        [loglevel]      Current value: 1
 enable              [on|off]        Current value: off
 silent mode         [silent-mode]   Current value: on
 speed               [speed]         Current value: 9600
 databits            [databits]      Current value: 8
 parity              [parity]        Current value: none
```

```
stopbits             [stopbits]      Current value: 2
port                 [port]          Current value: 2001
exec timeout (sec)   [exec-timeout]  Current value: 600
```

Table 3: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the line-aux subnode events. Default: 1
on|off	Sets the console port to work in "Line Aux" mode
silent-mode [on|off]	If set to "on", it does not display the regular output. Default: on
19200|38400|57600|115200]	Sets the rate at which bits are transmitted for the serial interface. Default value is 9600. Default: 9600
databits [7|8]	Sets the number of data bits to transmit over the serial interface Default: 8
parity [none|odd|even]	Specifies how the user want to check parity bits in the data bits transmitted via the serial port Default: none
stopbits [1|2]	Specifies the number of bits used to indicate the end of a byte Default: 2
port [0-2600]	Sets the port for the serial communication Default: 0
exec-timeout [0-65535|none]	Sets the timeout in sec to close the Telnet session. If set to "0" means that the Telnet session is always on. Default: 600

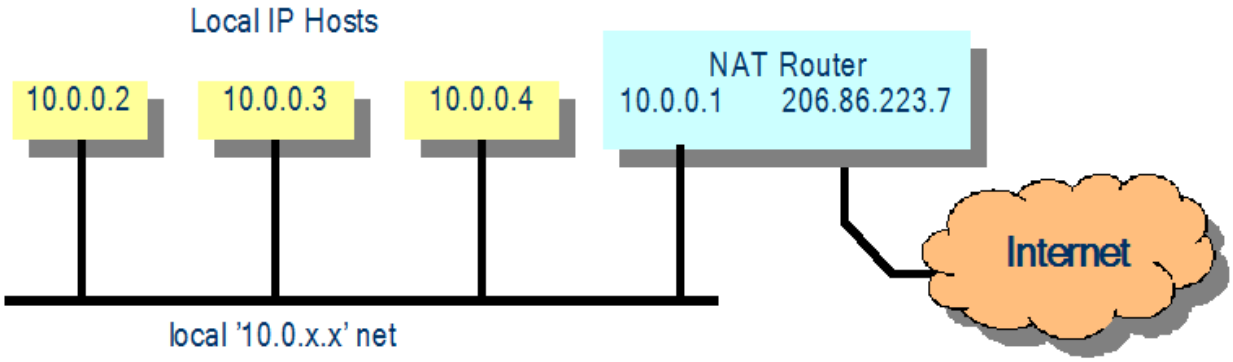
```
ATOSNT\line-aux>>show work
Show of ATOSNT line-aux
Level of log : 1

Show of ATOSNT line-aux console
Level of log       : 1
Enable             : on
Silent mode        : on
Speed              : 9600
Databits           : 8
Parity             : none
Stopbits           : 2
Port               : 2001
Exec timeout (sec) : 600
```

Command executed

ManNapt

NAPT

ATOSNT supports NAT (Network Address Translation) and PAT (Port address Translation) advanced functionalities. This allows you to use freely-assigned IP addresses over the local network and a public address (typically provided by the service provider) over the WAN ports.



You can use multiple PC's at the same time over the LAN to access external resources (i.e. Internet) even if you have subscribed only one contract with the service provider.

In the typical translation NAT, the source port remains the same (the PAT doesn't work), it is changed only if the port is already in use.

NAPT – Commands

```
ATOSNT\napt>>set ?

Nodes not available.
 Set command parameters:
 enable                          [on|off]          Current value: on
 level of log                    [loglevel]        Current value: 1
 timeout tcp value (min)         [tcptimeout]      Current value: 100
 timeout udp value (sec)         [udptimeout]      Current value: 100
 timeout sip value (sec)         [siptimeout]      Current value: 3600
 timeout icmp value (sec)        [icmptimeout]     Current value: 100
 timeout others value (sec)      [otherstimeout]   Current value: 100
 min port                        [min-port]        Current value: 49152
 max port                        [max-port]        Current value: 65535
 h323 alg enable                 [h323-alg]        Current value: off
 sip alg port start              [sip-port-start]  Current value: 5060
 sip alg port range (0=alg off)  [sip-port-range]  Current value: 0
```

Table 1: set

Syntax	Description
on|off	Activates/deactivates NAT and PAT functionalities in all interfaces. Default:on
loglevel [0-5]	Sets the detail level used by ATOSNT to record events for NAPT operations; −s option extends the same log level to all the NAPT subnodes. Default:1
tcptimeout (min) [1-7200]	Sets the timer used to delete the NAPT association with a remote host with TCP protocol. Default: 100.
udptimeout (sec) [10-3600]	Sets the timer used to delete the NAPT association with a remote host with UDP protocol. Default: 100.
siptimeout (sec) [10-3600]	Sets the timeout sip value. Default: 3600.
icmptimeout (sec) [10-3600]	Sets the timeout icmp value. Default: 100.
otherstimeout (sec) [10-3600]	Sets the timeout others value . Default: 100.
min-port [1024-65535]	Sets the first port used to translate the native port. Default: 49152.
max-port [1024-65535]	Sets the last port used to translate the native port. Default: 65535
h323-alg [on|off]	Enables/disables H323 calls managed by gatekeepers. Default: off.
sip1-port-start [0-65535]	Configures the start value for the SIP protocol UDP port range. The port taken into account is the destination port of ougoing SIP messages, (i.e. the port used by SIP Proxy to receive). Default: 5060
sip-port-range [0-65535]	Configures the UDP port range of SIP protocol. If this value is set to zero the SIP ALG doesn't work. Default: 0

```
ATOSNT\napt>>add ?

add  help :  Add a new pool
add  usage:
 <IFC><Interface name>

add command parameters:
 IFC
```

Table 2: add

Syntax	Description
IFC	keyword
Interface name	Interface name to which you want to apply the overload nat

To delete a created interface the following command must be used:

```
ATOSNT\napt>>del ?

del  help :  Delete pool
del  usage:
 <IFC><Name>
```

```
del command parameters:
 IFC
```

Table 3: del

Syntax	Description
IFC	keyword
Name	Existing interface name to be deleted.

NAPT – Nodes

Once an interface has been created a new subnode appears. For example:

```
ATOSNT\napt>>tree
napt vcc0
    eth0
```

NAPT\Interface name – Commands

For eachsubnode the following commands are available:

```
ATOSNT\napt>>set <interface name>?

Nodes not available.
Set command parameters:
 enable                           [on|off]       Current value: off
 description                      [description]  Current value:
 nat address(0.0.0.0 if notused)  [address]      Current value: 0.0.0.0
```

Table 4: set

Syntax	Description
onloff	Enables / disables the NAT and PAT interface. Default: off.
description	Up to 100 characters can be used to describe the node content
Address (0.0.0.0 if not used) [aa.bb.cc.dd]	Identifies the NAT IP address . Default: 0.0.0.0.

```
ATOSNT\napt\interface name>>add ?

add  help :  Add a new proxy server or a public address mapping or a hole address or an alias
add  usage:
 <PROXY><public-port-value><private-ip-addr><private-port-value><UDP|TCP|value>[<port-range-value]
 <MAP><private-net-ip-addr></bits-mask|mask-addr><public-ip-addr>
 <HOLE><ip-addr>[/bits-mask|mask-addr]
 <ALIAS><private-ip-addr><public-ip-addr>

add command parameters:
 PROXY
```

```
 MAP
 HOLE
 ALIAS
```

Proxy

Proxy is used to designate a host in the LAN to reply to service requests received from the relevant interface (proxy server) on a specified port. This is often referred to as “opening a port” in the NAT.

```
ATOSNT\napt>>add <interface name>?

<PROXY><public-port-value><private-ip-addr><private-port-value><UDP|TCP|value>
[<port-range-value>][public- ip-addr]
```

Table 5: add

Syntax	Description
PROXY	Keyword
Public-port-value [0-65535]	Number of the public port you want to use[2].
Private-ip-address [aa.bb.cc.dd]	Private IP address of the host you want to use as proxy .
Private-port-value [0-65535]	Number of the private port you want to use .
UDP|TCP|value	Protocol code assigned to the proxy (UDP,TCP, 0-65535).
port-range-value	Port range of the affected protocol. Zero is equivalent to a single port. Default:0
Public-ip-addr [aa.bb.cc.dd]	If specified, only traffic directed to this public Ip address (and to specified public port) is subject to proxy functioning. If not specified , all traffic directed to router and specified port is forwarded to proxy host.

```
ATOSNT\napt\interface name>>del ?

del  help :  Delete a proxy server or a public address mapping or an hole address or an alias
del  usage:
 <PROXY><public-port-value><UDP|TCP|value>
 <MAP><private-net-ip-addr>
 <HOLE><ip-addr>[/bits-mask|mask-addr]
 <ALIAS><private-ip-addr>

del command parameters:
 PROXY
 MAP
 HOLE
 ALIAS
```

Table 6: del

Syntax	Description
PROXY	Keyword
Public-port-value [0-65535] [all-proxy]	Identifies the number of the public port assigned to the proxy you want to delete. Value [all-proxy] is also allowed to delete all defined proxy.
UDP|TCP|value	Protocol code assigned to the proxy (UDP,TCP, 0-65535). Needed only if a value different from “all-proxy” is specified above.

Example: How to add a UDP proxy to public port 10, private IP address 192.168.118.70, private port 100 and to delete it:

ATOSNT\napt>>add interface name proxy 10 192.168.118.70 100 udp 0 80.105.111.111

ATOSNT\napt>>del interface name 10 udp

Alias

Alias is used to create associations between private IP addresses (LAN) and public IP addresses. You can designate one or more hosts in the LAN to answer the service requests from the WAN interfaces. The hosts that are statically associated with public addresses through alias are no longer subject to NAPT operations, but only to IP address translation. Following the example below, in packets forwarded from LAN to Internet, a source IP equal to 10.0.0.2 will be translated into 206.86.223.8; while packets forwarded from Internet to LAN, a destinatioon IP address equal to 206.86.223.8 is translated into 10.0.0.2.

The following configuration commands are available:

```
ATOSNT\napt>>add <interface name>?
add  help :  Add a new proxy server or a public address mapping or a hole address or an alias
add  usage:

<ALIAS><private-ip-addr><public-ip-addr>
```

Table 7: add

Syntax	Description
ALIAS	Keyword
Private-ip-addr [aa.bb.cc.dd]	Private IP address of the host in the LAN for association to a public address.
Public-ip-addr [aa.bb.cc.dd]	Public IP address used to reach the host over the LAN through a WAN or Loopback interface.

```
ATOSNT\napt>>delinterface name?

<ALIAS><private-ip-addr>
```

Table 8: del

Syntax	Description
ALIAS	Keyword
private ip addr [aa.bb.cc.dd]	Private IP address of the device in the LAN to delete the association to the public address.

Next example shows how to associate public IP addresses to hosts in the LAN

ATOSNT\napt>>add INTERFACE NAME ALIAS 10.0.0.4 206.86.223.7
Command executed

ATOSNT\napt>>add INTERFACE NAME ALIAS 10.0.0.7 206.86.223.8
Command executed

ATOSNT\napt>>add INTERFACE NAME ALIAS 10.0.0.10 206.86.223.9
Command executed

ATOSNT\napt>>show INTERFACE NAME conf
Show of ATOSNT napt INTERFACE NAME
Enable: on
Description:
Nat address(0.0.0.0 if notused): 0.0.0.0

LIST OF PROXY
Empty list

LIST OF MAP
Empty list

LIST OF HOLE ADDRESSES
Empty list

LIST OF ALIAS

PRIVATE ADDRESS	PUBBLIC ADDRESS
10.0.0.4	206.86.223.7
10.0.0.7	206.86.223.8
10.0.0.10	206.86.223.9

Map

Map allows to associate a public IP address to a part of a private network. It means that the traffic generated by local hosts configured in <private net ip addr> goes to the public network using the <public ip addr> public address.

```
ATOSNT\napt>>add <interface-name>?
add  help :  Add a new proxy server or a public address mapping or an hole address or an alias
add  usage:

<MAP><private-net-ip-addr></bits-mask|mask-addr><public-ip-addr>
```

Table 9: set

Syntax	Description
MAP	Keyword
Private-net-ip-addr [aa.bb.cc.dd[/0-32]]	IP address of a private network to associate to a public IP address.
mask-addr	Netmask of the private network, that can be configured as dotted decimal mask or as /bits mask (e.g. the dotted decimal mask 255.255.255.0 in /bits mask format is /24).
Public-ip-addr [aa.bb.cc.dd]	Public IP address used as NAT address for the private network

The below example shows the association of the first 6 hosts of the private network 10.0.0.0 to the public IP address 80.70.60.50

ATOSNT\napt>>add INTERFACE NAME ALIAS 10.0.0.0 255.255.255.248 80.70.60.50
Command executed

ATOSNT\napt>>show INTERFACE NAME CONF

Show of ATOSNT napt INTERFACE NAME
Enable: on
Description:
Nat address(0.0.0.0 if notused): 0.0.0.0

LIST OF PROXY
Empty list

LIST OF MAP

PRIVATE ADDRESS	MASK	PUBBLIC ADDRESS
10.0.0.0	255.255.255.248	80.70.60.50

LIST OF HOLE ADDRESSES
Empty list

LIST OF ALIAS
Empty list

```
ATOSNT\napt>>del <interface-name>?

<MAP><private-net-ip-addr>
```

Table 10: del

Syntax	Description
MAP	Keyword
Private-net-ip-addr [aa.bb.cc.dd]	Private IP address or network address that you want to delete.

Hole

Hole is a list of IP addresses/netmask that are ignored by the NAT operations. Incoming and outgoing packets having one of the IP addresses contained in the list, in the “destination” and “source” field respectively, are ignored by the NAT operations.

```
ATOSNT\napt>>add <interface-name>?

<HOLE><ip-addr>[/bits-mask|mask-addr]
```

Table 11: set

Syntax	Description
HOLE	Keyword
ip-addr [aa.bb.cc.dd]	IP address or network address that is ignored by the NAT operations.
mask-addr	Netmask of the public network, that can be configurd as dotted decimal mask or as /bits mask (e.g. the dotted decimal mask 255.255.255.0 in /bits mask format is /24).

The following example shows the application of the hole to the first 6 hosts public network 80.70.60.0

ATOSNT\napt>>add
INTERFACE NAME HOLE
80.70.60.0 255.255.255.248
Command executed

ATOSNT\napt>>show
INTERFACE NAME CONF

Show of ATOSNT napt
INTERFACE NAME
Enable: on
Description:
Nat address(0.0.0.0 if notused):
0.0.0.0

LIST OF PROXY
Empty list

LIST OF MAP
Empty list

LIST OF HOLE ADDRESSES

IP ADDRESS	MASK
80.70.60.0	255.255.255.248

LIST OF ALIAS
Empty list

```
ATOSNT\napt>>del <interface-name>?

 <HOLE><ip-addr>[/bits-mask|mask-addr]
```

Table 12: del

Syntax	Description
HOLE	Keyword
ip-addr [aa.bb.cc.dd.ee]	Public IP address or network address that you want to remove from the hole list
mask-addr	Netmask of the public network that has been configured as dotted decimal mask or as /bits mask (e.g. the dotted decimal mask 255.255.255.0 in /bits mask format is /24).

Nota 1 Session Initiation Protocol.

Nota 2 This number becomes the search key of the added proxy.

Index

ManNetwork Groups

Network Groups - Overview

network-groups node allows to define a sort of backup method, for example for specifying an alternative nexthop route in routing scenarios.

"network-groups" are also being used in Interfaces, routing and VRRP nodes.
Feel free to click on the above hyperlink words to get more information about the use on the referred nodes.

In routing scenarios, **network-groups** node allows to define backup routes that are installed as a second choice, when higher priority routes are not active.
Backup routes have an administrative distance of 254, that is superior to local, static or dynamic routes and are less preferable than the other ones.

Look at the below table to get more information about the type of routes and their administrative distance.

Route Type	Distance Adm.
Local	0
Static	1
Dynamic RIP	120
Dynamic OSPF	110
Dynamic BGP	200 (ibgp) or 20(ebgp)
Backup route on "network-groups"	**254**

If the “convenient” route is local, the backup route will be installed only if the transport protocol or the physical layer of the primary interface is down; instead if the “convenient” route is acquired by a dynamic routing protocol, the backup route activation will be performed when the watched network is unreachable, even if the primary interface is up.

The following commands are available in network-groups node:

Network Groups - Commands

In **network-groups** node you should use set, add and del to configure the following parameters

```
ATOSNT\network-groups>>set ?

Nodes not available.
Set command parameters:
 level of log  [loglevel]  Current value: 1
```

Table 1: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the Network Groups events. Default: 1

```
ATOSNT\network-groups>>add ?

add  help :  Add a new GROUP
add  usage:
 <GROUP>[numeric_suffix_name]

add command parameters:
 GROUP
```

```
ATOSNT\network-groups>>del ?

del  help :  Remove a GROUP
del  usage:
 <GROUP><name>

del command parameters:
 GROUP
```

Table 2: add/del GROUP

Syntax	Description
GROUP	Keyword
numeric_suffix_name [max 3 decimal digits]	Up to 3 digits can be used to name the GROUP. Even if the numeric suffix is not set, it will automatically add a progressive number to the GROUP name (e.g. group0)

Group - Node

When you add a new GROUP as a result, a new subnode named "group0" is created. Look at the below example

```
ATOSNT\network-groups>>add GROUP
Command executed

ATOSNT\network-groups>>tree
network-groups          group0
```

Group - Commands

In "group0" node you can configure the following parameters

```
ATOSNT\network-groups\group0>>set ?

Nodes not available.
Set command parameters:
 level of log                          [loglevel]                  Current value: 1
 route down announcement delay (sec)   [route-down-delay]          Current value: 0
 route up announcement delay (sec)     [route-up-delay]            Current value: 0
 route check initial delay (sec)       [route-check-initial-delay] Current value: 60
```

Table 3: set

Syntax	Description
loglevel [0-5]	Sets the level of log
route-down-delay [0-2147493]	Sets the route down announcement delay in sec. Default:0
route-up-delay [0-2147493]	Sets the route up announcement delay in sec. Default:0
route-check-initial-delay [0-2147493]	sets the route check initial delay in sec. Default:60

```
ATOSNT\network-groups\group0>>add ?

add  help :  Add a new network
add  usage:
<NETWORK><address>[netmask|/value]

add command parameters:
NETWORK
```

```
ATOSNT\network-groups\group0>>del ?

del  help :  Remove network
del  usage:
 <NETWORK><address><netmask>

del command parameters:
```

```
 NETWORK
```

Add a Network to the Group

```
ATOSNT\network-groups\group0>>add NETWORK ?

add command parameters:
network [aa.bb.cc.dd/0-32|xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/0-128]

ATOSNT\network-groups\group0>>add NETWORK 2004:db8::/64
Command executed
```

Table 3:add/del NETWORK

Syntax	Description
NETWORK	Keyword
<address/prefix-length> aa.bb.cc.dd/0-32|xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/0-128	Sets the IP network address and netmask or IPv6 nework address and prefix length value

Watched Network - Configuration Example

This example shows how to work with watched networks (or monitorised networks) in routing scenarios.
Suppose that a router has to reach a network with IP address 80.0.0.0 and netmask 255.0.0.0 on behalf a gateway default with IP address 9.0.0.1. To garantee this, the network 9.0.0.0/8 where the gateway is placed, must be monitorised.

In presence of the dynamic RIP route, network 9.0.0.0/8 is up and traffic reaches the final destination as defined in the static route with priority 1. Instead when RIP is not active, network 9.0.0.0/8 goes down and to reach the final destination, the router will install the backup route with the alternative next hop as defined in "network-groups" node.

Look at how to configure a network-groups "group3" with the network 9.0.0.0/8 to be monitorised.

ATOSNT\network-groups**>>show conf**

Show of ATOSNT network-groups

Level of log : 1

Show of ATOSNT network-groups group3

Level of log : 1

Route down announcement delay (sec) : 0

Route up announcement delay (sec) : 0

Route check initial delay (sec) : 5

LIST OF NETWORKS

9.0.0.0/8

Command executed

You should configure these two routes:

DESTINATION	NETMASK	GATEWAY ADDR	NOTES
80.0.0.0	255.0.0.0	9.0.0.1	Main Route
80.0.0.0	255.0.0.0	5.5.5.31	Route with an alternative next hop

---

ATOSNT\ip\route>>**show conf**

Show of ATOSNT ip route

ARP update period (sec) : off

LIST OF ROUTES

DESTINATION	NETMASK	GATEWAY ADDR	INTERFACE	DISTANCE	TYPE
1.0.0.0	255.0.0.0		eth0.31	1	STATIC
20.20.0.0	255.255.0.0	70.8.9.1		1	STATIC
80.0.0.0	255.0.0.0	9.0.0.1		1	STATIC

LIST OF ALTERNATIVE NEXT HOP

DESTINATION	NETMASK	GATEWAY ADDR	INTERFACE	NET GROUP
80.0.0.0	255.0.0.0	192.168.111.135		group3

LIST OF ADVANCED ALTERNATIVE NEXT HOP

Empty List

Command executed

When RIP is ON -----> Network 9.0.0.0/8 is UP

ATOSNT\ip\route>>**show work**

Show of ATOSNT ip route

ARP update period (sec) : off

LIST OF ROUTES

DESTINATION	NETMASK	GATEWAY ADDR	INTERFACE	DISTANCE	TYPE
1.0.0.0	255.0.0.0	0.0.0.0	eth0.31	1	STATIC
4.4.4.0	255.255.255.0	0.0.0.0	eth1	0	LOCAL
5.0.0.0	255.0.0.0	0.0.0.0	eth0.31	0	LOCAL
20.20.0.0	255.255.0.0	70.8.9.1 (via 7.7.7.1)	eth1:0	1	STATIC
9.0.0.0	255.0.0.0	4.4.4.4	eth1	120	**RIP**
80.0.0.0	255.0.0.0	9.0.0.1 (via 4.4.4.4)	eth1	1	STATIC
192.168.110.0	255.255.255.0	0.0.0.0	eth0	0	LOCAL

LIST OF ADVANCED ROUTES

Empty list

LIST OF ALTERNATIVE NEXT HOP

Empty list

LIST OF ADVANCED ALTERNATIVE NEXT HOP

Empty list

Command executed

When RIP is OFF -----> Network 9.0.0.0/8 goes DOWN

ATOSNT\ip\route>>**show work**

Show of ATOSNT ip route

ARP update period (sec) : off

LIST OF ROUTES

DESTINATION	NETMASK	GATEWAY ADDR	INTERFACE	DISTANCE	TYPE
1.0.0.0	255.0.0.0	0.0.0.0	eth0.31	1	STATIC
4.4.4.0	255.255.255.0	0.0.0.0	eth1	0	LOCAL
5.0.0.0	255.0.0.0	0.0.0.0	eth0.31	0	LOCAL
80.0.0.0	**255.0.0.0**	**5.5.5.31**	**eth0.31**	**254**	**STATIC**
192.168.110.0	255.255.255.0	0.0.0.0	eth0	0	LOCAL

LIST OF ADVANCED ROUTES

Empty list

LIST OF ALTERNATIVE NEXT HOP

DESTINATION	NETMASK	GATEWAY ADDR	INTERFACE	NET GROUP
80.0.0.0	255.0.0.0	5.5.5.31		group3

LIST OF ADVANCED ALTERNATIVE NEXT HOP

Empty list

Command executed

ManNetwork Monitor

Network Monitor

Overview

Network Monitor is a software tool for troubleshouting that allows to **sniff** the running traffic over all CPE available interfaces.

Network Monitor is based on "Snort" software. "Snort" is a free and open source network intrusion prevention and network intrusion detection system.

Network Monitor can be configured to work in three main modes:

- **sniffer**,
- **packet logger**,
- **network protocol analyzer**.

In sniffer mode, it will read network packets and display them on the console.

In packet logger mode, it will log packets to an external storage device like a USB pen or a local disk.

In network protocol analyzer mode, it will monitor network traffic and analyze protocols in “off-line” mode with the help of a third-party software tool such as "Wireshark" .

"Wireshark" is an open free software that allows administration, reporting and log analysis.

Network Monitor - Commands

Under **network-monitor** node, you can use the following commands.

```
ATOSNT>>network-monitor ?

Nodes not available.

Available commands:
up                      Move one step up from the current node
top                     Back to the root of the tree
quit                    Exit from CLI session
del                     Del monitor file from storage
conf                    Show the configuration in CLI command format
full-conf               Show full configuration in CLI command format
show                    Show 'network-monitor' settings
tree                    Show the tree structure of CLI interface
help                    Help of item
info                    Show the system informations
date                    Show or setting system date and time
save                    Save configuration data
restart                 Restart device
telnet                  Open telnet client session
ping                    Send an ICMP ECHO request
atmping                 Send an ATM loopback cells
tracert                 Display a trace of packet
```

```
mtrace                  Display a path for a multicast group
resolve                 Resolve a IP address or IP name
log                     Log Management
show-logging-level      Show logged level

capture                 capture on node ATOSNT\network-monitor>>
```

```
ATOSNT>>network-monitor capture ?

apture  help :  capture
capture  usage:
<START><listened ifc>[Drive][capture file name]
<STOP>
<ANALYZE>[capture file name]
<SAVE><Drive><capture file name>

capture command parameters:
 capture command type [START|STOP|ANALYZE|SAVE]
```

Table 1: capture

Syntax	Description
START	Keyword Sets the capturing start time
listened ifc [all-ifcleth0|loopback0]	Sets the interface name to sniff the traffic
Drive	Specifies the storage device to save the capture file. By default, if not specified any driver, the captured information is saved into the RAM in a temporary file named "nm-capture" that is lost every time that a restart of the CPE occurs.
capture file name	Sets the name of the capture file
STOP	Keyword Sets the capturing stop time
ANALYZE	Keyword Sets the packet processing and displaying on the console in hexadecimal. At the end of the process, it displays a summary of the packets information as well as of the protocols
SAVE	Keyword To save the processed information in a storage device

Example of how to save a capture file in a USB flash drive and to upload it to a remote server

1. Insert a USB flash drive into the USB port on the back of the router and check that the mass storage device is recognised by the CPE

```
ATOSNT>>storage list ?

list  help :  List drive contents
list  usage:
 <Drive>[List path]
```

```
list command parameters:
 disk id  [F:]
```

2. Check the disk content:

```
ATOSNT>>storage list F:

drwxr-xr-x    7 root     root          8192 Jan  1 00:00 .
drwxrwxrwt    3 root     root            60 Jan  1 16:29 ..
drwxr-xr-x    4 root     root          8192 Jul 30  2014 .Spotlight-V100
drwxr-xr-x    2 root     root          8192 Jul 30  2014 .Trashes
-rwxr-xr-x    1 root     root          4096 Jul 30  2014 ._.Trashes
-rwxr-xr-x    1 root     root          4096 Jul 30  2014 ._eNSP V100R002C00B350 Setup.exe
drwxr-xr-x    2 root     root          8192 Mar 11  2015 .fseventsd
-rwxr-xr-x    1 root     root            92 Jul 20  2011 Autorun.inf
drwxr-xr-x    3 root     root          8192 Feb 17  2015 PortableApps
-rwxr-xr-x    1 root     root        523264 Sep 10  2014 Start.exe
drwxr-xr-x    8 root     root          8192 Mar 13  2015 tmp
```

3. To save the capture select START command, the interface and assign a name to the file; follow the below syntax:

```
ATOSNT>>capture network-monitor START eth1 F: capture_1
```

4. Select STOP command to stop the capture:

```
ATOSNT>>capture network-monitor STOP
```

The file will be saved on the USB key under a folder named NM-CAPTURES with name "capture_1" and a numeric extension.

5. To upload the file from the USB key to a remote server, first of all, you shoud check that the file is available in NM-CAPTURES folder:

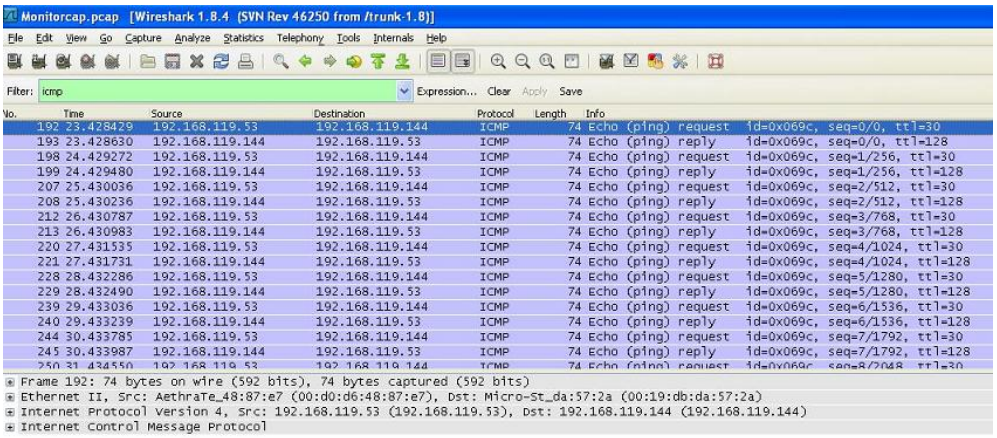
```
ATOSNT>>storage list f: NM-CAPTURES
drwxr-xr-x    2 root     root          8192 Jan  1 16:32 .
drwxr-xr-x    8 root     root          8192 Jan  1 16:32 ..
-rwxr-xr-x    1 root     root           108 Jan  1 16:35 capture_1.12885
```

6. Then with upload command and TFTP protocol, enter the the following sentence:

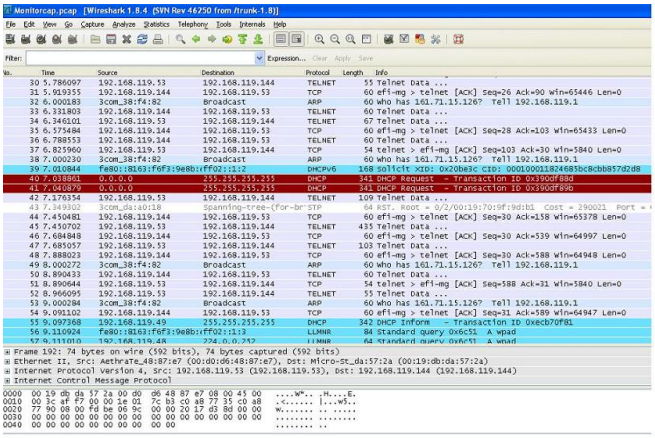
```
ATOSNT>>upload TFTP capture_1 192.168.111.22 local-file  F:/NM-CAPTURES/capture_1.12885
capture_1             100% |*******************************| 20874   0:00:00 ETA
Command executed
```

7. If needed, you can analyze the file information with the help of Wireshark application programm, for instance.
To do this, you should rename the file with a pcap extension (capture_1.12885.pcap).

Launch Wireshark programm and open the file; it looks like this when the ICMP filter is applied:



This is a complete picture showing all protocols when any filter is applied.



ManNPM

Network Performance Monitor

Overview

NPM is a tool used to network perfomance monitoring. It can measure response time, resource availability, jitter, connection duration, lost packets, application performance.

The informations are collected by an Agent, quering any router present in the net where some services as icmp is present or better act as NPM Responder. Then the Agent is capable to elaborate the information and show the report.

The Agent does the query "operation" sending packets on the net emulating several traffic shaping dependi of the type of test.

Aethra devices implements only Responder side.

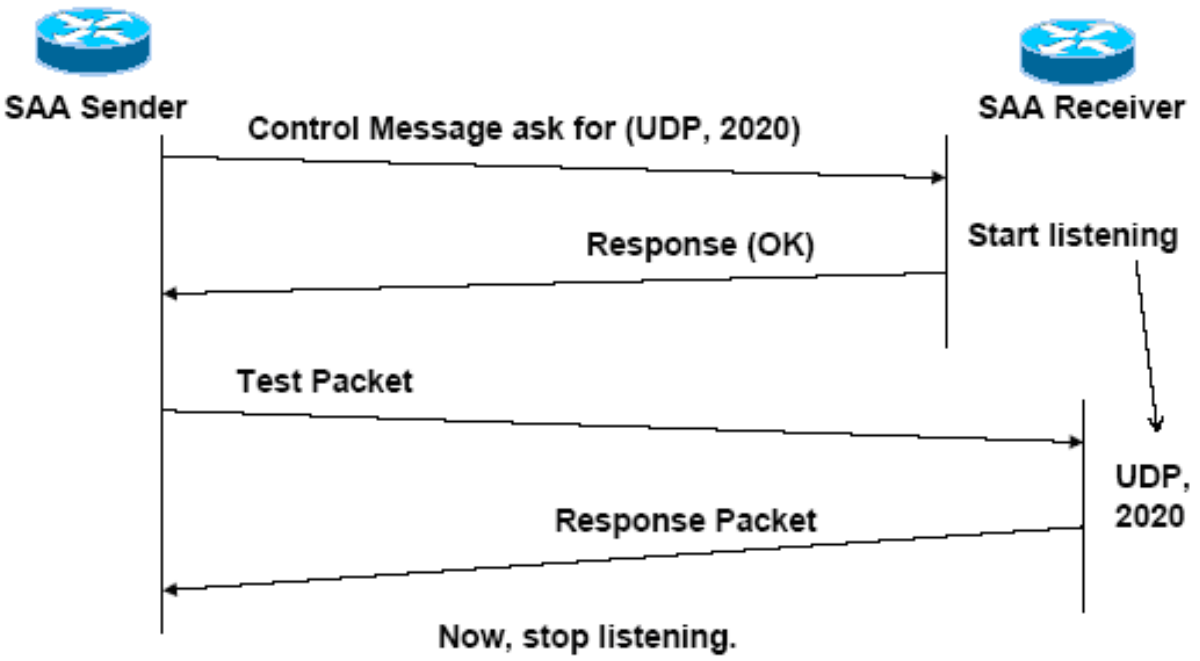
Control Protocol

The Control Protocol and communication protocol between Agent and Responder, owner Aethra, which serves to prepare the responder to stand listening for a certain period of time to respond and, on a specific port, packets sent by test Agent.

The responder, once enabled, listens on a port, protocol packets to intercept control from an Agent.

The control messages contain within them information about the type of protocol used for the test, the door, the type of test that the agent wants to perform, the duration of the test and more.

The responder accepts test packets and responds to them only for the duration that the was communicated by the agent, then disable the port used for testing.



NPM commands

```
ATOSNT\npm>>set ?

Nodes not available.
Set command parameters:
 level of log                        [loglevel]                 Current value: 1
 source ip address                   [source-ip-address]        Current value: 0.0.0.0
 enable control protocol responder   [control-protocol-enable]  Current value: off
```

Table 1: **set**

Table 1: set

Syntax	Description
Loglevel <0-5>	Sets the detail level used by ATOS to log the events of the interfaces, from the less detailed one (0) to the more detailed one (5). Adding the [- s] option, this command will be extended to all interfacessubnodes. Default: 1
source-ip-address [aa.bb.cc.dd]	IP address on which the CPE will be listening for Control protocol and data packets from remote. Also, source IP address in data packets transmitted from the CPE. It must be one of addresses assigned to the CPE. Default: 0.0.0.0
control-protocol-enable [on|off]	Disables the control protocol for the dynamic creation of responders

```
ATOSNT\npm>>add ?

add  help :  Add a Responder
add  usage:
 <RESPONDER><udp-round-trip><ip-addr><port>

add command parameters:
 RESPONDER
```

Table 2: add

Syntax	Description
RESPONDER	Keyword
udp-round-trip	This type of test calculates the time between the UDP datagram sent by the Agent and when it receives the response from the remote responder (roud-trip time).
ip-addr [aa.bb.cc.dd]	IP address on which the responder listens to the test packets
port [1-65535]	Port on which the responder listens to the test packets

Index

ManPointToPoint

Point to Point

Point-to-Point Protocol (PPP) defines a complete method for data link connectivity between units using physical layers. It includes numerous capabilities and features, including error detection, compression, authentication, Multilink PPP, encryption and much more.

ATOSNT allows to create several Point to Point profiles and use them in its internal applications such as PPP internet connections through an interface or VPN (client or server).

Once a new point-to-point profile is created, in the “Interfaces” node it can be used to add and manage a new virtual connection (for more details see “Interfaces” paragraph”).

Point-to-Point - Commands

```
ATOSNT\point-to-point>>set ?

Nodes not available.
Set command parameters:
 level of log  [loglevel]  Current value: 1
```

```
ATOSNT\point-to-point>>add ?

add  help :  Add a Point to Point profile
add  usage:

<PROFILE><PPP|PPPOE|MLPPP>[name]

add command parameters:
 PROFILE
```

```
ATOSNT\point-to-point>>del ?

del  help :  Delete a Point to Point profile
del  usage:
 <PROFILE><name>

del command parameters:
 PROFILE
```

Table 1: set

Syntax	Description
loglevel <value>	Set the detail level used by ATOSNT to log the Point to Point events. (default 1)

Table 2: add

Syntax	Description
PROFILE	Keyword
PPP	Add a PPP profile where it is possible to manage the typical parameters for PPP connections such as lcp(Link Control Protocol), authentication(configuration of authentication parameters), ipcp(configuration of compression type), ccp(use of the compression control protocol)". Once a PPP profile is added, a new "pppname" node is created. If name is not defined a progressive number will be added to PPP name (e.g. the first PPP name will be PPP0, the second PPP1 and so on).
PPPOE	Add a PPPoE profile where it is possible to manage the typical parameters for PPPoE connections such as Access Concentrator Name, Service name and timers. For PPPoE connections it is necessary to add a PPPoE profile even if you will leave the relevant field empty. Once a PPPoE profile is added, a new "pppoename" node is created. If name is not defined a progressive number will be added to PPPOE name (e.g. the first PPPOE name will be PPPOE0, the second PPPOE1 and so on).
MLPPP	Add a Multilink PPP profile where it is possible to manage the typical parameters for Multilink PPP connections such as EDO, BACP. Once a MLPPP profile is added, a new "mlpppname" node is created If name is not defined a progressive number will be added to MLPPP name (e.g. the first MLPPP name will be MLPPP0, the second MLPPP1 and so on).
name	Optionally, a string can be used to better identify the Profile. If name is not defined a progressive number will be added as described above for each profile type.

PPPx – Commands

The PPPx subnode is used to configure the PPP protocol.

```
ATOSNT\point-to-point\ppp0>>set ?

Available nodes:
                       lcp
                       authentication
                       ipcp
                       ccp

Set command parameters:
 level of log                          [loglevel]      Current value: 0
 description                           [description]   Current value:
 max configure value (rfc 1661)        [maxconfigure]  Current value: 10
 max terminate value (rfc 1661)        [maxterminate]  Current value: 2
 max failure value (rfc 1661)          [maxfailure]    Current value: 5
 max restart timer value (rfc 1661)    [restarttimer]  Current value: 3
 type ppp                              [type]          Current value: ppp-client
```

Table 3: set

Syntax	Description
loglevel <value> [-s]	Set the detail level for the information generated by ATOSNT following to errors on the services offered by the PPP subnode (default: 1). The command is extended to the subnodes by selecting the [–s] option (default 1).
maxconfigure <value>	Maximum number of requests to establish the PPP session over IFC (CFG REQUEST) in order to consider the attempt as failure. Range: 1- 20, default: 10.
maxterminate <value>	Maximum number of requests to clear the PPP connection (TERMINATE REQUEST) in order to clear the connection. Range: 1- 20, default: 2.
maxfailure <value>	Maximum number of negative acknowledgements during the negotiation phase of the PPP session parameters (CFG NAK) before sending the acknowledge message (CFG ACK). Range: 1- 20, default: 5.
restarttimer <value>	Set the timeout between two attempts for the parameters above. Range: 1- 30 secondi, default: 3 sec..
type ppp<type>	Configure the PPP type to use: • PPP-client (default) • PPP-server

PPP – Nodes

The PPP node contains the **lcp** (Link Control Protocol), **authentication** (configuration of authentication parameters), **ipcp** (configuration of compression type), **ccp** (use of the compression control protocol) and **server** subnodes (only visible if PPP-server has been selected).

LCP – Commands

```
ATOSNT\point-to-point\ppp0\lcp>>set ?

Available nodes:
                      echorequest

Set command parameters:
 mru value     [mru]   Current value: 1500
 pfc           [pfc]   Current value: off
 acfc          [acfc]  Current value: off
 echo request  [echo]  Current value: on
```

Table 4: set

Syntax	Description
mru <value>	Value of the MRU parameter (Max Receive Unit) in bytes. Range: 256-1500, default: 1500.
pfc <on|off>	Activate/deactivate the compression of the PID field (default: off)
acfc <on|off>	Activate/deactivate the compression of the Address and Control field (default:off).
echo <on|off>	Activate/deactivate the sending of PPP ECHO REQUEST packets to check the status of the PPP link (default: on).

LCP - Nodes

```
ATOSNT\point-to-point\ppp0\lcp\echorequest>>set ?

Nodes not available.
Set command parameters:
 max retries echo requests    [maxretries]  Current value: 5
 timeout echo requests (sec)  [timeout]     Current value: 30
```

Table 5: set

Syntax	Description
maxretries <value>	Maximum number of ECHO requests in order to terminate the PPP link in case of no reply from the server .Range: 1-255, default: 5.
timeout <value>	Time between two ECHO requests. Range: 1-255 seconds, default: 30 sec.

Authentication – Commands

The authentication command parameters are contained in the **authentication** node:

```
ATOSNT\point-to-point\ppp0\authentication>>set ?

Nodes not available.
Set command parameters:
  username     [username]   Current value:
  password     [password]   Current value:
  pap          [pap]        Current value: on
  chapmd5      [chapmd5]    Current value: on
  ms-chap v1   [ms-chapv1]  Current value: on
  ms-chap v2   [ms-chapv2]  Current value: on
  eap          [eap]        Current value: on
```

Table 6: set

Syntax	Description
username <string>	Username (typically provided by the ISP) for authentication with the remote server. Field with 0-128 characters, default: empty.
password <string>	Password (typically provided by the ISP) for authentication with the remote server. Field with 0-128 characters, default: empty.
pap <on|off>	Activate/deactivate the PAP authentication mode (default: on)
chapmd5 <on|off>	Activate/deactivate the CHAPMD5 authentication mode (default: on)
ms-chapv1 <on|off>	Activate/deactivate the MS-CHAPv1 authentication mode (default: on)
ms-chapv2 <on|off>	Activate/deactivate the MS-CHAPv2 authentication mode (default: on)
EAP <on|off>	Activate/deactivate the EAP-MD5 authentication mode (default: on)

ATOSNT supports the PAP and CHAP MD5 authentication modes. If ATOSNT does not supports the requested protocol during the negotiation phase of the authentication protocol, ATOSNT replies with the safest enabled protocol. The authentication phase ends when client and server agree on the protocol to use.

IPCP – Commands

```
ATOSNT\point-to-point\ppp0\ipcp>>set ?

Nodes not available.
Set command parameters:
  negotiation van jacobson compression  [vjcomp]        Current value: on
  van jacobson max slots                [vj-max-slots]  Current value: 16
```

Table 7: set vjcomp

Syntax	Description
Vjcomp <on|off>	Activate/deactivate the reception of packets compressed with the Van Jacobson technique. Default: on
vj-max-slots <value>	Configure the max slots identifier to use for Van Jacobson header. Range 2-16, default 16.

CCP – Commands

From the ATOSNT\point-to-point\ppp0\ccpnode you can activate the CCP protocol, configure up to 3 session keys and select the synchronization mode of the MPPE protocol.

```
ATOSNT\point-to-point\ppp0\ccp>>set ?

Available nodes:
                        mppe

Set command parameters:
  ccp  [on|off]  Current value: off
```

Table 8: set

Syntax	Description
on|off	Activate/deactivate the CCP protocol in the PPP profile. Default: off

CCP – Nodes

ATOSNT\point-to-point\ppp0\ccp\mppe subnode is used to define the 3 session keys and select the synchronization mode of the MPPE protocol.

```
ATOSNT\point-to-point\ppp0\ccp\mppe>>set ?

Nodes not available.
Set command parameters:
  key 40  bit           [key40]      Current value: off
  key 56  bit           [key56]      Current value: off
```

```
  key 128 bit           [key128]     Current value: off
  synchronization mode  [sync-mode]  Current value: stateless
```

Table 9: set

Syntax	Description
key40 <on|off>	Activate/deactivate the 40 bits MPPE session key. Default: off
key56 <on|off>	Activate/deactivate the 56 bits MPPE session key. Default: off
key128 <on|off>	Activate/deactivate the 128 bits MPPE session key. Default: off
sync-mode <stateless|stateful>	Select the MPPE synchronization mode. Default: stateless

PPP Server - Commands

```
ATOSNT\point-to-point\ppp0\server>>set ?

Nodes not available.
Set command parameters:
 aaa profile name   [aaa-profile]     Current value:
 address pool name  [pool-name]       Current value:
 primary dns        [primary-dns]     Current value: 0.0.0.0
 secondary dns      [secondary-dns]   Current value: 0.0.0.0
 primary wins       [primary-wins]    Current value: 0.0.0.0
 secondary wins     [secondary-wins]  Current value: 0.0.0.0
```

Table 10: set

Syntax	Description
aaa-profile	Indicate the AAA profile name (see Authentication, Authorization and Accounting chapter)
pool-name	Indicate the IP addresses pool name in the RAC-pool at the AAA node
primary-dns [aa.bb.cc.dd]	Indicate the address of the primary DNS server. Default:0.0.0.0
secondary-dns [aa.bb.cc.dd]	Indicate the address of the secondary DNS server. Default:0.0.0.0
primary-wins [aa.bb.cc.dd]	Indicate the address of the primary WINS server. Default:0.0.0.0
secondary-wins [aa.bb.cc.dd]	Indicate the address of the secondary WINS server. Default:0.0.0.0

PPPoE - Commands

Some ISP's use the PPP over Ethernet protocol for client access. This protocol makes account management and traffic monitoring easier. The technique provides for the transmission of PPP packets inside Ethernet frames.
To configure the PPP over Ethernet specific parameters for the selected profile you can use the following commands:

```
ATOSNT\point-to-point\pppoe0>> set ?

Nodes not available.
Set command parameters:
  level of log                    [loglevel]      Current value: 0
  description                     [description]   Current value:
```

```
  init value restart timer (sec)  [restarttimer]  Current value: 200
  maximum retry                   [maxretry]      Current value: 5
  service name                    [servicename]   Current value:
  access concentrator name        [acname]        Current value:
```

Table 11: set

Syntax	Description
loglevel <value>	Log level generated by ATOSNT for errors in the services offered by the PPPoE subnode. Default: 1.
description	You can use up to 100 characters to describe the PPPoE service profile.
restarttimer <value>	Initial value of the timer used in the *Discovery*phase when ATOSNT is trying to reach the PPPoE server. The timer is used for the first re-transmission of the “PADI” and "PADR" packets in case of no reply. The value doubles at every re-transmission. Range: 1-65535 msec., default: 200 msec.
maxretry <value>	Maximum number of re-transmission attempts of “PADI” and “PADR” packets. Range: 1-255, default: 5.
servicename <string>	Name of the service requested to listening servers. Maximum 40 characters (default: empty). ATOSNT accepts the first one proposed by the Access Concentrator.
acname <string>	Name of the Access Concentrator with the requested service. Maximum 40 characters (default: empty). ATOSNT accepts the first one.

MLPPP - Commands

MLPPP (Multilink over PPP) is an option of the PPP protocol that provides load balancing functionality over multiple WAN links, while providing multivendor interoperability, proper sequencing, and load calculation on both inbound and outbound traffic. Datagrams are split, sequenced, transmitted across multiple links, and then recombined at the destination. The multiple links together are called a **bundle**.

MLPPP is only working with ISDN WAN technology and is especially useful with ISDN BRI configurations, in which both B channels can be used to achieve 128-kbps throughput.

To configure specific parameters you can use the following commands:

```
ATOSNT\point-to-point\mlppp0>>set ?

Set command parameters:
 description            [description]           Current value:
 mrru                   [mrru]                  Current value: 1500
 short sequence number  [short-seq-num-enable]  Current value: off
 edo enable             [edo-enable]            Current value: off
```

Table 12: set

Syntax	Description
description	You can use up to 100 characters to describe the MLPPP service profile
mrru [256-2048]	It is the Max-Receive-Reconstructed unit and specifies the maximum number of octets of reassembled packets. Default: 1500
short-sequence-number [on|off]	This option advises the peer to receive fragments with short, 12 bit sequence numbers. Default: off
edo-enable [on|off]	Enable/disable the Endpoint Discrimination Option (EDO) feature. Endpoint Discriminator Option represents identification of the system transmitting the packets. Default: off

Multilink EDO - Commands

When edo-mode is enabled (on), "**edo**" subnode appears and you can configure the following parameters:

```
ATOSNT\point-to-point\mlppp0\edo>>set ?

Nodes not available.
Set command parameters:
 edo mode                 [edo-mode]          Current value: null-class

ATOSNT\point-to-point\mlppp0\edo>>set edo-mode ?

 edo mode  [null-class|locally-assigned|ip-address|mac-address|magic-number-block|
           directory-number]
```

Table 13: set

Syntax	Description
null-class	This class is the default value if the option is not present in a received Configure-Request.
locally-assigned	This class is defined to permit a local assignment, use of a device serial number is suggested.
ip-address	An address in this class contains an IP host address
mac-address	An address in this class contains an IEEE 802.1 MAC address in canonical (802.3) format
magic-number-block	This is not an address but a block of 1 to 5 concatenated 32 bit PPP Magic-Numbers
directory-number	An address in this class contains an octet sequence as defined by I.331 (E.164) representing an international telephone directory number suitable for use to access the endpoint via the public switched telephone network .

Point To Point – Configuration Examples

Here you can find some examples for the use of Point to Point profiles.

How lo configure a PPPoE Point to Point profile and use it for a PPPoE Wan connection:

```
add point-to-point profile PPP ppp0
add point-to-point profile PPPoE pppoe0
set point-to-point ppp0 authentication username myusername
set point-to-point ppp0 authentication password mypassword
add interfaces IFC vcc0 802.3-PPPoE vcc0-ppp0
set interfaces vcc0 on
set interfaces vcc0-ppp0 on
set interfaces vcc0-ppp0 service-ppp ppp-profile ppp0
set interfaces vcc0-ppp0 service-ppp pppoe-profile pppoe0
add ip route default vcc0-ppp0
```

How lo configure a PPPoA Point to Point profile and use it for a PPPoA Wan connection:

```
add point-to-point profile PPP ppp0
set point-to-point ppp0 authentication username myusername
set point-to-point ppp0 authentication password mypassword
add interfaces IFC vcc0 PPP vcc0-ppp0
set interfaces vcc0 on
set interfaces vcc0-ppp0 on
set interfaces vcc0-ppp0 service-ppp ppp-profile ppp0
add ip route default vcc0-ppp0
```

How lo configure a MLPPP Point to Point profile and use it for an ISDN Wan connection at 128 kb/s using the two B channels of one ISDN BRI access:

```
set isdn isdn-bri1 tei 0
set isdn isdn-bri1 bearer-capability UDI
add point-to-point PROFILE PPP ppp0
add point-to-point PROFILE MLPPP mlppp0
set point-to-point ppp0 authentication username nomei@dominio.it
set point-to-point ppp0 authentication password pass12345
add interfaces IFC eth0 eth0
add interfaces IFC ml PPP ml-ppp0
add interfaces IFC isdn-bri1 isdn-bri1-ppp0
add interfaces IFC isdn-bri1 isdn-bri1-ppp1
set interfaces eth0 ip address 192.168.1.1/24
add interfaces ml-ppp0 LINK isdn-bri1-ppp0 1
add interfaces ml-ppp0 LINK isdn-bri1-ppp1
set interfaces ml-ppp0 loglevel 5
set interfaces ml-ppp0 open-mode always-on
set interfaces ml-ppp0 ip loglevel 5
set interfaces ml-ppp0 service-ppp loglevel 5
```

```
set interfaces ml-ppp0 service-ppp ppp-profile ppp0
set interfaces ml-ppp0 service-ppp mlppp-profile mlppp0
set interfaces isdn-bri1-ppp0 loglevel 5
set interfaces isdn-bri1-ppp0 open-mode always-on
set interfaces isdn-bri1-ppp0 inactivitytime 120
set interfaces isdn-bri1-ppp0 ip loglevel 5
add interfaces isdn-bri1-ppp0 service-dialer NUMBER 70231111
set interfaces isdn-bri1-ppp0 service-dialer loglevel 5
set interfaces isdn-bri1-ppp0 service-ppp loglevel 5
set interfaces isdn-bri1-ppp0 service-ppp ppp-profile ppp0
set interfaces isdn-bri1-ppp1 open-mode always-on
add interfaces isdn-bri1-ppp1 service-dialer NUMBER 70231111
set interfaces isdn-bri1-ppp1 service-ppp ppp-profile ppp0
add dhcpserver IFC eth0
set dhcpserver on
set dhcpserver eth0 startaddress 192.168.1.2
set dhcpserver eth0 endaddress 192.168.1.254
set dhcpserver eth0 netmask 255.255.255.0
set dhcpserver eth0 defaultrouter 192.168.1.1
set dhcpserver eth0 dns1 192.168.1.1
set dhcpserver eth0 hostname PC_0
set dhcpserver eth0 domainname LocalDomain
add dns SERVER anydomain ml-ppp0
set dns on
add napt IFC ml-ppp0
set napt ml-ppp0 on
add ip route 0.0.0.0 0.0.0.0 ml-ppp0 1
set voip call-setting country it
```

Point To Point – Logs

Before a PPP connection you can trace the Point to Point phase using the following commands:

```
ATOSNT>>set point-to-point loglevel 5 –s
ATOSNT>>log start
L1: U 21/04/2010 11:27:12:940 PPP-vcc0-ppp0: Plugin rp-pppoe.so loaded.
L1: U 21/04/2010 11:27:12:950 PPP-vcc0-ppp0: RP-PPPoE plugin version 3.3 compiled against pppd 2.4.4
W2: U 21/04/2010 11:27:12:950 PPP-vcc0-ppp0: pppd 2.4.4 started by root, uid 0
L2: U 21/04/2010 11:27:13:070 PPP-vcc0-ppp0: PADS: Service-Name:
L1: U 21/04/2010 11:27:13:070 PPP-vcc0-ppp0: PPP session is 1839
L2: U 21/04/2010 11:27:13:070 PPP-vcc0-ppp0: using channel 2
L1: U 21/04/2010 11:27:13:080 PPP-vcc0-ppp0: Using interface ppp5
W2: U 21/04/2010 11:27:13:080 PPP-vcc0-ppp0: Connect: ppp5 <--> vcc0
L2: U 21/04/2010 11:27:13:080 PPP-vcc0-ppp0: sent [LCP ConfReq id=0x1 <mru 1492> <magic 0xac4abf66>]
L2: U 21/04/2010 11:27:13:130 PPP-vcc0-ppp0: rcvd [LCP ConfAck id=0x1 <mru 1492> <magic 0xac4abf66>]
L2: U 21/04/2010 11:27:16:090 PPP-vcc0-ppp0: sent [LCP ConfReq id=0x1 <mru 1492> <magic 0xac4abf66>]
```

L2: U 21/04/2010 11:27:16:130 PPP-vcc0-ppp0: rcvd [LCP ConfAck id=0x1 <mru 1492> <magic 0xac4abf66>]

L2: U 21/04/2010 11:27:19:100 PPP-vcc0-ppp0: sent [LCP ConfReq id=0x1 <mru 1492> <magic 0xac4abf66>]

L2: U 21/04/2010 11:27:19:140 PPP-vcc0-ppp0: rcvd [LCP ConfAck id=0x1 <mru 1492> <magic 0xac4abf66>]

L2: U 21/04/2010 11:27:22:110 PPP-vcc0-ppp0: sent [LCP ConfReq id=0x1 <mru 1492> <magic 0xac4abf66>]

L2: U 21/04/2010 11:27:22:150 PPP-vcc0-ppp0: rcvd [LCP ConfAck id=0x1 <mru 1492> <magic 0xac4abf66>]

L2: U 21/04/2010 11:27:25:120 PPP-vcc0-ppp0: sent [LCP ConfReq id=0x1 <mru 1492> <magic 0xac4abf66>]

L2: U 21/04/2010 11:27:25:170 PPP-vcc0-ppp0: rcvd [LCP ConfAck id=0x1 <mru 1492> <magic 0xac4abf66>]

L2: U 21/04/2010 11:27:28:130 PPP-vcc0-ppp0: sent [LCP ConfReq id=0x1 <mru 1492> <magic 0xac4abf66>]

L2: U 21/04/2010 11:27:28:180 PPP-vcc0-ppp0: rcvd [LCP ConfAck id=0x1 <mru 1492> <magic 0xac4abf66>]

L2: U 21/04/2010 11:27:31:140 PPP-vcc0-ppp0: sent [LCP ConfReq id=0x1 <mru 1492> <magic 0xac4abf66>]

L2: U 21/04/2010 11:27:31:180 PPP-vcc0-ppp0: rcvd [LCP ConfAck id=0x1 <mru 1492> <magic 0xac4abf66>]

L2: U 21/04/2010 11:27:33:060 PPP-vcc0-ppp0: rcvd [LCP ConfReq id=0x2 <mru 1492> <auth pap> <magic 0x82c2761c>]

L2: U 21/04/2010 11:27:33:060 PPP-vcc0-ppp0: sent [LCP ConfAck id=0x2 <mru 1492> <auth pap> <magic 0x82c2761c>]

L2: U 21/04/2010 11:27:33:060 PPP-vcc0-ppp0: sent [LCP EchoReq id=0x0 magic=0xac4abf66]

L2: U 21/04/2010 11:27:33:060 PPP-vcc0-ppp0: sent [PAP AuthReq id=0x1 user="aliceadsl" password=<hidden>]

L2: U 21/04/2010 11:27:33:100 PPP-vcc0-ppp0: rcvd [LCP EchoRep id=0x0 magic=0x82c2761c]

L2: U 21/04/2010 11:27:33:170 PPP-vcc0-ppp0: rcvd [PAP AuthAck id=0x1 ""]

W2: U 21/04/2010 11:27:33:170 PPP-vcc0-ppp0: PAP authentication succeeded

W2: U 21/04/2010 11:27:33:170 PPP-vcc0-ppp0: peer from calling number 00:19:2F:C7:87:A8 authorized

L2: U 21/04/2010 11:27:33:170 PPP-vcc0-ppp0: sent [IPCP ConfReq id=0x1 <addr 0.0.0.0> <ms-dns1 0.0.0.0> <ms-dns3 0.0.0.0>]

L2: U 21/04/2010 11:27:33:170 PPP-vcc0-ppp0: rcvd [IPCP ConfReq id=0x1 <addr 192.168.100.1>]

L2: U 21/04/2010 11:27:33:170 PPP-vcc0-ppp0: sent [IPCP ConfAck id=0x1 <addr 192.168.100.1>]

L2: U 21/04/2010 11:27:33:210 PPP-vcc0-ppp0: rcvd [IPCP ConfNak id=0x1 <addr 79.3.36.75> <ms-dns1 85.37.17.57> <ms-dns3 85.38.28.80>]

L2: U 21/04/2010 11:27:33:210 PPP-vcc0-ppp0: sent [IPCP ConfReq id=0x2 <addr 79.3.36.75> <ms-dns1 85.37.17.57> <ms-dns3 85.38.28.80>]

L2: U 21/04/2010 11:27:33:260 PPP-vcc0-ppp0: rcvd [IPCP ConfAck id=0x2 <addr 79.3.36.75> <ms-dns1 85.37.17.57> <ms-dns3 85.38.28.80>]

W2: U 21/04/2010 11:27:33:270 PPP-vcc0-ppp0: local IP address 79.3.36.75

W2: U 21/04/2010 11:27:33:270 PPP-vcc0-ppp0: remote IP address 192.168.100.1

W2: U 21/04/2010 11:27:33:270 PPP-vcc0-ppp0: primary DNS address 85.37.17.57

W2: U 21/04/2010 11:27:33:270 PPP-vcc0-ppp0: secondary DNS address 85.38.28.80

L2: U 21/04/2010 11:27:33:270 PPP-vcc0-ppp0: Script /etc/ppp/ip-up started (pid 841)

L2: U 21/04/2010 11:27:33:360 PPP-vcc0-ppp0: Script /etc/ppp/ip-up finished (pid 841), status = 0x0

Index

ManPOTS

Pots-x – Commands

In POTS node you can configure the physical parameters of the POTS ports. The POTS ports usually work as FXS in Aethra IADs, but they can also work as FXO. In the first case, they are associated to a logical entity like for exemple voip “user terminal” (see relevant chapter below.

POTS ports support decadic pulse dialing.

```
ATOSNT\pots1>>set ?

Nodes not available.
Set command parameters:
 level of log                      [loglevel]             Current value: 1
 caller id type                    [cid-type]             Current value: fsk-v23
 caller id delay (msec)            [cid-delay]            Current value: 500
 hook flash time (msec)            [hookflash-time]       Current value: 200
 off hook recognition time (msec)  [off-hook-rec-time]    Current value: 150
 on hook recognition time (msec)   [on-hook-rec-time]     Current value: 200
 tx loop gain (db)                 [tx-loop-gain]         Current value: 0
 rx loop gain (db)                 [rx-loop-gain]         Current value: -7
 ring amplitude (vrms)             [ring-amplitude]       Current value: 38
 ring trip dup time (msec)         [ring-trip-dup-time]   Current value: 10
 dcdc speed                        [dcdc-speed]           Current value: fast
```

Table 1: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOS to log the events from the less detailed one (0) to the more detailed one (5). Default: [1]
cid-type [fsk-bell202|fsk-v23|dtmf]	Sets the standard for the caller identifier generation (one of the two fsk flavours or DTMF). Default: [fsk-v23]
cid-delay [0-2000] msec	Sets the time delay in msec the system waits after first ring and before starting CID generation. Default: [500]
hookflash-time [50-1000]	Sets the time in msec the hook must be kept on in order to recognize the flash request. Default: [200]
off-hook-rec-time [50-1000]	Sets the recognition time in msec of off hook condition . Default: [150]
on-hook-rec-time [50-1000] msec	Sets the recognition time of on hook condition . Default: [200]
tx-loop-gain [0 – 4] db	Sets signal gain in tx direction . Default: [0]
rx-loop-gain [(-11) – (-7)] db	Sets signal gain in rx direction . Default: [-7]
ring-amplitude (vrms) [37-45]	Sets the ring amplitude . Default: [38]
ring-trip-dup-time (msec) [10-24]	If available (based on CPE model), this parameter allows for a fine tuning of hardware working parameters related to ring trip issues (off-hook not correctly detected during ring tone transmission). The problem is detected by the customer like a bad noise when answering. In some very rare cases could be necessary to modify the value of this parameter from its default value. Default [10]

dcdc-speed [fast-slow]	If the parameter is available (based on CPE model), it regulates the rate of the current changes in off hook condition. Default: [fast]

An example of show status command when the port is allocated to some application (e.g. VoIP FXS)

ATOSNT\pots1>>show status
Status of pots1 interface
AB FXS port - FSM state = ACTIVE
Call 0 Descriptor
Status = ACTIVE
call id = 0
Call 1 Descriptor
Status = IDLE
call id = NOT ALLOCATED

Index

ManISDNPRI

PRI1 - Overview

On **pri1** node it is possible to configure an **ISDN PRI** physical interface.

The **Primary Rate Interface** (PRI) is the telecommunications interface standard used on **ISDN (Integrated Services Digital Network)** to carry multiple voice and data transmissions between the network and a user.

PRI is the standard for providing telecommunication services to offices. It is based on the E-carrier (**E1**) line in Europe. In North America and japan, the T1 line consists of 24 channels, while an E1 has 32.

In Europe and Australia, PRI consists of 30xB channels + 2xD on an **E1 2.048 Mbit/s**. One timeslot on the E1 is used for synchronization purposes and is not considered to be a B or D channel.

B channels or bearer channels are 64 kbit/s digital channels; instead D channel is the delta channel at 64 kbit/s used for signaling/control channel.

PRI1 - Commands

On **pri1** node there are available the following commands and the following parameters

```
ATOS\pri1>>set ?

Nodes not available.
Set command parameters:
 level of log          [loglevel]       Current value: 1
 crc4                  [crc4]           Current value: on
 clock mode            [clockmode]      Current value: master
 ber alarm threshold   [ber-threshold]  Current value: OFF
```

Table 1: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record PRI ISDN events. Default: 1
crc4 [on|off]	Enables/disables CRC4 (Cyclic Redundancy Code 4) synchronization. Default: on CRC-4 is a form of cyclic redundancy checking, a method of checking for errors in transmitted data, that is used on E1 trunk lines. Certain ISDN signalling protocols utilise CRC4 by default. As referred CRC4 checking is a means of determining if an error has occurred in received data.
clockmode [master|slave]	• master the CPE provides the clock signal • slave the device obtains its clock signal from its peer device, a clock master. Default: master
ber-threshold [1E-4|5E-5|1E-5|5E-6|1E-6|OFF]	Specifies the bit error ratio (BER) alarm threshold Default: OFF

```
ATOS\pri1>>show work
Show of ATOS pri1
Level of log         : 1
Crc4                 : on
Clock Mode           : master
BER alarm threshold  : OFF

Command executed
```

```
ATOS\pri1>>show status

Status of pri1 interface
Is used

Command executed
```

Once you have configured the PRI ISDN physical interface, you should go to **ISDN** node to add a new PRI interface Index

ManPtm

PTM Configuration

PTM stands for Packet Transfer Mode. PTM is based on the Ethernet in the First Mile (EFM) IEEE802.3ah standard. The PTM mode transports Ethernet packets over the SHDSL lines.

PTM - Commands

```
ATOSNT\ptm>>set ?

Available nodes:
                        ptm0

Set command parameters:
  level of log  [loglevel]  Current value: 1
```

*Table 1:***set**

Syntax	Description
loglevel <0-5>	Set the level detail used by ATOS to log the events [default 1]

PTM - Node

You can show the structure of the PTM node using the **tree** command

```
ATOSNT\ptm>>tree
ptm                     ptm0
```

PTM0 - Commands

In the PTM0 subnode, there are visible the log level and send buffer parameter:

```
ATOSNT\ptm\ptm0>>set ?

Nodes not available.
Set command parameters:
  level of log         [loglevel]     Current value: 1
  send buffer (bytes)  [send-buffer]  Current value: auto
```

*Table 2:***set**

Syntax	Description
loglevel <0-5>	Set the level detail used by ATOS to log the events
send-buffer [1-256000|auto]	Send buffer is the parameter that allows to dimension the size of a buffer developed to adapt the fast internal data transfer speed to the slower physical link and thus to reduce the latency [default auto]

PTM0 Configuration example

```
ATOSNT\ptm\ptm0>>show
conf
Show of ATOSNT ptm ptm0
Level of log : 1
Physical Port : shdsl0.0
Send buffer (bytes) : auto
```

PTM0 Status example

```
ATOSNT\ptm\ptm0>>show status
status of ptm port ptm0
state : up
rate : 5696 kbps
```

ManQoS

QoS Overview

The term **"Quality of Service"** generally refers to a set of mechanisms that provide an optimal bandwidth utilization when different traffic types share a single communication link.

IP data networks traditionally provide a kind of "best effort" services, which may result in large delays, unpredictable transmission times ("jitter") and in some cases in packets loss. These impairments may be acceptable for some traffic types, for example when browsing an Internet site or when downloading a bulk file, but they may instead heavily affect some other traffic flows, such as voice, video or highly transactional or interactive data traffic.

For example, the small packets of a voice traffic flow are produced at a regular pace and require fast and timely service, while most types of bulk data traffic are composed of large packets with a "bursty" emission pattern. If these two traffics share a single communication path, it may happen that a voice packet may be queued behind multiple large packets and then it must be waiting for them to be forwarded, thus generating some variable amount of delay ("jitter").

Additionally, a communication node may become congested at some time due to heavy traffic conditions and it may decide to drop packets. Again, data traffic is much more resilient to packet loss than voice traffic, where instead the loss of a single voice packet may propagate into hundreds of milliseconds of corrupted speech.

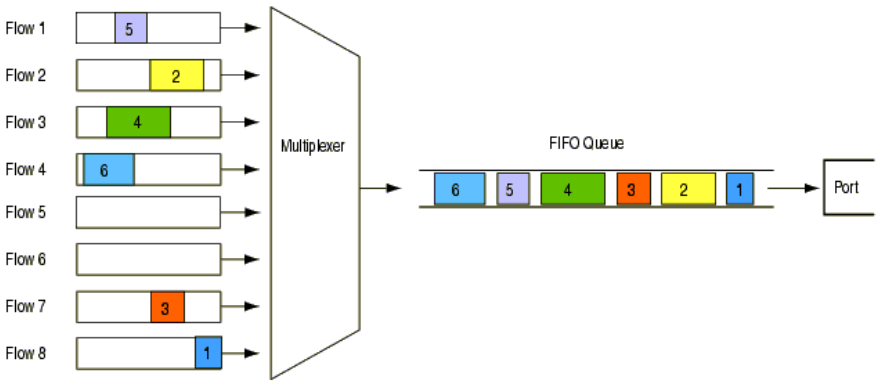
As long as the available end-to-end bandwidth is largely exceeding the actual data rates, these problems are minimized, but when the bandwidth becomes scarce, it becomes necessary to use some Quality of Service mechanisms. For example, QoS may provide a communication node with a mean to distinguish among the different traffic types, so that it may put packets from different flows into separate queues and properly schedule transmission from each queue or even select which packets are to be preferentially dropped when the node enters into a congested state.

	*QoS does not actually provide additional bandwidth; it only guarantees an optimal usage of the available bandwidth.*

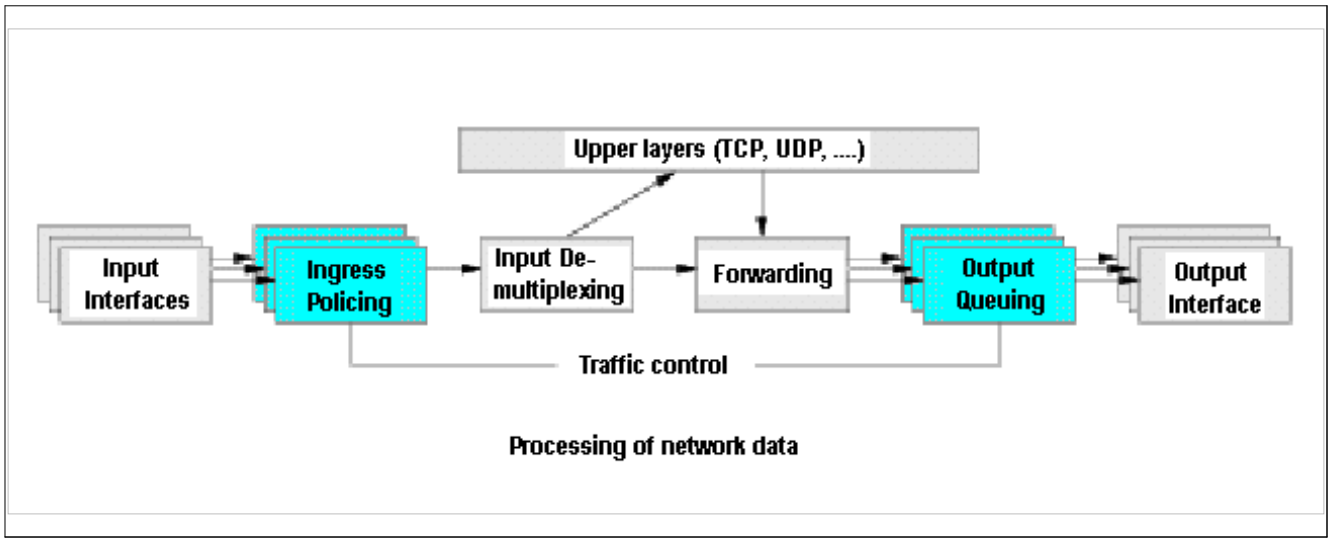
QoS is sometimes referred to as traffic control, or traffic shaping.

Traffic control is the name given to the sets of queuing systems and mechanisms by which packets are received and transmitted on a router. This includes deciding which (and whether) packets to accept at what rate on the input of an interface and determining which packets to transmit in what order at what rate on the output of an interface.

In the overwhelming majority of situations, traffic control consists of a single queue which collects entering packets and dequeues them as quickly as the hardware can accept them. This sort of queue is a **FIFO (First-in, first-out)**, see the bellow figure.



Under Linux kernel, the two major blocks of the traffic control are **Ingress Policing** and **Output Queuing** as you can see in the bellow figure.



Packets arrive on via an input interface, where they may be policed. **Policing** discards undesirable packets, e.g. if traffic is arriving too fast. After policing, packets are either directly forwarded to the network (e.g. on a different interface, if the machine is acting as a router or a bridge), or they are passed up to higher layers in the protocol stack (e.g. to a transport protocol like UDP or TCP) for further processing.

"Forwarding" includes the selection of the output interface, the selection of the next hop, encapsulation, etc. Once all this is done, packets are **queued** on the respective output interface. This is the second point where traffic control comes into play.

Traffic control can, among other things, decide if packets are queued or if they are dropped (e.g. if the queue has reached some length limit, or if the traffic exceeds some rate limit), it can decide in which order packets are sent (e.g. to give priority to certain flows), it can delay the sending of packets (e.g. to limit the rate of outbound traffic), etc. Once traffic control has released a packet for sending, the device driver picks it up and emits it on the network.

The following elements of traffic control have been implemented and supported by ATOSNT :
MARKING, DROPPING, CLASSIFYING, SCHEDULING, SHAPING and POLICING

MARKING

Marking is a mechanism by which the packet is altered. Traffic control marking mechanisms install a DSCP on the packet itself, which is then used and respected by other routers inside an administrative domain (usually for DiffServ). It operates both **inbound** and **outbound**.

DROPPING

Dropping is the mechanism by which a packet is discarded. It operates in **outbound**.

CLASSIFYING

Classifying is the mechanism by which packets are separated for different treatment, possibly different output queues. Classification can include marking the packet, which usually happens on the boundary of a network under a single administrative control or classification can occur on each hop individually.

SHEDULING

Scheduling is the mechanism by which packets are arranged between input and output of a particular queue. It operates in **outbound**. The most commom (and the default) scheduler is the FIFO (first-in first-out) scheduler.

SHAPING

Shaping is the mechanism by which packets are delayed before transmission in an output queue to meet a desired output rate. It operates in **outbound**.

Shapers attempt to limit or ration traffic to meet but not exceed a configured rate (frequently measured in packets per second or bits/bytes per second). As a side effect, shapers can smooth out bursty traffic . One of the advantages of shaping bandwidth is the ability to control latency of packets.

POLICING

Policing is a mechanism by which **inbound** traffic can be limited. A policer will accept traffic to a certain rate, and then perform an action on traffic exceeding this rate. A rather harsh solution is to drop the traffic, although the traffic could be reclassified instead of being dropped. A policer is a yes/no question about the rate at which traffic is entering a queue. If the packet is about to enter a queue below a given rate, take one action (allow the enqueuing). If the packet is about to enter a queue above a given rate, take another action. Although the policer uses a token bucket mechanism internally, it does not have the capability to delay a packet as a shaping mechanism does.

Traffic Control Components

The traffic control components are:

- **Policies**
- **Queues**
- **Classifiers**

Correlation between traffic control elements and Linux components

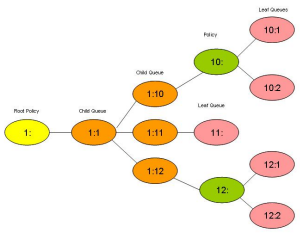
TC Elements	Components
Scheduling	A **Policy** is a scheduler. Schedulers can be simple as the FIFO or complex, containing *Queues* and other *Policies* such as HTB
Shaping	The **Queue** offers shaping capabilities
Classifying	The role of the **Classifier** is to classify packets. Classifiers allow the user to classify packets into an output queue with several different classifiers or a single classifier
Policing	A **policer** is a part of a Classifier. A policer calls one action above and another action bellow the specified rate. Although both policing and shaping are basic elements of traffic control for limiting bandwidth usage a policer will never delay traffic.
Dropping	To **drop** traffic requires a *classifier* with a *policer* which uses drop as an action
marking	The dsmark policy is used for marking

POLICY Definition

The **Policy** is the major building block on which traffic control is built. A Policy is basically the management of different output queues in which packets are classified for each output device interface . The policy establishes the order in which the packets will be picked up by the various queues. This operation defined **scheduling** could lead to decide that some packets must be transmitted before others due to the specific needs of the traffic class to which they belong.

Queues Hierarchy

Under Linux, there are a **Queues Hierarchy** as described in the bellow example



The concept of **Single Queue Policy** and **Multi Queue Policy** should be distinguished.

A **Single Queue Policy** is a Policy that does not include any other Policies or Queues while a **Multi Queue Policy** may be expected to have more Queues inside which in turn may contain Policies.

Single Queue Policies

Single Queue Policies are the fundamental schedulers and can be used as the primary policy on an interface, or can be used inside a leaf queue of a Multi Queue Policy.

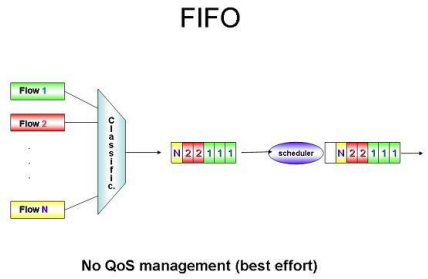
Note that **the default scheduler under Linux** is the **pfifo_fast**.

These are the fundamental schedulers used under Linux:

- **FIFO**
- **pfifo_fast**
- **SFQ**
- **TBF**
- **RED**

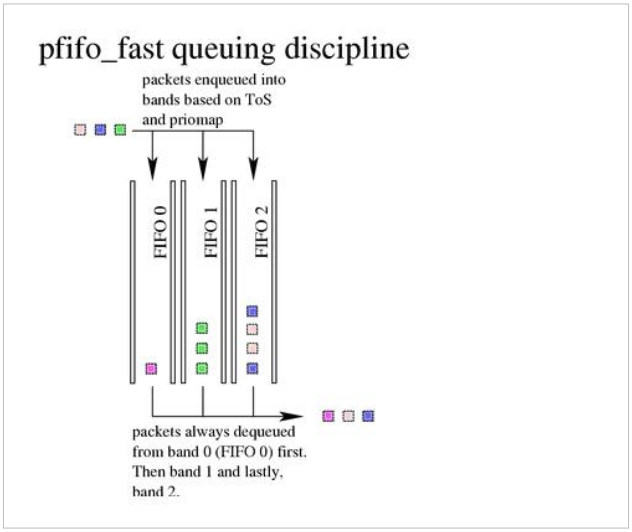
FIFO, First-In First-Out

FIFO queuing is the most basic scheduler or Policy. In FIFO queuing, all packets are treated equally by placing them into a single queue, and then servicing them in the same order that they were placed into the queue.



pfifo_fast, the DEFAULT POLICY for all interfaces

The default policy for any Network Interface Card is the **pfifo_fast**. This policy is based on a FIFO, but provides some prioritization due to the **bands** concept. The policy provides three different bands (individual FIFOs) for separating traffic. The highest priority traffic (e.g. interactive flows) are placed into **band 0** and are always serviced first. Similarly, **band 1** is always emptied of pending packets before **band 2** is dequeued.



Incoming traffic is classified and separated into the 3 bands based on TOS field of the packet IP Header.
In the bellow figure you can see a mapping between different traffic classes, the bands (band 0 is the highest priority, then band 1 and lastly band 2) and the associated priority:

TOS 4-bit Combination values

TOS	Decimal	Meaning	Traffic Class	Priority	Band
0x0	0	Normal Service	0	Best Effort	1
0x2	1	Minimize Monetary Cost (mc)	1	Filler	2
0x4	2	Maximize Reliability (mr)	0	Best Effort	1
0x6	3	mc+mr	0	Best Effort	1
0x8	4	Maximize Throughput (mt)	2	Bulk	2
0xa	5	mc+mt	2	Bulk	2
0xc	6	mr+mt	2	Bulk	2

0xe	7	mc+mt+mt	2	Bulk	2
0x10	8	Minimize Delay (md)	6	Interactive	0
0x12	9	mc+md	6	Interactive	0
0x14	10	mr+md	6	Interactive	0
0x16	11	mc+md+mr	6	Interactive	0
0x18	12	mt+md	4	Int. Bulk	1
0x1a	13	mc+md+mt	4	Int. Bulk	1
0x1c	14	mr+mt+md	4	Int. Bulk	1
0x1e	15	mc+mr+mt+md	4	Int. Bulk	1

Multi Queue Policies

The following are the Multi Queue Policy developed by ATOSNT. You can learn more about them in the next paragrahs.

- **PRIO**
- **DRR**
- **GRED**
- **CBQ**
- **HTB**
- **NATIVE**

QoS Configuration

QoS– Nodes

Under QoS node, the CLI defines three dynamic objects:

- **CLASSIFIER**

  defines the criteria used to identify, classify and separate the incoming packets into traffic classes.
  Classification criteria are based on:

  - The examination of the IP Header fields (protocol, TOS, DSCP, etc)
  - Layer 3 and Layer 2 protocols and parameters
  - CLASSIFIER-MAP defined under **Classifier Map** node and
  - BRIDGE-CLASSIFIER defined under **Bridges-node**.

- **POLICY**

  defines the set of QoS actions applied to one or multiple traffic classes;

- **SERVICE**

  binds a policy to an interface either in inbound or outbound direction.

Once classifiers and policies are defined, the user creates one or more associations to bind a policy to an interface and a direction.

In this way all packets belonging to certain traffic classes and arriving from (or destined to) an interface are subjected to the QoS actions specified by the policy bound to that interface.

In **qos** node, you can use set, add and del commands to configure the following parameters:

```
ATOSNT\qos>>set ?
```

```
Available nodes:
                        p-fifo-default
                        b-fifo-default

Set command parameters:
 level of log  [loglevel]  Current value: 1
```

Table 1: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the QoS events Default: 1

p-fifo-default and **b-fifo-default** are the simplest policies available in **qos** node; both are based on FIFO queues:

- pfifo is **packet** limited First In-First Out queue
- bfifo is **byte** limited First In-First Out queue

p-fifo-default and b-fifo-default can be modified as any policy:

```
ATOSNT\qos>>set p-fifo-default?

Nodes not available.
Set command parameters:
 level of log           [loglevel]         Current value: 1
 description            [description]      Current value:
 mean rate window (sec) [mean-rate-window] Current value: 0
 packets number         [packets-number]   Current value: 128
```

Table 2: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the QoS events . Default: 1
description [max 100 char]	Descriptive string of the created POLICY.
mean-rate-window (sec) [0-60]	Mean rate observation window. Default: 0 (disabled).
packets-number [16-10000]	Maximum queue size in packets. Default: 128.

```
ATOSNT\qos>>set b-fifo-default?

Nodes not available.
Set command parameters:
 level of log           [loglevel]         Current value: 1
 description            [description]      Current value:
 mean rate window (sec) [mean-rate-window] Current value: 0
 bytes number           [bytes-number]     Current value: 128000
```

Table 3: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the QoS events . Default: 1
description [max 100 char]	Descriptive string of the created POLICY.
mean-rate-window (sec) [0-60]	Mean rate observation window. Default: 0 (disabled).
bytes-number [2048-100000000]	Maximum queue size in bytes. Default: 128000 (bytes).

With **show conf** command, you can see a configuration example of the two mentioned policies.

```
ATOSNT\qos>>show conf

Show of ATOSNT qos
  Level of log : 1

LIST OF SERVICES
 Empty list

Show of ATOSNT qos p-fifo-default
 Level of log   : 1
 Description    :
 Type           : LIMIT
 Sub type       : P-FIFO
 Packets number : 128

LIST OF ACTIONS
  Empty list

Show of ATOSNT qos b-fifo-default
 Level of log : 1
 Description  :
 Type         : LIMIT
 Sub type     : B-FIFO
 Bytes number : 128000

LIST OF ACTIONS
 Empty list

Command executed
```

To add or delete a new **CLASSIFIER**, **POLICY** or **SERVICE**, you should use **add** and **del** commands respectevely :

```
ATOSNT\qos>>add ?
```

```
Available nodes:
                        p-fifo-default
                        b-fifo-default
add  help:  Add a new CLASSIFIER or POLICY or SERVICE list
add  usage:
 <CLASSIFIER>[name][type]
 <POLICY>[name][type][sub-type]
 <SERVICE><ifc-name><policy-name>[direction]

add command parameters:
 CLASSIFIER
 POLICY
 SERVICE
```

```
ATOSNT\qos>>del ?

Available nodes:
                        p-fifo-default
                        b-fifo-default
del  help :  Remove CLASSIFIER or POLICY or SERVICE list
del  usage:
 <CLASSIFIER><name>
 <POLICY><name>
 <SERVICE><ifc-name><policy-name>[direction]

del command parameters:
 CLASSIFIER
 POLICY
 SERVICE

ATOSNT\qos>>add CLASSIFIER ?

add command parameters:
 name           [max 16 char]
 type           [MATCH-ANY|MATCH-ALL]
 <cr>
```

Table 4: add CLASSIFIER

Syntax	Description
name [max 16 char]	Descriptive string of the created CLASSIFIER.
type [MATCH-ANY|MATCH-ALL]	Indicates the critera for the traffic classification: • MATCH-ALL indicates that all rules must occur • MATCH-ANY indicates that at least one rule must occur. Default: MATCH-ALL.

If the Classifier name is not specified, a classifier will be created with index sequence (**classifier0, classifier1….**).

```
ATOSNT\qos>>add POLICY ?

add command parameters:
 name     [max 16 char]
 type     [MARKING|LIMIT|PRIORITY|SCHEDULE|SHAPING|POLICING]
 <cr>
```

Table 5: add POLICY

Syntax	Description
name [max 16 char]	Descriptive string of the created POLICY.
type [MARKING|LIMIT| PRIORITY|SCHEDULE|SHAPING |POLICING]	Indicates the QoS actions to apply to the traffic classes: • MARKING is the action of marking the packets. In a Diffserv network, edge routers use to classify packets and mark them with either the IP Precedence or DSCP value. Other network devices in the core use the DSCP value in the IP header to select a PHB behavior for the packet and provide the appropriate QoS treatment. • LIMIT is the action of limiting (in packets or bytes) the queue size. It is applied to the Single Queue Policy like P-FIFO, B-FIFO and RED • PRIORITY is the action to prioritize the output traffic based on the use of specified filters • SCHEDULE is the action to prioritize the outbound traffic defining which packets and in which order they will be dequeued • SHAPING is the action to define the output packets transmission rate, it means the bandwith limitation or the maximum burst length • POLICING is the action to classify incoming traffic and to define traffic profile rules to decide what to do when they are in-profile or out-of-profile (drop)

If Policy name is not specified, a policy will be created with index sequence (**policy0, policy1…**).

```
ATOSNT\qos>>add SERVICE ?

add command parameters:
```

```
 ifc name      [eth0|loopback0]

ATOSNT\qos>>add SERVICE eth0 ?

add command parameters:
 policy name   [p-fifo-default|b-fifo-default|prio]
ATOSNT\qos>>add SERVICE eth0 prio ?

Command complete (enter cr)
ATOSNT\qos>>add SERVICE eth0 prio
The service is not active: the policy configuration is not complete or incompatible with interface
Command executed
```

Table 6: add SERVICE

Syntax	Description
ifc name [eth0|loopback0]	Sets the interface name to deliver the service
policy name [p-fifo-default|b-fifo-default|prio]	Sets the name of the policy to apply to the interface

Except for MARKING and POLICING, with **POLICY** you can define sub-types of policies, see bellow.

```
ATOSNT\qos>>add POLICY LIMIT?

add command parameters:
 sub type [P-FIFO|B-FIFO|RED]
 <cr>

ATOSNT\qos>>add POLICY PRIORITY?

add command parameters:
 sub type [PRIO]
 <cr>

ATOSNT\qos>>add POLICY SCHEDULE?

add command parameters:
 sub type [SFQ|DRR|GRED]
 <cr>

ATOSNT\qos>>add POLICY SHAPING?

add command parameters:
 sub type [TBF|CBQ|HTB]
 <cr>
```

CLASSIFIER - Commands

In each classifier node you can configure the following parameters:

```
ATOSNT\qos\classifier0>>set ?

Nodes not available.
Set command parameters:
 description  [description]  Current value:
 type         [type]         Current value: MATCH-ANY
```

Table 7: set

Syntax	Description
description [max 100 char]	Descriptive string of the created CLASSIFIER.
type[MATCH-ANY|MATCH-ALL]	Two different match types can be applied to the rules list: • MATCH-ALL requires that all the listed rules must be matched • MATCH-ANY requires that at least one of the listed rules must be matched

Defining the RULES to classify and separate the incoming packets into traffic classes

Under each Classifier node, add command is used to specify a new rule.

Each classification rule is based on:

- The examination of the IP Header fields (protocol, TOS, DSCP, etc)
- Layer 3 and Layer 2 protocols and parameters
- CLASSIFIER-MAP defined under **Classifier Map** node and
- BRIDGE-CLASSIFIER defined under **Bridges-node**.

```
ATOSNT\qos\classifier0>>add ?

add  help :  Add a new rule
add  usage:
 <CLASSIFIER-MAP><name>[priority]
 <PROTOCOL><TCP|UDP|ICMP|protocol-id>[priority]
 <IP-HDR><match-type><parameters>[priority]
 <DSCP><value>[priority]
 <PREC><value>[priority]
 <TOS><value>[priority]
 <NETWORK-PROTOCOL><IPv4|ARP|802.1Q|protocol-id>[priority]
 <HDR><match-type><parameters>[priority]
 <MAC-HDR><match-type><parameters>[priority]
 <VLAN-ID><value>[priority]
 <VLAN-PRIO><value>[priority]
 <BRIDGE-CLASSIFIER><name>[priority]
 <POLICY-MARKER><value>[priority]

add command parameters:
```

```
type              [CLASSIFIER-MAP|PROTOCOL|IP-HDR|DSCP|PREC|TOS|NETWORK-PROTOCOL|
                  HDR|MAC_HDR|VLAN-ID|VLAN-PRIO|BRIDGE-CLASSIFIER|POLICY-MARKER]
```

In the following paragraphs, you can find how to create a new classification rule:

- Rule based on a Classifier Map defined on **classifier-map** node

Table 8: add CLASSIFIER-MAP

Syntax	Description
CLASSIFIER-MAP	Keyword
name [string]	The name of the CLASSIFIER MAP created on classifier-map node.
priority [1-65535]	Indicates the rules order to be processed.

- Rule based on the **protocol** field of the IP Header.

Protocol field identifies the next higher level protocol. Incoming packets with TCP, UDP and ICMP protocol type or protocol number (TCP and UDP are identified by numbers 6 and 17 respectively) will be separated in a certain traffic class and futherly be subjected to a QoS Policy.

Table 9: add PROTOCOL

Syntax	Description
PROTOCOL	Keyword
protocol id [1-254|tcp|udp|icmp]	Sets the higher level protocol type or the protocol number.
priority [1-65535]	Indicates the rules order to be processed.

- Rule based on **match type** of the following IP Header fields.

Table 10: add IP-HDR

Syntax	Description
IP-HDR	Keyword. IP-HDR stands for IP Header
match type[SRC|DST|SPORT|DPORT|TOS|U32|U16|U8]	Sets a filter for packets that match: • SRC: source IP address [aa.bb.cc.dd/0-32] • DST: destination IP address [aa.bb.cc.dd/0-32] • SPORT: source port id [0-65535] mask-16bit [0-FFFF hex] • DPORT: destination port id [0-65535] mask-16bit [0-FFFF hex] • TOS: type of service, value-8bit [0-FF hex] mask-8bit [0-FF hex] • U32: value-32bit [0-FFFFFFFF hex], it is the full IP header mask-32bit [0-FFFFFFFF hex], Indicates a range hdr-offset [0-255] identifies where is located in the IP header • U16: value-16bit [0-FFFF hex] mask-16bit [0-FFFF hex] hdr-offset [0-255] • U8: value-8bit [0-FF hex]

	mask-8bit [0-FF hex] hdr-offset [0-255]
priority [1-65535]	Indicates the rules order to be processed.

- Rule based on **DSCP** field of the IP Header.

DSCP stands for Differenciated Services CodePoint [6 bits= PREC(3 bits)+ TOS (first 3 bits)]

Table 11: add DSCP

Syntax	Description
DSCP	Keyword
value [0-63]	DSCP value
priority [1-65535]	Indicates the rules order to be processed.

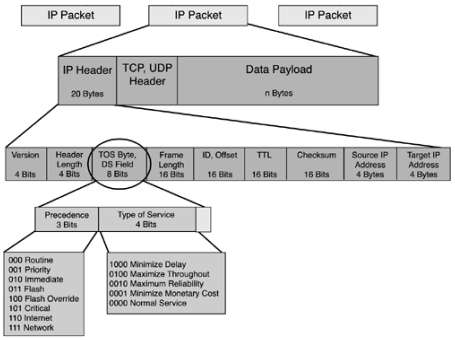
- Rule based on **PREC** "Precedence" flag (3 bits) of the IP Header.

Table 12: add PREC

Syntax	Description
PREC	Keyword
value [0-7]	PREC value
priority [1-65535]	Indicates the rules order to be processed.

- Rule based on **TOS** "Type of Service" field (8 bits) of the IP Header.

Look at the picture



TOS 4-bit values

Binary	Decimal	Meaning
1000	8	Minimize Delay (md)
0100	4	Maximize Throughput (mt)
0010	2	Maximize Reliability (mr)
0001	1	Minimize Monetary Cost (mc)
0000	0	Normal Service

TOS 4-bit Combination values

TOS	Decimal	Meaning
0x0	0	Normal Service
0x2	1	Minimize Monetary Cost (mc)
0x4	2	Maximize Reliability (mr)
0x6	3	mc+mr
0x8	4	Maximize Throughput (mt)
0xa	5	mc+mt
0xc	6	mr+mt
0xe	7	mc+mt+mt
0x10	8	Minimize Delay (md)
0x12	9	mc+md
0x14	10	mr+md
0x16	11	mc+md+mr
0x18	12	mt+md
0x1a	13	mc+md+mt
0x1c	14	mr+mt+md
0x1e	15	mc+mr+mt+md

Table 13: add TOS

Syntax	Description
TOS	Keyword
value [minimize-delay|maximize-throughput|maximize-reliability |minimize-monetary-cost|normal-service]	TOS value identifies what are the requirements of the application that is sending the packet: • Minimize Delay • Maximize Throughput • Maximize Reliability • Minimize monetary cost • Normal Service
priority [1-65535]	Indicates the rules order to be processed.

- Rule based on **Layer 2** and **Layer 3** protocols and parameters

Table 14: add NETWORK-PROTOCOL

Syntax	Description
NETWORK PROTOCOL	Keyword
network protocol [0-FFFF hex|IPv4|ARP|802.1Q| X25|PPPoE-Discovery|PPPoE-Session]	Traffic classification is based on: • L3 protocol number • IP packets version 4 • ARP protocol • the 3-bit field (Class of Service) in the IEEE 802.1Q header • X.25 layer 2 protocol • PPPoE Discovery as one of the stages in a PPP session (identifies the remote peer destination MAC address) • PPPoE Session as PPPoE discovery takes part of a PPP session
priority [1-65535]	Indicates the rules order to be processed.

- Rule based on a **Header** "match type" of the IP packet or frame

Table 15: add HDR

Syntax	Description
HDR	Keyword
match type [U32|U16|U8]	• U32: value-32bit [0-FFFFFFFF hex] mask-32bit [0-FFFFFFFF hex], indicates a range hdr-offset [0-255] identifies the starting point in the IP header or frame • U16: value-16bit [0-FFFF hex] mask-16bit [0-FFFF hex] hdr-offset [0-255] • U8: value-8bit [0-FF hex] mask-8bit [0-FF hex] hdr-offset [0-255]
priority [1-65535]	Indicates the rules order to be processed.

- Rule based on a **MAC HDR** "match type" of the L2 Ethernet frame

MAC address is a unique identifier of each manufactured Network Interface Card. The MAC address format is composed of 48-bits.

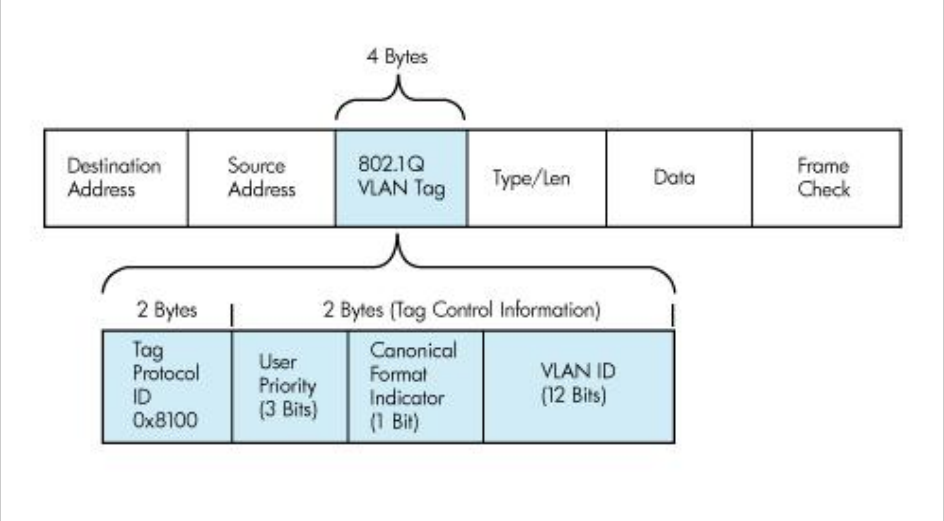
Table 16: add MAC_HDR

Syntax	Description
MAC HDR	Keyword
match type [U32|U16|U8]	• U32: value-32bit [0-FFFFFFFF hex] matches 32 bits of the total 48 defined in the MAC address mask-32bit [0-FFFFFFFF hex], indicates a range hdr-offset [0-255] identifies the starting point in the frame • U16: value-16bit [0-FFFF hex] mask-16bit [0-FFFF hex] hdr-offset [0-255] • U8: value-8bit [0-FF hex] mask-8bit [0-FF hex] hdr-offset [0-255]

priority [1-65535]	Indicates the rules order to be processed.

- Rule based on a **VLAN ID** and **VLAN PRIO** of the L2 Ethernet frame

When the frame is tagged with the 802.1Q, 4 bytes are added to the L2 frame header, as you can see in the bellow figure.



- User priority field (3 bits)

  is used to classify the VLAN traffic

- VLAN ID (12 bits)

  allows to identify the VLAN (from 0 to 4094 VLANs can be created)

It identifies and separates the VLAN frames based on the defined VLAN id

Table 17: add VLAN-ID

Syntax	Description
VLAN-ID	Keyword
vlan id [1-4094]	VLAN identifier
priority [1-65535]	Indicates the rules order to be processed.

It identifies and separates the VLAN frames based on the defined VLAN PRIO

Table 18: add VLAN-PRIO

Syntax	Description
VLAN-PRIO	Keyword
vlan priority [0-7]	VLAN priority
priority [1-65535]	Indicates the rules order to be processed.

- Rule based on a **BRIDGE-CLASSIFIER** defined on **Bridges-Node** section under Bridge node.

Table 19: add BRIDGE-CLASSIFIER

Syntax	Description
BRIDGE-CLASSIFIER	Keyword
name [empty list]	The name of the BRIDGE-CLASSIFIER created on "Bridges-Node" section under Bridge node.
priority [1-65535]	Indicates the rules order to be processed.

- Rule based on **POLICY-MARKER** of the flow configured in POLICY POLICING

Table 19.1: add POLICY-MARKER

Syntax	Description
POLICY-MARKER	Keyword
value [1-65535]	Allows to classify the incoming traffic flow configured in POLICY POLICING and to send it to the desired queue
priority [1-65535]	Indicates the rules order to be processed.

POLICY - Commands

Except for the marking and policing, policy can define subtypes of policies:

MARKING

```
ATOSNT\qos>>add POLICY MARKING
Command executed
```

A new node **policy0** has been created where you can configure the following parameters with set, add and del commands.

```
ATOSNT\qos\policy0>>set ?

Nodes not available.
Set command parameters:
level of log  [loglevel]     Current value: 1
description   [description]  Current value:
```

Table 20: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the Policy events. Default: 1
description	Descriptive string of the created POLICY.

The following commands can be used to mark or remak the incoming traffic identified by the classifiers defined above:

```
ATOSNT\qos\policy0>>add ?

add  help:  Add a new action
add  usage:
```

```
 <marking-type><value><classifier-name>

add command parameters:
 marking type    [DSCP|PREC|TOS|VLAN_PRIO]
```

Table 21: add DSCP

Syntax	Description
DSCP	Keyword
value [0-63]	DSCP value
classifier-name	Sets the name of the classifier associated.

Table 22: add PREC

Syntax	Description
PREC	Keyword
value [0-7]	PREC value
classifier-name	Sets the name of the classifier associated.

Table 23: add TOS

Syntax	Description
TOS	Keyword
value [minimize-delay|maximize-throughput|maximize-reliability |minimize-monetary-cost|normal-service]	TOS value identifies what are the requirements of the application that is sending the packet: • Minimize Delay • Maximize Throughput • Maximize Reliability • Minimize monetary cost • Normal Service
classifier-name	Sets the name of the classifier associated.

Table 24: add VLAN_PRIO

Syntax	Description
VLAN-PRIO	Keyword
value [0-7]	VLAN priority value
classifier-name	Sets the name of the classifier associated.

Use **del** command to delete the action of marking applied to the streams identified by the classifiers. If you do not specify the classifier, the command will delete all entries identified by the marking-type specified.

```
ATOSNT\qos\policy0>>del ?

del  help :  Remove an action
del  usage:
 <marking-type><value><classifier-name>
```

```
del command parameters:
 marking type    [DSCP|PREC|TOS|VLAN_PRIO]
```

LIMIT

LIMIT is the action of limiting (in packets or bytes) the queue size. For POLICY LIMIT type, you should specify the subtype (default P-FIFO).

```
ATOSNT\qos>>add POLICY LIMIT ?

add command parameters:
 sub type [P-FIFO|B-FIFO|RED]
 <cr>
```

P-FIFO

```
ATOSNT\qos>>add POLICY LIMIT P-FIFO
Command executed
```

A new node **policy1** has been created, look at the result with **tree** command.

```
ATOSNT\qos>>tree
qos                    p-fifo-default
                       b-fifo-default
                       classifier0
                       prio0                    best-effort
                                                queue0
                       policy0
                       policy1
```

Under policy1 node you can configure the following parameters:

```
ATOSNT\qos\policy1>>set ?

Nodes not available.
Set command parameters:
 level of log            [loglevel]          Current value: 1
 description             [description]       Current value:
 mean rate window (sec)  [mean-rate-window]  Current value: 0
 packets number          [packets-number]    Current value: 128
```

Table 25: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the Policy events. Default: 1
description	Descriptive string of the created POLICY.
mean-rate-window (sec) [0-60]	Sets the mean rate observation window Default: 0
packets-number [16-10000]	Sets the queue size in packets. Default: 128

B-FIFO

```
ATOSNT\qos>>add POLICY LIMIT B-FIFO
Command executed
```

A new node **policy2** has been created.

Under policy2 node you can configure the following parameters:

```
ATOSNT\qos\policy2>>set ?

Nodes not available.
Set command parameters:
 level of log            [loglevel]          Current value: 1
 description             [description]       Current value:
 mean rate window (sec)  [mean-rate-window]  Current value: 0
 bytes number            [bytes-number]      Current value: 128000
```

Table 26: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the Policy events. Default: 1
description	Descriptive string of the created POLICY.
mean-rate-window (sec) [0-60]	Sets the mean rate observation window Default: 0
bytes-number [2048-100000000]	Sets the queue size in bytes. Default: 128000

The following commands can be used to mark or remak the incoming traffic identified by the classifiers defined above:

```
ATOSNT\qos\policy1 or policy2>>add ?

add  help:  Add a new action
add  usage:
 <marking-type><value><classifier-name>
```

```
add command parameters:
 marking type    [DSCP|PREC|TOS|VLAN_PRIO]
```

Table 27: add DSCP

Syntax	Description
DSCP	Keyword
value [0-63]	DSCP value
classifier-name	Sets the name of the classifier associated.

Table 28: add PREC

Syntax	Description
PREC	Keyword
value [0-7]	PREC value
classifier-name	Sets the name of the classifier associated.

Table 29: add TOS

Syntax	Description
TOS	Keyword
value [minimize-delay|maximize-throughput|maximize-reliability |minimize-monetary-cost|normal-service]	TOS value identifies what are the requirements of the application that is sending the packet: • Minimize Delay • Maximize Throughput • Maximize Reliability • Minimize monetary cost • Normal Service
classifier-name	Sets the name of the classifier associated.

Table 30: add VLAN_PRIO

Syntax	Description
VLAN-PRIO	Keyword
value [0-7]	VLAN priority value
classifier-name	Sets the name of the classifier associated.

Use **del** command to delete the action of marking applied to the streams identified by the classifiers. If you do not specify the classifier, the command will delete all entries identified by the marking-type specified.

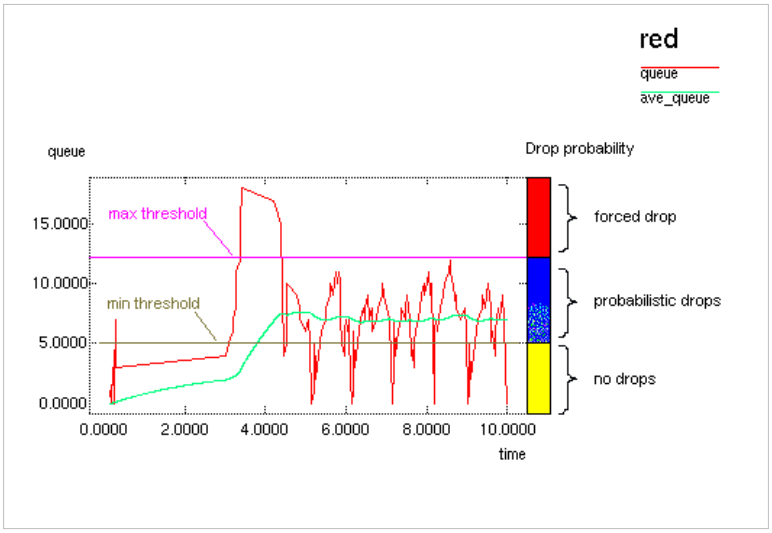
```
ATOSNT\qos\policy0 or policy2>>del ?

del  help :  Remove an action
del  usage:
 <marking-type><value><classifier-name>

del command parameters:
```

```
marking type    [DSCP|PREC|TOS|VLAN_PRIO]
```

RED

Random Early Detection (**RED**), also known as random early discard is a queuing algorithm based on the FIFO queue; FIFO queue is also known as **Drop Tail** queue. Drop-tail is the policy of dropping the arriving packet when the queue is full.

The idea behind RED is to provide, as soon as possible, a feedback to responsive flows (like TCP) before the queue overflows in an effort to indicate that congestion is inminent, instead of waiting until the congestion has become excessive. The main goal is to provide congestion avoidance by controlling the **average queue size**.



The RED algorithm calculates the average queue size, using a low-pass filter with an exponential weighted moving average. The average queue size is compared to two thresholds, a **minimum threshold** and a **maximum threshold**. When the average queue size is less than the minimum threshold, no packets are marked. When the average queue size is greater than the maximum threshold, every arriving packet is marked. If marked packets are in fact dropped, or if all source nodes are cooperative, this ensures that the average queue size does not significantly exceed the maximum threshold. When the average queue size is between the minimum and the maximum threshold, each arriving packet is marked with probability pa, where pa is a function of the average queue size avg.

Use the following syntax to configure a RED Policy:

```
ATOSNT\qos>>add POLICY LIMIT RED
Command executed
```

A new node **policy3** has been created; to configure the following parameters use set, add and del commands.

```
ATOSNT\qos\policy3>>set ?

Nodes not available.
Set command parameters:
 level of log                    [loglevel]          Current value: 1
 description                     [description]       Current value:
 mean rate window (sec)          [mean-rate-window]  Current value: 0
 average packet (bytes)          [avpkt]             Current value: 1000
 min threshold (bytes)           [min-threshold]     Current value: 100000
 max threshold (bytes)           [max-threshold]     Current value: 1000000
```

```
burst (packets)                    [burst]            Current value: 400
limit (bytes)                      [limit]            Current value: 10000000
explicit congestion notification   [ecn]              Current value: true
probability (%)                    [probability]      Current value: 2
```

Table 31: set

Syntax	Description
loglevel [0-5]	Sets the level of detail to see the events of the created POLICY. Default: 1.
Description [max 100 char]	Descriptive string of the created POLICY.
mean-rate-window (sec) [0-60]	Sets the mean rate observation window
avpkt (bytes) [1-2048]	Sets average packet size in bytes. Used with burst to determine the time constant for average queue size calculations Default: 1000.
min-threshold (bytes) [10000-4294967295]	Sets minimum threshold below which the packets are not marked or dropped and transmission is guaranteed. Default: 100000.
max-threshold (packets) [10000-4294967295]	Sets maximum threshold at which marking or dropping probability is maximal.Should be at least twice min to prevent synchronous retransmits. Default: 1000000.
burst (packets) [1-1000]	Used for determining how fast the average queue size is influenced by the real queue size. Larger values make the calculation more sluggish, allowing longer bursts of traffic before marking starts. Real life experiments support the following guideline: (min+min+max)/(3*avpkt).. Default: 400.
limit (bytes) [11000-4294967295]	Hard limit on the real (not average) queue size in bytes. Further packets are dropped. Should be set higher than max+burst. It is advised to set this a few times higher than max. Default: 10000000.
ecn [truelfalse]	Sets **explicit congestion notification**. RED can either 'mark' or 'drop'. Explicit Congestion Notification allows RED to notify remote hosts that their rate exceeds the amount of bandwidth available. Non-ECN capable hosts can only be notified by dropping a packet. If this parameter is specified, packets which indicate that their hosts honor ECN will only be marked and not dropped, unless the queue size hits limit bytes. Default: true.
probability (%)	Maximum probability for marking. Suggested values are 1 or 2%. Default: 2%.

Example 1

How to configure a POLICY LIMIT RED assuming a bandwith of 512 kbps and a maximum desired latency of 500 ms

Bandwith = 512kbps = 512000 bps = 64000 bytes/sec

<max> is maximum threshold. To set this value we use link bandwidth and maximum desired

latency. Assuming a bandwidth of 512 kbps and a maximum desired latency of 500 ms we have 512 kbps ~ 512000 bps = 64000 bytes / sec

<max> = 64000 bytes / sec * 0.5 sec = 32000 bytes

Above <max> threshold we will have a packet massacre and latency doesn't matter.

<min> is minimum threshold. Must be set half of <max> threshold. Following recommendation, let's set <min> threshold such that <max> ~ 3 * <min>. Then we will set <min> to 12000 bytes.

<limit> is hard limit on the real queue size. This limit should never be reached. Following recommendation let's set this as 8 * <max>; then <limit> will be 256000 bytes.

<avpkt> is average packet size. We set this to 1000 bytes.

<burst> allows longer burst of traffic before marking (dropping) starts; just to accommodate bursty flows. Following RED man page recommendations we have:

<burst> = (2 * <min> + <max>) / (3 * <avpkt>)

<burst> = (2 * 12000 + 32000) / (3 * 1000) = 18.67 ~ 20.

<probability> is maximum probability of marking; we set this to 2%.

[ecn] is an optional parameter. If our end TCP systems are configured to respond to 'early congestion notification' you can use this flag to avoid packet dropping when average queue size is above <min> threshold and below <max> threshold. Above <max> threshold all packets are dropped; this perhaps occurs when dealing with unresponsive flows.

Configuration Commands Summary

ATOSNT\qos\policy0>>**conf**

add qos POLICY policy0 LIMIT RED

set qos policy0 min-threshold 12000

set qos policy0 max-threshold 32000

set qos policy0 burst 20

set qos policy0 limit 256000

add qos SERVICE eth0 policy0

ATOSNT\qos\policy0>>**show work**

Show of ATOSNT qos policy0

Level of log : 1

LIST OF SERVICES

Interface name	Policy name	Direction
eth0	policy0	EGRESS

Description :
Type : LIMIT
Sub type : RED
Mean rate window (sec) : 0
Average packet (bytes) : 1000
Min threshold (bytes) : 12000
Max threshold (bytes) : 32000
Burst (packets) : 20
Limit (bytes) : 256000
Explicit congestion notification : true
Probability (%) : 2

PRIORITY

Under **qos** node, for a POLICY PRIORITY, you should use add command and specify the subtype (default **PRIO**).

```
ATOSNT\qos>>add POLICY prio PRIORITY ?

add command parameters:
 sub type       [PRIO]
 <cr>
```

PRIO

The POLICY PRIORITY PRIO is a Multi Queue Policy that contains an arbitrary number of queues of different priority (up to 8 priorities).

PRIO policy allows to prioritize the outcoming traffic, it defines which packets and in which order they will be dequeued. Under each queue, the default policy applied is the p-fifo-default but other policies or schedulers like SFQ or TBF can also be defined .

PRIO is a scheduler and does not delay packets.
It is very useful for lowering latency when there is no need for slowing down traffic.

PRIO works in this way:
the incoming traffic is classified based on different rules and further is prioritized in bands or queues, up to 8 priorities.
In comparison with a pfifo-fast, PRIO is more powerful, because a pfifo_fast only offers 3 bands or priorities and the 3 FIFO are hardcoded and not configurable at all.
Incoming traffic is classified or separated into traffic classes using the classifiers or filters and not the TOS flag.

When dequeueing, queue with priority 1 is tried first and only if it did not deliver a packet does PRIO try priority 2 and so onwards.

```
ATOSNT\qos>>add POLICY prio PRIORITY PRIO
Command executed

ATOSNT\qos>>set ?
```

```
Available nodes:
                        p-fifo-default
                        b-fifo-default
                        prio

Set command parameters:
 level of log  [loglevel]  Current value: 1
```

In addition to the two basic policies or schedulers, p-fifo-default and b-fifo-default, a new node **prio** has been created and corresponds to a POLICY PRIORITY type with prio name.

In this node, with set, del and add commands you can configure the following parameters.

Table 31.1: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the POLICY events. Default: 1
description	Descriptive string of the created POLICY.
mean-rate-window (sec) [0-60]	Mean rate observation window. Default 0 (disabled).

To create a QUEUE or an ACTION (marking the traffic) you should use add command

```
ATOSNT\qos\prio>>add ?

add  help :  Add a new action or queue
add  usage:
 <ACTION><marking-type><value><classifier-name>
 <QUEUE>[name]<priority>

add command parameters:
 ACTION
 QUEUE

ATOSNT\qos\prio>>add QUEUE ?

add command parameters:
 name          [max 16 char]
 priority      [1-8]

ATOSNT\qos\prio>>add QUEUE 1
Command executed
ATOSNT\qos\prio>>tree
prio                    best-effort
                        queue0
```

With the addition of the PRIO Policy, automatically creates a default queue for low priority traffic named **best-effort**

Table 32: add QUEUE

Syntax	Description
QUEUE	Keyword
name [max 16 char]	Sets the name of the QUEUE
priority [1-8]	Sets the queue priority: • **1** is the highest priority • **8** is the lowest priority

If queue-name is not specified, a queue will be created with index sequence (**queue0, queue1…**).

Doing in this way, incoming traffic is divided into 2 queues.

```
ATOSNT\qos\prio>>set ?

Available nodes:
                       best-effort
                       queue0

Set command parameters:
 level of log            [loglevel]          Current value: 1
 description             [description]       Current value:
 mean rate window (sec)  [mean-rate-window]  Current value: 0
```

Table 33: add ACTION

Syntax	Description
ACTION	Keyword
marking type [DSCP|PREC|TOS|VLAN_PRIO]	Allows to remark the incoming traffic specified by the classifiers defined above, altering the following fields of the IP Header: • DSCP value [0-63] • PREC value [0-7] • TOS value [minimize-delay|maximize-throughput|maximize-reliability| minimize-monetary-cost|normal-service] • VLAN_PRIO value [0-7]
classifier name	Sets the name of the classifier to apply the traffic remarking action

```
ATOSNT\qos\prio>>del ?

Available nodes:
                       best-effort
                       queue0
del  help :  Remove an action or queue
del  usage:
 <ACTION><marking-type><value><classifier-name>
```

```
 <QUEUE><name>

del command parameters:
 ACTION
 QUEUE
```

Use **del** command to delete the action of marking applied to streams identified by the classifiers. If you do not specify the classifier, it will delete all entries identified by the specified marking-type specified.

PRIO - Queue

Under **queue0** node, you can use set, del and add commands to configure the following parameters:

```
ATOSNT\qos\prio\queue0>>set ?

Nodes not available.
Set command parameters:
 description             [description]           Current value:
 priority                [priority]              Current value: 1
 policy name             [policy-name]           Current value: p-fifo-default
 packet priority list    [packet-priority-list]  Current value: empty
```

Table 34: set

Syntax	Description
description [max 100 char]	Sets a brief description of the created queue
priority [1-8]	Sets the queue priority. Default: 8
policy name [<cr>|p-fifo-default|b-fifo-default |prio|policy0|policy1]	Sets the name of the policy associated to the queue. Default: p-fifo-default
packet-priority-list [list of up to 16 items chosen from empty |0|1|2|3|4|5|6|7|8|9|10|11|12|13|14|15]	Sets the list of Linux packet priority. A Linux packet is composed of Data and Info. Packet priority is based on Info, instead Data is used to define classifiers. By default, the band or priority associated to the elements of a packet priority list is the same than the one of a Best-Effort queue.

Once you have defined the policy and created the queue, you must associate a classifier to the queue.

```
ATOSNT\qos\prio\queue0>>add ?

add  help :  Add a new classifier
add  usage:
 <CLASSIFIER><name>

add command parameters:
 CLASSIFIER
ATOSNT\qos\prio\queue0>>add CLASSIFIER ?

add command parameters:
 name          [classifier0]
```

```
ATOSNT\qos\prio\queue0>>add CLASSIFIER classifier0
Command executed
```

Table 35: add CLASSIFIER

Syntax	Description
CLASSIFIER	Keyword
name	Sets the name of the classifier associated to the queue.

```
ATOSNT\qos\prio\queue0>>del ?

del help : Remove a classifier
del usage:

  <CLASSIFIER><name>

del command parameters:
 CLASSIFIER
```

Example 2

This example shows how to manage, separate and mark with PRIO policy the incoming traffic from a specified host and the traffic with specified Linux packet priority .

To do this, we'll use two queues: queue0 is managing the traffic from the host with source address 2.2.2.2/32 and traffic with specified Linux packet priority; instead the rest of the incoming traffic will be associated to a best-effort queue.

As a scheduler, for queue0, we'll use a SFQ policy; instead for the best effort queue, the policy to use will be the default.

Start defining a classifier or filter to separate the traffic from the host

ATOSNT\qos\add CLASSIFIER

Command executed

ATOSNT\qos\classifier0>>add IP-HDR SRC 2.2.2.2/32

Command executed

Define a Policy Priority PRIO with name "prio"

ATOSNT\qos>>add POLICY prio PRIORITY PRIO

Command executed

Add a Queue with priority 1

ATOSNT\qos\prio>>add QUEUE 1

Command executed

ATOSNT\qos\prio>>tree

prio best-effort

queue0

Add an SFQ scheduler

ATOSNT\qos>>add POLICY SCHEDULE SFQ

Associate SFQ scheduler and traffic with packet priority list to queue0

set qos prio queue0 policy-name policy0

set qos prio queue0 packet-priority-list 0 2 3 7 9 13

Separate and remark incoming traffic with TOS Minimize Delay and associate to classifier1

add qos prio ACTION TOS minimize-delay classifier1

Add Service to the interface and define Direction

add qos SERVICE eth0 prio

Commands Summary

ATOSNT\qos>>conf

add qos CLASSIFIER classifier0

add qos CLASSIFIER classifier1

add qos POLICY prio PRIORITY PRIO

add qos POLICY policy0 SCHEDULE SFQ

add qos SERVICE eth0 prio

add qos classifier0 IP-HDR SRC 2.2.2.2/32

add qos prio ACTION TOS minimize-delay classifier1

add qos prio QUEUE queue0 1

set qos prio queue0 priority 1

set qos prio queue0 policy-name policy0

set qos prio queue0 packet-priority-list 0 2 3 7 9 13

ATOSNT\qos>>**show work**

Show of ATOSNT qos

Level of log : 1

LIST OF SERVICES

Interface name	Policy name	Direction
eth0	prio0	EGRESS

Show of ATOSNT qos p-fifo-default

Level of log : 1

Description :

Type : LIMIT

Sub type : P-FIFO

Mean rate window (sec) : 0

Packets number : 128

LIST OF ACTIONS

Empty list

Show of ATOSNT qos b-fifo-default

Level of log : 1

Description :

Type : LIMIT

Sub type : B-FIFO

Mean rate window (sec) : 0

Bytes number : 128000

LIST OF ACTIONS

Empty list

Show of ATOSNT qos classifier0

Description :

Type : MATCH-ANY

LIST OF RULES

Type	Value/Type Value Mask	Byte-id	Priority
IP-HDR	SRC 2.2.2.2/32		1

Show of ATOSNT qos prio0
Level of log : 1
Description :
Type : PRIORITY
Sub type : PRIO
Mean rate window (sec) : 0
LIST OF ACTIONS
Empty list
Show of ATOSNT qos prio0 best-effort
Description :
Type : PRIO
Priority : 8
Policy name : p-fifo-default
Packet priority list : empty
LIST OF CLASSIFIERS
Empty list
Show of ATOSNT qos prio0 queue0
Description :
Type : PRIO
Priority : 1
Policy name : p-fifo-default
Packet priority list : empty
LIST OF CLASSIFIERS
classifier0
Command executed

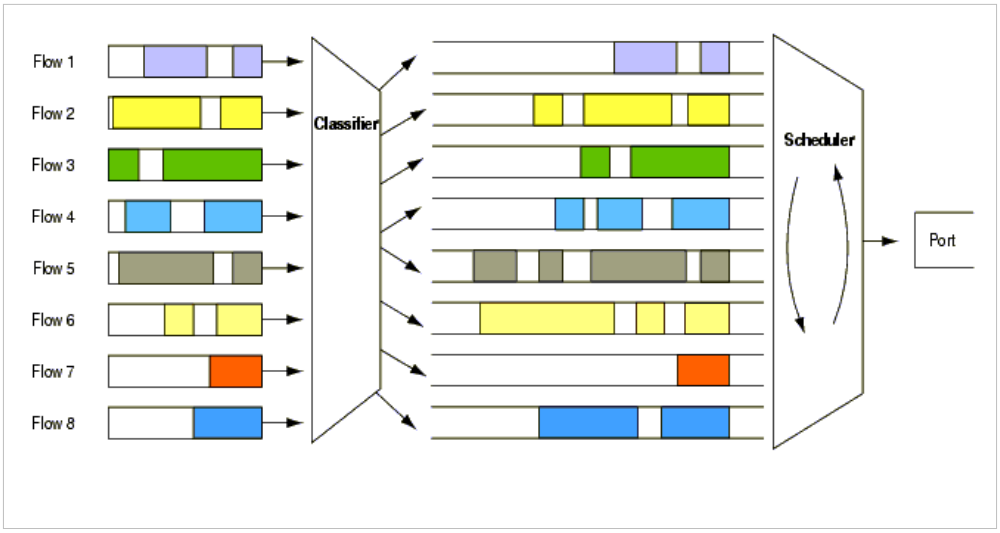
SHEDULE

For a POLICY SHEDULE the subtype can be specified (default SFQ).

```
ATOSNT\qos>>add POLICY SCHEDULE ?

add command parameters:
 sub type       [SFQ|DRR|GRED]
 <cr>
```

SFQ

Stochastic Fairness Queuing (SFQ) policy is based on the fair queuing algorithmt and is designed to ensure that each flow has fair access to network resources and to prevent a bursty flow from consuming more than its fair share of output port bandwidth. In FQ, packets are first classified into flows by the system and then assigned to a queue that is specifically dedicated to that flow. Queues are then serviced one packet at a time in roundrobin order, in this way the service is 'fair' for every queue. Empty queues are skipped.



SFQ is called "Stochastic" because it does not really allocate a queue for each session or flow, it has an algorithm which divides traffic over a limited number of queues using a hashing algorithm.

On enqueueing, each packet is assigned to a hash bucket, based on:

- Source address
- Destination address
- Source port

Each of these buckets should represent a unique flow. Because multiple flows may get hashed to the same bucket, the hashing algorithm is perturbed at configurable intervals so that the unfairness lasts only for a short while. Perturbation may however cause some inadvertent packet reordering to occur.

When dequeuing, each hashbucket with data is queried in a round robin fashion.

The compile time maximum length of the SFQ is 128 packets, which can be spread over at most 128 buckets of 1024 available. In case of overflow, tail-drop is performed on the fullest bucket, thus maintaining fairness.

The only parameters to be configured are **perturb** that reconfigures hashing once this many seconds and **quantum**, the amount of bytes a flow is allowed to dequeue during a round of the round robin process.

```
ATOSNT\qos>>add POLICY SCHEDULE SFQ
Command executed
```

A new node **policy4** has been created. Under this node, you can configure the following parameters with set, add and **del** commands:

```
ATOSNT\qos\policy4>>set ?

Nodes not available.
Set command parameters:
 level of log                    [loglevel]          Current value: 1
 description                     [description]       Current value:
 mean rate window (sec)          [mean-rate-window]  Current value: 0
 perturb (sec)                   [perturb]           Current value: 10
 quantum (bytes)                 [quantum]           Current value: MTU
```

Table 36: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the Policy events. Default: 1
description	Descriptive string of the created POLICY.
mean-rate-window (sec) [0-60]	Sets the mean rate observation window Default: 0
perturb (sec) [0-60]	Sets the interval in seconds to reconfigure hashing algorithm. If unset, hash will never be reconfigured. Not recommended. "10 seconds is a good value." Default: 10
quantum (bytes) [1-65535|MTU]	Sets the amount of bytes a stream is allowed to dequeue before the next queue gets a turn. Default: 1 maximum sized packet (MTU)

With "add" and "del" commands, you can mark/remark or delete the marked incoming traffic using the classifiers described above.

```
ATOSNT\qos\policy4>>add ?

add  help :  Add a new action
add  usage:
 <marking-type><value><classifier-name>

add command parameters:
 marking type    [DSCP|PREC|TOS|VLAN_PRIO]
```

```
ATOSNT\qos\policy0>>del ?

del  help :  Remove an action
del  usage:
 <marking-type><value><classifier-name>

del command parameters:
 marking type    [DSCP|PREC|TOS|VLAN_PRIO]
```

Example 3

How to configure a POLICY SCHEDULE SFQ assuming a quantum of 1514 bytes and a reconfiguration hashing of 10 seconds

ATOSNT\qos\policy4>>**conf**

add interfaces IFC eth0 eth0

set interfaces eth0 ip address 192.168.1.1/24

set interfaces eth0 ip dhcp-client on

add qos POLICY policy0 SCHEDULE SFQ

add qos SERVICE eth0 policy0

set qos policy0 quantum 1514

ATOSNT\qos>>**show work**

Show of ATOSNT qos

Level of log : 1

LIST OF SERVICES

Interface name	Policy name	Direction
eth0	policy0	EGRESS

Show of ATOSNT qos p-fifo-default

Level of log : 1

Description :

Type : LIMIT

Sub type : P-FIFO

```
Mean rate window (sec) : 0
Packets number : 128
LIST OF ACTIONS
Empty list
Show of ATOSNT qos b-fifo-default
Level of log : 1
Description :
Type : LIMIT
Sub type : B-FIFO
Mean rate window (sec) : 0
Bytes number : 128000
LIST OF ACTIONS
Empty list
Show of ATOSNT qos policy0
Level of log : 1
Description :
Type : SCHEDULE
Sub type : SFQ
Mean rate window (sec) : 0
Perturb (sec) : 10
Quantum (bytes) : 1514
LIST OF ACTIONS
Empty list
Command executed
```

DRR

Deficit Round Robin (DRR) scheduler is based on a different implementation of the algorithm **Weighted Round Robin (WRR)** scheduling discipline.
DRR is used for servicing queues in a router or gateway. WRR serves every non-empty queue whereas DRR serves packets at the head of every non-empty queue whose deficit counter is greater than the packet's size at the head of the queue (HoQ). For more details, see bellow.

The algorithm works in this way:

Packets coming in on different flows are stored in different queues. For each flow or queue, it is specified a quantity in bytes called **Quantum** that indicates the bandwith share given to each queue.

Each queue is allowed to send out packets in the first round subject to the restriction that the packet's size at the head of the queue (HoQ) called *bytes* is inferior to Quantum. If there are no more packets in the queue after the queue has been serviced, a state variable called **Deficit Counter**, is reset to 0. Otherwise, the remaining amount (Quantum - bytes) is stored in the state variable *Deficit Counter*. In subsequent rounds, the amount of bandwith usable by this flow is the sum of *Deficit Counter* of the previous round added to *Quantum*.

Look at the bellow figures:

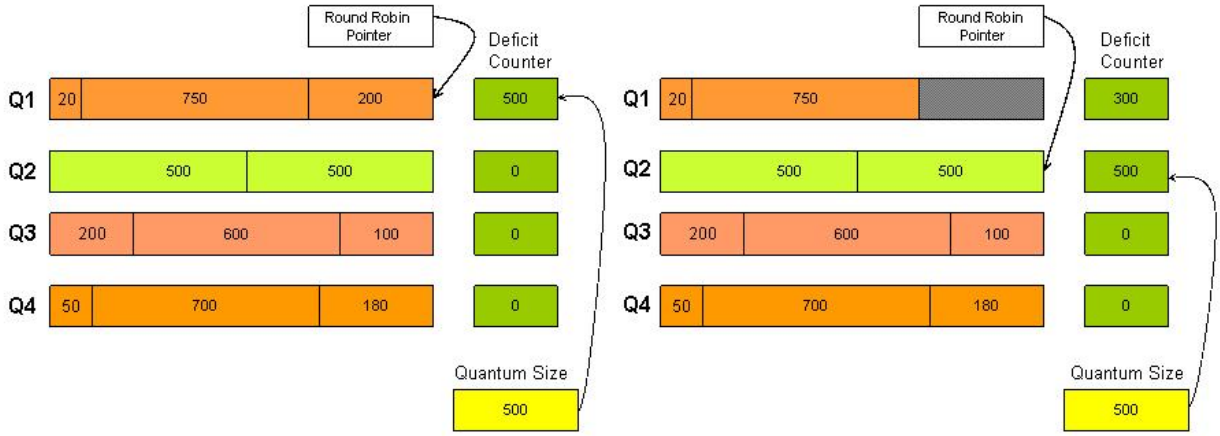


Figure Deficit Round Robin (1) Figure Deficit Round Robin (2)

Figure Deficit Round Robin (1)

At the start, all the *Deficit Counter* variables are initialized to zero. The round robin pointer points to the top of the active queues list. When the first queue is serviced the *Quantum* value of 500 is added to the *Deficit Counter* value. The remainder after serving the queue is left in the *Deficit Counter* variable.

Figure Deficit Round Robin (2)

After sending out a packet of size 200, the queue had 300 bytes of its quantum left. It could not use it the current round, since the next packet in the queue is 750 bytes. Therefore, the amount 300 will carry over to the next round when it can send packets of size totaling 800 (deficit from previous round) + 500 (quantum).

```
ATOSNT\qos>>add POLICY DRR0 SCHEDULE DRR
Command executed
```

A new node **drr0** has been created. Under this node, you can configure the following parameters with set, add and del commands:

```
ATOSNT\qos\drr0>>set ?

Nodes not available.
Set command parameters:
 level of log           [loglevel]         Current value: 1
 description            [description]      Current value:
 mean rate window (sec) [mean-rate-window] Current value: 0
```

Table 37: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the Policy events. Default: 1
description	Descriptive string of the created POLICY.
mean-rate-window (sec) [0-60]	Sets the mean rate observation window Default: 0

To create or delete a QUEUE or an ACTION (marking the traffic) use add and del commands respectively, see bellow

```
ATOSNT\qos\drr0>>del?

Available nodes:
                 queue0

del help : Remove an action or queue
del usage:
 <ACTION><marking-type><value><classifier-name>
 <QUEUE><name>

del command parameters:
 ACTION
 QUEUE
```

```
ATOSNT\qos\drr0>>add ?

add  help :  Add a new action or queue
add  usage:
 <ACTION><marking-type><value><classifier-name>
 <QUEUE>[name][quantum]

add command parameters:
 ACTION
 QUEUE

ATOSNT\qos\drr0>>add QUEUE ?

add command parameters:
 name           [max 16 char]
 quantum        [1-65535|MTU]
 <cr>

ATOSNT\qos\drr0>>tree
drr0                   queue0
```

Table 38: add ACTION

Syntax	Description
ACTION	Keyword

marking type [DSCP|PREC|TOS|VLAN_PRIO]	Allows to remark the incoming traffic specified by the classifiers defined above, altering the following fields of the IP Header: • DSCP value [0-63] • PREC value [0-7] • TOS value [minimize-delay|maximize-throughput|maximize-reliability|minimize-monetary-cost|normal-service] • VLAN_PRIO value [0-7]
classifier name	Sets the name of the classifier to apply the traffic remarking action

Table 39: add QUEUE

Syntax	Description
QUEUE	Keyword
name [max 16 char]	name of the created Queue
quantum [1-65535|MTU]	Sets the quantum allocated to Queue

In **queue0** you can associate to the queue, the name of the classifier specified above

```
ATOSNT\qos\drr0\queue0>>add ?

add  help :  Add a new classifier
add  usage:
 <CLASSIFIER><name>

add command parameters:
 CLASSIFIER
```

Table 40: add CLASSIFIER

Syntax	Description
CLASSIFIER	Keyword
name	name of the classifier associated to the queue

Example 4

How to configure a POLICY SCHEDULE DRR to select VoIP traffic and to give twice bandwith with respect to the Best-effort traffic

Start making a classifier map for VOIP traffic

ATOSNT\qos>>**conf**

add classifier-map CLASS-VOIP 1 permit udp host 192.168.1.1 any range 18000 18032 anyport

add qos CLASSIFIER Classifier-VOIP

add qos POLICY DRR0 SCHEDULE DRR

add qos SERVICE eth0 DRR0

add qos classifier-voip CLASSIFIER-MAP CLASS-VOIP

add qos drr0 QUEUE VOIP 3000

add qos drr0 QUEUE Best-effort 1500

add qos drr0 voip CLASSIFIER Classifier-VOIP

set qos drr0 voip quantum 3000

set qos drr0 best-effort quantum 1500

ATOSNT\qos>>**show work**

Show of ATOSNT qos

Level of log : 1

LIST OF SERVICES

Interface name	Policy name	Direction
eth0	DRR0	EGRESS

Show of ATOSNT qos p-fifo-default

Level of log : 1

Description :

Type : LIMIT

Sub type : P-FIFO

Mean rate window (sec) : 0

Packets number : 128

LIST OF ACTIONS

Empty list

Show of ATOSNT qos b-fifo-default

Level of log : 1

Description :

Type : LIMIT

Sub type : B-FIFO

Mean rate window (sec) : 0

Bytes number : 128000

LIST OF ACTIONS

Empty list

Show of ATOSNT qos classifier-voip

Description :

Type : MATCH-ANY

LIST OF RULES

Type	Value/Type	Value Mask	Byte-id	Priority
CLASSIFIER-MAP	CLASS-VOIP			1

Show of ATOSNT qos drr0
Level of log : 1
Description :
Type : SCHEDULE
Sub type : DRR
Mean rate window (sec) : 0
LIST OF ACTIONS
Empty list
Show of ATOSNT qos drr0 voip
Description :
Type : DRR
Mean rate window (sec) : 0
Quantum (bytes) : 3000
LIST OF CLASSIFIERS
Classifier-VOIP
Show of ATOSNT qos drr0 best-effort
Description :
Type : DRR
Mean rate window (sec) : 0
Quantum (bytes) : 1500
LIST OF CLASSIFIERS
Empty list
Command executed

GRED

Generalized RED is a different implementation of the RED algorithm. RED only offer one queue and one dropping probability. GRED has been implemented for provisioning of drop priorities. The traffic is classified into a series of virtual queues. **GRED** allows you to define a priority in the scheduling of queues. Each queue is a RED queue.

```
ATOSNT\qos>>add POLICY SCHEDULE GRED
Command executed
```

A new node **policy0** has been created and you can configure the following parameters with set, add and del commands. GRED is configured in two steps

```
ATOSNT\qos\policy0>>set ?

Nodes not available.
Set command parameters:
 level of log                    [loglevel]          Current value: 1
 description                     [description]       Current value:
 mean rate window (sec)          [mean-rate-window]  Current value: 0
 use priority                    [use-prio]          Current value: false
```

Table 41: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the Policy events. Default: 1
description	Descriptive string of the created POLICY.
mean-rate-window (sec) [0-60]	Sets the mean rate observation window Default: 0
use-prio [truelfalse]	Sets the priority use in each RED queue. Possible values are: • **true** means that each queue must have an assigned priority • **false** means that you will not use the priority

The different flow types are defined by adding queues.

In GRED policy you can also configure directly the action of marking the traffic on a specific classifier defined above.

```
ATOSNT\qos\policy0>>add ?

add  help :  Add a new action or queue
add  usage:
 <ACTION><marking-type><value><classifier-name>
 <QUEUE>[name]

add command parameters:
 ACTION
 QUEUE
```

```
ATOSNT\qos\policy0>>add QUEUE
Command executed
```

The second step is to set parameters for individual RED queues.

```
ATOSNT\qos\policy0\queue0>>set ?

Nodes not available.
Set command parameters:
 description             [description]          Current value:
 priority                [priority]             Current value: 1
 average packet (bytes)  [avpkt]                Current value: 1000
 min threshold (bytes)   [min-threshold]        Current value: 50000
 max threshold (bytes)   [max-threshold]        Current value: 100000
 burst (packets)         [burst]                Current value: 50
 limit (bytes)           [limit]                Current value: 150000
 probability (%)         [probability]          Current value: 2
```

Table 42: set

Syntax	Description
description [max 100 char]	Descriptive string of the created POLICY.
priority [1-16]	Sets the priority assigned to this RED queue. Priorities range from 1 to 16 with 1 the highest. This parameter is to be used only when "use-prio" is used in the generic configuration
avpkt (bytes) [1-2048]	Sets average packet size in bytes. Used with burst to determine the time constant for average queue size calculations Default: 1000.
min-threshold (bytes) [10000-1500000]	Sets minimum threshold below which the packets are not marked or dropped and transmission is guaranteed. Default: 50000.
max-threshold (packets) [10000-1500000]	Sets maximum threshold at which marking or dropping probability is maximal.Should be at least twice min to prevent synchronous retransmits. Default: 100000.
burst (packets) [1-1000]	Used for determining how fast the average queue size is influenced by the real queue size. Larger values make the calculation more sluggish, allowing longer bursts of traffic before marking starts. Real life experiments support the following guideline: (min+min+max)/(3*avpkt).. Default: 50.
limit (bytes) [10000-1500000]	Hard limit on the real (not average) queue size in bytes. Further packets are dropped. Should be set higher than max+burst. It is advised to set this a few times higher than max. Default: 150000.
probability (%) [0-100]	Maximum probability for marking, specified as a number from 0 to 100. Suggested values are 1 or 2%. Default: 2%.

In **queue0** node you can associate a classifier with add command.

```
ATOSNT\qos\policy0\queue0>>add ?

add  help :  Add a new classifier
add  usage:
 <CLASSIFIER><name>

add command parameters:
 CLASSIFIER
```

Use **del** command, to remove an action or queue.

```
ATOSNT\qos\policy0>>del ?

Available nodes:
                      best-effort
                      queue0
del  help :  Remove an action or queue
del  usage:
 <ACTION><marking-type><value><classifier-name>
 <QUEUE><name>

del command parameters:
 ACTION
 QUEUE
```

Example 5

Suppose:

- Trying to select the VOIP traffic type
- Assigning a priority 1 to VOIP traffic against the other traffic and a discard probability of 1%

How to configure a POLICY SCHEDULE GRED to select VoIP traffic and to give a drop probability of 1% with respect to the Best-effort traffic

Start making a classifier map for VOIP traffic

ATOSNT\qos>>**conf**

add classifier-map CLASS-VOIP 1 permit udp host 192.168.1.1 any range 18000 18032 anyport

add qos CLASSIFIER classifier-VOIP

add qos POLICY GRED0 SCHEDULE GRED

add qos classifier-voip CLASSIFIER-MAP CLASS-VOIP

add qos gred0 QUEUE queue-VOIP

set qos gred0 use-prio true

add qos gred0 queue-voip CLASSIFIER classifier-VOIP

set qos gred0 queue-voip priority 1

set qos gred0 queue-voip probability 1

add qos SERVICE eth0 GRED0

ATOSNT\qos>>**show work**

Show of ATOSNT qos

Level of log : 1

LIST OF SERVICES

Interface name	Policy name	Direction
eth0	GRED0	EGRESS

Show of ATOSNT qos p-fifo-default

Level of log : 1

Description :

Type : LIMIT

Sub type : P-FIFO

Mean rate window (sec) : 0

Packets number : 128

LIST OF ACTIONS

Empty list

Show of ATOSNT qos b-fifo-default

Level of log : 1

Description :

Type : LIMIT

Sub type : B-FIFO

Mean rate window (sec) : 0

Bytes number : 128000

LIST OF ACTIONS

Empty list

Show of ATOSNT qos classifier-voip

Description :

Type : MATCH-ANY

LIST OF RULES

Type	Value/Type	Value Mask	Byte-id	Priority
CLASSIFIER-MAP	CLASS-VOIP			1

Show of ATOSNT qos gred0
Level of log : 1
Description :
Type : SCHEDULE
Sub type : GRED
Mean rate window (sec) : 0
Use priority : true
LIST OF ACTIONS
Empty list
Show of ATOSNT qos gred0 best-effort
Description :
Type : GRED
Priority : 16
Average packet (bytes) : 1000
Min threshold (bytes) : 50000
Max threshold (bytes) : 100000
Burst (packets) : 50
Limit (bytes) : 150000
Probability (%) : 2
LIST OF CLASSIFIERS
Empty list
Show of ATOSNT qos gred0 queue-voip
Description :
Type : GRED
Priority : 1
Average packet (bytes) : 1000
Min threshold (bytes) : 50000
Max threshold (bytes) : 100000
Burst (packets) : 50
Limit (bytes) : 150000
Probability (%) : 1
LIST OF CLASSIFIERS
classifier-VOIP
Command executed

SHAPING

For a SHAPING policy you should specify the subtype (default **TBF**).

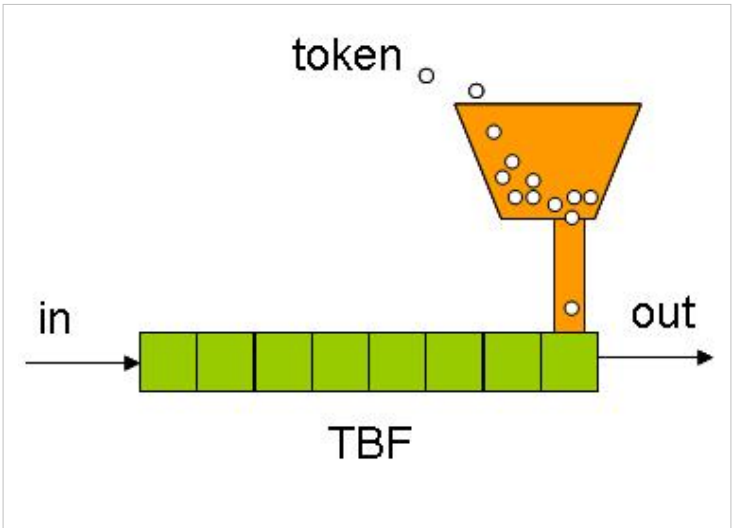
```
ATOSNT\qos>>add POLICY SHAPING ?

add command parameters:
 sub type       [TBF|CBQ|HTB]
 <cr>
```

TBF

Token Bucket Filter (TBF)

This Policy allows to limit the packets transmission rate (shaping) absorbing occasionally burst traffic.

The Policy is built on tokens and buckets. Packets are only transmitted if there are sufficient tokens available. Otherwise, packets are delayed in the TBF queue. TBF Policy is the simplest way to slow down transmitted traffic to the specified rate.



Associating the algorithm with the two flows -- token and data, gives us three possible scenarios:

- The data arrives in TBF at a rate that is equal to the rate of incoming tokens. In this case each incoming packet has its matching token and passes the queue without delay.
- The data arrives in TBF at a rate that is smaller than the token rate. Only a part of the tokens are deleted at output of each data packet that is sent out the queue, so the tokens accumulate, up to the bucket size. The unused tokens can then be used to send data at a speed that is exceeding the standard token rate, in case short data bursts occur.
- The data arrives in TBF at a rate bigger than the token rate. This means that the bucket will soon be devoid of tokens, which causes the TBF to throttle itself for a while. This is called an "overlimit situation". If packets keep coming in, packets will start to get dropped.

```
ATOSNT\qos>>add POLICY SHAPING TBF
Command executed
```

A new node **policy0** has been created and you can configure the following parameters with set, add and del commands.

```
ATOSNT\qos\policy0>>set ?

Nodes not available.
Set command parameters:
 level of log                    [loglevel]          Current value: 1
 description                     [description]       Current value:
 mean rate window (sec)          [mean-rate-window]  Current value: 0
 rate (kbps)                     [rate]              Current value: 1000
 buffer size (bytes)             [buff-size]         Current value: 10000
 latency (msec)                  [latency]           Current value: 70
```

```
 mpu (bytes)                          [mpu]              Current value: 0
 peakrate (kbps)                      [peakrate]         Current value: 20000
```

Table 44: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the Policy events. Default: 1
description [max 100 char]	Descriptive string of the created POLICY.
mean rate window (sec) [0-60]	Sets the mean rate observation window. Default: 0
rate (kbps) [0-100000]	Sets the output packets transmission rate or Shaping rate. The transmission rate is the same than the token rate Default: 1 Mbps
buff-size (bytes) [2048-10000000]	Sets the bucket size in bytes and represents the maximum number in bytes that can be delivered from the TBF queue at a time. It is recommended that for a shaping rate of 10 Mbps to have a bucket size of at least 10 Kbytes. Default: 10000.
latency (msec) [1-1000]	Maximum waiting time that a packet must wait before leaving the TBF queue. Default: 70 msec.
mpu (bytes) [0-2048]	Minimum packet unit. Default: 0.
peakrate (kbps) [0-100000]	Peak rate is the maximum transmission rate when a burst occurs. Default: 20 Mbps.

Wtih add command you can add or remove the action of marking the traffic

```
ATOSNT\qos\policy0>>add ?

add  help :  Add a new action
add  usage:
 <marking-type><value><classifier-name>

add command parameters:
 marking type    [DSCP|PREC|TOS|VLAN_PRIO]
```

```
ATOSNT\qos\policy0>>del ?

del  help :  Remove an action
del  usage:
 <marking-type><value><classifier-name>

del command parameters:
  marking type    [DSCP|PREC|TOS|VLAN_PRIO]
```

Example 6

Suppose:

- The shaping rate is selected as 500 kbps with a 5 kbyte buffer and a pick rate of 1 Mbps for short burst of packets
- The bucket queue size (5 kbyte) is calculated so that a maximum of 70 ms of latency a packet will suffer on the queue.
- The minimum packet unit parameter is selected as the MTU of the interface

How to configure a POLICY SHAPING TBF

ATOSNT\qos>>**conf**

add interfaces IFC eth0 eth0

set interfaces eth0 ip address 192.168.1.1/24

set interfaces eth0 ip dhcp-client on

add qos CLASSIFIER classifier0

add qos POLICY policy0 SHAPING TBF

add qos SERVICE eth0 policy0

set qos policy0 rate 500

set qos policy0 buff-size 5000

set qos policy0 mpu 1540

set qos policy0 peakrate 1000

ATOSNT\qos>>**show work**

Show of ATOSNT qos

Level of log : 1

LIST OF SERVICES

Interface name	Policy name	Direction
eth0	policy0	EGRESS

Show of ATOSNT qos p-fifo-default

Level of log : 1

```
Description :
Type : LIMIT
Sub type : P-FIFO
Mean rate window (sec) : 0
Packets number : 128
LIST OF ACTIONS
Empty list
Show of ATOSNT qos b-fifo-default
Level of log : 1
Description :
Type : LIMIT
Sub type : B-FIFO
Mean rate window (sec) : 0
Bytes number : 128000
LIST OF ACTIONS
Empty list
Show of ATOSNT qos policy0
Level of log : 1
Description :
Type : SHAPING
Sub type : TBF
Mean rate window (sec) : 0
Rate (kbps) : 500
Buffer size (bytes) : 5000
Latency (msec) : 70
MPU (bytes) : 1540
Peakrate (kbps) : 1000
LIST OF ACTIONS
Empty list
Show of ATOSNT qos classifier0
Description :
Type : MATCH-ANY
LIST OF RULES
Empty list
Command executed
```

CBQ

Class Based Queueing - CBQ is a kind of shaping policy subtype that implements a rich **hierarchical link-sharing**.

Hierarchical link-sharing allows multiple agencies, protocol families (IP, SNA, etc), or traffic types, such as telnet, ftp, real-time audio and video, to share the bandwidth on a link in a controlled fashion.

The **link-sharing** structure specifies the desired policy in terms of the division of bandwidth for a particular link in times of congestion. For example, for the link-sharing structure in the bellow Figure, the link is shared by a number of real-time and non-real-time traffic classes. In the Figure, the telnet class could be a class of delay-sensitive traffic. Similarly, the mail class could be a class of delay-insensitive traffic such as FAX as well as mail traffic.

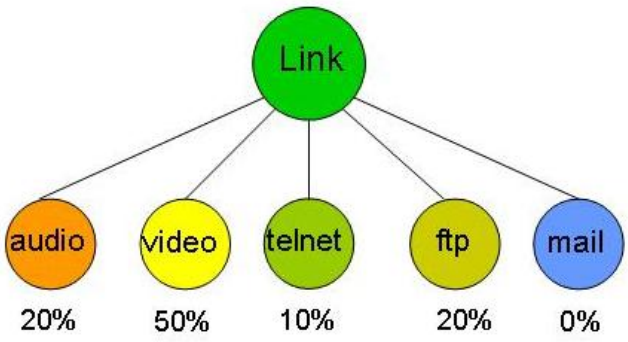


Figure: Link-sharing allocation between service classes

A link-sharing bandwidth is allocated to each class (expressed in Figure as a percentage of the overall link bandwidth).

The first link-sharing goal is that each class with sufficient demand should be able to receive roughly its allocated bandwidth, over some interval of time, in times of congestion.

As a consequence of this link-sharing goal, in times of congestion some classes might be restricted to their link-sharing bandwidth. For a class with a link-sharing allocation of zero, such as the mail class in Figure, the bandwidth received by this class is determined by the other scheduling mechanisms at the router; the link-sharing mechanisms do not “guarantee” any bandwidth to this class in times of congestion.

Associated with these link-sharing goals is the time interval over which the linksharing goals apply; this is determined by the time constant used in estimating the past bandwidth used by each class. For example, in Figure it might be considered unacceptable if the telnet and ftp classes were denied service for minutes at a time.

Priority-based scheduling can be used to reduce delay for the real-time traffic, while the link-sharing mechanisms prevent starvation of the ftp traffic over longer time intervals.

A secondary link-sharing goal is that when some class is not using its allocated bandwidth, the distribution of the **"excess"** bandwidth among the other classes should not be arbitrary, but should follow some appropriate set of guidelines.

Multiple link-sharing constraints at a router can be expressed by a hierarchical link-sharing structure such as in Figure.

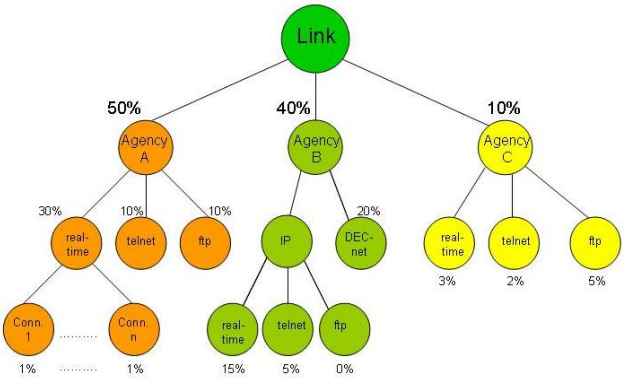


Figure: Hierarchical link-sharing structure

The Figure illustrates link-sharing between organizations, between protocol families, between service classes, and between individual connections within a service class. All arriving packets at the router are assigned to one of the leaf classes; the "LINK" class is used to designate guidelines about how "excess" bandwidth should be allocated. Thus, the goal is that the three service classes for agency A should collectively receive 50% of the link bandwidth over appropriate time intervals, given sufficient demand. If the real-time class for agency A has little data to send, the hierarchical link-sharing structure specifies that the "excess" bandwidth should be allocated to other subclasses of agency A.

The algorithm works in this way: Shaping is performed using link **idle time** calculations based on the timing of dequeue events and underlying link bandwidth.

When shaping a 10 Mbit/s connection to 1 Mbit/s, the link will be idle 90% of the time.

During operations, the effective idletime is measured using an exponential weighted moving average (EWMA), which considers recent packets to be exponentially more important than past ones.

The calculated idle time is subtracted from the EWMA measured one, the resulting number is called **avgidle**. A perfectly loaded link has an avgidle of zero: packets arrive exactly at the calculated interval.

An overloaded link has a negative avgidle and if it gets too negative, CBQ throttles and is then 'overlimit'.

Conversely, an idle link might amass a huge avgidle, which would then allow infinite bandwidths after a few hours of silence. To prevent this, avgidle is capped at maxidle.

If overlimit, in theory, the CBQ could throttle itself for exactly the amount of time that was calculated to pass between packets, and then pass one packet, and throttle again. Due to timer resolution constraints, this may not be feasible, see the minburst parameter below.

Look at the syntax and the parameters you can configure under the new node **policy0**.

```
ATOSNT\qos>>add POLICY SHAPING CBQ
Command executed
```

```
ATOSNT\qos\policy0>>set?

Nodes not available.
Set command parameters:
 level of log                    [loglevel]          Current value: 1
 description                     [description]       Current value:
 mean rate window (sec)          [mean-rate-window]  Current value: 0
```

```
 average packet (bytes)            [avpkt]             Current value: 1000
 bandwidth (bit)                   [bandwidth]         Current value: 100000000
 cell (bytes)                      [latency]           Current value: 8
 ewma                              [ewma]              Current value: 5
 mpu (bytes)                       [mpu]               Current value: 0
```

Table 45: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the Policy events. Default: 1
description [max 100 char]	Descriptive string of the created POLICY.
mean rate window (sec) [0-60]	Sets the mean rate observation window. Default: 0
avpkt (bytes) [0-2048]	Sets the average size of a packet Default: 1000
bandwidth (bit/s) [1-100000000]	Sets the bandwith of the physical interface. To determine the idle time, CBQ must know the bandwidth. This is a mandatory parameter. Default: 100000000
latency (bytes) [0-2048]	Sets the packet granularity in terms of bytes to define the packet waiting time before leaving the CBQ queue. This parameter must be an integer multiple of 2. For example with a latency value of 8, n bytes +/- 7 length packets, will have the same waiting time in the queue. Default: 8.
ewma [0-31]	This parameter adjusts the EWMA algorithm for the calculation of the avgidle parameter. It must be a value between 0 and 31: lower values imply a greater sensitivity of the algorithm. Default: 5.
mpu (bytes) [0-2048]	Sets the minimum packet size. A zero sized packet may still take time to transmit. This parameter is needed to calculate the idle time. Default: 0.

Use del and add command to remove or to add a new action or queue.

```
ATOSNT\qos\policy0>>del ?

del  help :  Remove an action or queue
del  usage:
 <ACTION><marking-type><value><classifier-name>
 <QUEUE><name>

del command parameters:
 ACTION
 QUEUE
```

```
ATOSNT\qos\policy0>>add ?

add  help :  Add a new action or queue
add  usage:
 <ACTION><marking-type><value><classifier-name>
```

```
 <QUEUE>[name]<rate>[priority][parent-queue]

add command parameters:
 ACTION
 QUEUE
```

When adding the policy, a default queue that occupies the full bandwith is created

Additional flows, bandwiths and priorities are defined by adding queues.

Unclassified traffic will be conveyed to the default queue and will be scheduled at the lowest priority.

```
ATOSNT\qos\policy0\queue0>>set ?

Nodes not available.
Set command parameters:
 description             [description]          Current value:
 priority                [priority]             Current value: 1
 policy name             [policy-name]          Current value:
 mean rate window (sec)  [mean-rate-window]     Current value: 0
 rate (bps)              [rate]                 Current value: 1000000
 allot (bytes)           [allot]                Current value: 1514
 average packet (bytes)  [avpkt]                Current value: 1000
 bounded                 [bounded]              Current value: false
 isolated                [isolated]             Current value: false
```

Table 46: set

Syntax	Description
description	Descriptive string of the created POLICY.
priority [1-8]	Sets the queue priority to be scheduled . The priority value of 1 corresponds to the highest priority. Default: 8.
policy-name [<cr>|p-fifo-default|b-fifo-default|policy0]	Name of the policy associated to the created queue.
rate (bps) [1-100000000]	Sets the maximum rate this queue and all its children combined can send at. Default: 10000000
Allot (bytes) [1-100000000]	Allot specifies how many bytes the policy can dequeue during each round of the process. This is a mandatory parameter. Default: 1514.
avpkt (bytes) [0-2048]	Sets the average size of packets in transit. Default: 1000.
Bounded [true|false]	This queue will not borrow bandwidth from its siblings. Default: false.
Isolated [true|false]	This queue will not borrow bandwidth to its siblings. Default: false

Use add and del commands to add or delete a classifier associated to the queue.

```
ATOSNT\qos\policy0\queue0>>add ?
```

```
add  help :  Add a new classifier
add  usage:
 <CLASSIFIER><name>

add command parameters:
 CLASSIFIER
```

```
ATOSNT\qos\policy0\queue0>>del ?

del  help :  Remove a classifier
del  usage:
 <CLASSIFIER><name>

del command parameters:
 CLASSIFIER
```

Example 7

Suppose:

- Having a 100 Mbps interface eth0.
- Trying to select VOIP and WEB traffic types
- Wanting to give to VoIP and WEB traffic, a maximum bandwidth of 13 Mbps
- Wanting to give to VoIP traffic, a priority 1 and a band of 5 Mbps
- Wanting to give to WEB traffic, a priority 5 and a band of 8 Mbps
- The remaining bandwidth of the interface is available to the Best Effort traffic and will have the lowest priority

How to configure a POLICY SHAPING CBQ to select and give the VoIP and WEB traffic a maximum bandwidth of 13 Mbps, assigning to VOIP traffic priority 1 and a band of 5 Mbps and to WEB traffic, a priority 5 and a band of 8 Mbps. The remaining bandwith will be for the best-effort traffic with the lowest priority

ATOSNT\qos>>**conf**

add classifier-map CLASS-VOIP 1 permit udp host 192.168.1.1 any range 18000 18032 anyport

add qos CLASSIFIER classifier-VOIP

add qos CLASSIFIER classifier-WEB

add qos POLICY shaper0 SHAPING CBQ

add qos SERVICE eth0 shaper0

add qos classifier-voip CLASSIFIER-MAP CLASS-VOIP

add qos classifier-web IP-HDR SPORT 80 FFFF

add qos shaper0 QUEUE queue-13M 13000000

add qos shaper0 QUEUE queue-voip 5000000 1 queue-13M

add qos shaper0 QUEUE queue-WEB 8000000 5 queue-13M

set qos shaper0 queue-13m rate 13000000

set qos shaper0 queue-13m bounded true

add qos shaper0 queue-voip CLASSIFIER classifier-VOIP

set qos shaper0 queue-voip priority 1

set qos shaper0 queue-voip rate 5000000

set qos shaper0 queue-voip bounded true

add qos shaper0 queue-web CLASSIFIER classifier-WEB

set qos shaper0 queue-web priority 5

set qos shaper0 queue-web rate 8000000

set qos shaper0 queue-web bounded true

ATOSNT\qos>>**show work**

Show of ATOSNT qos

Level of log : 1

LIST OF SERVICES

Interface name	Policy name	Direction
eth0	shaper0	EGRESS

Show of ATOSNT qos p-fifo-default

Level of log : 1

Description :

Type : LIMIT

Sub type : P-FIFO

Mean rate window (sec) : 0

Packets number : 128

LIST OF ACTIONS

Empty list

Show of ATOSNT qos b-fifo-default

Level of log : 1

Description :

Type : LIMIT

Sub type : B-FIFO

Mean rate window (sec) : 0

Bytes number : 128000

LIST OF ACTIONS

Empty list

Show of ATOSNT qos classifier-voip

Description :

Type : MATCH-ANY

LIST OF RULES

Type	Value/Type	Value	Mask	Byte-id	Priority
CLASSIFIER-MAP	CLASS-VOIP				1

Show of ATOSNT qos classifier-web

Description :

Type : MATCH-ANY

LIST OF RULES

Type	Value/Type	Value	Mask	Byte-id	Priority
IP-HDR	SPORT	80	FFFF		1

Show of ATOSNT qos shaper0

Level of log : 1

Description :

Type : SHAPING

Sub type : CBQ

Mean rate window (sec) : 0

Average packet (bytes) : 1000

Bandwidth (bit) : 100000000

Cell (bytes) : 8

EWMA : 5

MPU (bytes) : 0

LIST OF ACTIONS

Empty list

Show of ATOSNT qos shaper0 queue-13m

Description :

Type : CBQ

Priority : 8

Policy name :

Parent name :

Mean rate window (sec) : 0

Rate (bps) : 13000000

Allot (bytes) : 1514

Average packet (bytes) : 1000

Bounded : true

Isolated : false

LIST OF CLASSIFIERS

Empty list

Show of ATOSNT qos shaper0 queue-voip

Description :

Type : CBQ
Priority : 1
Policy name :
Parent name : queue-13M
Mean rate window (sec) : 0
Rate (bps) : 5000000
Allot (bytes) : 1514
Average packet (bytes) : 1000
Bounded : true
Isolated : false
LIST OF CLASSIFIERS
classifier-VOIP
Show of ATOSNT qos shaper0 queue-web
Description :
Type : CBQ
Priority : 5
Policy name :
Parent name : queue-13M
Mean rate window (sec) : 0
Rate (bps) : 8000000
Allot (bytes) : 1514
Average packet (bytes) : 1000
Bounded : true
Isolated : false
LIST OF CLASSIFIERS
classifier-WEB
Command executed

HTB

Hierarchy Token Bucket - HTB

HTB is meant as a more understandable and intuitive replacement for the CBQ policy. Both CBQ and HTB help you to control the use of the outbound bandwidth on a given link. Both allow you to use one physical link to simulate several slower links and to send different kinds of traffic on different simulated links. In both cases, you have to specify how to divide the physical link into simulated links and how to decide which simulated link to use for a given packet to be sent.

Unlike CBQ, HTB shapes traffic based on the Token Bucket Filter algorithm which does not depend on interface characteristics and so does not need to know the underlying bandwidth of the outgoing interface.

HTB ensures that the amount of service provided to each queue is at least the minimum of the amount it requests and the amount assigned to it. When a queue requests less than the amount assigned, the remaining (excess) bandwidth is distributed to other queues which request service.

This is the syntax to use:

```
ATOSNT\qos>>add POLICY shaper0 SHAPING HTB
Command executed
```

A new node **shaper0** has been created where you can configure the following parameters with the help of set, add and del commands.

```
ATOSNT\qos\shaper0>>set ?

Nodes not available.
Set command parameters:
 level of log            [loglevel]          Current value: 1
 description             [description]       Current value:
 mean rate window (sec)  [mean-rate-window]  Current value: 0
```

Table 47: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the Policy events. Default: 1
description	Descriptive string of the created POLICY.
mean-rate-window (sec) [0-60]	Sets the mean rate observation window Default: 0

When adding the policy, a default queue that occupies the full bandwith is created

Additional flows, bandwiths and priorities are defined by adding queues.

Unclassified traffic will be conveyed to the default queue and will be scheduled at the lowest priority.

Under the new node **shaper0**, you can add or delete an Action or a new Queue.

```
ATOSNT\qos\shaper0>>add?

add  help :  Add a new action or queue
add  usage:
 <ACTION><marking-type><value><classifier-name>
 <QUEUE>[name]<rate><burst>[priority][parent-queue]

add command parameters:
 ACTION
 QUEUE
```

Table 48: add QUEUE

Syntax	Description
QUEUE	Keyword
name [max 16 char]	Name of the created Queue
rate (bps) [1-100000000]	Maximum rate this queue and all its children are guaranteed.
burst (bytes) [1-150000]	Amount of bytes that can be burst at ceil speed, in excess of the configured rate. Should be at least as high as the highest burst of all children.
priority [1-8]	Sets the queue priority to be scheduled
parent [Empty list]	sets the list of the parent queues

```
ATOSNT\qos\shaper0>>del ?

del help: Remove an action or queue del usage:

<ACTION><marking-type><value><classifier-name>
 <QUEUE><name>

del command parameters:

ACTION
QUEUE
```

In the created node **queue0**, you can configure the following parameters:

```
ATOSNT\qos\shaper0\queue0>>set ?

Nodes not available.
Set command parameters:
 description             [description]          Current value:
 priority                [priority]             Current value: 1
 policy name             [policy-name]          Current value:
 mean rate window (sec)  [mean-rate-window]     Current value: 0
 rate (bps)              [rate]                 Current value: 5000000
 burst (bytes)           [burst]                Current value: 15000
 ceil rate (bps)         [ceil-rate]            Current value: 5000000
 default                 [default]              Current value: false
```

Table 49: set

Syntax	Description
description	Descriptive string of the created POLICY.
priority [1-8]	Sets the queue priority to be scheduled . The priority value of 1 corresponds to the highest priority. Default: 8.
policy-name [<cr>|p-fifo-default|b-fifo-default|shaper0]	Name of the policy associated to the created queue.
mean-rate-window (sec) [0-60]	Sets the mean rate observation window. Default: 0
rate (bps) [1-100000000]	Sets the minimum bandwith that will be guaranteed to a queue when all the queues in the policy are underprovisioned.
burst (bytes) [1-150000]	Amount of bytes that can be burst at ceil speed, in excess of the configured rate. Should be at least as high as the highest burst of all children.
ceil-rate (bps) [1-100000000]	The ceil parameter specifies the maximum bandwidth that a queue can use. The default ceil is the same as the rate. Default: 100000000.
default	Parameter that automatically modifies the queue in default queue. Default: false

```
ATOSNT\qos\shaper0\queue0>>add ?

add  help :  Add a new classifier
add  usage:
 <CLASSIFIER><name>

add command parameters:
 CLASSIFIER

ATOSNT\qos\shaper0\queue0>>add CLASSIFIER ?

add command parameters:
 name     [classifier0]
```

It creates a correspondence table between the queue and the classifiers.

A queue can convey different classifiers, but the same classifier can not exist in two different queues.

To separate and manage the different traffic types (bandwidth and priority) under the newly created QUEUE, you should add a “sub-queue”: when creating the sub-queue, you must specify the main queues with **parent-queue** .

Within each subqueue, packets will be issued following a **P-FIFO** policy by default.

You can assign to each queue, a policy of traffic control different from the P-FIFO. In this case you should add a new policy.

```
ATOSNT\qos\shaper0\queue0>>del ?

del help : Remove a classifier del usage:

<CLASSIFIER><name>

del command parameters:

CLASSIFIER
```

Example 8

Suppose:

- Having a 100 Mbit interface eth0.
- Trying to select a traffic type of VOIP and WEB traffic
- Wanting to give VoIP + WEB + Best Effort traffic a maximum bandwidth of 20 Mbps
- Wanting to give VoIP traffic priority 1 and a band of 5 Mbps
- Wanting to give WEB traffic priority 5 and a band of 8 Mbps
- Wanting to give Best Effort traffic priority 8 and a band of 7 Mbps
- If the bandwidth is available, all traffic types can individually reach 20 Mbps

How to configure a POLICY SHAPING HTB to select and give the VoIP, WEB and Best Effort traffic a maximum bandwidth of 20 Mbps, assigning to VOIP traffic priority 1 and a band of 5 Mbps, to WEB traffic, a priority 5 and a band of 8 Mbps and to the Best Effort priority 8 and band of 7 Mbps. With ceil parameter set to 20 Mbps, the excess bandwith can be distributed into all traffic types which can individually reach the same rate, if the bandwith is available.

ATOSNT\qos>>**conf**

add classifier-map CLASS-VOIP 1 permit udp host 192.168.1.1 any range 18000 18032 anyport

add qos CLASSIFIER classifier-VOIP

add qos CLASSIFIER classifier-WEB

add qos POLICY shaper0 SHAPING HTB

add qos SERVICE eth0 shaper0

add qos classifier-voip CLASSIFIER-MAP CLASS-VOIP

add qos classifier-web IP-HDR SPORT 80 FFFF

add qos shaper0 QUEUE queue-20M 20000000 15000 1

add qos shaper0 QUEUE queue-voip 5000000 15000 1 queue-20M

add qos shaper0 QUEUE queue-web 8000000 15000 5 queue-20M

add qos shaper0 QUEUE queue-besteffort 7000000 15000 5 queue-20M

set qos shaper0 queue-20m priority 1

set qos shaper0 queue-20m rate 20000000

set qos shaper0 queue-20m ceil-rate 20000000

add qos shaper0 queue-voip CLASSIFIER classifier-VOIP

set qos shaper0 queue-voip priority 1

set qos shaper0 queue-voip rate 5000000

set qos shaper0 queue-voip ceil-rate 20000000

add qos shaper0 queue-web CLASSIFIER classifier-WEB

set qos shaper0 queue-web priority 5

set qos shaper0 queue-web rate 8000000

set qos shaper0 queue-web ceil-rate 20000000

set qos shaper0 queue-web default true

set qos shaper0 queue-besteffort rate 7000000

set qos shaper0 queue-web ceil-rate 70000000

ATOSNT\qos>>**show work**

Show of ATOSNT qos

Level of log : 1

LIST OF SERVICES

Interface name	Policy name	Direction
eth0	shaper0	EGRESS

Show of ATOSNT qos p-fifo-default

Level of log : 1

Description :

Type : LIMIT

Sub type : P-FIFO

Mean rate window (sec) : 0

Packets number : 128

LIST OF ACTIONS

Empty list

Show of ATOSNT qos b-fifo-default

Level of log : 1

Description :

Type : LIMIT

Sub type : B-FIFO

Mean rate window (sec) : 0

Bytes number : 128000

LIST OF ACTIONS

Empty list

Show of ATOSNT qos classifier-voip

Description :

Type : MATCH-ANY

LIST OF RULES

Type	Value/Type	Value	Mask	Byte-id	Priority
CLASSIFIER-MAP	CLASS-VOIP				1

Show of ATOSNT qos classifier-web

Description :

Type : MATCH-ANY

LIST OF RULES

Type	Value/Type	Value	Mask	Byte-id	Priority
IP-HDR	SPORT	80	FFFF		1

Show of ATOSNT qos shaper0

Level of log : 1

Description :

Type : SHAPING

Sub type : HTB

Mean rate window (sec) : 0

LIST OF ACTIONS

Empty list

Show of ATOSNT qos shaper0 queue-20m

Description :

Type : HTB

Priority : 1

Policy name :

Parent name :

Mean rate window (sec) : 0

Rate (bps) : 20000000

Burst (bytes) : 15000

Ceil rate (bps) : 20000000

Default : false

LIST OF CLASSIFIERS

Empty list

Show of ATOSNT qos shaper0 queue-voip

Description :

Type : HTB

Priority : 1

Policy name :

Parent name : queue-20M

Mean rate window (sec) : 0

Rate (bps) : 5000000

Burst (bytes) : 15000
Ceil rate (bps) : 20000000
Default : false
LIST OF CLASSIFIERS
classifier-VOIP
Show of ATOSNT qos shaper0 queue-web
Description :
Type : HTB
Priority : 5
Policy name :
Parent name : queue-20M
Mean rate window (sec) : 0
Rate (bps) : 8000000
Burst (bytes) : 15000
Ceil rate (bps) : 20000000
Default : false
LIST OF CLASSIFIERS
Empty List
Show of ATOSNT qos shaper0 queue-besteffort
Description :
Type : HTB
Priority : 8
Policy name :
Parent name : queue-20M
Mean rate window (sec) : 0
Rate (bps) : 7000000
Burst (bytes) : 15000
Ceil rate (bps) : 70000000
Default : false
LIST OF CLASSIFIERS
Empty List
Command executed

POLICING

Policing is the process of discarding packets (by a dropper) within a traffic stream in accordance with the state of a corresponding meter enforcing a traffic profile.

The policing process is done on **ingress** edge router's domain. The policer avoids brute flows from entering the domain by policing them before they enter.

The policer is in charge of:

- Classify incoming packets to put them in behavior aggregates or flows.
- Apply traffic policing rules to fulfill the service level agreement
- Drop those packets that violate the rules

After doing the classification, it just marks a field in the packet's buffer to signaling the result of this, **flow aggregation** is done using the filter elements based on actual **throughput** and **bursty** conditions. In this way, packets marked are placed in different flows.

Apply **policing rules** to fulfill the service level agreement.
Keywords for policing are as follows:
<rate> : defines the maximum rate (throughput) admitted for this type of traffic.
<burst> : defines the maximum burst admitted for this type of traffic.
continue : this means, packets violating this rule must be passed to the next police rule (next filter element).
drop : this means, packets violating this rule must be dropped.
policy marker : allows to associate the incoming traffic to the flow that is transiting the data packets

This is the syntax to be used:

```
ATOSNT\qos>>add POLICY POLICING
Command executed
```

A new node **policy0** has been created where you can configure the following parameters with set, add and del commands.

```
ATOSNT\qos\policy0>>set ?

Nodes not available.
Set command parameters:
 level of log  [loglevel]     Current value: 1
 description   [description]  Current value:
```

Table 50: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the ATM events. Default: 1
description [max 100 char]	A brief description of the created policy

For flows aggregation, you should use add command as bellow.

```
ATOSNT\qos\policy0>>add ?

add  help :  Add a new action or flow
add  usage:
 <ACTION><marking-type><value><classifier-name>
 <FLOW>[name]<rate><burst>[precedence]

add command parameters:
 ACTION
 FLOW
```

Table 51: add FLOW

Syntax	Description
FLOW	Keyword
name [max 16 char]	Name of the created Flow
rate (kbps) [0-100000]	Defines the maximum rate (throughput) admitted for this type of traffic.
burst (bytes) [1-10000000]	Defines the maximum burst admitted for this type of traffic.
precedence [1-65535]	Sets the order in which Flows will be managed

Two words about **burst**. Bursting here is not synonymous of buffering. There's no any packet buffering here because **ingress POLICING** doesn't enqueue packets. Policing filters act using a **token bucket** to control bandwidth. You can learn more about this by reading the section **POLICY SHAPING TBF**. When you define 'police rate 1500 kbps burst 90k', what you are saying is: when throughput is less than 1500 kbps, **tokens** are saved (because they are injected into the bucket to a 1500 kbps rate and retired to a lower rate) to be used later, when throughput increases and this saving is needed. Then, burst 90 KB means that you can save up to a maximum of 90 KB of equivalent tokens. This setting permits to deal with bursty flows, but at the same time controlling the maximum permitted burstiness.

To remove an Action or Flow, you should use del command.

```
ATOSNT\qos\policy0>>del ?

Available nodes:
                        flow0
                        flow1
                        flow2
del  help :  Remove an action or flow
del  usage:
 <ACTION><marking-type><value><classifier-name>
 <FLOW><name>

del command parameters:
 ACTION
 FLOW
ATOSNT\qos\policy0>>del FLOW ?

del command parameters:
 name           [flow0|flow1|flow2]
```

Example 9

- Admiting incoming traffic up to a maximum of 4000 kbps in three scales
- First scale admits traffic from 0 up to 1500 kbps with a maximum burst of 90KB.
- Second scale admits traffic above 1500kbps, but up to a maximum of 1500 kbps more, with a maximum burst of 90 KB
- Third scale admits traffic above 3000kbps, but up to a maximum of 1000 kbps more, with a maximum burst of 60 KB.
- Traffic from network exceeding this profile is dropped.
- Traffic from any other network is admited from 0 up to 1000 kbps, with a maximum burst of 60KB (no scales are implemented in this case). Traffic exceeding this profile will be dropped.

How to configure a POLICY POLICING to admit incoming traffic up to a maximum of 4000 kbps, but in three scales.

The **first policy rule** applied is to traffic marked and agreggated to flow0. Traffic that exceeds this setting must be passed to the next police rule (CONTINUE).

Second police rule is applied to traffic that:
a.- does not match the first police rule, or,
b.- has matched but exceeds the first police rule.

The second rule will be applied to traffic marked, admitted and aggregated to flow1 up to a maximum rate of 1500 kbps with a maximum burst of 90 KB. Traffic that exceeds this setting must be passed to the next police rule (CONTINUE).

Third police rule is applied to traffic that:
a.- does not match the second police rule, or,
b.- has matched but exceeds the second police rule.
The third rule will be applied to traffic marked, admitted and aggregated to flow2 up to a maximum rate of 1000 kbps with a maximum burst of 60 KB. Traffic that exceeds this setting must be dropped (drop).

Fourth police rule is applied to traffic that does not match the third police rule (neither the first and second, of course). We can't have traffic that match the three previous rules here, because all this traffic was dropped by the third rule. Fourth policy rule will be applied to traffic marked, admitted and aggregated to flow3 up to a maximum rate of 1000 kbps with a maximum burst of 60 KB. Traffic that exceeds this setting must be dropped (drop).

ATOSNT\qos>>**conf**

add qos POLICY policy0 POLICING

add qos POLICY policy1 POLICING

add qos policy0 FLOW flow0 1500 90 1

add qos policy0 FLOW flow1 1500 90 2

add qos policy0 FLOW flow2 1000 60 3

set qos policy0 flow0 rate 1500

set qos policy0 flow0 burst 90

set qos policy0 flow0 action-on-traffic-exceeding CONTINUE

set qos policy0 flow1 rate 1500

set qos policy0 flow1 burst 90

set qos policy0 flow1 action-on-traffic-exceeding CONTINUE

set qos policy0 flow1 policy-marker 2

set qos policy0 flow2 burst 60

set qos policy0 flow2 policy-marker 3

add qos policy1 FLOW flow3 1000 60 1

set qos policy1 flow3 burst 60

set qos policy1 flow3 policy-marker 4

ATOSNT\qos>>**show work**

Show of ATOSNT qos

Level of log : 1

LIST OF SERVICES

Empty list

Show of ATOSNT qos p-fifo-default

Level of log : 1

Description :

Type : LIMIT

Sub type : P-FIFO

Mean rate window (sec) : 0

Packets number : 128

LIST OF ACTIONS

Empty list

Show of ATOSNT qos b-fifo-default

Level of log : 1

Description :

Type : LIMIT

Sub type : B-FIFO

Mean rate window (sec) : 0

Bytes number : 128000

LIST OF ACTIONS

Empty list

Show of ATOSNT qos policy0

Level of log : 1

Description :

Type : POLICING

LIST OF ACTIONS

Empty list

Show of ATOSNT qos policy0 flow0
Description :
Precedence : 1
Rate (kbps) : 1500
Burst size (bytes) : 90
Action on traffic exceeding : CONTINUE
Policy marker : 1
LIST OF CLASSIFIERS
Empty list
Show of ATOSNT qos policy0 flow1
Description :
Precedence : 2
Rate (kbps) : 1500
Burst size (bytes) : 90
Action on traffic exceeding : CONTINUE
Policy marker : 2
LIST OF CLASSIFIERS
Empty list
Show of ATOSNT qos policy0 flow2
Description :
Precedence : 3
Rate (kbps) : 1000
Burst size (bytes) : 60
Action on traffic exceeding : DROP
Policy marker : 3
LIST OF CLASSIFIERS
Empty list
Show of ATOSNT qos policy1
Level of log : 1
Description :
Type : POLICING
LIST OF ACTIONS
Empty list
Show of ATOSNT qos policy1 flow3
Description :
Precedence : 1
Rate (kbps) : 1000
Burst size (bytes) : 60
Action on traffic exceeding : DROP
Policy marker : 4
LIST OF CLASSIFIERS
Empty list
Command executed

In **flow0** node you can configure the following parameters con set and add commands

```
ATOSNT\qos\policy0\flow0>>set ?
```

```
Nodes not available.
Set command parameters:
 description                 [description]                 Current va
 rate (kbps)                 [rate]                        Current va0
 burst size (bytes)          [burst]                       Current va0
 action on traffic exceeding [action-on-traffic-exceeding] Current vaP
 policy marker               [policy-marker]               Current va1

ATOSNT\qos\policy0\flow0>>add ?

add  help :  Add a new classifier
add  usage:
 <CLASSIFIER><name>

add command parameters:
 CLASSIFIER
```

NATIVE

Unlike the other policies we have seen so far, software based on ATOSNT, **POLICY NATIVE** is a policy that depends on the CPE hardware characteristics and that varies from CPE model to model . In particular, it is based on the hardware QoS implementation of the chosen microprocessor ethernet controller for that particular board. Examples of hardwarer aided features can be:

— QoS with up to 8 Tx priority queues

— Up to eight Tx (buffer descriptor - i.e. queues) rings to satisfy QoS requirements.

— Transmit Scheduler with SPQ/WFQ (*WFQ is only supported by some CPE models like BG7420*) and Rate Limiter

— ...

Receive and Transmit Buffer Descriptors (BDs)

The Ethernet Controller maintains multiple Tx Buffer Descriptor (BD) rings to satisfy QoS requirements.Up to **eight** Transmit BD rings are supported.

Quality of Service (QoS)

The Ethernet scheduling system is composed of two main functional modules:

- A **work-conserving scheduler**, and a
- data **shaper**.

The scheduling is **work-conserving**, meaning that if one flow is out of packets, the next data flow will take its place. Hence, the scheduling tries to prevent link resources from going unused.

Ethernet Scheduler

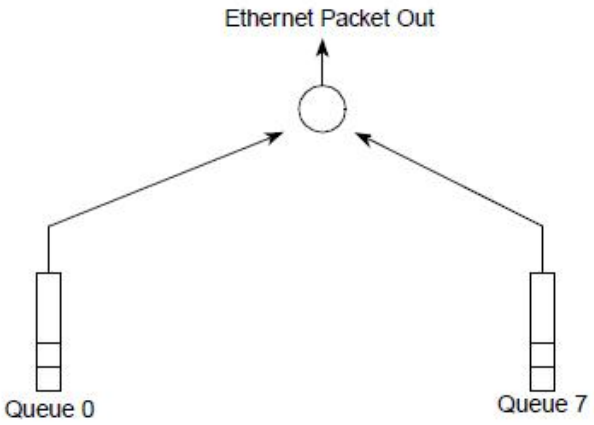
The scheduling scheme of the Ethernet controller transmitter role is to select the next packet to be transmitted on the line. A single transmitter resource (ethernet port) is shared by **8 queues**, as depicted in the figure below. Each of the queues contains a random number of packets with a random length. The scheduling system is invoked whenever a new packet has to be transmitted, and updated after packet transmission completion.

The scheduler module selects the next queue to be handled by an ethernet controller. The Traffic Shaper controls the data rate on the line using a real time scale, enabling the user either to limit data rate to a certain value, or to limit the maximum burst length, or both.

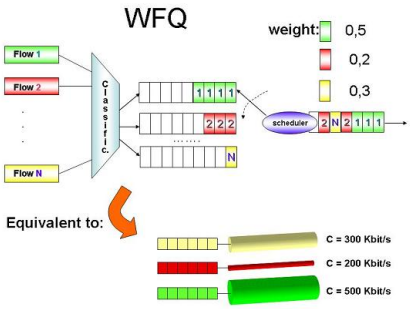
The scheduler module may support two scheduling hierarchies. The upper hierarchy imposes a scheduling policy of **Strict priority (SP)** . The lower hierarchy implies a scheduling policy of **Weighted Fair Queuing (WFQ)**. The scheduler module handles up to 8 queues, each of them may be associated either with a different QoS or pre allocated BW.

The **Strict Priority (SP)** scheduler works in this way: it services the highest priority queue until it is empty, and then moves to the next highest priority queue, and so on. It is possible that if there is enough high priority traffic, the lower priorities could be completely frozen out.

Any queue may be configured either as SP queue or as a WFQ queue. The SP queues are always with higher priority than the WFQ queues.



In the below figure, there is an example of a **Weighted Fair Queuing (WFQ)** policy with the bandwith distribution between three queues.



This is the syntax to use:

```
ATOSNT\qos>>add POLICY NATIVE ?

add command parameters:
 sub type       [NATIVE]
 <cr>

ATOSNT\qos>>add POLICY NATIVE NATIVE
Command executed
```

A new node **policy2** has been created where you can configure the following parameters with set, add and del commands.

```
ATOSNT\qos\policy2>>set ?

Nodes not available.
Set command parameters:
 level of log                    [loglevel]          Current value: 1
 description                     [description]       Current value:
 rate (kbps)                     [rate]              Current value: shaping-disabled
 burst (bytes)                   [burst]             Current value: 0
```

Table 52: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the Policy events. Default: 1
description [max 100 char]	A brief description of the created policy
rate (kbps) [100-100000|shaping-disabled]	Sets the output packets transmission rate or Shaping rate. Default: shaping-disabled
burst (bytes) [0-4294967295]	Amount of bytes that can be burst in excess of the configured rate. Default: 0

To add or del a new Action or Queue, you should use add and del commands.

```
ATOSNT\qos\policy2>>del ?

Available nodes:
                        queue0
del  help :  Remove an action or queue
del  usage:
 <ACTION><marking-type><value><classifier-name>
 <QUEUE><name>

del command parameters:
 ACTION
 QUEUE
```

```
ATOSNT\qos\policy2>>add ?

add  help :  Add a new action or queue
add  usage:
 <ACTION><marking-type><value><classifier-name>
 <QUEUE>[name]<type><value>>

add command parameters:
 ACTION
 QUEUE

ATOSNT\qos\policy2>>add QUEUE queue0 ?
```

```
add command parameters:
type          [SP|WFQ]
ATOSNT\qos\policy2>>add QUEUE queue0 SP ?

add command parameters:
 priority      [1-8]

ATOSNT\qos\policy2>>add QUEUE queue0 SP 1
Command executed
```

WFQ *policy is only supported by some CPE models like BG7420.*
In this case, the syntax to be used is :

```
ATOSNT\qos\policy0>>add QUEUE queue0 WFQ ?

 add command parameters:
 weight        [1-99]

ATOSNT\qos\policy0>>add QUEUE queue0 WFQ 50
Command executed
```

Table 53: add QUEUE SP

Syntax	Description
QUEUE	Keyword
name [max 16 char]	Name of the created Queue
type [SP]	Sets the sub-type policy to apply to the queue. • **SP** stands for Strict Priority scheduling. the queue always gets its priority if it is not empty
burst (bytes) [0-4294967295]	Amount of bytes that can be burst in excess of the configured rate.
priority [1-8]	Sets the queue priority to be scheduled

A new node **queue0** has been created where you can configure the following parameters with set, add and del commands.

```
ATOSNT\qos\policy2\queue0>>set ?

Nodes not available.
Set command parameters:
 description             [description]          Current value:
 priority                [priority]             Current value: 1
 policy name             [policy-name]          Current value: p-fifo-default
```

Table 54: set

Syntax	Description
description [max 100 char]	A brief description of the created Queue
priority [1-8]	Sets the queue priority to be scheduled. Default: 8
policy-name [<cr>|p-fifo-default|b-fifo-default|policy0]	Sets the policy to apply to the queue

Table 55: add QUEUE SP/WFQ *only available in some CPE models like BG7420*

Syntax	Description
QUEUE	Keyword
name [max 16 char]	Name of the created Queue
type [SP|WFQ]	Sets the sub-type policy to apply to the queue. • **SP** stands for Strict Priority scheduling. the queue always gets its priority if it is not empty • **WFQ** Weighted Fair Queuing prevents the case of starvation if there is a chance that the SP queue will be busy most of the time allowing the remaining bandwith distribution between the data flows. It is recommended that if a Queue that has to be in high priority is empty most of the time, it will be configured as SP queue. If a Queue that has to get high priority is not empty most of the time, it is recommended to configure it as WFQ queue with low WeightFactor in order to prevent starvation
weight [1-99]	Weight parameter specifies the bandwith distribution in percentage (%) assigned to each data flow or queue in case of congestion
rate (kbps) [100-100000|shaping-disabled]	Sets the output packets transmission rate or Shaping rate. Default: shaping-disabled
burst (bytes) [2000-65535]	Amount of bytes that can be burst in excess of the configured rate. Default: 2000

When a **WFQ** policy is applied, a new node **queue0** is created and you can configure the following parameters with set and add commands.

```
ATOSNT\qos\policy0\queue0>>set ?

Nodes not available.
Set command parameters:
 description             [description]          Current value:
 policy name             [policy-name]          Current value: p-fifo-default
 weight                  [weight]               Current value: 50
 rate (kbps)             [rate]                 Current value: shaping-disabled
 burst (bytes)           [burst]                Current value: 2000
```

```
ATOSNT\qos\policy2\queue0>>add ?

add  help :  Add a new classifier
add  usage:
 <CLASSIFIER><name>

add command parameters:
```

```
 CLASSIFIER

ATOSNT\qos\policy0\queue0>>add CLASSIFIER ?

add command parameters:
 name          [classifier0]
```

Table 56: add CLASSIFIER

Syntax	Description
CLASSIFIER	Keyword
name	Sets the name of the classifier associated to the queue.

Example 10

Suppose:

- Trying to select voice traffic type using the DSCP field in the IP header
- Assigning priority 1 to voice traffic against the remaining traffic named best effort

How to configure a POLICY NATIVE NATIVE to select Voice traffic to give it the highest priority against the remaining traffic named Best-effort

ATOSNT\qos>>**conf**

set xdsl0 mode vdsl2_over_pots

add interfaces IFC ptm0 ptm0

add qos CLASSIFIER voce

add qos POLICY policy0 NATIVE NATIVE

add qos POLICY shape_native NATIVE NATIVE

add qos SERVICE ptm0 shape_native

add qos policy0 QUEUE queue0 SP 1

set qos policy0 queue0 priority 1

add qos voce DSCP 46

add qos shape_native QUEUE queue_voce SP 1

add qos shape_native QUEUE queue_be SP 8

add qos shape_native queue_voce CLASSIFIER voce

set qos shape_native queue_voce priority 1

ATOSNT\qos>>**show work**

Show of ATOSNT qos

Level of log : 1

LIST OF SERVICES

Interface name	Policy name	Direction
ptm0	shape_native	EGRESS

Show of ATOSNT qos p-fifo-default

Level of log : 1

Description :

Type : LIMIT

Sub type : P-FIFO

Mean rate window (sec) : 0

Packets number : 128

LIST OF ACTIONS

Empty list

Show of ATOSNT qos b-fifo-default

Level of log : 1

Description :

Type : LIMIT

Sub type : B-FIFO

Mean rate window (sec) : 0

Bytes number : 128000

LIST OF ACTIONS

Empty list

Show of ATOSNT qos policy0

Level of log : 1

Description :

Type : NATIVE

Sub type : NATIVE

Rate (kbps) : shaping-disabled

Burst (bytes) : 0

LIST OF ACTIONS

Empty list

Show of ATOSNT qos policy0 queue0

Description :

Type : NATIVE

Priority : 1

Policy name : p-fifo-default

LIST OF CLASSIFIERS

Empty list

Show of ATOSNT qos voce

Description :

Type : MATCH-ANY

LIST OF RULES

Type	Value/Type	Value Mask	Byte-id	Priority
DSCP	46			1

Show of ATOSNT qos shape_native

Level of log : 1

Description :

Type : NATIVE

Sub type : NATIVE

Rate (kbps) : shaping-disabled

Burst (bytes) : 0

LIST OF ACTIONS

Empty list

Show of ATOSNT qos shape_native queue_voce

Description :

Type : NATIVE

Priority : 1

Policy name : p-fifo-default

LIST OF CLASSIFIERS

voce

Show of ATOSNT qos shape_native queue_be

Description :

Type : NATIVE

Priority : 8

Policy name : p-fifo-default

LIST OF CLASSIFIERS

Empty list

Command executed

ATOSNT\qos>>**show statistics**

statistics of egress policy shape_native on ifc ptm0

statistics of policy

packets : 32229

bytes : 2096532

dropped : 0

statistics of queue queue_voce in policy

packets : 16340

bytes : 1143192

dropped : 0

atatistics of queue queue_be in policy

packets : 15889

bytes : 953340

Example 11

Suppose:

- Trying to select voice traffic type using the DSCP field in the IP header
- Output shaping is 50 Mbps distributed like this:

  20 Mbps is assigned to voice traffic (highest priority)

  30 Mbps are distributed in 3 queues to manage besteffort, Management and UDP traffic with weights w1-w2-w3 of 50-30-20% respectively.

How to configure a POLICY NATIVE NATIVE to manage voice traffic with SP policy and besteffort, Management and UDP traffic with WFQ policy

ATOSNT>>**conf**

set xdsl0 mode vdsl2_over_pots

add classifier-map MANAGEMENT 1 permit tcp 10.0.120.0 0.0.1.255 router anyport equ telnet

add interfaces IFC eth0 eth0

add interfaces IFC ptm0 ptm0

add qos CLASSIFIER voice

add qos CLASSIFIER MANAGEMENT

add qos CLASSIFIER UDP

add qos POLICY shape_native NATIVE NATIVE

add qos SERVICE ptm0 shape_native

add qos voice DSCP 46

add qos udp PROTOCOL udp

add qos shape_native QUEUE shape-voice SP 1

add qos shape_native QUEUE shape-besteffort WFQ 50

add qos shape_native QUEUE shape-management WFQ 30

add qos shape_native QUEUE shape-udp WFQ 20

set qos shape_native rate 50000

set qos shape_native burst 15000

add qos shape_native shape-voice CLASSIFIER voice

set qos shape_native shape-voice priority 1

set qos shape_native shape-besteffort weight 50

add qos shape_native shape-management CLASSIFIER MANAGEMENT

set qos shape_native shape-management weight 30

add qos shape_native shape-udp CLASSIFIER UDP

set qos shape_native shape-udp weight 20

ATOSNT\qos>>**show work**

Show of ATOSNT system

Level of log : 1

Show of ATOSNT xdsl0

Enable : on

Level of log : 1

Mode : vdsl2_over_pots

Show of ATOSNT ptm

Level of log : 1

Show of ATOSNT ptm ptm0

Level of log : 1

Physical Port : xdsl0.0

Tx rate limit (kbps) : no-limit

Tx burst (bytes) : 2000

Show of ATOSNT classifier-map

Level of log : 1

LIST OF CLASSIFIER MAPS

Classifier map name : MANAGEMENT

RULE N. : 1

Right : permit

Protocol/profile : tcp

Source address : 10.0.120.0

Source wild mask : 0.0.1.255

Dest address : router

Source port : anyport

Dest port : equ

Max dest port : telnet

```
Show of ATOSNT qos
Level of log : 1
LIST OF SERVICES
Interface name  Policy name      Direction
ptm0            shape_native     EGRESS
Show of ATOSNT qos p-fifo-default
Level of log          : 1
Description           :
Type                  : LIMIT
Sub type              : P-FIFO
Mean rate window (sec) : 0
Packets number        : 64
LIST OF ACTIONS
Empty list
Show of ATOSNT qos b-fifo-default
Level of log          : 1
Description           :
Type                  : LIMIT
Sub type              : B-FIFO
Mean rate window (sec) : 0
Bytes number          : 128000
LIST OF ACTIONS
Empty list
Show of ATOSNT qos voice
Description :
Type       : MATCH-ANY
LIST OF RULES
Type              Value/Type                  Value     Mask     Byte-id   Priority
DSCP              46                                              1
Show of ATOSNT qos management
Description :
Type       : MATCH-ANY
LIST OF RULES
Empty list
Show of ATOSNT qos udp
Description :
Type       : MATCH-ANY
LIST OF RULES
Type              Value/Type                  Value     Mask     Byte-id   Priority
PROTOCOL          udp                                             1
Show of ATOSNT qos shape_native
Level of log                : 1
Description                 :
Type                        : NATIVE
Sub type                    : NATIVE
Rate (kbps)                 : 50000
Burst (bytes)               : 15000
```

LIST OF ACTIONS

Empty list

Show of ATOSNT qos shape_native shape-voice

Description :

Type : NATIVE

Priority : 1

Policy name : p-fifo-default

Rate (kbps) : shaping-disabled

Burst (bytes) : 2000

LIST OF CLASSIFIERS

voice

Show of ATOSNT qos shape_native shape-besteffort

Description :

Type : NATIVE

Policy name : p-fifo-default

Weight : 50

Rate (kbps) : shaping-disabled

Burst (bytes) : 2000

LIST OF CLASSIFIERS

Empty list

Show of ATOSNT qos shape_native shape-management

Description :

Type : NATIVE

Policy name : p-fifo-default

Weight : 30

Rate (kbps) : shaping-disabled

Burst (bytes) : 2000

LIST OF CLASSIFIERS

MANAGEMENT

Show of ATOSNT qos shape_native shape-udp

Description :

Type : NATIVE

Policy name : p-fifo-default

Weight : 20

Rate (kbps) : shaping-disabled

Burst (bytes) : 2000

LIST OF CLASSIFIERS

UDP

Index

ManSecurity

Security

Introduction

IPSec is a suite of protocols used to create secure VPNs on the public network (“tunnel” mode) or to provide secure end-to-end connections (“transport” mode) between pairs of hosts.

IPSec provides security services to the set of IP protocols, including all the higher level protocols, by offering the following services:

- data integrity;
- data origin authentication;
- replay protection;
- confidentiality.

A number of information structures are necessary for IPSec to operate.

A **Security Association** (SA) defines an IPSec connection. A SA is a kind of contract between the two endpoints, which contains the security policy that applies to some specific type of traffic sent or received by either endpoint. SAs are unidirectional in nature, so different SAs may apply in either direction.

An IPSEC implementation manages a **Security Association Database** (SAD). Each entry in the SAD contains the information necessary to describe a specific SA (the encapsulation protocol to be used, a number of fields used to provide protection to anti-replay attacks, the authentication and the encryption algorithms used with the relevant cryptographic keys and initialization vectors). Each SA is identified with a **Security Parameter Index** (SPI).

An IPSec entity also manages a **Security Policy Database** (SPD). An entry in the SPD describes a specific traffic flow using a number of **Selector Fields** (source and destination address, source destination protocol, protocol type, etc.) and points to an entry in the SAD.

Each individual outbound packet is checked against the SPD. A matching SPD entry contains a pointer to the SA that must be applied to that packet.

The SPI field is always transmitted in the clear and it is used to identify the SA applicable to incoming packets. Once the SA is identified, the packet can be properly processed (removal of security encapsulation, decryption, authentication and integrity checks, etc.).

An SA can be either manually configured or, if a matching SPD entry does not contain a valid SA pointer, the applicable SA can be automatically negotiated between the two peers using the IKE1protocols.

IPSec encapsulates traffic using the Authentication Header Protocol (AH)2or the Encapsulating Security Payload Protocol (ESP)3.

These two encapsulations can be cascaded in order to have IPSec connections with a combination of security features.

IPSec operating modes

IPsec uses two different protocols - AH and ESP - to ensure the authentication, integrity and confidentiality of the communication. It can protect either the entire IP datagram or only the upper-layer protocols. The appropiate modes are called tunnel mode and transport mode. In tunnel mode the IP datagram is fully encapsulated by a new IP datagram using the IPsec protocol. In transport mode only the payload of the IP datagram is handled by the IPsec protocol inserting the IPsec header between the IP header and the upper-layer protocol header.

The IPSec "Transport" mode is typically used to provide a secure end-to-end connection between two hosts. Each packet is encapsulated based on the security protocol (AH or ESP) indicated in the relevant SP.

Figure 1– "Transport" mode

The AH protocol inserts an AH header after the existing IP header. The AH header contains an SPI, and the information used to authenticate the whole packet. The existing IP payload and some fields in the IP header are not modified. However, a number of fields in the IP header may change during the packet transport. These "mutable" fields cannot be included in the authentication process.

The ESP encapsulation inserts an ESP header after the existing IP header, with an SPI. The IP payload may be encrypted and is followed by an ESP trailer, that contains information used to authenticate the whole packet.

The "Tunnel" mode is typically configured between two gateways, named security gateways. The original packet generated by a host behind a gateway is encapsulated with an "outer" IP header containing the addresses the two security gateways. The AH and the ESP headers are inserted after the "outer" IP header. An optional ESP trailer may follow the IP payload.

In the tunnel mode with ESP the whole "inner" IP packet is encrypted, thus also hiding any information contained in the IP header of the original packet.

Figure 2 –"Tunnel" mode

Starting from version 5.4, ATOSNT provides support to both "tunnel" and "transport" mode.

Security protocols: AH and ESP

The IPsec protocol family consists of two protocols: Authentication Header (AH) and Encapsulated Security Payload (ESP). Both are independent IP protocols. AH is the IP protocol 51 and ESP is the IP protocol 50.

AH - Authentication Header

The AH protocol protects the integrity of the IP datagram. To achieve this, the AH protocol calculates a HMAC to protect the integrity. When calculating the HMAC the AH protocol bases it on the secret key, the payload of the packet and the immutable parts of the IP header like the IP addresses. It then adds the AH header to the packet. The AH header is shown infigure below.

Figura 1

The AH header is 24 bytes long. The first byte is the*Next Header*field. This field specifies the protocol of the following header. In tunnel mode a complete IP datagram is encapsulated; therefore the value of this field is 4. When encapsulating a TCP datagram in transport mode the corresponding value is 6. The next byte specifies the length of the payload. This field is followed by two reserved bytes. The next double word specifies the 32 bit long*Security Parameter Index*(SPI). The SPI specifies the security association to use for the decapsulation of the packet. The 32 bit*Sequence Number*protects against replay attacks. Finally the 96 bit holds the*hash message authentication code*(HMAC). This HMAC protects the integrity of the packets since only the peers knowing the secret key can create and check the HMAC.

Since the AH protocol protects the IP datagram including immutable parts of the IP header like the IP addresses the AH protocol does not allow NAT. Network address translation (NAT) replaces an IP address in the IP header (usually the source IP) by a different IP address. After the exchange the HMAC is not valid anymore.

ESP - Encapsulated Security Payload

The ESP protocol can both ensure the integrity of the packet using a HMAC and the confidentiality using encryption. After encrypting the packet and calculating the HMAC the ESP header is generated and added to the packet.

The ESP protocol operates in three distinct modes: authentication and encryption, authentication only, encryption only.

The ESP header consists of two parts and is shown in Figure 3 [1].

Figure 3. The ESP header

The first doubleword in the ESP header specifies the *Security Parameter Index* (SPI). This SPI specifies the SA to use for the decapsulation of the ESP packet. The second doubleword holds the *Sequence Number*. This sequence number is used to protect against replay attacks. The third doubleword specifies the *Initialization Vector* (IV) which is used in the encryption process. Symmetric encryption algorithms are susceptible to a frequency attack if no IV is used. The IV ensures that two identical payloads lead to different encrypted payloads.

IPsec uses block ciphers for the encryption process. Therefore the payload may need to be padded if the length of the payload is not a multiple of the block length. The length of the pad is then added. Following the pad length the 2 byte long *Next Header* field specifies the next header. Lastly the 96 bit long HMAC is added to the ESP header ensuring the integrity of the packet. This HMAC only takes the payload of the packet into account. The IP header is not include in the calculation process.

The usage of NAT therefore does not break the ESP protocol. Still in most cases NAT is not possible in combination with IPsec.

Table 1 summarizes the configurations allowed for AH and ESP protocols:

*Table 1:**ATOSNT modes and algorithms for AH and ESP protocols***

Protocol	Mode	Hash Algorithm	Cipher Algorithm
AH	Tunnel, Transport	MD5**4**, SHA-1**5**	-
ESP	Tunnel, Transport	MD5, SHA-1, NULL6	DES**7**, 3DES**8**, NULL**9**

To protect the integrity of the IP datagrams the IPsec protocols use hash message authentication codes (HMAC). To derive this HMAC the IPsec protocols use hash algorithms like MD5 and SHA to calculate a hash based on a secret key and the contents of the IP datagram. This HMAC is then included in the IPsec protocol header and the receiver of the packet can check the HMAC if it has access to the secret key.

To protect the confidentiality of the IP datagrams the IPsec protocols use standard symmetric encryption algorithms. Usually stronger algorithms are used like 3DES, AES.

Security Associations

Peers need a way to store the secret keys, algorithms and IP addresses involved in the communication to be able to encapsulate and decapsulate the IPsec packets. All these parameters needed for the protection of the IP datagrams are stored in a security association (SA). The security associations are in turn stored in a security association database (SAD).

it can only protect one direction of the traffic in a full duplex IPsec communication..

Since the security association defines the source and destination IP addresses,a SA is a unidirectional logical connection that provides security to traffic. To protect both directions each peer must define two SAs for each IPSec connection, one for the incoming packets (inbound SA) and one for the outgoing ones (outbound SA). Thus, an IPSec connection has a total of four SAs.

Each security association defines the following parameters:

- security protocol (AH or ESP);
- hash algorithm;
- cipher algorithm (for ESP only);
- keys used for authentication and encryption;
- time to live;
- IP addresses of the two peers (in the “tunnel” mode, the public IP addresses of the two security gateways);
- the SPI (Security Parameter Index), a 32-bit number that, together with the authentication protocol and the destination IP address is used to unambiguously identify an SA.

These parameters can be either manually configured or automatically negotiated between the peers. IKE is used in ATOSNT to implement the automatic mode.

Security Policy

A Security Policy (SP) describes how IPSec processes a specific packets.

Selector fields10in each packet are used to select an SP. The selected SP determines if the packet must be **discarded**, transparently **forwarded** or if a Security Association in the SAD applies to this packet. If the selected SP does not refer to an existing SA, then IKE comes into play to negotiate an SA for this policy.

IKE protocol

The IKE protocol solves the most prominent problem in the setup of secure communication: the authentication of the peers and the exchange of the symmetric keys. It then creates the security associations and populates the SAD.

ATOSNT uses the IKE protocol to exchange keys and to configure the SA between the peers in automatic mode.

IKE has its own policy settings (a set of "protection suites" in order of preference) which is used to build an IKE Security Association. An IKE protection suite includes encryption and authentication algorithms, Diffie-Hellman group, a method of authentication and an optional lifetime.

The IKE protocol functions in two phases. The first phase establishes a *Internet Security Association Key Management Security Association* (ISAKMP SA). During this phase, the two peers negotiate a protection suite to build the IKE SA, then create a common secret using a Diffie-Hellman exchange, and finally authenticate each other's material and identity using the hash algorithm and the authentication method determined during the IKE SA negotiation.

In the second phase the ISAKMP SA is used to negotiate and setup the IPsec SAs. Multiple Phase 2 negotiations can use the "underlying" IKE SA to establish the required IPSEC SAs. The IKE SA remains active and is used to exchange connection management messages (SA time-to-live, SA cancellation, etc.) until its lifetime expires or an external event causes its termination.

IKE Operation

IKE is an hybrid protocol that supports 3 standards: ISAKMP, Oakley and Skeme.

ATOSNT uses the following algorithms and methods in its IKE implementation:

- symmetric ("bulk") coding algorithms
  DES/3DES in CBC11mode
- asymmetric ("public key") coding algorithms
  Diffie-Hellman12
- authentication methods
  pre-shared key (PSK): the two peers share a secret key for received messages authentication

- hash algorithms
  MD513in H-MAC14version
  SHA15in H-MAC version

The IKE protocol operates in two phases.

Phase 1 can be realized in **Main** or in **Aggressive** Mode, according to the required security level. Both modes can use preshared keys, digital signatures or Public Key Encryption. ATOSNT supports Main Mode and Aggressive modes with Pre-Shared Keys (PSK).

Phase 2 is used to negotiate parameters for an IPSEC SA. Phase 2 only supports a **Quick** Mode.

Phase 1 – Main Mode with Preshared Keys

This mode consists of a 6 message exchange between the **initiator** (the peer which starts the session and sends the first message) and the **responder** (the peer which receives a request for starting IKE traffic).

A description of messages for a main mode phase 1 exchange with pre-shared keys is included below.

Message 1: the initiator proposes one or more protections suites for the IKE SA which is being established. When **Pre-Shared Keys** are used, either peer knows in advance a piece of information related to the other peer. This is usually associated to the peer's IP address, as this is the only known information on the peer when the phase1 exchange is started.

Message 2: the responder selects a protection suite for the IKE SA.

Messages 3-4: the two peer exchange their Diffie-Hellman public keys and NONCEs (random numbers). Either peer then computes keying material using the NONCEs, the DH keys and the pre-shared secret. These keys are used for encrypting and authenticating messages in this IKE SA and to generate further keying material on subsequent IPSEC SA

Messages 5-6 are exchanged to mutually verify the peer identity. These messages contain an encrypted peer's ID and a hash built using the preshared key, the D-H keys, and the a part of the content of previously exchanged messages. These messages authenticates the remote peer's identity by proofing that it knows the pre-shared key, has correctly derived the DH key, and implicitly confirms that the correct hash and encryption algorithms are known.

At this point the IKE SA is established and can be used for Phase 2 exchanges to establish IPSEC SAs to carry the user's traffic.

Phase 2 – Aggressive Mode

This mode (implemented from version 2.2) consists of a 3-message exchange. This greater efficiency is traded-off with less security, as the peers identity are not protected as when using a main mode phase1 exchange.

As the initiatior's ID is transmitted in the initial message, the responder has the capability to select a PSK based on the initiator's ID, and not only on the remote IP address, as in the main mode.

For this reason, the aggressive mode is applicable in a scenario where the initiator ("road warrior") attempts to establish IPSec connections from different locations and may be using different (dynamically assigned) IP addresses.

A description of messages for an aggressive mode phase 1 exchange with pre-shared keys is included below.

Message 1: the initiator indicates the proposed protections suites for the IKE SA being built, followed by a public DH key, a random NONCE value and its ID value (note that, opposite to the Main Mode, the ID is sent as cleartext)

Message 2: the responder selects a protection suite for the IKE SA and transmits a DH public key, a NONCE, its ID value and a hash value to authenticate the negotiation.

Message 3: the initiator validates the negotiation sending its hash value.

Phase 3 – Quick Mode

The Quick mode is the used for phase 2 exchanges, after an IKE SA has been successfully established. It consists of 3 messages encrypted using the IKE SA. Either peers can start a Quick Mode negotiation.

A description of the messages used in a Quick Mode Phase 2 exchange is included below.

Message 1: the initiator sends a list of proposed IPSEC SAs, a hash value to authenticate the message and a NONCE. Additional information can be optionally added to this message, such an ID value and a new public DH key (otherwise the DH keys from phase 1 are used in the IPSEC SA being created).

Message 2: the responder selects an IPSec SA among those proposed by the initiator, then it sends its NONCE value and authenticates the message with a hash. If message 1 contains extra information, the responder adds the corresponding information to this message (e.g. a new public DH key).

Message 3: the initiator sends a new hash to the responder to confirm that the negotiation has been successfully completed.

Security - Nodes

```
ATOSNT\security>>set ?

Available nodes:
                       ike
                       ipsec
                       crypto

Set command parameters:
 enable        [on|off]    Current value: on
 level of log  [loglevel]  Current value: 1
```

Table 2: set

Syntax	Description
[on|off]	Enables/disables the security feature
loglevel <value>	Set the detail level used by ATOSNT to log security process events.

security node has 3 subnodes: ike, ipsec, crypto.

The **ike** node defines policies ("protection suites") used by IKE and establishes Pre-Shared Keys.

The **ipsec** node creates and configures abstract IPSec policies (security protocol, authentication and encryption algorithm, lifetime). These policy "templates" are then used to create a database of policies in the crypto node.

The **crypto** node sets IPSEC Policies by creating associations between the abstract policies defined in the ipsec node and specific traffic streams, classified with a classifier map. Policies defined in this node actually represent entries in the Security Policy Database (SPD).

Ike - node

```
ATOSNT\security\ike>>add ?

add  help :  Add IKE profile or key
add  usage:
 <KEY><peer-addr or peer-name><key value>
 <PROFILE><peer-addr or name>

add command parameters:
 KEY
 PROFILE
```

Creating new key

A new PSK is added using the following command:

```
ATOS\security\ike>>add KEY peer-addr key-value
```

Table 3: add key

Syntax	Description
KEY	Keyword
Peer addr/peer name [1-64 char]	A string that contains the remote IP/IPv6 address or remote peer name associated to this PSK
key value [max 128 char]	A string with the value of pre-shared key.

The key is used to authenticate the negotiation with peers in a range of IP/IPv6 address. Both peers should use the same key value.

PSKs can be added or deleted but never modified. To delete a key, use the command:

```
ATOS\security\IKE>>del KEY <peer addr or peer-name>
```

Table 4: del key

Syntax	Description
KEY	Keyword
Peer addr	The remote IP/IPv6 address or remote peer name associated to this PSK

Creating new profile

To configure the other parameters required for Phase 1 and Phase 2 negotiation the user has to add a profile corresponding to the peer addr (or peer name) previously specified.

A profile is added using the following command:

```
ATOS\security\ike>>add PROFILE name
```

Table 5: add profile

Syntax	Description
PROFILE	Keyword
name (ip-addr remote) [aa.bb.cc.ddlxxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx| all-address]	The string that contains the IP/IPv6 remote address. You can also specify all-address.

If the user configure a profile all-address, the profile's settings will be used for all the peers.

After adding a profile, a new node prof-name will be created, where name represents the name previously chosen. Under this node, automatically a sub node policy1 will be present.

To delete a profile, use the command:

```
ATOS\security\IKE>>del PROFILE <name>
```

Table 6: del profile

Syntax	Description
PROFILE	Keyword
name (ip-addr remote) [aa.bb.cc.ddlxxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx|all-address]	The name to specify for deletion is the complete profile name, that is prof-name.

PROFILE – node

The example below shows how to add profile for peer 23.56.78.90.

ATOSNT\security\ike\>>>add PROFILE 23.56.78.90

Command executed

Then a new subnode named "prof-23.56.78.90" will be created.

There is possible to configure the following parameters:

```
ATOSNT\security\ike\prof-23.56.78.90>>set ?

Available nodes:
                      policy1

Set command parameters:
 exchange mode         [exchange-mode]      Current value: main
 local id type         [local-id-type]      Current value: default
 local id address      [local-id-address]   Current value: 0.0.0.0
 local id user-fqdn    [local-id-Ufqdn]     Current value:
 local id fqdn         [local-id-fqdn]      Current value:
 remote id type        [remote-id-type]     Current value: default
 remote id address     [remote-id-address]  Current value: 0.0.0.0
 remote id user-fqdn   [remote-id-Ufqdn]    Current value:
```

```
remote id fqdn        [remote-id-fqdn]     Current value:
verify id             [verify-id]          Current value: off
nat traversal         [nat-traversal]      Current value: off
create policy         [create-policy]      Current value: off
server                [server]             Current value: off
```

Table 7: set

Syntax	Description
exchange-mode [main|aggressive|main,aggressive|aggressive,main]	The exchange mode type for phase 1 negotiation when the router acts as initiator. Also it means the acceptable exchange mode when the router is responder. More than one mode can be specified by separating them with a comma. The first exchange mode in the list is what router uses when it is the initiator. If negotiation fails, it will try with the second mode. [default main]
local-id-type [default|address|user_fqdn|fqdn]	Selects the type of local identifier to use in the phase 1 negotiation: • default: the default type is an ip address; • address: the type is an ip address; • user_fqdn: the type is a User Fully Qualified Domain Name; • fqdn: the type is a Fully Qualified Domain Name; [default default]
local-id-address [aa.bb.cc.dd|xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]	Sets the address local identifier value (ip/ipv6). [default 0.0.0.0]
local-id-Ufqdn [max 64 char]	Sets the User Fully Qualified Domain Name local identifier value. [default empty]
local-id-fqdn [max 64 char]	Sets the Fully Qualified Domain Name local identifier value. [default empty]
remote-id-type [default|address|user_fqdn|fqdn]	Selects the type of remote identifier to use in the phase 1 negotiation: • default: the default type is an ip address; • address: the type is an ip address; • user_fqdn: the type is a User Fully Qualified Domain Name; • fqdn: the type is a Fully Qualified Domain Name; [default default]
remote-id-address [aa.bb.cc.dd|xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]	Sets the address remote identifier value(ip/ipv6). [default 0.0.0.0]
Remote-id-Ufqdn [max 64 char]	Sets the User Fully Qualified Domain Name remote identifier value. [default empty]
Remote-id-fqdn [max 64 char]	Sets the Fully Qualified Domain Name local remote identifier value. [default empty]
verify-id [on|off]	Sets to on if you want to verify the peer's identifier. In this case, if the value defined by remote-id-type is not same to the peer's identifier in the ID payload, the negotiation will failed. [default off]
nat-traversal [on|off|forced]	Enables use of the NAT-Traversal IPsec extension. NAT-T allows one or both peers to reside a NAT gateway. If a NAT gateway is detected during phase1 racoon will attempt to negotiate the use of NAT-T with the remote peer. Possible value are: • off: NAT-T is not proposed/accepted; • on: NAT-T is used when a NAT gateway is detected between the peers; • forced: NAT-T is used regardless of whether a NAT gateway is detected or not. [default off]

create-policy	This directive is for the responder. If the responder does not have any policy in SPD during phase 2 negotiation, and the parameter create-policy is set on, then router will choice the first proposal in the SA payload from the initiator, and generate policy entries from the proposal. It is useful to negotiate with the client which is allocated IP address dynamically. Note that inappropriate policy might be installed into the responder's SPD by the initiator. This directive is ignored in the initiator case. If is set to on, the local-peer, remote-peer and classifier-map defined in the crypto association will be ignored. [default off]
server	If set to on, the router acts as server and do not initiate the negotiation. [default off]

POLICY – node

After adding an IKE profile a policy named policy1 will be automatically created:

```
ATOSNT\security\ike\prof-peeraddress\policy1>>

Nodes not available.
Set command parameters:
 encryption algorithm      [encryption]      Current value: des
 hash algorithm            [hash]            Current value: md5
 authentication algorithm  [authentication]  Current value: pre_shared_key
 diffie-hellman group      [group]           Current value: 1
 life-time (seconds)       [life-time]       Current value: 60
```

Table 8: set

Syntax	Description
encryption <des|3des|aes_128|aes_192|aes_256>	Sets the encryption algorithm for the phase 1 negotiation. [default DES]
hash <md5|sha1>	Sets the HMAC authentication algorithm used for the phase 1 negotiation. [default MD-5]
authentication <pre-share>	Sets the authentication method used for the phase 1 negotiation. Only pre-shared key supported.
group <1|2|5|14|15|16|17|18>	Sets the group used for the Diffie-Hellman group used to Diffie-Hellman exponentions. [default :1].
life-time [60-86400|none]	Sets the time to live, in seconds, for the phase 1 SA proposal. [default 60 sec]

Ipsec - node

In this node look at the commands you can use to configure the parameters.

```
ATOSNT\security\ipsec>>set ?

Nodes not available.
```

```
ATOSNT\security\ipsec>>add ?

add  help :  Add IPSec policy
add  usage:
 <POLICY><policy name>

add command parameters:
```

```
 POLICY

ATOSNT\security\ipsec>>add POLICY ?

add command parameters:
 policy name   [max 16 char]
```

```
ATOSNT\security\ipsec>>del ?

del  help :  Del IPSec policy
del  usage:
 <POLICY><policy name>

del command parameters:
 POLICY
```

Creating new policy

An IPSEC policy is used during packet encryption .

The example below shows how to add a policy

ATOSNT\security\ipsec\>>>add POLICY my_ipsec

Command executed

Then a new subnode named "pol-my_ipsec" will be created.

There is possible to configure the following parameters:

```
ATOSNT\security\ipsec\pol-my_ipsec>>set ?

Nodes not available.
Set command parameters:
 description               [description]     Current value:
 encryption algorithm      [encryption]      Current value: des
 authentication algorithm  [authentication]  Current value: hmac_md5
 life-time (seconds)       [life-time]       Current value: none
 pfs group                 [group]           Current value: disable
```

Table 9: set

Syntax	Description
description [max 100 char]	100 char available for policy description
encryption [des|3des|aes_128|aes_192|aes_256|none]	Sets the encryption algorithm. [default DES]
authentication [hmac_md5|hmac_sha1|none]	Sets the authentication algorithm. [default hmac_md5]
life-time [60-86400|none]	The time to live, in seconds, for an IPSEC SA associated to this policy. [default none]
group [1|2|5|14|15|16|17|18|disable]	The Diffie-Hellman group used to DH keys. [default disable]

Crypto - node

In crypto node it is possible to create an association to specify traffic to make secure.

In "crypto" node you can use **add** and **del** commands to configure the following parameters

```
ATOSNT\security\crypto>>add ?

add  help :  Add association
add  usage:
 <ASSOCIATION><mode><name><family>

add command parameters:
 ASSOCIATION

ATOSNT\security\crypto>>add ASSOCIATION ?

add command parameters:
 association mode [tunnel|transport]

ATOSNT\security\crypto>>add ASSOCIATION tunnel ?

add command parameters:
 association name [max 16 char]

ATOSNT\security\crypto>>add ASSOCIATION tunnel my_association ?

add command parameters:
 address family   [inet|inet6]
 <cr>

ATOSNT\security\crypto>>add ASSOCIATION tunnel my_association inet6
Command executed
```

```
ATOSNT\security\crypto>>del ?

del  help :  Delete association
del  usage:
 <ASSOCIATION><name>
```

```
del command parameters:
 ASSOCIATION
```

Table 10: set

Syntax	Description
ASSOCIATION	Keyword
mode [tunnel|transport]	Sets the traffic type: transport mode or tunnel mode.
name [max 16 char]	Sets the name of association
family [inet|inet6]	Sets address family of association.

The example below show how to add a tunnel association named my_assoc.

ATOSNT\security\crypto>>add ASSOCIATION tunnel my_assoc

Command executed

Then a new subnode named "my_assoc" will be created.

There is possible to configure the following parameters:

```
ATOSNT\security\crypto\my_assoc>>set ?

Nodes not available.
Set command parameters:
 enable                [on|off]              Current value: off
 description           [description]         Current value:
 classifier map name   [classifier-map]      Current value:
 ipsec policy name     [ipsec-policy-name]   Current value:
 protocol              [protocol]            Current value: esp
 remote peer addr      [remote-peer]         Current value: none
 local peer addr       [local-peer]          Current value: none
 level                 [level]               Current value: require
```

Table 11: set

Syntax	Description
onloff	Enables/disables the association. [default off]
description	100 char available for description.
classifier-map	Name of the "classifier-map" used to select traffic. See **Classifier-map** section if family association is inet. See **classifier-ipv6** section if family association is inet6. [default empty] *Ignored if the create-policy parameter in ike profile is set to on. To avoid encryption of local traffic, if it is included in the destination subnet defined in the classifier-map, the adding of a deny rule for local ip address is needed in the classifer-map.*

ipsec-policy-name	Sets the name of policy ipsec used to encrypt traffic, described above. [empty default]
protocol [ah|esp]	Sets the protocol used to encapsulate packets. [default esp]
Remote-peer [aa.bb.cc.dd|none] or [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx|none]	Sets the address of the remote peer • ip address - if association familiy is AF_INET. • ipv6 address - if association familiy is AF_INET6 Available only in tunnel mode. *Ignored if the create-policy parameter in ike profile is set to on.* [default none]
Local-peer [aa.bb.cc.dd|none] or [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx|none]	Sets the address of the local peer • ip address - if association familiy is AF_INET. • ipv6 address - if association familiy is AF_INET6 Available only in tunnel mode. *Ignored if the create-policy parameter in ike profile is set to on.* [default none]
level [require|unique]	Specifies what to do is some of the SAs for this policy cannot be found: -require:drop packet and acquire SA; -unique:drop packet and acquire a unique SA that is only used with this particular policy. [default require]

1Internet Key Exchange Protocol, rfc. 2409.

2IP Authentication Header, rfc. 2402.

3IP Encapsulating Security Payload, rfc. 2406.

4The Use of HMAC-MD5-96 within ESP and AH, rfc. 2403.

5The Use of HMAC-SHA-1-96 within ESP and AH, rfc. 2404.

6In the ESP protocol the authentication attribute may be 0 (NULL). In this case the ESP protocol only provides integrity and confidentiality services (rfc 2406, paragrafo 2.7).

7The ESP DES-CBC Chiper Algorithm With Explicit IV, rfc. 2405.

8The ESP CBC-Mode Cipher Algorithms, rfc. 2451.

9The NULL Encryption Algorithm and Its Use With Ipsec, rfc. 2410.

10Selector fields include source/destination IP address, transport protocol type, etc., as extracted from the IP packet during the routing process.

11Schneier, B., "Applied Cryptography Second Edition", John Wiley & Sons, New York, NY, 1996. ISBN 0-471-12845-7.

12Diffie, W., and Hellman M., "New Directions in Cryptography", IEEE Transactions on Information Theory, V. IT-22, n. 6, June 1977.

13The MD5 Message-Digest Algorithm, rfc. 1321.

14HMAC: Keyed- Hashing forMessage Authentication, rfc. 2104.

15NIST, "Secure Hash Standard", FIPS 180-1, National Institue of Standards and Technology, U.S. Department of Commerce, May 1994.

Index

References

[1] http://www.ipsec-howto.org/x202.html#ESP-HEADER

ManSerialV/X

Serial multiprotocol VX interface configuration

Serial multiprotocol V/X is the physical interface for Frame Relay service.

Serial VX is a WAN interface.

The interface is multiprotocol and supports the following protocols: V.35, X.21/V.11, RS449/V.36.

The physical connector is an ISO 2593 34-pole female connector that supports 24 data, clock and control signals.

Electrical levels comply with ITU-T V.35 recommendations for data circuits and clock and V.28 for control circuits.

The VX interface can be configured as a DTE (Data Terminal Equipment) or DCE (Data Communications Equipment) (V.35, X.21/V.11, RS449/V.36) and implements circuits 102, 103, 104, 105 106, 107, 108, 109, 113, 114 and 115.

The user interface can be programmed at any rate multiple of 64 kbps up to a maximum of 2048 kbps.

DCE functionality is a software feature available from ATOSNT ver.6.0.0.

serial0 - Node

The VX interface is available on **Serial0** node.

```
ATOSNT\serial0>>?

Nodes not available.

Available commands:
up                      Move one step up from the current node
top                     Back to the root of the tree
quit                    Exit from CLI session
set                     Set 'serial0' options
conf                    Show configuration in CLI command format
full-conf               Show full configuration in CLI command format
show                    Show 'serial0' settings
delete                  Delete statistics
tree                    Show the tree structure of CLI interface
help                    Help of item
info                    Show the system informations
date                    Show or setting system date and time
save                    Save configuration data
restart                 Restart device
telnet                  Open telnet client session
ssh                     Open SSH2 client session
ping                    Send an ICMP ECHO request
tracert                 Display a trace of packet
mtrace                  Display a path for a multicast group
```

```
resolve                 Resolve a IP address or IP name
log                     Log Management
show-logging-level      Show logged level
banner                  Edit pre and post login banners

loop                    Make interface loop on node ATOSNT\serial0>>
```

serial0 - Operational Command

In **serial0** there is an operational command:

```
loop                    Make interface loop on node ATOSNT\serial0>>
```

loop command is used for debuging purposes and allows to do different loopback tests to isolate the serial line issue accurately.

```
ATOSNT\serial0>>loop ?

loop  help :  Make interface loop
loop  usage:
 <OFF|LOCAL|REMOTE>

loop command parameters:
 Loop [off|local|remote]
```

Table 1: loop

Syntax	Description
OFF	Disables the interface loop.
LOCAL	Setting local, all data received from serial physical interface are looped.
REMOTE	Setting remote, all data received from network to serial physical interface are looped.

serial0 - Commands

serial0 node allows to set the following parameters:

in DCE mode for ATOSNT ver. 6.0.0 and further

```
ATOSNT\serial0>>set ?

Nodes not available.
Set command parameters:
 level of log          [loglevel]          Current value: 5
 internal rate         [rate]              Current value: 2048
 dte tx clock source   [txclk-source]      Current value: internal
 dte tx clock invert   [dte-clk-invert]    Current value: off
 dce rx clock invert   [dce-rxclk-invert]  Current value: off
 dce tx clock invert   [dce-txclk-invert]  Current value: off
```

In DTE mode for ATOSNT software versions previous to release 6.0.0

```
ATOSNT\serial0>>set ?

Nodes not available.
Set command parameters:
 level of log          [loglevel]          Current value: 5
 tx clock source       [txclk-source]      Current value: external
 dte clock invert      [dte-clk-invert]    Current value: off
 dce rx clock invert   [dce-rxclk-invert]  Current value: off
 dce tx clock invert   [dce-txclk-invert]  Current value: off
```

Table 2:**set**

Syntax	Description
loglevel [0-5]	Sets the level detail used by ATOS to log the events on the serial VX interface [default: 1]
rate [64|128|192|256|384|512|768|1024|1536|2048]	In DCE mode sets the serial connection rate in kbps. [default: 2048]
txclk-source [external|internal]	Sets the source clock used by serial VX interface [default: external]
dte-clk-invert [on|off]	Enables/disables the transmission clock polarity invertion on DTE (for example on V.35 interface: C113) [default: off]
dce-rxclk-invert <on|off>	Enables/disables the receiving clock polarity invertion on DCE (for example on V.35 interface: C115) [default: off]
dce-txclk-invert <on|off>	Enables/disables the transmission clock polarity invertion on DCE (for example on V.35 interface: C114) [default: off]

serial0 Configuration example

In DCE mode ATOSNT\serial0>>show work

Show of ATOSNT serial0

Level of log : 5

Internal Rate: 2048

DTE tx clock source : internal

DTE tx clock invert : off

DCE rx clock invert : off

DCE tx clock invert : off

serial0 Status example

In DTE mode

ATOSNT\serial0>>show status -s

Status of serial0 interface

Status : Up

Ifc mode : DTE

V/X cable: V.35

Loop mode: OFF

C.105 : ON

C.106 : ON

C.107 : ON

C.108 : ON

C.109 : ON

ATOSNT\serial0>>show status -s

Status of serial0 interface

Status : Down

Ifc mode : DCE

V/X cable: V.35

Loop mode: OFF

C.105 : OFF

C.106 : OFF

C.107 : OFF

C.108 : OFF

C.109 : OFF

serial0 Statistics example

Statistics of serial0 interface

******* upstream direction *******

bytes : 1446184

packets : 71722

errors : 0

****** downstream direction ******

bytes : 1286877

packets : 71491

errors : 0

drops : 0

ManSharing

Sharing

The CPE allows you to connect **storage devices** such as USB pen, compact flash, USB hard disk and **USB printers**.

Sharing application allows to share these devices on your TCP/IP network.

The share procedure consists of configuring:

- Sharing server
- Sharing profiles (storage or printer)

The share procedure can be configured ONLY when logged at **Administrator** level

Sharing application is located in **sharing** node under the Root node.

Set command allows to configure the share server service.

```
ATOS\sharing>>set ?

Set command parameters:

enable                [on|off]       Current value: on
level of log          [loglevel]     Current value: 1
server description    [description]  Current value: ATOSNT SHARING SERVER
network workgroup     [workgroup]    Current value: WORKGROUP
enabled interface     [interface]    Current value: eth0
```

Table 1: set

Syntax	Description
onloff	Enables/disables the sharing server. When server is enabled and there aren't any profiles configured, all USB storage devices connected are sharing. Default: on
loglevel [0-5]	Sets the detail level used by ATOS to record sharing events. Default: 1
description [max 100 char]	Defines a string description for sharing server. Default: ATOSNT SHARING SERVER
workgroup [max 64 char]	Defines the local network workgroup. Default: WORKGROUP
interface [<cr>|all|eth0|loopback0]	Sets network interfaces allowed to access to sharing server. Default: eth0

Add command allows to create a new sharing rule.

```
ATOS\sharing>>add ?

add  help :  Add a new storage or printer sharing
add  usage:
```

```
 <STORAGE>[name]
 <PRINTER>[name]

add command parameters:
 STORAGE
 PRINTER

ATOSNT\sharing>>add STORAGE ?

add command parameters:
 name     [max 16 char]
 <cr>
ATOSNT\sharing>>add STORAGE
Command executed
```

If the STORAGE name is not specified, a storage node will be created with index sequence (storage0, storage1….).

Table 2: add STORAGE

Syntax	Description
STORAGE	Keyword to add a file sharing
name	Sets an optional string name for file sharing. Default: storage(n)(where n is 0 for the first adding STORAGE, 1 for the second and so on)

```
ATOSNT\sharing>>add PRINTER ?

add command parameters:
 name     [max 16 char]
 <cr>
ATOSNT\sharing>>add PRINTER
Command executed
```

If the PRINTER name is not specified, a printer node will be created with index sequence (printer0, printer1….).

Table 3: add PRINTER

Syntax	Description
PRINTER	Keyword to add a printer sharing
name	Sets an optional string name for printer sharing. (Max 16 characters) Default: printer(n)(where n is 0 for the first adding PRINTER, 1 for the second and so on)

Del command allows to delete a sharing rule.

```
ATOSNT\sharing>>del ?

del  help :  Remove a storage or printer sharing
del  usage:
 <STORAGE><name>
 <PRINTER><name>
```

```
del command parameters:
 STORAGE
 PRINTER
```

Table 4: del STORAGE/PRINTER

Syntax	Description
STORAGE	Keyword to del a file sharing
PRINTER	Keyword to del a printer sharing
name	Sets the shared resource to be deleted.

Show status command lets you view current status of sharing service.

```
ATOS\sharing>>show status

Sharing Service Status: activated

Storages Shared: all disk
```

Set command allows to modify a file sharing.

```
ATOSNT\sharing\storage0>>set ?

Nodes not available.
Set command parameters:
 enable       [on|off]       Current value: on
 description  [description]  Current value:
 disk         [disk]         Current value: ALL-DISK
 shared path  [shared-path]  Current value:
 write mode   [write-mode]   Current value: RW
 password     [password]     Current value:
```

Table 5: set

Syntax	Description
onloff	Activates/deactivates the sharing. Default: on
description [max 100 char]	It is optional and defines a string description for sharing rule. Default: shared storage
disk [ALL-DISK|F:|G:|H:|I:|J:|K:|L:|M:|N:|O:|P:|Q:|R:|S:]	Set storage disk to sharing. Default: ALL DISK
shared-path [max 120 char]	Set a string to define file system path of sharing. (Max 120 characters) Default: EMPTY

write-mode [RO|RW]	It is optional and defines write privilege for sharing rule. RO = Read Only RW = Read and Write Default: RW
password [max 32 char]	It is optional and set a password string to access to the shared resource. (Max 32 characters) Default: EMPTY

```
ATOSNT\sharing\printer0>>set ?

Nodes not available.
Set command parameters:
 enable          [on|off]          Current value: on
 description     [description]     Current value: shared pr
 printer device  [printer-device]  Current value: lp0
```

Table 6: set

Syntax	Description
on|off	Activates/deactivates the sharing. Default: on
description [max 100 char]	It is optional and defines a string description for sharing rule. Default: shared printer
printer-device [lp0|lp1|lp2|lp3]	Setds the printer device to sharing Default: lp0

ManSnmp

SNMP

The SNMP (Simple Network Management Protocol) allows management of Aethra devices through a remote SNMP manager. The SNMP agent software allows to monitor some statistic parameters and change the device configuration according to the results. Aethra devices implement SNMPv11SNMPv2C2and SNMPv33which allow the remote manager to manage the objects represented in the structures defined in the MIB-24.

SNMP – Commands

```
ATOSNT\snmp>>set ?

Set command parameters:
 level of log                      [loglevel]                Current value: 1
 enable                            [on|off]                  Current value: off
 local ipv4 address                [local-ip-address]        Current value: all
 local ipv6 address                [local-ipv6-address]      Current value: none
 local udp port                    [agent_transport_address] Current value: 161
 manager server                    [manager]                 Current value:
 trap enable                       [trap-enable]             Current value: off
 trap server                       [trap-server-address]     Current value:
 trap udp port                     [trap-server-port]        Current value: 162
 authentication trap enable        [authentication_trap]     Current value: off
 management accesses trap enable   [mgmt_access_trap]       Current value: off
 system contact                    [syscontact]              Current value: Me
 system location                   [syslocation]             Current value:
```

Table 1: set

Syntax	Description
[on|off]	Activates/deactivates the SNMP service. Default: off.
loglevel [value] [-s]	Sets the detail level used by ATOS to record SNMP events. Default: 1.
all|none|loopback0|eth0|eth0-ppp0|eth1]	Configures the IPv4 address for SNMP Agent. This address can be viewed by sending trap also. Default: all
all|none|loopback0|eth0|eth0-ppp0|eth1]	Configures the IPv6 address for SNMP Agent. This address can be viewed by sending trap also. Default: none
agent-transport-address [1-65535]	Defines the UDP port used by SNMP agent to transport packets. Default 161.
manager [aa.bb.cc.dd|xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx|max 100 char or <cr>]	Sets IP address or hostname of the SNMP server Manager. Default:<cr>
trap-enable [on|off]	Enables/disables trap messages. Default:off
trap-server-address [aa.bb.cc.dd|xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx|max 100 char or <cr>]	Sets the Server IP address or hostname for receinving trap messages. Default:<cr>

trap-server-port [aa.bb.cc.dd|xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx|max 100 char or <cr>]	Sets the trap server port. Default:162
authentication_trap [on|off]	Activates/deactivates the TRAP authentication messages sent to the Manager by the Agent when the authentication procedure fails. Default: off.
syscontact [max 64 char]	Sets the contact of the device manager. You can use an e-mail address, IP address or Internet site. Default: null
syslocation [max 64 char]	Sets the geographical location of Aethra CPE. Default: null

```
ATOSNT\snmp>>add ?

add  help :  Add SNMP Views, Server Community or V3 USER
add  usage:
 <VIEWS><name><OID><mode>
 <COMMUNITIES><comm-name>[RO|RW][version][view-name][source]
 <V3-USER><username>[RO|RW][view-name]<NO-AUTH>
 <V3-USER><username>[RO|RW][view-name]<AUTH-NO-PRIV><auth-prot><auth-pass>
 <V3-USER><username>[RO|RW][view-name]<PRIV><auth-prot><auth-pass><encr-prot>[encr-pass]

add command parameters:
 VIEWS
 COMMUNITIES
 V3-USER
```

Table 2: add

Syntax	Description
VIEWS	Keyword
Name [Any value(max 16 char)]	Name of the view to be defined . The predefined default_view allows to see the whole tree.
.1|.1.3.6.1.2.1| .1.3.6.1.4.1.7745.5]	Object identifier associated to the view
mode [included|excluded]	Sets a rule to include or exclude the defined oid.
COMMUNITIES	Keyword
community-name [Any value(max 32 char)]	Sets the name of the community enabled for the CPE parameters management, to read or read/write, depending of the RO/RW configuration.
RO|RW	Sets access permissions: • RO = Read only, • RW = Read and Write. Default: [RO]
version [V1-V2c|V1]	V1-V2c]. Default: [V1-V2c]
view-name [default_view|view1]	Name of the view the community is allowed to see. Default: [default_view]
source ipv4/mask or ipv6/prefix [aa.bb.cc.dd/0-32| xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/0-128]	Specifies allowed sources for SNMP requests. Default:0.0.0.0

V3-USER	Keyword
username [Any value(max 32 char)]	String of the V3 user name. Up to 16 characters can be used
authentication mode [PRIV|AUTH-NO-PRIV|NO-AUTH]	Configures the SNMP V3 authentication mode: • PRIV = with authentication and encryption, • AUTH-NO-PRIV =with authentication, without encryption, • NO-AUTH = without authentication
authentication protocol [MD5|SHA]	In case authentication has been selected two different authentication protocols are availble:MD5, SHA
authentication password	It sets the authentication password [min 8, max 20 characters can be used].
encription protocol [AES|DES]	In case of “PRIV” option has been selected encription protocol is needed to define. You can chose between AES and DES encription protocol.
encription password	It sets the encription password [min 8, max 20 characters can be used].

1Rfc.1157.

2 Rfc1901.

3 Rfc 3514

4Rfc.1155, rfc.1213.

Standard MIBS

List of the Standard MIBS supported on Software Rel.v.5_5_0 :

- MIB-II - RFC 1213 - MIB
- IF-MIB - RFC 2863(Partially)
- IP-FORWARD-MIB - RFC 4292(Partially)
- ENTITY-MIB - RFC 4133(Partially)
- EtherLike-MIB - RFC 3635(Partially)
- HDSL2-SHDSL-LINE-MIB - RFC 4319 (Partially, only available in some CPE models)
- DOT3-OAM-MIB - RFC 4878 (Partially, only available in some CPE models)
- IEEE8021-CFM-MIB - (Partially, only available in some CPE models)

Proprietary MIBS

Aggiungere alla pagina http://atlcwiki/wiki/index.php/ManSnmp sezione Proprietary MIBS che per il prodotto RPF2000 è disponibile anche una mib privata specifica per la sua gestione e configurazione. List of the proprietary MIBS supported on Software Rel.v.5_5_0:

- File transfer Download / Upload
    - firmware,
    - boot,
    - userconf,
    - logs,
    - package,
    - localfile,
    - welcome,
    - prelogin banner,
    - postlogin banner,
    - license,

    - certificate,
    - defaultconf
- Ping and Ping results
- System Node Configuration
- Save
- Reboot
- Performance Monitor (system statistics)
- xDSL and SHDSL information
- VoIP - trunk and user terminal Configuration - Partially)
- Interfaces (The current and effective TX and RX rate in bit per second, the current media selected and SFP pluggable module inserted)
- Wan 3G: list, configuration and status of the connected mobile devices
- Traps: snmp messages about interfaces status (up/down), VoIP trunk (register/deregister) and Management Accesses
- For RPF2000: available a private MIB for the system configuration and management.
- Info: The same value of the info command

Index

ManSysLog

Syslog

The increasing complexity of operating systems and applications suggested the development of real-time monitoring systems that transmit and receive log messages from different processes running on a host and subdivide them into categories. In this way a network administrator can manage messages which have been already selected according to predefinite parameters.

Most operating systems adopt syslogas a monitoring system.

Syslogis an application that sends notification messages produced by running applications to a syslog server. ATOSNT allows to display these messages also locally. The remote syslog server typically stores messages in a database and/or forwards them to another server. the remote. The syslog client does not receive any confirmation from the server about message reception.

Syslog uses the UDP protocol at port 514 as a transport layer.

Syslog messages includes the information described below.

Facility

This parameter indicates the facility that generated the message. ATOSNT manages the following values:

Kernel messages;

User-level messages.

Severity

This parameter indicates the severity of the message. Allowed values for this parameter are:

Error: fatal errors for a correct system behaviour;

Warning: warning conditionsthat could cause a partial incorrect behaviour;

Notice: normal but significant conditions that do not affect the correct system behaviour;

Informational: informational messages;

Debug: debug-level messages.

Mapping between syslog severity levels and ATOS Severity values is shown here :

Error	◂▸	**E!**
Warning	◂▸	**W1**
Notice	◂▸	**W2**
Informational	◂▸	**L1**
Debug	◂▸	**L2**

Timestamp

This parameter indicates the local time referred to message creation.

Hostname

This parameter indicates the name of the device which generated the log.

Tag

This parameter indicates the name of the programm or application that genetated the message.

Content

This parameter contains the details of the message.

Syslog – Commands

```
ATOSNT\syslog>>set ?

Nodes not available.
Set command parameters:
 level of log                          [loglevel]          Current value: 1
 enable                                [on|off]            Current value: off
 syslog server                         [server]            Current value:
 syslog port                           [syslog-port]       Current value: 514
 facility                              [facility]          Current value: loc4
 severity                              [severity]          Current value: debg
 local ip address (0.0.0.0 if notused)  [local-ip-address]  Current value: 0.00
```

Table 1: set

Syntax	Description
on|off	Enables/disables the syslogclient, default value: off
echo <on|off>	Enables/disables messages to be displayed on the console, default value: off.
server [ip addr|name]	The IP address or the name of the receiving syslog server (default null).
syslog-port <value>	It identifies the udp port used to receive the syslog message (default 514).
facility <kernel| user| mail| daemon| auth| syslog| lpr| news| uucp| cron | system0| system1| system2| system3| system4| system5| local0|local1|local2|local3| local4|local5|local6|local7>	Configures the facility assigned to all the log messages generated by the system. The defaul value is "local4".
severity1 <error| warning| notice| informational| debug>	Creates a filter on the log severity. Starting from the one configured, all the messages having an higher severity level are sent to the server. The default value is "debug"; it means that all the log messages generated by the system are forwarded to the server.
local-ipaddress <ip addr>	Configures the Syslog IP address (default 0.0.0.0).
loglevel <0-5>	Sets the detail level used by ATOSNT to log the syslog events, default value: 1.

Syslog – Configuration Examples

Here you can find some examples of Syslog service configuration:

ATOSNT\syslog>>**config**

set syslog on

set syslog server 192.168.110.163

set syslog severity warning

ATOSNT\syslog>>**show work**

Show of ATOSNT syslog

Level of log : 1

Enable : on

Local echo : off

Syslog server : 192.168.110.163

Syslog port : 514

Facility : local4

Severity : warning

Local IP Address (0.0.0.0 if notused) : 0.0.0.0

1Severity levels start from the lowest (debug) to the highest (error).

Index

ManSystem

System - Overview

System node is used to manage some general parameters.

Enter **system** from the root to go to the node. You will find the following operational and configuration commands, as well as the available nodes:

```
ATOSNT\system>>?

Available nodes:
                        timesync
                        intservices
                        privilege-map
                        scheduler
Available commands:
up                       Move one step up from the current node
top                      Back to the root of the tree
quit                     Exit from CLI session
set                      Set 'system' options
add                      Add a new option
del                      Remove an added option
conf                     Show configuration in CLI command format
full-conf                Show full configuration in CLI command format
show                     Show 'system' settings
delete                   Delete statistics
tree                     Show the tree structure of CLI interface
help                     Help of item
info                     Show the system informations
date                     Show or setting system date and time
save                     Save configuration data
restart                  Restart device
telnet                   Open telnet client session
ssh                      Open SSH2 client session
ping                     Send an ICMP ECHO request
atmping                  Send an ATM loopback cells
tracert                  Display a trace of packet
mtrace                   Display a path for a multicast group
resolve                  Resolve a IP address or IP name
log                      Log Management
show-logging-level       Show logged level
banner                   Edit pre and post login banners

logins                   Show list of logs on node ATOSNT\system>>
password                 Set admin/user/others password on node ATOSNT\system>>
privilege                Create, configure privilege on node ATOSNT\system>>
```

System – Operational Commands

These are the operational commands:

```
logins                  Show list of logs on node ATOSNT\system>>
password                Set admin/user/others password on node ATOSNT\system>>
privilege               Create, configure privilege on node ATOSNT\system>>
```

logins Command

logins command shows the last 16 accesses made by administrators and users. For each access, it indicates the username (User), the level at which the user logged in (level), the date and time when the login session started (Opened), the date and time of session termination (Closed) and the used source (source); this can be via the console port, using a Telnet or SSH session, the Web Server application (the last three being identified with the IP address of the source terminal).

This is an example of logins command

ATOSNT\system>>logins

USER	LEVEL	OPENED		CLOSED		SOURCE	
rossi	Admin	06/05/2010	13:28:41	06/05/2010	13:28:43	WEB	192.168.110.231
bianchi	User	06/05/2010	13:28:47	06/05/2010	13:28:48	telnet	192.168.110.231
verdi	Admin	06/05/2010	13:28:50	06/05/2010	13:28:51	telnet	192.168.110.231
rossi	Admin	06/05/2010	13:28:52	07/05/2010	14:38:36	SSH	192.168.110.231
admin	Admin	06/05/2010	13:28:56	06/05/2010	13:28:57	telnet	192.168.110.231
admin	Admin	06/05/2010	13:28:59	06/05/2010	13:29:01	SSH	192.168.110.231
rossi	Admin	06/05/2010	13:29:02	06/05/2010	13:29:03	telnet	192.168.110.231
bianchi	User	06/05/2010	13:29:06	06/05/2010	13:29:39	SSH	192.168.110.231
admin	Admin	06/05/2010	14:21:59	06/05/2010	14:33:18	Console	
rossi	Admin	07/05/2010	11:56:08	07/05/2010	12:01:23	Console	

date Command

```
ATOSNT>>system date
```

date command returns you the date and time when you call it without any options. If you want to set the local date and time you can use the following syntax:

```
ATOSNT\system>>date ?

date  help :  Show or setting system date and time
date  usage:
 [dd mm yyyy hh mm ss]
```

```
date command parameters:
 day     [1-31]
 <cr>

ATOSNT\system>>date 28 10 2011 9 30 00
Date Friday 28 October 2011 Time 09:30:00
Command executed
```

Note: **date** command is actually available all over the CLI and not only in the system node.

save Command

Save command allows to save the current "user" configuration, as the default configuration. If you make a reset, the device will restart working with the "user" configuration, instead of the factory default configuration.

Notice that after the keyword "as-default", you must write the keyword "confirm" to avoid any mistake.

Look at the syntax of the command:

```
ATOSNT\system>>save ?

save  help :  Save configuration data
save  usage:
 [option]

save command parameters:
 option      [as-default]
 <cr>

ATOSNT\system>>save as-default ?

save command parameters:
 confirm     [confirm]

ATOSNT\system>>save as-default confirm

Command executed
```

Table 1: save

Syntax	Description
save	Keyword. Saves configuration data
as-default	Saves the user configuration as default configuration.
confirm	Keyword. Sets the current user configuration as the machine default configuration replacing the factory default configuration.

password Command

The password command allows to set the login password for the administrative, the user or/and others.

```
ATOSNT\system>>password ?

password  help :  Set admin/user/others password
password  usage:
 <ProfileList>[Old password]<New password><Repeat password>

password command parameters:
 Profile         [ADMIN|USER]
```

Where ADMIN and USER are keywords to select the privilege to be set.

In case the old or new password are empty, you should use the following syntax:

<empty>

privilege Command

By default, ATOSNT has two levels of access to commands: User and Administrator mode.
However, additional levels of access (called privilege profiles) can be configured to meet the needs of final users while protecting the system from unauthorized access.
Up to 16 privilege profiles can be configured.

Access to each privilege profile is enabled through separate passwords, which you specify when configuring the privilege procedure.

For example, if you want that some users would be able to configure certain interfaces, but avoiding them the access to other configuration options, you can create a separate privilege profile only for specific interface configuration commands and distribute the password for that profile to those users.

Privilege procedure consists of :

- Configure privilege using specific command
- Configure related password using specific command
- Setting privilege-map node if requested

The privilege procedure can be ONLY configured when logged in as **Administrator** level

privilege command allows to create a new profile, delete an existing profile , modify a configuration or command options.
Privilege profiles can be added up to a maximum of 16 (User and Administrator included).

```
ATOSNT\system>>privilege ?

privilege  help :  Create, configure privilege
privilege  usage:
<ADD><name>[from <privilegeList>]
<privilegeList>
<CONFIGURE><privilegeList><RD|WR|RW|NONE><node-path list>[param list]
<COMMAND><privilegeList><ENABLE|DISABLE><command list>[node-path list]
<SHOW>[privilegeList]
```

```
privilege command parameters:
Privilege Command           [ADD|DEL|CONFIGURE|COMMAND|SHOW]
```

Add a new privilege

add command specifies the name of a new privilege profile that will be shown in “privilegeList”.

Optionally, an existing privilege name can be specified: in this case the new one inherits all its rules; then it can be modified to fulfil specific requirements.

When you make a new privilege, it becomes only effective when it is assigned to a level of privilege map (see below).

```
ATOSNT\system>>privilege ADD ?

privilege command parameters:
 new privilege name          [max 32 char]

ATOSNT\system>>privilege ADD priv-name ?

privilege command parameters:
 from privilege              [ADMIN|USER]
 <cr>

ATOSNT\system>>privilege ADD priv-name ADMIN ?

Command complete (enter cr)

ATOSNT\system>>privilege ADD priv-name ADMIN
Command executed
```

Delete a privilege

An existing privilege can be deleted

The command specifies the name of a privilege selected from the privilege list.

```
ATOSNT\system>>privilege del ?

privilege command parameters:
 privilege profile           [..list of created privileges...]
```

Configure a privilege

The CONFIGURE keyword defines if an entire node or a specific parameter within a node has the right to be:

- Read(RD)
- Write (WR)
- Read and write (RW)
- No Operation (NONE)
- Remove existing statement (REMOVE-STATEMENT)

When you specify a node, the privilege is extended to all existing subnodes.

The command specifies the type of privilege and the list of nodes and subnodes. Optionally you can choose a single parameter for the selected node.

Notice that with this keyword, the user can be allowed to perform, on a specified node, operations like: setting parameters, show conf/work, show status/statistics. To Enable/Disable commands like add, del and so on, the “COMMAND” keyword described below is to be used instead.

```
privilege  usage:
 <CONFIGURE><privilegeList><RD|WR|RW|NONE><node-path list>[param list]
```

An example of Privilege CONFIGURE rule adding on the “priv-name” profile previously created. Use of dynamic help is enphasized:

ATOS\system>privilege CONFIGURE ?

privilege command parameters:

privilege profile [priv-name |…list of created privileges…]

ATOS\system>>privilege CONFIGURE priv-name ?

privilege command parameters:

privilege type [RD|WR|RW|NONE|REMOVE-STATEMENT]

ATOS\system>>privilege CONFIGURE priv-name RD ?

privilege command parameters:

main node path [system|storage|dpa|xdsl0|eth0|bri1|bri2|pots1|pots2|

pots3|pots4|dect|w3g|atm|isdn|point-to-point|aaa|

syslog|bridges|classifier-map|interfaces|firewall|

dhcpserver|dhcpclient|backup|dns|naptlarp|

scheduler|captive-portal|vrrp|ip|qos|voip|ddns|

snmp|npm]

ATOS\system>>privilegeCONFIGURE priv-name RD voip ?

privilege command parameters:

first subnode path [call-setting|sip|fax|user-terminal|terminal-group|

trunk|call-mng]

parameter [loglevel|max-connections]

<cr>

ATOS\system>>privilege CONFIGURE priv-name RD voip call-setting ?

privilege command parameters:

second subnode path [it|italy]

parameter [loglevel|country]

<cr>

ATOS\system>>privilege CONFIGURE priv-name RD voip call-setting

Command executed

An example of Privilege CONFIGURE rule removing of the above added rule:

ATOS\system>>privilege CONFIGURE priv-name REMOVE-STATEMENT voip call-setting

Command executed

Privilege COMMAND Configuring

As stated in the previous paragraph, in order to define the possibility, for a certain profile, to use CLI commands like add, del, and so on, the COMMAND keyword must be used. Using it, it is possible to define whether a specific command has the right to:

- work (ENABLE)
- Not to work (DISABLE)
- Remove an inserted “COMMAND” statement (REMOVE-STATEMENT)

Depending on command, you can also determine the node or subnode in which the requested command needs to act or not.

The command specifies the name of a privilege selected by the privilegelist:the rule that you are entering will belong to that profile; the type of privilege and the list of command and nodes .

```
privilege usage:

<COMMAND><privilegeList>< ENABLE | DISABLE ><command list>[node-path list]
```

An example of Privilege COMMAND rule adding on the “priv-name” profile previously created. Use of dynamic help is enphasized:

ATOSNT\system>>privilege COMMAND priv-name ?
privilege command parameters:
privilege type [ENABLE|DISABLE|REMOVE-STATEMENT]
ATOSNT\system>>privilege COMMAND priv-name ENABLE ?
privilege command parameters:
command [add|de||conf|full-conf|show|delete|tree|info|
date|save|restart|te|net|ssh|ping|atmping|
tracert|mtrace|resolve||log|
show-logging-level|banner|download|upload|
swap-firmware|logins|password|list|remove|
create|erase|copy|rename|bitpertone|modify|
line-test|import|connect|disconnect|
training-stop|loopeth|no-keepalive|clear|
flush|capture|npm-responders-status|
import-site|remove-site]
ATOSNT\system>>privilege COMMAND priv-name ENABLE add ?
privilege command parameters:
command main node path [ALL|system|storage|eth0|wlan0|atm|

point-to-point|aaa|bridges|certificate|
classmap-profile|classifier-map|
classifier-ipv6|connectivity-monitor|
line-aux|interfaces|dhcpserver|dhcp6server|
dhcpclient|security|backup|dns|naptlarp|
neighbor6|network-groups|ip|ipv6|vrrp|
firewall|qos|voip|ddns|ethernet-oam|
ethernet-cfm|sharing|snmp|npm|hot-spot|web]
ATOSNT\system>>privilege COMMAND priv-name ENABLE add voip ?
privilege command parameters:
command first subnode path or key [call-setting|sip|user-terminal|
terminal-group|trunk|call-mng]
<cr>

SHOW

List of all the privileges or rules defined for a specific profile.

```
privilege usage:
  <SHOW>[privilegeList]
```

ATOSNT\system>>privilege SHOW ?
privilege command parameters:
show privilege profile [priv-prova|priv-test]
<cr>
ATOSNT\system>>privilege SHOW
PRIVILEGE CONDITIONS
priv-prova nothing
priv-prova RD system
priv-prova RW system privilege-map
priv-prova RW voip terminal-group
priv-prova RW voip user-terminal
priv-test nothing
priv-test RD system

Privilege-map – Node

Change the privilege level by choosing from an administrator, user or selected from the privilege list

```
ATOSNT\system\privilege-map>>set ?

Nodes not available.
Set command parameters:
 privilege level 0   [privilege-level-0]   Current value:
 privilege level 1   [privilege-level-1]   Current value: USER
 privilege level 2   [privilege-level-2]   Current value:
 privilege level 3   [privilege-level-3]   Current value:
 privilege level 4   [privilege-level-4]   Current value:
 privilege level 5   [privilege-level-5]   Current value:
```

```
 privilege level 6   [privilege-level-6]   Current value:
 privilege level 7   [privilege-level-7]   Current value:
 privilege level 8   [privilege-level-8]   Current value:
 privilege level 9   [privilege-level-9]   Current value:
 privilege level 10  [privilege-level-10]  Current value:
 privilege level 11  [privilege-level-11]  Current value:
 privilege level 12  [privilege-level-12]  Current value:
 privilege level 13  [privilege-level-13]  Current value:
 privilege level 14  [privilege-level-14]  Current value:
 privilege level 15  [privilege-level-15]  Current value: ADMIN
```

Show Statistics

```
ATOSNT>>show system statistics

Dynamic memory usage (KBytes)
   Total   RamDisk      Free
  187828       676    104792
           ( 0.4%)   (55.8%)

Average CPU usage in last 2 seconds
       Idle   User   Kernel Waste  HWIrq  SWIrq  IRQ/sec
CPUs  94.9%   3.2%   1.5%   0.0%   0.1%   0.2%   845.50
CPU0  98.5%   0.4%   0.8%   0.0%   0.1%   0.2%   541.00
CPU1  91.4%   6.0%   2.1%   0.0%   0.2%   0.3%   304.50

Average CPU usage in last 1 minutes
       Idle   User   Kernel Waste  HWIrq  SWIrq  IRQ/sec
CPUs  94.7%   3.3%   1.6%   0.0%   0.1%   0.2%   871.08
CPU0  98.1%   0.7%   1.0%   0.0%   0.1%   0.2%   572.68
CPU1  91.4%   5.9%   2.3%   0.0%   0.2%   0.3%   298.40

Average CPU usage in last 5 minutes
       Idle   User   Kernel Waste  HWIrq  SWIrq  IRQ/sec
CPUs  94.7%   3.3%   1.6%   0.0%   0.1%   0.2%   851.60
CPU0  98.1%   0.7%   1.0%   0.0%   0.1%   0.2%   560.40
CPU1  91.4%   5.9%   2.3%   0.0%   0.2%   0.3%   291.20

Average CPU usage in last 15 minutes
       Idle   User   Kernel Waste  HWIrq  SWIrq  IRQ/sec
CPUs  94.8%   3.3%   1.6%   0.0%   0.1%   0.2%   840.88
CPU0  98.1%   0.7%   1.0%   0.0%   0.1%   0.2%   553.14
CPU1  91.4%   5.9%   2.3%   0.0%   0.2%   0.3%   287.73

Average CPU usage from last statistics clear (81722 seconds)
       Idle   User   Kernel Waste  HWIrq  SWIrq  IRQ/sec
CPUs  94.8%   3.3%   1.6%   0.0%   0.1%   0.2%   844.16
CPU0  98.1%   0.7%   0.9%   0.0%   0.1%   0.2%   562.91
```

```
CPU1   91.4%    5.9%    2.3%    0.0%    0.1%    0.2%    281.25
```

System – Parameters

```
ATOSNT\system>>set ?


Available nodes:
                      timesync
                      intservices
                      privilege-map
                      scheduler


Set command parameters:
 level of log                                [loglevel]                Current value: 1
 description                                 [description]             Current value: SystemNT description
 system name                                 [name]                    Current value: ATOSNT
 local domain                                [localdomain]             Current value: LocalDomain
 default tftp server                         [deftftpserver]           Current value:
 tftp local ip address                       [tftp-local-ipaddress]    Current value: 0.0.0.0
 tftp local ipv6 address                     [tftp-local-ipv6address]  Current value: ::
 default ftp server name:port                [defftpserver-port]       Current value:
 ftp local ip address                        [ftp-local-ipaddress]     Current value: 0.0.0.0
 ftp local ipv6 address                      [ftp-local-ipv6address]   Current value: ::
 ftp username                                [ftp-username]            Current value: anonymous
 ftp password                                [ftp-password]            Current value: ATOS
 default scp server name:port                [defscpserver-port]       Current value:
 scp local ip address                        [scp-local-ipaddress]     Current value: 0.0.0.0
 scp local ipv6 address                      [scp-local-ipv6address]   Current value: ::
 scp username                                [scp-username]            Current value: ATOS
 scp password                                [scp-password]            Current value: ATOS
 aaa profile name                            [aaa-profile]             Current value:
 aaa login timeout (sec)                     [aaa-login-timeout]       Current value: 60
 aaa bypass                                  [aaa-bypass]              Current value:
 backup authentication                       [bkp-auth]                Current value: on
 console enable                              [console-enable]          Current value: on
 scroll line (lines)                         [scroll-line]             Current value: 30
 kernel logs                                 [kernel-logs]             Current value: on
 crypted passwords enable                    [crypted-passwords]       Current value: off
 max log messages rate per min (0=unlimited) [log-messages-rate]       Current value: 0
```

Table 2: set

Syntax	Description
loglevel <value> [-s]	Defines the log level, from the lowest level of information (0), to the highest level of information (5). Default is 1
description <string>	You can use up to 100 characters to describe System information.
name <string>	Replace the system name ATOSNT>>with the one entered, up to 100 characters (default ATOSNT plus the last six digits of the serial number).
localdomain <name>	Indicates for which domain name the system is a 'DNS Authority' (default LocalDomain)
deftftpserver <ip addr>	Configures the tftp server IP address that the device heads for files download (default 0.0.0.0).
tftp-local-ipaddress <ip addr>	Configures the TFTP client IP address used by ATOSNT (default 0.0.0.0: IP address of Outgoing interface is used). It is necessary that the configured IP address is an interface IP address (e.g. a loopback)
tftp-local-ipv6address <ipv6 addr>	Configures the TFTP client IPv6 address used by ATOSNT (default ::)
defftpserver-port <ftp server name:port>	Configures the ftp server address and port that the device needs for ftp files download. Up to 129 characters can be used (default null).
ftp-local-ipaddress [aa.bb.cc.dd]	Configures the FTP client IP address used by ATOSNT (default 0.0.0.0: IP address of Outgoing interface is used). It is necessary that the configured IP address is an interface IP address (e.g. a loopback)
ftp-local-ipv6address [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]	Configures the FTP client IPv6 address used by ATOSNT (default ::)
ftp-username <string>	Configures the ftp username that the device uses to authenticate the ftp download session. Up to 64 characters can be used (default anonymous).
ftp-password <string>	Configures the ftp password that the device uses to authenticate the ftp download session. Up to 64 characters can be used (default ATOSNT).
defscpserver-port	Configures the scp server name and port that the device needs for scp files download. Up to 128 characters can be used (default null).
scp-local-ip-address [aa.bb.cc.dd]	Configures the scp local IP address (default 0.0.0.0)
scp-local-ipv6-address [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]	Configures the scp local IPv6 address (default ::)
scp-username <string>	Configures the scp username that the device uses to authenticate the scp download session. Up to 64 characters can be used (default ATOS).
scp-password <string>	Configures the scp password that the device uses to authenticate the scp download session. Up to 64 characters can be used (default ATOS).
aaa-profile <string>	Associates a predefined AAA authentication profile to the device login, via console port, via Eth interface or remotely (default null).
aaa-login-timeout <seconds>	Configures the AAA login timeout attempt in seconds. Range 1-300 sec, default 60
aaa-bypass	Sets an AAA bypass list of up to 16 items chosen from [any|ADMIN|USER|priv-name]
bkp-auth <on|off>	Enables/disables the authentication using the password previously configured with the "set system password"command, in case of aaa.profile failed because the server is not reached . The default value is on.
console-enable <on|off>	Enables/disables the management by console. The default value is on.
scroll-line <value>	Defines the number of lines the user can display at a time (1 to 255, default 22).
kernel-logs <on|off>	Enables/disables the kernel logs of linux based applications (default on)

crypted-passwords <on|off>	Enables/disables the encryption of the password used by the application (e.g. PPP autenthication, Voice authenticathion user password). Default off
log-messages-rate [0 – 2048]	Sets the maximum log message rate (log/min) in order not to overload the CPU with a huge amount of logs. Default [0] (unlimited)

bkp-auth command becomes only active when the authentication try made by AAA profile doesn't have any result. Infact, in case of authetication success or failure, this parameter is ignored.

System – Nodes

Timesync - Commands

ATOSNT has a SNTP client that allows to synchronize the internal system clock to a network provided time source by configuring an SNTP, TCP/TIME or UDP/TIME client.

SNTP v4 protocol [1] (which is an adaptation of the NTP protocol[2]) and the TIME protocol, either in a TCP and UDP versions, allow the internal clock synchronization by sending a request to a SNTP or to a TIME server, respectively.

ATOSNT allows to configure different servers in a list. By enabling **timesync** parameter, a request is sent to the first server in the list. Default configuration provides two alternative entries for the same SNTP server, the first one in numerical format (IP address), the second in alphanumeric format (Internet name).
The www.ntp.org [3] web site provides a list of SNTP servers. Independently from their geographical location, all SNTP servers provide information on the Greenwich Mean Time (GMT).

Table 2: SNTP server list

ISO	Area	HostName
	Worldwide	pool.ntp.org
	Asia	asia.pool.ntp.org
	Europe	europe.pool.ntp.org
	Oceania	oceania.pool.ntp.org
	North America	north-america.pool.ntp.org
AT	Austria	at.pool.ntp.org
AU	Australia	au.pool.ntp.org
CA	Canada	ca.pool.ntp.org
CH	Switzerland	ch.pool.ntp.org
DE	Germany	de.pool.ntp.org
DK	Denmark	dk.pool.ntp.org
ES	Spain	es.pool.ntp.org
FI	Finland	fi.pool.ntp.org
FR	France	fr.pool.ntp.org
IT	Italy	it.pool.ntp.org
LU	Luxemburg	lu.pool.ntp.org
MX	Mexico	mx.pool.ntp.org

MY	Malaysia	my.pool.ntp.org
NL	Netherland	nl.pool.ntp.org
NO	Norway	no.pool.ntp.org
NZ	New Zealand	nz.pool.ntp.org
PH	Philippines	ph.pool.ntp.org
PL	Poland	pl.pool.ntp.org
SE	Sweden	se.pool.ntp.org
SI	Slovenia	si.pool.ntp.org
UK	Great Britain	uk.pool.ntp.org
US	USA	us.pool.ntp.org

```
ATOSNT\system\timesync>>set ?


Nodes not available.
Set command parameters:
 level of log                  [loglevel]              Current value: 1
 enable                        [on|off]                Current value: off
 sync frequency (sec)          [frequency]             Current value: 86400
 gmt offset (min)              [gmt-offset]            Current value: 60
 daylight saving time period   [daylight-saving-time]  Current value: last Sun Mar 02:00 last Sun Oct 03:00
 local ip address              [local-ip-address]      Current value: 0.0.0.0
 local ipv6 address            [local-ipv6-address]    Current value: ::
```

Table 3: set

Syntax	Description
loglevel <value>	Set the detail level used by ATOSNT to log the events of the timesync node (values: 0-5, default 1).
onloff	Enable/disable the time synchronization client. As soon as this parameter is enabled, a request is sent to the first server of the list (default off).
frequency <value>	Set the frequency of synchronization requests, in seconds (default: 8600; range: 0-86400).
gmt-offset <value>	Define the offset in minutes between the local time and the GMT time provided by the time server. The default value, is +60, the configurable range is ± 720.
daylight-saving-time <string>	Configure the summer time (or daylight saving time). Configuration string requires the start and the end time: Daylight saving time [(start) wwww ddd mmm hh:mm (end) wwww ddd mmm hh:mm] wwww = 1..4, last - ddd = mon..sun - mmm = jan..dec Current value: last Sun Mar 02:00 last Sun Oct 03:00 Default fw value: last Sun Mar 02:00 last Sun Oct 03:00
local-ipaddress <ip addr>	Set the SNTP client IP address (default 0.0.0.0).
local-ipv6-address [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]	Set the SNTP client IPv6 address (default ::).

```
ATOSNT\system\timesync>>add ?
```

```
add  help:  Add a new interface
add  usage:
 <ip addr|name>[type]

add command parameters:
 Server      [max 40 char]

ATOSNT\system\timesync>>add 2001:32::/64 ?

add command parameters:
 Server type [sntp|tcp|udp|ntp]
 <cr>
```

```
ATOSNT\system\timesync>>del ?

del  help:  Remove an interface
del  usage:
 <ip addr|name>[type]

del command parameters:
 Server      [max 40 char]
```

Table 4: add-del

Syntax	Description
ip addr|name	Insert/delete a “time server” to/from the list. A server is identified by its IP address or its domain name.
type [sntp|tcp|udp|ntp]	As an additional information the protocol to be used (SNTP, TCP, UDP or NTP) can be added. If this information is omitted, the default protocol is SNTP or NTP.

Timesync – Configuration Examples

Here you can find some examples of SNTP service configuration:

ATOSNT\syslog>>**config**

add system timesync ntp1.inrim.it

set system timesync on

set system timesync frequency 180

ATOSNT\system\timesync>>**show work**

Show of ATOSNT system timesync

Level of log : 1

Enable : on

Sync frequency (sec) : 180

GMT offset (min) : 60

Daylight saving time period : last Sun Mar 02:00 last Sun Oct 03:00

Local IP Address (0.0.0.0 if notused) : 0.0.0.0

LIST OF TIMER SERVER

Time Server Type

ntp1.inrim.it sntp

Timesync – Logs

You can trace the SNTP logs using the following commands:

```
ATOSNT>>set system timesync loglevel 5
ATOSNT>>log start
L2: U 10/05/2010 17:15:26:030 OFSntp: send query to server:ntp1.inrim.it prot:sntp
L2: U 10/05/2010 17:15:26:070 OFSntp: server:ntp1.inrim.it prot:sntp response ok
L2: U 10/05/2010 17:15:26:070 OFSntp: Day light saving time active
```

Intservices - Commands

intservices node is used to configure some internal services such as telnet, SSH and http services.

This operation is needed when you configure an internal server in the network. It allows to identify the requests for connection to an internal server that typically uses a wellknown port number (23 for telnet, 22 for SSH and 80 for http service).

```
ATOSNT\system\intservices>>set ?

Nodes not available.
Set command parameters:
 telnet port             [telnet]  Current value: 23
 ssh port                [ssh]     Current value: 22
 http port               [http]    Current value: 80
 https port              [https]   Current value: 0
 internal services tos   [tos]     Current value: 00
```

Table 5: set

Syntax	Description
telnet <value>	Configure the port for TELNET application. Range: 0-65535, default: 23. It is recommended not to use port 0. In this case any telnet session will not be enabled
ssh <value>	Configure the port for SSH2 application. Range: 0-65535, default: 22. The use of port 0 means SSH access disabled.
http <value>	Configure the port for HTTP access. Range: 0-65535, default: 80. The use of port 0 means http access is disabled.
https <value>	Configure the port for HTTPS access. Range: 0-65535, default: 0. The use of port 0 means https is access disabled.
IP-TOS <hex value>	Set IP TOS value for internal services packets such as telnet, Internal Web server, SNMP etc. (8 hexadecimal bits) [default: 0]

Scheduler - An Overview

When action planning is needed a sort of scheduler must be designed. In this design implementation a list of scheduling profiles is provided, in order to have an automatic starting of an action execution at a specified time and facultative periodic repetition. Action that is goal of profile will be elsewhere specified, in proper configuration context.

“scheduler” – Node

Starting from top “system\scheduler” node , where following actions can be carried out:

1. Adding/deleting a scheduling profile by add/del PROFILE command;
2. Displaying configuration by show conf command;
3. Displaying status of active scheduling profiles by show status command.

“scheduler” – Add command

```
ATOSNT\system\scheduler>>add ?

add  help :  Add a new scheduler profile
add  usage:
 <PROFILE><name><day-start><month-start><year-start><hour-start><min-start>
                 [sec-period][min-period][hour-period][day-period][month-period]

add command parameters:
 PROFILE
```

Table 6: add profile

Syntax	Description
PROFILE <profile-name name>	Indicates a new profile name to add to scheduler profile list.
day-start< value>	Specifies the day of starting time. Mandatory.
month-start< value>	Specifies the month of starting time. Mandatory.
year-start < value>	Specifies the year of starting time. Mandatory.
hour-start <value>	Specifies the hour of starting time. Mandatory.
min-start < value>	Specifies the minute of starting time. Mandatory.
sec-period < value>	Specifies the seconds after which action will be repeated. Optional.
min-period < value>	Specifies the minutes after which action will be repeated. Optional.
hour-period < value>	Specifies the hours after which action will be repeated. Optional.
day-period < value>	Specifies the days after which action will be repeated. Optional.
month-period < value>	Specifies the months after which action will be repeated. Optional.
year-period < value>	Specifies the years after which action will be repeated. Optional.

“scheduler” – del command

```
ATOS\system\scheduler>> del PROFILE <profile-name>
```

Table 7: del profile

Syntax	Description
PROFILE <profile name>	Indicates profile to remove from scheduler profile list.

"scheduler" - set command

```
ATOSNT\scheduler>>set ?

Nodes not vailable.
Set command arameters:
 level of log  [loglevel]  Current value: 1
```

Table 8: set

Syntax	Description
loglevel <value>	Sets the detail level used by ATOSNT to record the scheduler events. Default: 1

“scheduler” – Show conf/work command

```
ATOSNT\system\scheduler>>show conf
Show of ATOS scheduler
Level of log : 5

LIST OF PROFILES
PROFILE START: dd mm yyyy hour min PERIOD: sec min hour dd mm yy
prof1 15 6 2011 16 13 15 0 0 0 0 0
prof2 30 7 2011 0 0 0 0 0 0 0 0
cpsched 29 7 2011 12 45 30 0 0 0 0 0
Command executed
```

“scheduler” – Show Status command

```
ATOS\system\scheduler>>show status

Next expiration in: 18 seconds
Status of 1 entries:
cpsched: period=30 deltaTime=30</pre>
```

Notes

[1] Rfc 2030
[2] Rfc 1305
[3] http://www.ntp.org/

Index

ManStorage

Storage Configuration

The **Storage** feature allows to manage local storage devices, like external unit disks, connected to the router.

It also allows to connect remote storage devices and manage them as they were locally connected to the router.

Under storage node, it is also possible to work on **files or folders**, so you can:

- **List** the file contents of the drive
- **Remove** safely the drive or
- **Create, Erase, Copy** and **Rename** files or folders between drives

storage - Node

Storage feature is available at the **storage** node

storage – Commands

At the **storage** node you can set the following parameters:

```
ATOSNT\storage>>set ?

Nodes not available.
Set command parameters:
 level of log                       [loglevel]  Current value: 1
```

Table 1: **set**

Syntax	Description
loglevel <0-5>	Set the detail level used by ATOS to log the Storage events [default: 1]

Add/del commands permit to connect or delete remote network storage devices. Associating the remote network address of the shared folder to one of the local unit disks (D:|E:|.....Z:), the user can manage the remote storage device in a easy way as it was connected to the router locally.

```
ATOSNT\storage>>add ?

add  help :  Add a new network storage
add  usage:
 <NET-STORAGE><Name><Network-path><Local-disk>[Network-user <Network-password>]

add command parameters:
 NET-STORAGE
```

Table 2: **add - del NET-STORAGE**

Syntax	Description
NET-STORAGE	Keyword
name [max 16 char]	Name of the network to be defined
Network-path [max 120 char]	Standard network path such as \\server-name or ip address\folder
Local-disk [D:|E:|F:|G:|H:|I:|J:|K:|L:|M:|N:|O:|P:|Q:|R:| S:|T:|U:|V:|W:|X:|Y:|Z:]	Select a disk unit letter from the recommended list.
Network-user [max 32 char]	Optional username to access to the remote network storage
Network-password [max 32 char]	Optional password to access to the remote network storage

To work on files contents or folders, you should use the following commands:

List command permits to view the drive files and folders contents.

```
ATOSNT\storage>>list ?

list  help :  List drive contents
list  usage:
 <Drive>[List path]

list command parameters:
 disk id                          [D:|E:|.....Z:]
```

Table 3: **list**

Syntax	Description
Drive	Select a unit disk letter to list from the recommended list.
List path [max 32 char]	Optional path

Remove command permits to remove safely the storage device connected to the router.

```
ATOSNT\storage>>remove ?

remove  help :  Remove drive safely
remove  usage:
 <Drive>

remove command parameters:
 disk id                          [D:|E:|.....Z:]
```

Table 4: **remove**

Syntax	Description
Drive	Select a unit disk letter to remove from the recommended list.

Create command permits to create an empty file or a folder on a selected drive

```
ATOSNT\storage>>create ?

create  help :  Create file or folder
create  usage:
```

```
 <Type><Drive><Name>

create command parameters:
 type                                [FILE|FOLDER]
```

Table 5: **create**

Syntax	Description
FILE|FOLDER	Select to create a new File or Folder
Drive	Select a unit disk letter from the recommended list for the drive.
Name [max 120 char]	Set the file or folder path

Copy command permits to copy a file or a folder between storage devices.

```
ATOSNT\storage>>copy ?

copy  help :  Copy file or folder
copy  usage:
 <Source-Drive><Source-Name><Dest-Drive><Dest-Name>

copy command parameters:
 source disk                         [G:]
```

Table 6: **copy**

Syntax	Description
Source-Drive	Select source unit disk letter from the recommended list.
Source-Name [max 120 char]	Source file or folder path.
Dest-Drive	Select destination unit disk letter from the recommended list.
Dest-Name [max 120 char]	Destination file or folder path.

Rename command permits to change file name or folder name on the storage devices.

```
ATOSNT\storage>>rename ?

rename  help :  Rename file or folder
rename  usage:
 <Drive><Name><New-Name>

rename command parameters:
 disk id                             [D:|E:|...]
```

Table 7: **rename**

Syntax	Description
Drive	Select a unit disk letter from the recommended list.
Name [max 120 char]	Name of file or folder.
New-Name [max 120 char]	New name for selected file or folder.

Storage – Subnodes

With **tree** command, you can see all the subnodes added to the storage node

```
ATOSNT\storage>>tree
storage                Rossi
                       Documents

ATOSNT\storage\Rossi>>set ?

Nodes not available.
Set command parameters:
 network path      [network-path]      Current value: 192.169.110.50
 network user      [network-user]      Current value: Rossi
 network password  [network-password]  Current value: mario
```

Table 8: **set**

Syntax	Description
Network-path [max 120 char]	Standard network path such as \\server-name or ip address\folder .
Network-user [max 32 char]	Optional username to access to network storage
Network-password [max 32 char]	Optional password to access to network storage

storage Configuration example

```
ATOSNT\storage>>show conf
Show of ATOSNT storage
Level of log                    : 1

Show of ATOSNT storage Rossi
Network Path     : //192.168.110.75/shared
Local Disk Id    : G:
Network User     : Alfonso
Network Password : key

Command executed
```

```
ATOSNT\storage>>list ?

list  help :  List drive contents
list  usage:
 <Drive>[List path]
```

```
list command parameters:
  disk id                           [M:|F:]
ATOSNT\storage>>list f:
drwxr-xr-x    5 root     root          4096 Jan  1 00:00 .
drwxrwxrwt    4 root     root            80 Jan  1 00:00 ..
drwxr-xr-x    5 root     root          4096 Nov 28  2012 .Trash-1000
drwxr-xr-x    5 root     root          4096 Jan  1  1980 protected
drwxr-xr-x    2 root     root          4096 Jan  1  1980 public
Command executed
```

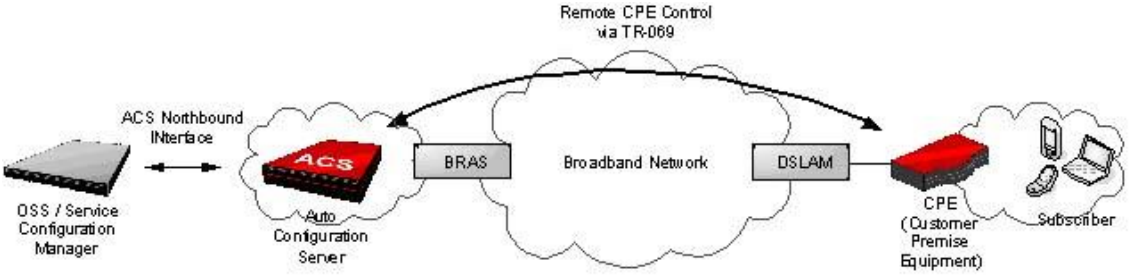
```
ATOSNT\storage>>list M:
drwx------    8 1000     1000             0 Dec 12  2012 .
drwxrwxrwt    4 root     root            80 Jan  1 00:00 ..
drwx------    2 1000     1000             0 Oct  9  2012 img
drwx------    2 1000     1000             0 Jan 16  2012 mp3
drwx------    2 1000     1000             0 Apr 16  2012 torrent
drwx------    2 1000     1000             0 May  2  2012 video
-rwxr-xr-x    1 1000     1000           887 Dec 12  2012 wwwsh
```

Command executed

ManTr069

TR069

TR-069 (short for Technical Report 069) is a DSL Forum technical specification entitled CPE WAN Management Protocol (**CWMP**). It defines an application layer protocol for remote management of end-user devices.
ACS stands for Auto-Configuration Server. This is a component in the broadband network responsible for auto-configuration of the CPE for advanced services.



Current Aethra TR069 Remote Procedure Call (RPC) supported

The following table shows the current Aethra TR069 RPC supported:

Table 1: Current TR069 RPC

RPC	Note
GetRPCMethods	
SetParameterValues	
GetParameterValues	
GetParameterNames	
SetParameterAttributes	
GetParameterAttributes	
AddObject	
DeleteObject	
Reboot	
Upload	User Configuration file.
FactoryReset	
Download	User configuration file, firmware upgrade, firmware package, license, boot, certificate.

The CPE manages the notification procedures for the parameters of the data model, as required by TR069 and TR098 documents.

Current Aethra Data Model

The following table shows the current Aethra TR069 Data Model (R means read only, RW means read and write):

Table 2: Current Data Model

Syntax	Description
InternetGatewayDevice.DeviceSummary	**R**
InternetGatewayDevice.DeviceInfo.Manufacturer	**R**
InternetGatewayDevice.DeviceInfo.ManufacturerOUI	**R**
InternetGatewayDevice.DeviceInfo.ProductClass	**R**
InternetGatewayDevice.DeviceInfo.SpecVersion	**R**
InternetGatewayDevice.DeviceInfo.Description	**R**
InternetGatewayDevice.DeviceInfo.SerialNumber	**R**
InternetGatewayDevice.DeviceInfo.ModelName	**R**
InternetGatewayDevice.DeviceInfo.SoftwareVersion	**R**
InternetGatewayDevice.DeviceInfo.HardwareVersion	**R**
InternetGatewayDevice.DeviceInfo.SpecVersion	**RW**
InternetGatewayDevice.ManagementServer.ConnectionRequestPassword	**RW**
InternetGatewayDevice.ManagementServer.ConnectionRequestURL	**RW**
InternetGatewayDevice.ManagementServer.ConnectionRequestUsername	**RW**

InternetGatewayDevice.ManagementServer.ParameterKey	**R**
InternetGatewayDevice.ManagementServer.Password	**RW**
InternetGatewayDevice.ManagementServer.PeriodicInformEnable	**RW**
InternetGatewayDevice.ManagementServer.PeriodicInformInterval	**RW**
InternetGatewayDevice.ManagementServer.PeriodicInformTime	**RW**
InternetGatewayDevice.ManagementServer.URL	**RW**
InternetGatewayDevice.ManagementServer.Username	**RW**
InternetGatewayDevice.ManagementServer.ManageableDevice.{i}.ManufacturerOUI	**R**
InternetGatewayDevice.ManagementServer.ManageableDevice. {i}.ProductClass	**R**
InternetGatewayDevice.ManagementServer.ManageableDevice. {i}.SerialNumber	**R**
InternetGatewayDevice.LANDevice.{i}.Hosts.HostNumberOfEntries	**R**
InternetGatewayDevice.LANDevice.{i}.Hosts.Host.{i}.IPAddress	**R**
InternetGatewayDevice.LANDevice.{i}.Hosts.Host.{i}.HostName	**R**
InternetGatewayDevice.LANDevice.{i}.Hosts.Host.{i}.AddressSource	**R**
InternetGatewayDevice.LANDevice.{i}.Hosts.Host.{i}.MACAddress	**R**
InternetGatewayDevice.LANDevice.{i}.LANHostConfigManagement.DHCPServerEnable	**R**
InternetGatewayDevice.LANDevice.{i}.LANHostConfigManagement.MinAddress	**R**
InternetGatewayDevice.LANDevice.{i}.LANHostConfigManagement.SubnetMask	**R**
InternetGatewayDevice.LANDevice.{i}.LANHostConfigManagement.MaxAddress	**R**
InternetGatewayDevice.LANDevice.{i}.LANHostConfigManagement.DNSServers	**R**
InternetGatewayDevice.LANDevice.{i}.LANHostConfigManagement.IPRouters	**R**
InternetGatewayDevice.WANDevice.{i}.WANCommonInterfaceConfig.Layer1DownstreamMaxBitRate	**R**
InternetGatewayDevice.WANDevice.{i}.WANCommonInterfaceConfig.Layer1UpstreamMaxBitRate	**R**
InternetGatewayDevice.WANDevice.{i}.WANCommonInterfaceConfig.PhysicalLinkStatus	**R**
InternetGatewayDevice.WANDevice.{i}.WANCommonInterfaceConfig.TotalPacketsReceived	**R**
InternetGatewayDevice.WANDevice.{i}.WANCommonInterfaceConfig.TotalPacketsSent	**R**
InternetGatewayDevice.WANDevice.{i}.WANCommonInterfaceConfig.TotalBytesSent	**R**
InternetGatewayDevice.WANDevice.{i}.WANCommonInterfaceConfig.TotalBytesReceived	**R**
InternetGatewayDevice.WANDevice.{i}.WANDSLInterfaceConfig.UpstreamAttenuation	**R**
InternetGatewayDevice.WANDevice.{i}.WANDSLInterfaceConfig.DownstreamAttenuation	**R**
InternetGatewayDevice.WANDevice.{i}.WANDSLInterfaceConfig.UpstreamNoiseMargin	**R**
InternetGatewayDevice.WANDevice.{i}.WANDSLInterfaceConfig.DownstreamNoiseMargin	**R**
InternetGatewayDevice.WANDevice.{i}.WANDSLInterfaceConfig.DownstreamCurrRate	**R**
InternetGatewayDevice.WANDevice.{i}.WANDSLInterfaceConfig.UpstreamCurrRate	**R**
InternetGatewayDevice.WANDevice.{i}.WANDSLInterfaceConfig.ModulationType	**R**
InternetGatewayDevice.WANDevice.{i}.WANDSLInterfaceConfig.Stats.Total.CRCErrors	**R**
InternetGatewayDevice.WANDevice.{i}.WANDSLInterfaceConfig.Stats.Showtime.CRCErrors	**R**
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANDSLLinkConfig.DestinationAddress	**RW**
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANDSLLinkConfig.VCSearchList	**R**

InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANIPConnection.{i}.ExternalIPAddress	**R**
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANIPConnection.{i}.Enable	**RW**
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANIPConnection.{i}.ConnectionType	**R**
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANIPConnection.{i}.ConnectionTrigger	**R**
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANIPConnection.{i}.Name	**RW**
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANIPConnection.{i}.NATEnabled	**RW**
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANIPConnection.{i}.ConnectionStatus	**R**
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANPPPConnection.{i}.ExternalIPAddress	**R**
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANPPPConnection.{i}.ConnectionType	**R**
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANPPPConnection.{i}.ConnectionStatus	**R**
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANPPPConnection.{i}.Enable	**RW**
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANPPPConnection.{i}.Uptime	**R**
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANPPPConnection.{i}.LastConnectionError	**R**
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANPPPConnection.{i}.ConnectionTrigger	**R**
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANPPPConnection.{i}.Name	**RW**
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANPPPConnection.{i}.NATEnabled	**RW**
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANPPPConnection.{i}.Password	**RW**
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANPPPConnection.{i}.Username	**RW**
InternetGatewayDevice.Services.VoiceService.{i}.VoiceProfile.{i}.Enable	**R**
InternetGatewayDevice.Services.VoiceService.{i}.VoiceProfile.{i}.DTMFMethod	**R**
InternetGatewayDevice.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Codec.List.{i}.Enable	**RW**
InternetGatewayDevice.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Codec.List.{i}.Priority	**RW**
InternetGatewayDevice.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Codec.List.{i}.PacketizationPeriod	**R**
InternetGatewayDevice.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Codec.List.{i}.Codec	**R**
InternetGatewayDevice.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Codec.List.{i}.BitRate	**R**
InternetGatewayDevice.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Enable	**RW**
InternetGatewayDevice.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.DirectoryNumber	**RW**
InternetGatewayDevice.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.CallingFeatures.CallerIDName	**RW**
InternetGatewayDevice.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.SIP.URI	**R**
InternetGatewayDevice.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.SIP.AuthUserName	**RW**
InternetGatewayDevice.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.SIP.AuthPassword	**RW**
InternetGatewayDevice.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.ProxyServer	**RW**
InternetGatewayDevice.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.UserAgentPort	**RW**
InternetGatewayDevice.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.ProxyServerPort	**RW**
InternetGatewayDevice.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.UserAgentDomain	**RW**

For CPE models provided with WAN Eth1 physical interface, it is possible to configure the device as a WANDevice."

TR069 CLI Commands

```
ATOSNT\tr069>>set ?

Nodes not available.
Set command parameters:
 level of log                      [loglevel]                 Current value: 1
 enable                            [on|off]                   Current value: on
 interface name                    [interface-name]           Current value:
 acs url                           [acs-url]                  Current value:
 acs username                      [acs-username]             Current value:
 acs password                      [acs-password]             Current value:
 periodic inform enable            [periodic-inform-enable]   Current value: off
 periodic inform interval          [periodic-inform-interval] Current value: 1
 connection request username       [cr-username]              Current value:
 connection request password       [cr-password]              Current value:
 use mac address as serial number  [mac-addr-as-sn]           Current value: off
 connection request port           [cr-port]                  Current value: 8082
 connection request path           [cr-path]                  Current value: acscall
```

Table 3: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the TR069 events. Default: 1
onloff	Enables/disables the CWMP protocol
interface-name	defines the interface to use for the CWMP session
acs-url [max 100 char]	Sets the URL for the CPE to connect to the ACS using the CPE WAN Management Protocol.This parameter MUST be in the form of a valid HTTP or HTTPS URL. The “host” portion of this URL is used by the CPE.
acs-username [max 100 char]	Sets the Username to use to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol.
acs-password [max 100 char]	Sets the Password to use to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol.
off]	Enables/disables the CPE to send periodically CPE information to Server using the Inform method call. Default: off
periodic-inform-interval [1-999999]	Sets the duration in seconds of the interval for which the CPE must attempt to connect with the ACS and call the Inform method if PeriodicInformEnable is true. Default: 1
cr-username [max 100 char]	Sets the Username to authenticate an ACS making a Connection Request to the CPE.
cr-password [max 100 char]	Sets the Password used to authenticate an ACS making a Connection Request to the CPE.
mac-addr-as-sn [offlon]	Enables/Disables to use the Mac address as a serial number of the CPE • on the mac address wihout **":"** is used • off the serial number of the CPE is used Default: off

cr-port [1-65535]	Defines the port of the CPE HTTP URL provided to the ACS to make a Connection Request notification to the CPE. The form of a Connection Request URL is http://host:port/path. Default: 80882
cr-path [max 100 char]	Defines the path of the CPE HTTP URL provided to the ACS to make a Connection Request notification to the CPE. The form of a Connection Request URL is http://host:port/path. Default: acsall

Index

ManVoiceServ

Voice Service - Configuration

PBX functionalities are available from ATOS Version: 5.7.0.rc1 (37@BVMEDtjuukbpjWcwovv)

In **voice-serv** node you can set the voice service requested to the CPE. The CPE can work in **VoIP** or **PBX** mode. You must select which operation mode you want to use. Look at the syntax.

```
ATOSNT\voice-serv>>set ?

Nodes not available.
Set command parameters:
 mode  [mode]  Current value: VOIP

ATOSNT\voice-serv>>set mode ?

mode  [VOIP|PBX]

 Current value:    VOIP
 Default fw value: VOIP
```

To switch from VoIP to PBX working mode, you should use set command.

```
ATOSNT\voice-serv>>set mode PBX ?


Command complete (enter cr)


ATOSNT\voice-serv>>set mode PBX
Warning!! 'PBX' mode is requested while it's working as 'VOIP': need to save and restart and configure the  nodes related
Command executed
```

At this point you should insert save and then restart commands

```
*ATOSNT\voice-serv>>save
Command executed
*ATOSNT\voice-serv>>restart no-save-conf
System will be restarted in 1 sec
Command executed
*ATOSNT\voice-serv>>Restarting...

ATOS-NT boot system V2.1.6
```

```
Starting OS...................Done
Starting ATOSNT...
ATOSNT is running
VDSL2 over POTS FW file is available
ADSL2plus/2/1 Annex A FW file is available
VDSL2 over ISDN FW file is available
ADSL2plus/2/1 Annex B FW file is available
Init Command Line Interface...
ATOS Version: 5.7.0.rc1 (37@BVMEDtjuukbpjWcwovv)
ATOS Date: 31/07/2013 12:16
ATOS License: FullFeatures
Hardware: SV6044VW - 2320B
Product Code: 708190244
Serial Number: 310638
eth0 MAC Address: 00:D0:D6:48:87:E7
Wireless card: Atheros Communications, Inc. - AR9227 Wireless Network Adapter
.......................
```

To check the current operating mode, follow the next steps

```
User name :aethra
Password :

<a> logged at Administrator level

ATOSNT\voice-serv>>set ?

Nodes not available.
Set command parameters:
 mode  [mode]  Current value: PBX
```

At this point, you can notice that the **pbx** node and the related subnodes are on the root menu, see below

```
ATOSNT>>tree
ATOSNT                   system                   timesync
                                                 intservices
                                                 privilege-map
                                                 scheduler
                         storage
                         xdsl0
                         eth0                    port1
                                                 port2
                                                 port3
                                                 port4
.......................

                         voice-serv
                         pbx                     service-code
                                                 call-setting           it
```

```
                                                                    be
                                                                    italy
                                                                    belgium
                                                sip
                                                fax
                                                user-terminal
                                                ring-group
                                                trunk
                                                messages *
                                                call-mng            rules
                                                directory-number
                                                address-book
                                                voicemail *
                                                parking
                                                music-on-hold
Note:
```

* only available on CPE models with advance PBX license

ManVoip

VoIP

Physical Interfaces

Voip service relies on the use of physical equipment like analog telephones, ISDN terminals and/or DECT cordless telephones. The physical interfaces to be configured are: POTS (FXS and FXO), BRI ISDN ports and/or DECT.

voip – Commands

Integrated Access Devices, IADs, provide a gateway function between legacy devices (POTS, ISN BRI or ISDN PRI) and VoIP service based on SIP protocol.

The CLI structure is the following:

```
ATOSNT\voip>>set ?

Available nodes:
                      call-setting
                      sip
                      fax
                      user-terminal
                      terminal-group
                      trunk
                      call-mng

Set command parameters:
 level of log               [loglevel]             Current value: 1
```

```
system clock                [sysclock]              Current value: free-running
max trunk sip connections   [max-connections]       Current value: 16
international prefix        [international-prefix]  Current value: 00
country code                [country-code]          Current value: 39
strip country prefix        [strip-country-prefix]  Current value: off
```

Table 5:set

Syntax	Description
loglevel [value]	Sets the detail level used by ATOS to log the events of the VoIP, from the less detailed one (0) to the more detailed one (5). Adding the [- s] option, this command will be extended to all voip subnodes. Default: [1]
sysclock [ntr|external|free-running]	Clock setting • **ntr** means that timing is derived from the ShDSL interface. This clock is supposed to be synchronous to the network timing (where available). • **external** means that timing is derived from the Synk IN interface (where available) • **free-running** means that the clock is derived from the internal clock (default). *Note:*In CPE where only free-running mode is available, this parameter is not presented to user.
max-connections [1 - max]	Sets the maximum number of simultaneous calls allowed. The value of max depends on CPE capabilities. Default:[max]
international-prefix [1-3 decimal digits]	Sets the digits (from 1 to 3) for the prefix of international phone numbers. Default: [00]
country-code [max 3 decimal digits]	Sets the digits (from 1 to 3) for the prefix of the country from which the caller is dialing. Default: [39] (Italy)
strip-country-prefix [on|off]	In incoming calls, it allows to strip or take off international prefix and country code in the calling number presentation conditioned that both informations are available. • on international prefix and country code (e.g. +39 or 0039) are stripped when presenting Calling Line Identity to local user. • off calling number presentation is complete of international prefix and country code information. Default: [off]

Configuration example with "show conf" command:

ATOS\voip>>**show conf**

Show of ATOS voip

Level of log : 1

System Clock : free-running

Max Trunk SIP Connections : 16

International Prefix : 00

Country Code : 39

Strip Country Prefix : off

voip – Nodes

Configuration of VoIP service is structured in subnodes as follows:

```
call-setting it
             italy
             country_name_n
             profile_name_n
sip
 profile_name_1
 profile_name_n
fax
user-terminal pots-line-1
              pots-line-n
              isdn-line-1
              isdn-line-n
              isdn-line-x-number
dect-base0.1
dect-base0.6
terminal-group ring-gr-number_1
               ring-gr-number_n
trunk trunk_name_1
      trunk_name_n
call-mng
```

call-setting – Commands

In **call-setting** subnode it is possible to define a set of “country” parameters and a “call-profile” parameters set.

Notice that “it” country and “italy” call-profile are pre-defined and not editable neither deletable.

In this node is set the value of country parameter, which is unique for the whole VoIP service, while call-profile is settable separately for each user terminal.

```
ATOSNT\voip\call-setting>>set ?

Set command parameters:
 level of log            [loglevel]  Current value: 1
 country                 [country]   Current value: it
```

Table 6:set

Syntax	Description
loglevel [value]	Set the detail level used by ATOS to log the events of the SIP, from the less detailed one (0) to the more detailed one (5). default: [1]
country [itlother listedcountries]	Set the active country parameter set. default: [it]

Configuration example with "show conf" command:

ATOS\voip\call-setting>>show conf

Show of ATOSNT voip call-setting

Level of log: 5

Country: it

```
ATOSNT\voip\call-setting>>add ?

add  help :  Add a new COUNTRY or CALL-PROFILE
add  usage:
 <COUNTRY><name>
 <CALL-PROFILE><name>

add command parameters:
 COUNTRY
 CALL-PROFILE
```

Table 7: **add COUNTRY**

Syntax	Description
COUNTRY	keyword
[name] [max 2 char]	Name of new country parameter set

Table 8: :**add CALL-PROFILE**

Syntax	Description
CALL-PROFILE	keyword
[name][max 16 char]	Name of new call profile parameter set

In order to speed up the creation of both a new country or call-profile, in this node is also available a special command “copy”.

```
ATOSNT\voip\call-setting>>copy ?

copy  help :  Copy a COUNTRY or a CALL-PROFILE
copy  usage:
 <COUNTRY|CALL-PROFILE><from name><new name>

copy command parameters:
 copy                    [COUNTRY|CALL-PROFILE]
```

Table 9:**copy**

Syntax	Description
COUNTRY [from name][new name]	Creates a new country (new name) with the parameter values of the existing “from name” country
CALL-PROFILE [from name][new name]	Creates a new call profile (new name) with the parameter values of the existing “from name” country

```
ATOSNT\voip\call-setting>>del ?

del  help :  Remove COUNTRY or CALL-PROFILE
del  usage:
 <COUNTRY><name>
 <CALL-PROFILE><name>

del command parameters:
 COUNTRY
 CALL-PROFILE
```

For parameter explanation refer to add command tables.

call-setting – Nodes

country_name_n – Commands

In this node typical telephone parameters for any country are configurable. For Italy, a predefined, not modifiable and not deletable node (it) is present.

Notice that the names allowed should be two characters long.

```
ATOSNT\voip\call-setting\country_name_n>>show conf
Show of ATOSNT voip call-setting it
Description                    : Italy
Ring Cadence                   : 1000 4000
Dial Tone Frequence            : 425
Dial Tone pattern              : periodic 200 200 600 1000
Busy Tone Frequence            : 425
Busy Tone pattern              : periodic 500 500
RingBack Tone Frequence        : 425
RingBack Tone pattern          : periodic 1000 4000
Call Waiting Tone Frequence    : 425
Call Waiting Tone pattern      : periodic 400 100 250 100 150 14000
Congestion Tone Frequence      : 425
Congestion Tone pattern        : periodic 200 200
Call Held Tone Frequence       : 425
Call Held Tone pattern         : periodic 50 200 50 4700
Attention Tone Frequence       : 425
Attention Tone pattern         : three-shot 200 200
Confirm Tone Frequence         : 425
Confirm Tone pattern           : periodic 200 200 200 2000
Message Waiting Tone Frequence : 425
Message Waiting Tone pattern   : five-shot 100 100 100 100 100 500
Special Tone Frequence         : 950 1400 1800
```

```
Special Tone pattern           : three-shot 330 30 330 30 330 1000
RingBack CW Tone Frequence     : 425
RingBack CW Tone pattern       : periodic 200 200 1000 4000 1000 4000 1000 4000

Command executed
```

***Table 10:*set**

Syntax	Description
description [string][max 100 char]	Description of the node content
ring-cadence [up to 4 pairs of values (50-10000)]	From 1 to 4 couples duration/pause for ringing
busy-tone-freq [value][10 - 2000] Hz	Frequency of busy tone. Default [425]
busy-tone-pattern [continuous|periodic|one-shot|two-shot|three-shot|four-shot|five-shot] [up to 4 pairs of values (10-60000)]	Pattern of busy tone. From 1 to 4 couples duration/pause for tone can be defined, except if “continuous” value is selected. In this case no additional parameters are accepted. Otherwise the pattern is reproduced periodically or the number of times specified by the first parameter. Default [periodic,200 200 600 1000]
ringback-tone-freq [value] [10 - 2000] Hz	Frequency of ringback tone. Default [425]
ringback-tone-pattern [continuous|periodic|one-shot|two-shot|three-shot|four-shot|five-shot] [up to 4 pairs of values (10-60000)]	Pattern of ringback tone. From 1 to 4 couples duration/pause for tone can be defined, except if “continuous” value is selected. In this case no additional parameters are accepted. Otherwise the pattern is reproduced periodically or the number of times specified by the first parameter. Default [periodic,1000 4000]
callwaiting-tone-freq [value] [10 - 2000] Hz	Frequency of callwaiting-tone tone. Default [425]
callwaiting-tone-pattern [continuous|periodic|one-shot|two-shot|three-shot|four-shot|five-shot] [up to 4 pairs of values (10-60000)]	Pattern of callwaiting tone. From 1 to 4 couples duration/pause for tone can be defined, except if “continuous” value is selected. In this case no additional parameters are accepted. Otherwise the pattern is reproduced periodically or the number of times specified by the first parameter. Default [periodic,400 100 250 100 150 14000]
congestion-tone-freq [value] [10 - 2000] Hz	Frequency of congestion-tone tone. Default [425]
congestion-tone-pattern [continuous|periodic|one-shot|two-shot|three-shot|four-shot|five-shot] [up to 4 pairs of values (10-60000)]	Pattern of congestion tone. From 1 to 4 couples duration/pause for tone can be defined, except if “continuous” value is selected. In this case no additional parameters are accepted. Otherwise the pattern is reproduced periodically or the number of times specified by the first parameter. Default [periodic,200 200]
callheld-tone-freq [value] [10 - 2000] Hz	Frequency of callheld tone. Default [425]
callheld-tone-pattern [continuous|periodic|one-shot|two-shot|three-shot|four-shot|five-shot] [up to 4 pairs of values (10-60000)]	Pattern of callheld tone. From 1 to 4 couples duration/pause for tone can be defined, except if “continuous” value is selected. In this case no additional parameters are accepted. Otherwise the pattern is reproduced periodically or the number of times specified by the first parameter. Default [periodic, 50 200 50 4700]
attention -tone-freq [value] [10 - 2000] Hz	Frequency of attention tone. "Attention tone" is the tone played on a user terminal participating in a three-way call, to notify that another terminal is leaving the conference. Default [425]
attention-tone-pattern [continuous|periodic|one-shot|two-shot|three-shot|four-shot|five-shot] [up to 4 pairs of values (10-60000)]	Pattern of attention tone. From 1 to 4 couples duration/pause for tone can be defined, except if “continuous” value is selected. In this case no additional parameters are accepted. Otherwise the pattern is reproduced periodically or the number of times specified by the first parameter. Default [one-shot,200 200 200 200 200 200]
confirm-tone-freq [value] [10 - 2000] Hz	Frequency of confirm tone. Default [425]

confirm-tone-pattern [continuous|periodic|one-shot|two-shot|three-shot|four-shot|five-shot] [up to 4 pairs of values (10-60000)]	Pattern of confirm tone. From 1 to 4 couples duration/pause for tone can be defined, except if “continuous” value is selected. In this case no additional parameters are accepted. Otherwise the pattern is reproduced periodically or the number of times specified by the first parameter. Default [periodic,200 200 200 2000]
msgwait-tone-freq [value] [10 - 2000] Hz	Frequency of message waiting tone. "Message Waiting Tone" is the tone played on a user terminal going off-hook, in place of the dial tone, in case of pending voice messages for the terminal (example: voicemail service) with waiting messages notified via SIP NOTIFY requests with "Messages-Waiting" header set to "yes" Default [425]
msgwait-tone-pattern [continuous|periodic|one-shot|two-shot|three-shot|four-shot|five-shot] [up to 4 pairs of values (10-60000)]	Pattern of message waiting tone. From 1 to 4 couples duration/pause for tone can be defined, except if “continuous” value is selected. In this case no additional parameters are accepted. Otherwise the pattern is reproduced periodically or the number of times specified by the first parameter. Default [periodic,100 100 100 100 100 500]
special-tone-freq [value] [10 - 2000] Hz	Frequency of special tone. "Special Tone" is the tone to be played on a User Terminal, in case of a SIP response code 500 "Server Internal Error" is received over a trunk in reply to an outbound SIP request. "Special Tone" can be configured at "trunk" node (setting trunk parameter "rx-server-internal-error" to value "special-tone"). Default [950]
special-tone-pattern [continuous|periodic|one-shot|two-shot|three-shot|four-shot|five-shot] [up to 4 pairs of values (10-60000)]	Pattern of special tone. From 1 to 4 couples duration/pause for tone can be defined, except if “continuous” value is selected. In this case no additional parameters are accepted. Otherwise the pattern is reproduced periodically or the number of times specified by the first parameter. Default [periodic,330 30 330 30 330 1000]
ringbackcw-tone-freq [value] [10 - 2000] Hz	Frequency of ringback call waiting tone. "Ringback Call Waiting Tone" is played on a user terminal in case of: • a SIP response code 182 "Queued" is received over a trunk in reply to an outbound SIP request • a SIP response code 180 "Ringing" including an "Alert-Info" header (whose value matches the locally defined SIP trunk parameter "ringing-cw-string") is received over a trunk in reply to an outbound SIP request. Default [425]
ringbackcw-tone-pattern [continuous|periodic|one-shot|two-shot|three-shot|four-shot|five-shot] [up to 4 pairs of values (10-60000)]	Pattern of ringback call waiting tone. From 1 to 4 couples duration/pause for tone can be defined, except if “continuous” value is selected. In this case no additional parameters are accepted. Otherwise the pattern is reproduced periodically or the number of times specified by the first parameter. Default [periodic,200 200 1000 4000 1000 4000 1000 4000]

An example of configuration:

```
ATOS\voip\call-setting\ro>>show conf
Show of ATOS voip call-setting ro
Description: contry_name_n parameters
Ring Cadence: 1000 4000
Dial Tone Frequence: 425
Dial Tone pattern: continuous
Busy Tone Frequence: 425
Busy Tone pattern: periodic,500 500
RingBack Tone Frequence: 425
RingBack Tone pattern: periodic,1000 4000
Call Waiting Tone Frequence: 425
Call Waiting Tone pattern: periodic,400 100 250 100 150 14000
Congestion Tone Frequence: 425
Congestion Tone pattern: periodic,200 200
Call Held Tone Frequence: 425
Call Held Tone pattern: periodic,50 200 50 4700
Attention Tone Frequence: 425
Attention Tone pattern: one-shot,200 200 200 200 200 200
Confirm Tone Frequence: 425
Confirm Tone pattern: periodic,200 200 200 2000
Message Waiting Tone Frequence: 425
Message Waiting Tone pattern: periodic,100 100 100 100 100 500
Special Tone Frequence: 950
Special Tone pattern: periodic,330 30 330 30 330 1000
RingBack CW Tone Frequence: 425
RingBack CW Tone pattern: periodic,200 200 1000 4000 1000 4000 1000 4000
```

Call_profile_name_n – Commands

In this node another set of parameters, which can be separately associated to each user terminal, can be defined.

Currently two kind of parameter are availabe: timers and keypad sequences for supplementary services.

Supplementary Services are implemented externally by the Service Provider.
The scope of these parameters is to:

- speed up Invite sending as soon as a sequence is recognized, without waiting for interdigit timer;
- manage special condition related to the special function of '#' key wich is normally used as a "sending complete" at the end of a number dialing in order not to wait for interdigit timer. In particular:
- Call forwarding sequences requires a final '#' (e.g. *21*1234567#). So it is not to be intended as "sending complete" and stripped as usual.
- In CLIR on per call basis, when dialing a similar sequence (e.g. *31*1234567#) the final # is to be intended as "sending complete" and stripped.

An example using default "italy" call-profile:

ATOS\voip\call-setting\italy>>show work
Show of ATOS voip call-setting italy
Description : Italy timer values and ss code
Interdigit Timer : 2
Alert Timer : 60
Ringback Timer : 60
Call Forward Always Query Code : *#21#
Call Forward Always Act Code : *21*
Call Forward Always Deact Code : #21#
Call Forward Busy Query Code : *#67#
Call Forward Busy Act Code : *67*
Call Forward Busy Deact Code : #67#
Call Forward No Answer Query Code : *#61#
Call Forward No Answer Act Code : *61*
Call Forward No Answer Deact Code : #61#
CLIR Permanent Query Code : *#31#
CLIR Permanent Act Code : *31#
CLIR Permanent Deact Code : #31#
CLIR on Call Basis Code : *31*

When dialing the sequence: *21*12345678# (Call forwarding)
The following Invite is sent:
INVITE sip:*21*12345678#@192.168.29.11:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.110.112:5060;branch=z9hG4bK154668c5;rport
Max-Forwards: 70
From: "402" <sip:402@192.168.110.112>;tag=as5ce33726
To: <sip:*21*12345678#@192.168.29.11:5060>
.....
With final '#' included
While dialing the sequence: *31*12345678# (CLIR on per call basis)
The following Invite is sent:
INVITE sip:*31*12345678@192.168.29.11:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.110.112:5060;branch=z9hG4bK154668c5;rport
Max-Forwards: 70
From: "402" <sip:402@192.168.110.112>;tag=as5ce33726
To: <sip:*31*12345678@192.168.29.11:5060>
.....
Without final '#'

```
ATOSNT\voip\call-setting\call_profile_name_n>>set ?

Nodes not available.
Set command parameters:
 description                    [description]                    Current value:
 interdigit timer (sec)         [interdigit-timer]               Current value: 2
 alert timer (sec)              [alert-timer]                    Current value: 60
 ringback timer (sec)           [ringback-timer]                 Current value: 60
```

```
use hash ('#') key as dial key     [use-hash-as-dial-key]              Current value: auto
call forward always query code     [call-forward-always-query-code]    Current value:
call forward always act code       [call-forward-always-act-code]      Current value:
call forward always deact code     [call-forward-always-deact-code]    Current value:
call forward busy query code       [call-forward-busy-query-code]      Current value:
call forward busy act code         [call-forward-busy-act-code]        Current value:
call forward busy deact code       [call-forward-busy-deact-code]      Current value:
call forward no answer query code  [call-forward-noanswer-query-code]  Current value:
call forward no answer act code    [call-forward-noanswer-act-code]    Current value:
call forward no answer deact code  [call-forward-noanswer-deact-code]  Current value:
clir permanent query code          [clir-permanent-query-code]         Current value:
clir permanent act code            [clir-permanent-act-code]           Current value:
clir permanent deact code          [clir-permanent-deact-code]         Current value:
clir on call basis code            [clir-on-call-code]                 Current value:
```

Table 11: **set**

Syntax	Description
Description <string> [max 100 char]	Description of the node content
interdigit-timer <value> [1 - 7] sec	Timer started every time a digit is dialled. When elapsed an Invite is sent with all previously dialed digits. If '#' digit is pressed an Invite is sent without waitng for timer elapsing. Default [2]
alert-timer <value> [30 - 999] sec	Timer started when a call is received and ringing sent to user terminal. When elapsed (local user not answering) the call is refused with a STATUS "480 Temporarily unavailable" message. Default [60]
ringback-timer <value> [30 - 999] sec	Timer started every time a "180 ringing" message is received for an outgoing call and ringback tone is played out towards local user. When elapsed (remote user not answering) the call is released with a CANCEL message. Default [60]
use-hash-as-dial-key [on|off|auto|calls-only]	• **on**: # digit is always used as dial string terminator • **off**: # digit is never used as dial string terminator (any # digit will thus be included in dial string) • **auto**: as in on mode. However, when dialing strings formatted as service codes (starting with * or # character), the # digit will not be considered dial string terminator. • **calls-only**: as in on mode. However, when dialing explicitly configured service codes (in the call-setting/call-profile node), the # digit will not be considered dial string terminator. Default [auto]
call-forward-always-query-code<value> [max 6 decimal digits,#,*]	Interrogation code for Unconditional Call Forwarding service. Default [empty]
call-forward-always-act-code <value> [max 6 decimal digits,#,*]	Activation code for Unconditional Call Forwarding service. The request must be completed from the user with the destination number and final '#'. Default [empty]
call-forward-always-deact-code <value> [max 6 decimal digits,#,*]	Deactivation code for Unconditional Call Forwarding service. Default [empty]
call-forward-busy-query-code <value> [max 6 decimal digits,#,*]	Interrogation code for Busy Call Forwarding service. Default [empty]
call-forward-busy-act-code <value> [max 6 decimal digits,#,*]	Activation code for Busy Call Forwarding service. The request must be completed from the user with the destination number and final '#'. Default [empty]
call-forward-busy-deact-code <value> [max 6 decimal digits,#,*]	Deactivation code for Busy Call Forwarding service. Default [empty]

call-forward-noanswer-query-code <value> [max 6 decimal digits,#,*]	Interrogation code for No Reply Call Forwarding service. Default [empty]
call-forward-noanswer-act-code <value> [max 6 decimal digits,#,*]	Activation code for No Reply Call Forwarding service. The request must be completed from the user with the destination number and final '#'. Default [empty]
call-forward-noanswer-deact-code <value> [max 6 decimal digits,#,*]	Deactivation code for No Reply Call Forwarding service. Default [empty]
clir-permanent-query-code <value> [max 6 decimal digits,#,*]	Interrogation code for Permanent Calling Line Identity Restriction service. Default [empty]
clir-permanent-act-code <value> [max 6 decimal digits,#,*]	Activation code for Permanent Calling Line Identity Restriction service. Default [empty]
clir-permanent-deact-code <value> [max 6 decimal digits,#,*]	Deactivation code for Permanent Calling Line Identity Restriction service. Default [empty]
clir-on-call-code<value> [max 6 decimal digits,#,*]	Activation code Calling Line Identity Restriction service on per call basis. The activation code must be completed from the user with the called number. Default [empty]

Sip - Commands

The available commands in **sip** node are the following:

```
ATOSNT\voip\sip>>set ?

Available nodes:
                        profile_name_n

Set command parameters:
 level of log           [loglevel]              Current value: 1
 local ip address       [local-ip-address]      Current value: 0.0.0.0
 local rtp ip address   [local-rtp-ip-address]  Current value: 0.0.0.0
 local sip port         [local-sip-port]        Current value: 5060
 local rtp port         [rtp-port]              Current value: 5100
 ip tos code (hex)      [ip-tos]                Current value: B8
```

***Table 12:*set**

Syntax	Description
loglevel <value>	Set the detail level used by ATOS to log the events of the SIP, from the less detailed one (0) to the more detailed one (5). Default: [1]
local-ip-address [ip-address]	Value of IP address to be used as source address for all voice packets (SIP, RTP, RTCP protocols) unless a different IP address is specified for RTP and RTCP protocol (local-rtp-ip-address parameter set to a value different from 0.0.0.0). If local-ip-address is set to 0.0.0.0 address of outgoing interface is used. Default: [0.0.0.0]
local-rtp-ip-address [ip-address]	Value of IP address to be used as source address for RTP packets. If set to 0.0.0.0 address of outgoing interface is used. Default: [0.0.0.0]
local-sip-port <value> [1024 – 60000]	Value of transport port to be used as source port for SIP protocol. Default: [5060]
rtp-port <value> [5000 – 60000]	Initial value to be used as port number for RTP protocol. Starting from this, consecutive values are used for RTP and RTCP (alternately) for all active calls. Default: [5100].
ip-tos <value> [0 - FF hex |maximize-reliability| maximize-throughput| mt+mr|minimize-delay| md+mr|md+mt|md+mt+mr]	Value of TOS bits to be set in all voice packets (SIP, RTP and RTCP protocols). Either a predefined mnemonic value or a raw hexadecimal value can be set. Default [B8]

Value 4 for loglevel parameter is the most suitable to obtain a SIP trace with minimum overhead of other logs.

Using this value combined with the same 4 value for loglevel of ATOS\isdn node provides a composite SIP + local ISDN log which is suitable for ISDN calls troubleshooting or monitoring.

```
ATOSNT\voip\sip>>add ?

add  help :  Add a new SIP PROFILE
add  usage:
 <PROFILE><name>

add command parameters:
 PROFILE
```

***Table 13:*add a SIP PROFILE**

Syntax	Description
PROFILE	Keyword:
name[max 16 char]	Name of a new SIP profile.

```
ATOSNT\voip\sip>>del ?

del  help :  Remove a SIP PROFILE
del  usage:
 <PROFILE><name>

del command parameters:
 PROFILE
```

***Table 14:*del a SIP PROFILE**

Syntax	Description
PROFILE	Keyword:
name[max 16 char]	Name of a new SIP profile.

A configuration example:

ATOS\voip\sip>>**show conf**

Show of ATOS voip sip

Local IP Address (0.0.0.0 if notused) : 0.0.0.0

Local SIP Port : 5060

Local RTP Port : 5100

Ip TOS code (Hex) : B8

Show of ATOSNT voip sip nome_profile

Description :

Proxy Host : 192.168.31.200

Sip Registration : on

Registrar Host : 192.168.31.200

Registration Retry Timer (sec) : 15

Registration Retry Random Interval (sec) : 0

Registration Expiry (sec) : 600

Expire Time Percentage : 70

Sip Domain :

Port : 5060

Fax Mode : t38-reinvite,g711-reinvite

Dtmf mode : rfc2833

RFC2833 Payload Type : 101

RFC4040 Clearmode enable : on

RFC4040 Payload Type : 97

RFC3325 Incoming : off

RFC3325 Preferred Outgoing Type : off

RFC3325 Asserted Outgoing Type : off

Hold type : RFC2543

CLIR type : anonymous

Enable PRACK : off

Username from field : to

Ringing CW string :

Rx server internal error : congestion-tone

Rx Ringing no SDP after 183 Prog : no-action

Sending 183 Progress Enable : off

Not escaped charset : include'#'

```
ATOSNT\voip\sip>>show status
```

With show status command, the registration of all activated SIP trunks is shown.

ATOS\voip\sip>>**show status**

Host dnsmgr Username Refresh State Reg.Time

192.168.29.11:5060 N 402 420 Registered Sat, 01 Jan 2000 22:18:07

192.168.29.11:5060 N 401 420 Registered Sat, 01 Jan 2000 22:18:07

2 SIP registrations.

profile_name_n – Commands

A SIP profile contains a set of parameters that describe the general functioning of a SIP connection (with a SIP Proxy/Registrar). These parameters are typically shared by several SIP trunk.

If a trunk defines a SIP profile, all of its general parameters will be hidden (see trunk “sip-profile” parameter) and only the subset of parameters necessary to define a SIP account (username, password…) will be taken into account.

If, as opposite, a trunk does not define a SIP profile, then its own general parameters (identical to sip profile ones) will work.

Available commands in these nodes are the following:

```
ATOSNT\voip\sip\profile_name_n>>set ?


Nodes not available.
Set command parameters:
 description                              [description]                      Current value:
 srv record                               [srv-record]                       Current value:
 proxy host                               [proxy-host]                       Current value: 30.253.253.71
 sip registration                         [sip-registration]                 Current value: on
   registrar host                         [registrar-host]                   Current value: 30.253.253.71
   registration retry timer (sec)         [registration-retry-timer]         Current value: 120
   registration retry random interval (sec)  [registration-random-interval]  Current value: 0
   registration expiry (sec)              [registration-expiry]              Current value: 3600
   expire time percentage                 [expire-time-percentage]           Current value: 98
   register uri                           [register-uri]                     Current value: Registrar-host
   automatic deregister                   [automatic-deregister]             Current value: on
 sip domain                               [sip-domain]                       Current value:
 port                                     [port]                             Current value: 5060
 fax mode                                 [fax-mode]                         Current value:       t38-reinvite, g711-reinvite
   declare t.38 on first invite           [declare-t38-on-first-invite]      Current value: off
   fax passtrough before t38 reinvite     [fax-pass-trough-before-t38]       Current value: on
dtmf mode                                 [dtmf]                             Current value: rfc2833
   rfc2833 payload type                   [rfc2833-payload-type]             Current value: 101
 rfc4040 clearmode enable                 [rfc4040-enable]                   Current value: off
   rfc4040 payload type                   [rfc4040-payload-type]             Current value: 97
 rfc3325 incoming                         [rfc3325-incoming]                 Current value: off
 rfc3325 preferred outgoing type          [rfc3325-preferred-outgoing-type]  Current value: off
 rfc3325 asserted outgoing type           [rfc3325-asserted-outgoing-type]   Current value: off
 hold type                                [hold-type]                        Current value: RFC2543
 clir type                                [clir-type]                        Current value: anonymous
 privacy content type                     [privacy-content-type]             Current value: id
 enable prack                             [enable-prack]                     Current value: off
 username from field                      [username-from-field]              Current value: start-line
 ringing cw string                        [ringing-cw-string]                Current value:
 rx server internal error                 [rx-server-internal-error]         Current value:  congestion-tone
 rx ringing no sdp after 183 prog         [rx-ringing-no-sdp-after-183prog]  Current value: no-action
 sending 183 progress enable              [send-183-progress]                Current value: off
 not escaped charset                      [not-escaped-charset]              Current value: include'#'
 overlap timer (sec)                      [overlap-timer]                    Current value: 12
```

```
voice activity detector                    [voice-activity-detector]          Current value: off

max sip request retransmission time (sec)  [max-retransmission-time]          Current value: Default(32)

provisional keep alive                     [provisional-keep-alive]           Current value: on

send 503 no isdn channel available         [send-503-no-ISDN-channel]         Current value: off

session timers support                     [session-timers-support]           Current value: accept
```

Table 15: set

Syntax	Description
description [string][max 100 char]	Description of the node content. Default [empty]
srv-record [_service._protocol.domainname]	If the parameter is configured, DNS resolution (mydomainname.com) is made through an srv_query; in practice an srv-query message is sent to a server encharged to answer the queries for a given service which in turn is specified in the parameter; in our case SIP is the service and UDP is the protocol used. Typically the response to the query contains the proxies addresses (IP format or DNS) to which the REGISTER messages are sent. There may also be several proxies addresses with different priorities; in this case the address with highest priority is used as a primary proxy and the others as secondary proxies. Obviously, in case of srv_query, proxies (primary and secondary) statically configured, will not be used; instead those received in response to the query will be used. SRV records are commonly used by SIP clients to discover the IP address and port of the SIP server.
proxy-host [ip-address|string]	Assigns the address of Proxy host. All SIP messages excepted registration are sent to this host. In case it would be not defined, the Registrar address is used for all SIP messages. • **ip-address**: In the form aa.bb.cc.dd is the actual IP address of the outbound proxy host. • **string**: is the URL associated to outbound proxy host to be resolved via DNS. A DNS server is to be defined on the device to make this configuration working.
sip-registration [on|off|on-light]	• **on**: the trunk account is registered versus registrar. • **off**: no registration is performed. This functioning mode can only work in a point to point scenario (trunk) or if the IP address of the device is statically assigned and known by SIP Proxy. • **On-light**: the trunk account is registered versus registrar, but when refreshing registration, credentials obtained in the first registration are reused (instead of sending a REGISTER message without credential then receiving 401 and finally a new REGISTER with credentials) in order to minimize network congestion. Default [on]
registrar-host <ip-address|string]>	Assigns the address of Registrar host. Messages relevant to SIP registration are sent to this host. In case it would be not defined, the Outbound Proxy address is used for registration too. • **ip-address**: In the form aa.bb.cc.dd is the actual IP address of the registrar host. • **string**: is the URL associated to registrar host to be resolved via DNS. A DNS server is to be defined on the device to make this configuration working.
registration-retry-timer [5 – 1200] sec	Sets the time interval after which the device retry the registration in the case it has failed. Notice that a registration is considered as failed after the number of message repetition (11) specified by SIP protocol. It is advisable to wait for a while before trying again, in order to avoid a useless “avalanche” effect in the network in case of registrar failure (all CPEs would continuously transmit REGISTER messages…).
registration-random-interval [0 - 1200] sec	If different from 0, a random time, from 0 to its value, is added each time to registration-retry-timer before trying again a registration after a failure.

registration-expiry [1-3600] sec	Is the time a registration to registrar remains valid. Before it expires, registration must be refreshed. Notice that this is the value proposed by device to registrar which could, in its answer, change it. Default [600]
expire-time-percentage [1−100]%	Set at which percentage of registration expiry timer the registration is refreshed. Default [70] Example: if registration-expiry is 600 sec and expire-time-percentage is 50%, registration is refreshed after 300 sec.
register-uri [Registrar-host|SIP-domain]	This parameter allows to put in the URI Request, the registrar-host address or the SIP domain. • **Registrar-host**:registrar host ip address is used in Register URI • **SIP-domain**: sip-domain is used in Register URI Default: Registrar-host
automatic-deregister [on|off]	This parameter is used to ignore the changes of the interface state when an account is registered. • **ON**:when the interface goes down, the account will be considered unregistered. This means that if the user pick up the phone to make a call, he will receive the congestion tone. • **OFF**:when the interface goes down, the account ignores the change and continues to be registered. Obviusly with the physical interface down, if the user tries to make a call, this should not be successful, the user would hear a congestion tone but not immediately, just at the end of the SIP transaction (32 seconds) . Default: on
port [0-65535]	Sets the used UDP port for SIP protocol. Default [5060]
fax-mode <g711-reinvite| g711-no-reinvite| t38-no-reinvite| t38-reinvite,g711-reinvite| t38-reinvite,g711-no-reinvite| g711-reinvite-before-t38-reinvite>	Sets the working mode when a local fax answering a call (CED tone) is detected. In any case transmission codec is immediately switched from G.729 (compressed) to G.711, echo cancellation disabled (if relevant parameter is set to auto) and Voice Activity Detection disabled (if supported). All this is done while waiting for actions below. Default [t38-reinvite,g711-reinvite] • **g711-reinvite**: a reinvite indicating G.711 only (not G.729) is sento to peer; • **g711-no-reinvite**: no additional actions are performed; • **t38-no-reinvite**:transmission switches to T38 without renegotiating: • **t38-reinvite-g711-reinvite**: a reinvite indicating T38 is sent to peer. If positive answer is received, transmission switches to T38, otherwise a further reinvite is sent indicating G.711; • **t38-reinvite-g711-no-reinvite**: a reinvite indicating T38 is sent to peer. If positive answer is received, transmission switches to T38, otherwise no other actions are performed (transmission is already G.711); • **g711-reinvite-before-t38-reinvite**: a G711 reinvite is sent before; then, regardless the result, a T38 reinvite is sent.
declares t.38 on first invite [on|off]	If fax mode supports T.38, sets declare t.38 on first invite on Default [off]
fax-passtrough-before-t38 [on|off]	If a local fax tone is recognized and the parameter is set: • **ON**: the device switches to G.711. • **OFF**: when set off, after the transmission of T38 reinvite and waiting for receiving 200 OK message, the fax interrupts any transmission. Default: on

dtmf [info|inband|rfc2833]	Sets the transport mode for DTMF tones: Default [rfc2833] • **info**: DTMF are locally detected, and notified to remote peer using “INFO” SIP message. Notice that outgoing audio is csoon as the tone is detected in order not to overlap with “logical” information; • **rfc2833**: DTMF are locally detected, and notified to remote peer using special RTP packet according to RFC 2833. Notice that outgoing audio is soon as the tone is detected in order not to overlap with “logical” information; • **inband**: no operations are performed on DTMF tones which are transported as normal audio signal.
rfc2833-payload-type [96-127]	Set the payload type value to be used in SIP/RTP for DTMF relay when using rfc2833. Default [101]
rfc4040-enable [on|off]	If set, RFC 4040 is used to negotiate (in SIP messages) a clear channel. Used for example to transport on SIP an Unrestricted Digital (UDI) call from a ISDN port. Negotiation of RFC 4040 for outgoing calls is automatically activated when a UDI call is detected.
rfc4040-payload-type [77-127]	Set the payload type value to be used in SIP/RTP for clear channel transport. Default [97]
rfc3325-incoming <off|preferred-prior|asserted-prior>	• **off**: neither “asserted identity” nor “preferred identity” header are taken into account to establish the caller identity; • **preferred-prior**: RFC3325 header are taken into account when establishing caller identity. Priority is given to “preferred identity” if both are present; • **asserted-prior**: RFC3325 header are taken into account when establishing caller identity. Priority is given to “asserted identity” if both are present.
rfc3325-preferred-outgoing-type [off|use-from|from-trunk|user-defined]	• **off**: header “preferred identity is not included in outgoing INVITE; • **use-from**: preferred identity is included in outgoing INVITE and its content is copied from “from” header. Notice that it could differ from trunk username (see trunk OPTION, “username” parameter); • **from-trunk**:preferred identity is included in outgoing INVITE and its content is built using the trunk username. • **user-defined**:preferred identity is included in outgoing INVITE and its content is defined by the user in "rfc3325-preferred-outgoing-user-defined-string" parameter in section **sip-trunk_name_n – Commands** of Trunk SIP node.
rfc3325-asserted-outgoing-type [off|use-from|from-trunk|user-defined]	• **off:**header “asserted identity is not included in outgoing INVITE; • **use-from**: asserted identity is included in outgoing INVITE and its content is copied from “from” header. Notice that it could differ from trunk username (see trunk OPTION, “username” parameter); • **from-trunk**: asserted identity is included in outgoing INVITE and its content is built using the trunk username. • **user-defined**:asserted identity is included in outgoing INVITE and its content is defined by the user in "rfc3325-asserted-outgoing-user-defined-string" in section **sip-trunk_name_n – Commands** of Trunk SIP node.
hold-type [RFC2543|RFC3264]	Set the reference RFC based on which the hold request is performed. Default [RFC2543]
clir-type [none|anonymous|keypad|privacy]	Specifies how to translate in SIP the identity restriction required by a user terminal (see “clir-outgoing” parameter in user terminal nodes) • **none**:no restriction, in any form, is contained in outgoing INVITE even if requested from user terminal; • **anonimous**:standard SIP “anonymous” syntax is used. “privacy id” header is also included; • **keypad:**the keypad string specified by “clir-on-call-code” parameter value in active call profile is prepended to called number in outgoing INVITE; • **privacy**:the “privacy” header is included in outgoing INVITE.

privacy-content-type	This parameter is only applied if clir-type is set to "privacy". List of up to 6 items chosen from: • header • user • session • critical • history • id
enable-prack [off|supported|required]	• **off**: Provisional Reliable (PRACK) is not supported; • **supported**: Provisional Reliable (PRACK) is supported but interoperability with peers not supporting PRACK is granted; • **required**: Provisional Reliable (PRACK) is supported and interoperability is granted with PRACK supporting peers only.
username-from-field [start-line|to]	Specifies where to get the called number from in incoming INVITE when there is an ambiguity between start-line (request URI) and “to” field
ringing-cw-string <Any value(0-80 char)|[http://127.0.0.1/Beep2 http://127.0.0.1/Beep2]>	Specifies the string to be recognized in incoming “Alert info” header in 180 ringing message, in order to understand that the outgoing call has been put in waiting. One of proposed string can be chosen or a user defined string can be set.
rx-server-internal-error [special-tone|congestion-tone]	Specifies the behaviour in case a 503 Server Internal Error message is received as an answer to outgoing INVITE. A special (tri-tone) or congestion tone can be selected.
rx-ringing-no-sdp-after-183prog[local-ring|no-action]	Specifies the behaviour in case a 180 ringing without SDP is received after a 183 progress with SDP (so audio channel with remote is open). • **no-action**: the channel is left open. • **local-ring**: channel with remote is closed and ringback tone is locally generated.
send-183-progress [on|off]	If enabled, a 183 Progress SIP message is sent: With SDP when from ISDN a Call Proceeding or Progress or SetupAck or Alerting message with Progress Indicator equal 1 or 8 is received
not-escaped-charset [exclude'#'|include'#']	Some not numeric characters, when included in the request URI or “to” field could be “escaped” (as their hexadecimal value). For example ‘#’ char could, or not, be translated in ‘0x23’. Character “included” in not escaped list are not translated in hexadecimal. Currently only ‘#’ char is managed. Default [include'#']
overlap-timer [0 – 15] sec	This timer is started when receiving a STATUS 404 or 484 as a response to an outgoing INVITE. If the timer expires, the call is considered as failed and congestion tone is sent to user. If the user press more digits before expiration, the timer is stopped and new digits will be queued to previous ones and a new INVITE will be transmitted according to interdigit timer rules. Default: [12]
voice-activity-detector [on|off]	Enable/Disable the Voice Activity Detection feature. If enabled, silences in the speech are detected and suppressed. Special packets are sent in order to notify remote side about silence. Also Comfort Noise is generated when receiving silence notifications from remote.
max-retransmission-time (sec) [3-30|Default(32)]	Sets the maximum retransmission time in seconds of SIP request messages to the proxy before taking any action (i.e. proxy redundancy activation) because the proxy is no longer reachable.This timer matches RFC 3261 SIP timers B and F. Default: [32]
provisional-keep-alive [on|off]	Enables or disables the provisional keep alive functionality. • **on**: the provisional responses (180 or 183 ringing progress) to an INVITE message received from the network would be repeated every 60 seconds until the call goes to active state. • **off**: the provisional response would be sent just once time. Default: [on]

send-503-no-ISDN-channel [on|off]	Only applicable if ISDN terminals are connected to the CPE. • on the disconnection cause "ISDN 34 no-channel-available", is mapped into SIP message as 503 "Service Unavailable". • off the disconnection cause "ISDN 34 no-channel-available", is mapped into SIP message as 486 "User busy" Default: [off]
session-timers-support [originate|accept|refuse]	Enables a session expiration mechanism with periodic refreshes to keep the session active, and to avoid "hanging" calls when the connection is interrupted. **session-timers** parameter supports RFC 4028. It is known that SIP does not define a keepalive mechanism for the sessions it establishes. User agents may be able to determine whether the session has timed out by using session specific mechanisms, but proxies will not be able to do so. The result is that call stateful proxies will not always be able to determine whether a session is still active. The refresher is responsible for sending polling messages to the other peer whenever the refresh timer expires. Both, the refresher and the peer that is receiving the refresh, activate a timer that lasts twice the refresh timer; the timer is reset whenever there is an exchange of keep-alive messages. If the timer expires before this exchange took place, it means that the call is no longer active, and both peers will cut down the call. The parameter can be configured with 3 possible values: • originate - In outgoing calls, SIP declares in the header field of the message (supported:timer) that supports the feature . - In incoming calls, SIP answers offering to work as a refresher and add a Session Expires header field. • accept - In outgoing calls, the behaviour is passive and SIP does not declare that supports the feature. - In incoming calls, instead SIP accepts the feature activation, whenever is proposed. • refuse The feature is not activated but the CPE responds to the refresh messages in any case Default: [accept]

A configuration example:

ATOS\voip\sip\profile_name_n>>**show work**

Show of ATOSNT voip sip profile_name_n

Description :

SRV Record :

Proxy Host : 192.168.31.200

Sip Registration : on

Registrar Host : 0.0.0.0

Registration Retry Timer (sec) : 60

Registration Retry Random Interval (sec) : 0

Registration Expiry (sec) : 60

Expire Time Percentage : 70

Register URI : Registrar-host

Automatic Deregister : on

Sip Domain :

User Param : off

Port : 5060

Fax Mode : t38-reinvite,g711-reinvite

Declare T.38 on first INVITE : off

Fax PassTrough before T38 reinvite : on

Reject media with port 0 : on

Dtmf mode : inband

RFC2833 Payload Type : 101

RFC4040 Clearmode enable : on

RFC4040 Payload Type : 97

RFC3325 Incoming : off

RFC3325 Preferred Outgoing Type : off

RFC3325 Asserted Outgoing Type : off

Hold type : RFC2543

CLIR type : anonymous

Privacy content type : id

Enable PRACK : off

Username from field : start-line

Ringing CW string :

Rx server internal error : congestion-tone

Rx Ringing no SDP after 183 Prog : no-action

Sending 183 Progress Enable : off

Not escaped charset : include'#'

Overlap timer (sec) : 12

Voice Activity Detector : off

Max SIP Request Retransmission time (sec) : 10

Provisional Keep Alive : on

Send 503 No ISDN channel available : off

Session Timers support : accept

LIST OF SECONDARY PROXY

192.168.110.50

LIST OF SWAPPING CAUSE

Empty list

Command executed

SIP Proxy Redundancy

This feature permits to switch to a secondary proxy when the primary becomes unreachable or it doesn't work properly.

For example, when the CPE does not receive any reply to the INVITE or REGISTER messages sent to the proxy, if proxy redundancy feature is enabled, the CPE will decide to switch to the secondary proxy (or to the next in the list of available proxies) by sending a REGISTER to it.

Every time the refresh timer expires, the CPE first tries to restore the normal operation by sending a REGISTER to the main proxy. If the registration isn't successfull, the CPE will continue to use the secondary proxy, otherwise it restores the primary one.

Proxy redundancy is activated any time the CPE receives a negative response to an INVITE (or to a REGISTER) containing specific disconnection causes.

Swapping-Cause parameter allows the user to configure a list of possible disconnection causes.

Eg. set voip sip swapping-proxies-causes 500..590

This setting means that every disconnection with a cause between 500 and 590 will activate redundancy proxy feature and the CPE will swap on the secondary one

To add a secondary proxies List or a Swapping Cause you should use **add** command, see below.

```
ATOSNT\voip\sip\wild>>add ?

add  help :  Add a Secondary Proxies list or add a Swapping Cause
add  usage:
 <SECONDARY-PROXY><proxy>
 <SWAPPING-CAUSE><cause>
```

Table 16: add SECONDARY-PROXY or a SWAPPING-CAUSE

Syntax	Description
SECONDARY-PROXY	Keyword
Proxy Host [aa.bb.cc.dd|max 40 char]	Sets the Secondary Proxy address or name.
SWAPPING-CAUSE	Keyword
Swapping cause [400-999|4xx|40x|41x|42x|48x|49x|5xx|50x|51x|60x]	Sets a list of possible disconnection causes

Secondary Proxy and Swapping Causes List - Configuration Example

This example shows how to configure a Secondary Proxy when the Primary is unreachable
When SIP 404 message is received, the CPE activates the proxy swapping from primary to secondary one.
Start looking at the SIP message received by the CPE:

SIP/2.0 404 Not Found

Via: SIP/2.0/UDP 127.0.0.1:5060;branch=z9hG4bK5b8a24ab;received=127.0.0.1;rport=5060

From: "999" <sip:999@127.0.0.1:5060>;tag=as28a75200

To: <sip:89596@127.0.0.1:5060>;tag=as5f2e2ec3

Call-ID: 4ca30ded78b5425c28b625c30b7c5111@127.0.0.1

CSeq: 102 INVITE

Server: Aethra Telecommunications PBX

Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, UPDATE

Content-Length: 0

ATOSNT\voip\sip\wild>>**conf**

add voip sip PROFILE wild

add voip sip wild SECONDARY-PROXY <sip:111@127.100.0.0:5060>

add voip sip wild SWAPPING-CAUSE 40x

ATOSNT\voip\sip\wild>>**show work**

Show of ATOSNT voip sip wild

Description :

Proxy Host : <sip:999@127.0.0.1:5060>

Sip Registration : on

Registrar Host : <sip:999@127.0.0.1:5060>

Registration Retry Timer (sec) : 600

Registration Retry Random Interval (sec) : 0

Registration Expiry (sec) : 600

Expire Time Percentage : 70

Register URI : Registrar-host

Automatic Deregister : on

Sip Domain :

Port : 5060

Fax Mode : t38-reinvite,g711-reinvite

Declare T.38 on first INVITE : off

Fax PassTrough before T38 reinvite : on

Dtmf mode : rfc2833

RFC2833 Payload Type : 101

RFC4040 Clearmode enable : off

RFC4040 Payload Type : 97

RFC3325 Incoming : off

RFC3325 Preferred Outgoing Type : off

RFC3325 Asserted Outgoing Type : off

Hold type : RFC2543

CLIR type : anonymous

Privacy content type : id

Enable PRACK : off

Username from field : start-line

Ringing CW string :

Rx server internal error : congestion-tone

Rx Ringing no SDP after 183 Prog : no-action

Sending 183 Progress Enable : off

Not escaped charset : include'#'

Overlap timer (sec) : 12

Voice Activity Detector : off

Max SIP Request Retransmission time (sec) : Default(32)

Provisional Keep Alive : on

Send 503 No ISDN channel available : off

LIST OF SECONDARY PROXY

<sip:111@127.100.0.0:5060>

LIST OF SWAPPING CAUSE

40x

Command executed

Fax - Commands

In this node a set of parameters related to the fax functionality can be set. Notice that fax operating mode (T38 or G.711…) is set on per trunk basis on trunk nodes.

The available commands in the node are:

```
ATOSNT\voip\fax>>set ?


Nodes not available.
Set command parameters:
 t38 port                                        [t38-port]                          Current value: 6004
 t38 max bit rate                                [t38-maxbit-rate]                   Current value: 14400
 t38 rate management                             [t38-rate-management]               Current value: transferred-TCF
 t38 error correction                            [t38-error-correction]              Current value: redundancy
 t38 high speed error recovery additional packets  [t38-high-speed-error-recovery-pkts]  Current value: 0
 t38 low speed error recovery additional packets   [t38-low-speed-error-recovery-pkts]   Current value: 0
 t38 number of packets to calculate fec          [t38-pkts-to-calculate-fec]         Current value: 0
 t38 max datagram                                [t38-maxdatagram]                   Current value: 176
```

```
t38 packet time (msec)                          [t38-packet-time]                 Current value: 40
t38 nsx patch                                   [t38-nsxpatch]                    Current value: on
t38 old asn98                                   [t38-oldasn98]                    Current value: on
t38 severe ip impairments                       [t38-severeimp]                   Current value: off
t38 fax error correction mode disable           [fax-ecm-disable]                 Current value: on
```

Table 17: set

Syntax	Description
t38-port [1024-60000|reuse-rtp-port]	• 1024-60000 Initial value to be used as port number for T38 protocol. Starting from this, consecutive values are used for all active calls. • reuse-rtp-port T.38 port is the same than the one used by RTP in the active call Default [6004].
t38-maxbit-rate <2400|4800|7200|9600|12000|14400>	Set the max speed used for the fax connection when T.38 signaling is used. Default [14400]
t38-rate-management <localTCF|transferredTCF>	Specify the Training check failure frame management: • localTCF: the frame is localy genetated by DSP • transferedTCF: the frame is reveived by the remote side Default [transferedTCF]
t38-error-correction <off|redundancy|fec>	Configures the Error Correction of the “T38FaxUdpEC” in the SDP of sip message: • off: the T38FaxUdpEC is not specified • redundancy: the T38FaxUdpEC indicates “t38UDPRedundancy” • fec: the T38FaxUdpEC indicates “t38UDPFEC” Default [redundancy]
t38-high-speed-error-recovery-kts <0 - 3>	Configures the number of error recovery messages (IFP secondary packets in case of redundancy or FEC messages in case of FEC) to be sent for high speed V.17, V.27 and V29 T.4 fax machine image data. Default [0]
t38-low-speed-error-recovery-pkts <0 - 3>	Configures the number of error recovery messages (IFP secondary packets in case of redundancy or FEC messages in case of FEC) to be sent for low speed V.21-based T.30 fax machine protocol. Default [0]
t38-pkts-to-calculate-fec [0-5]	For FEC only: configures the number of ifp-primary packets recovered by a single fec message in a packet. Default [0]
t38-maxdatagram <value> [0 - 65535]	Set the max datagram size used for the T.38 signaling. Default [176]
t38-packet-time <value> [0 - 90] msec	Set the duration in ms of each T.38 packet. Default [40]
t38-nsxpatch <on|off>	If enabled prevents propagation of non standard facilities (NSF, NSC, NSS) received from T38 to local fax (T30). Default [on]
t38oldasn98 <on|off>	Enable/disable the ASN.1 notation. Default [on]

t38-severeimp	If enabled, the device tries to work even in presence of strong impairment on the network (packet loss, jitter…). Default [off]
fax-ecm-disable <on|off>	Disable/enable Error Correction Mode versus local fax. Default [on]

In case of "t38-error-correction" equal redundancy, the "t38-high-speed-error-recovery-pkts"and "t38-low-speed-error-recovery-pkts" are the number of redundant-ifp- packets sent in every udptl packet respectively for high and low speed.

In case of "t38-error-correction" equal fec, the "t38-high-speed-error-recovery-pkts" and "t38-low-speed-error-recovery-pkts" are the number of fec messages sent (in a single udptl packet) every n udptl packets respectively for high and low speed. Where n is the number of packets possibly recovered, and its value is:

t38-high-speed-error-recovery-pkts* t38-pkts-to-calculate-fec or t38-low-speed-error-recovery-pkts* t38-pkts-to-calculate-fec.

n must not exceed the value 6!.

user-terminal – Commands

This node is intended as a container of effective user terminal nodes which are dynamically created.

No parameters are configurable on this node where only the add command (to add new user terminal) is available.

In this node you can add a POTS, ISDN or a DECT terminal.

```
ATOSNT\voip\user-terminal>>add ?

add  help :  Add an User Terminal
add  usage:
 <POTS><line-id>
 <ISDN><line-id>[number]
 <DECT><line-id>[handset id]

add command parameters:
 Type       [POTS|ISDN|DECT]
```

To delete a user terminal, you should use **del** command

```
ATOSNT\voip\user-terminal>>del ?

del  help :  Delete an User Terminal
del  usage:
 <name>

del command parameters:
 Name       [pots-line-1|pots-line-2|isdn-line-1|dect-base0.1|dect-base0.2]
```

user-terminal – Nodes

pots-line-n – Commands

In this node, “logical” parameters, mainly related to VoIP service, can be configured for each POTS user terminal. Notice that physical parameters for the physical port (where user terminal is to be connected) are configurable in “pots_n” nodes just above the root of configuration tree.

Available commands and parameters in this node are the following:

```
ATOSNT\voip\user-terminal\pots-line-1>>set ?

Set command parameters:
 enable                            [on|off]                      Current value: on
 description                       [description]                 Current value:
 call profile                      [call-profile]                Current value: italy
 echo cancellation enable          [echo-cancellation]           Current value: auto
 reminder ringing enable           [reminder-ringing-enable]     Current value: off
 delayed clearing timer (sec)      [delayed-clearing-tmr]        Current value: off
 jitter buffer (msec)              [jitter-buffer]               Current value: 50
 cid dtmf end code                 [cid-dtmf-end-code]           Current value: tone'#'
 caller id enable                  [caller-id-enable]            Current value: both
 plus to double zero in clip enable [plus-to-double-zero-in-clip] Current value: off
 modem fax detection enable        [modem-fax-detection-enable]  Current value: on
 hold enable                       [hold-enable]                 Current value: off
 call waiting enable               [call-waiting-enable]         Current value: off
 three party enable                [three-party-enable]          Current value: off
 call held local tone              [held-local-tone]             Current value: off
 clir outgoing                     [clir-outgoing]               Current value: off
```

Table 19: set

Syntax	Description
[on|off]	Enable/disable the user terminal voip functioning
Description <string> [max 100 char]	Description of the node content. Default [empty]
call-profile [call_profile_1 | call_profile_n]	Set the active call profile. Only proposed values (defined in call-setting node) can be chosen. Default [italy]
echo-cancellation [on|off|auto]	• **on**: local echo cancellation always enabled; • **off**: local echo cancellation always disabled; • **auto**: normally enabled, but automatically disabled when a fax or a modem is detected; Default [auto]
reminder-ringing-enable [on|off]	If a second call on exists, both on hold or waiting, when the user goes on hook with this feature enabled, the terminal will ring to remind the user of the second call. If the feature is disabled, the second call is automatically released. Default [off]
delayed-clearing-tmr [off|1–60] sec	• **1 – 60**: During an active call , if the user goes “on hook”, the call is not disconnected immediately, but only after the specified timer. Active for incoming calls only. • **off**: calls are always immediately disconnected when user goes on hook;
jitter-buffer <value> [20 – 200] msec	Duration in ms of the jitter buffer used in the local reproduction of the voice. Default [50]

hold-enable [on|off]	If enabled, putting an active call on hold will be possible. When one call is already active, the user can put it on hold and place a new one (intermediate call) by pressing 'R'key followed by a phone number. Also, this parameter must be enbled in order to make the call waiting working. When the second call goes active, the user has all possibilities typical of telephone supplementary service: • **R2**: switch among the 2 calls; • **R0,R1**: drop one of the 2 call; • **R3**: go on 3 party conference. Default [off]
call-waiting-enable [on|off]	If enabled and an incoming call (Invite) is received for the terminal while a previous call is in the active state, the user is notified with a proper tone and a 180 Ringing message is answered . If the user accept the new call, with R2 key sequence, the first call is put on hold and the second one is accepted. Then the user has all possibilities typical of telephone supplementary service: • **R2**: switch among the 2 calls; • **R0, R1**: drop one of the 2 call; • **R3**: go on 3 party conference. If disabled, the new incoming call is refused with a STATUS 486 busy message. Default [off]
three-party-enable [on|off]	If enabled, the user can activate the 3 party conference starting from a state with one active plus one held call. Notice that the audio mixer function is prformed inside the device and not by Central Office. Default [off]
held-local-tone [on|off]	If enabled, a local tone is generated to the user when an indication of call held is received from remote. Default [off]
clir-outgoing [off|always|per-call-basis]	Modulates the decision to request or not to the relevant trunk to insert the restriction in outgoing invite (see "clir-type" parameter in trunk nodes) based its value and request from the terminal (the configured keypad sequence is dialed before the called number). • **Off**: restriction is never requested to trunk even if requested from terminal; • **Always**: restriction is always requested to trunk even if not requested from terminal; • **per-call-basis**: restriction is requested to trunk only when requested from terminal.
cid-dtmf-end-code [tone'#'|tone'c']	In case of DTMF Caller Id functioning, this parameter specify the closing DTMF to be used.
caller-id-enable [off|on_hook|both]	• **off**: disables the CLIP on the selected POTS port; • **on-hook**: enables CLIP reception in on hook status only; • **both**: enables CLIP both in on-hook and in off-hook status. [default both]
plus-to-double-zero-in-clip-enable [on|off]	When set on, the international calling calls numbers starting with '+' will be forwarded to the user terminals changing the '+' by '00'. The type of number will remain set "unknown". Default: off.
modem-fax-detection-enable [on|off]	If set to off disables the fax/modem tone detection and the related procedure activation of G.711 fallback or reinvite FAX. Default: on

A configuration example:

ATOS\voip\user-terminal\pots-line-1>>show conf

Show of ATOS voip user-terminal pots-line-1

Enable : on

Description : POTS on FXS1

Line : pots1

Call profile : italy

Echo cancellation enable : auto

Reminder ringing enable : on

Delayed Clearing Timer (sec) : off

Jitter buffer (msec) : 60

Call Waiting enable : on

Hold enable : on

Three Party enable : on

Caller ID enable : both

Held Local Tone : off

Caller Id Type : fsk-v23

Cid Dtmf End Code : tone'#'

In this node also available are commands to show status and statistics;

```
ATOSNT\voip\user-terminal\pots-line-1>>show status
```

```
ATOSNT\voip\user-terminal\pots-line-1>>show statistics
```

An example of show status/statistics command

ATOS\voip\user-terminal\pots-line-1>>show status

Status of pots-line-1

Configuration status : enable, used into InBoundList,OutBoundList

Status : INCOMING ACTIVE

DSP Slic : OFF-HOOK

DSP Resource : ALLOCATED

DSP Media : OPEN

DSP Protocol : VOICE

DSP Encoder : CODE-G729_8

DSP Decoder : CODE-G729_8

Echo cancellation : ON

Command executed

ATOS\voip\user-terminal\isdn-line-1>>show statistics

Statistics of pots-line-1

Incoming Outgoing

Calls : 1 1

Calls Answer : 1 1

Calls Busy : 0 0

Calls No Answer: 0 0

Calls Failed : 0 0

VOICE pkts from Lines : 1763

VOICE pkts to Lines : 1764

Command executed

isdn-line-n – Commands

In these nodes, “logical” parameters, mainly related to VoIP service, can be configured for each ISDN user terminal. Notice that ISDN specific parameters for the physical port (where user terminal is to be connected) are configurable in “isdn\isdn-brin” nodes below the root of configuration tree.

Available commands in these nodes are the following:

```
ATOSNT\voip\user-terminal\isdn-line-1>>set ?

Set command parameters:
 enable                            [on|off]                      Current value: on
 description                       [description]                 Current value:
 call profile                      [call-profile]                Current value: italy
 echo cancellation enable          [echo-cancellation]           Current value: auto
 jitter buffer (msec)              [jitter-buffer]               Current value: 50
 sip 183 progress to isdn progress [sip183-to-progress]          Current value: off
 plus to double zero in clip enable [plus-to-double-zero-in-clip] Current value: off
 modem fax detection enable        [modem-fax-detection-enable]  Current value: on
 hold enable                       [hold-enable]                 Current value: off
 call waiting enable               [call-waiting-enable]         Current value: off
 call held local tone              [held-local-tone]             Current value: off
 clir outgoing                     [clir-outgoing]               Current value: off
```

***Table 20:*set**

Syntax	Description
[on|off]	Enable/disable the user terminal voip functioning
Description <string> [max 100 char]	Description of the node content. Default [empty]
call-profile [call_profile_1 | call_profile_n]	Set the active call profile. Only proposed values (defined in call-setting node) can be chosen. Default [italy]
echo-cancellation [on|offlauto]	• **on**: local echo cancellation always enabled; • **off**: local echo cancellation always disabled; • **auto**: normally enabled, but automatically disabled when a fax or a modem is detected; Default [auto]
jitter-buffer<value> [20 – 200] msec	Duration in ms of the jitter buffer used in the local reproduction of the voice. Default [50]
plus-to-double-zero-in-clip [on|off]<value> [20 – 200] msec	If the parameter is set to on and if from SIP you receive a calling number that contains the '+' as the first digit (eg +390712506566), when you send the calling number in FSK to the ISDN terminal, the '+' is replaced by 00. Default [off]
sip183-to-progress [on|off]<value> [20 – 200] msec	If the value is set to ON, at the moment of the reception of a SIP message 183 progress, it will generate a message PROGRESS towards ISDN terminal. Default [off]
plus-to-double-zero-in-clip [on|off]<value> [20 – 200] msec	If the parameter is set to on and if from SIP you receive a calling number that contains the '+' as the first digit (eg +390712506566), when you send the calling number in FSK to the ISDN terminal, the '+' is replaced by 00. Default [off]
hold-enable [on|off]	If enabled, putting an active call on hold will be possible. When one call is already active, the user can put it on hold and place a new one (intermediate call). Also, this parameter must be enbled in order to make the call waiting working. Default [off]
call-waiting-enable [on|off]	If enabled, when an incoming call (Invite) is received for the port and both B channel are in use, then a SETUP specifying “no channel” is sent. Consequent SIP signalling will be related to ISDN messages received from terminal (e.g. 180 ringing will be sent if an ALERT is received or a reinvite sendonly if a HOLD message is received). If disabled, the new incoming call is refused with a STATUS 486 busy message. Default [off]
held-local-tone [on|off]	If enabled, a local tone is generated to the user when an indication of call held is received from remote.
Caller id number [read-only]	If the isdn-line has been created specifying a number (see add ISDN line command) it is shown, otherwise the field is empty.
clir-outgoing[off|always|per-call-basis]	Modulates the decision to request or not to the relevant trunk to insert the restriction in outgoing invite (see “clir-type” parameter in trunk nodes) based its value and request from the terminal (restriction is specified in Calling number information element or the configured keypad sequence is dialed before the called number). • **Off**: restriction is never requested to trunk even if requested from terminal; • **Always**: restriction is always requested to trunk even if not requested from terminal; • **per-call-basis**: restriction is requested to trunk only when requested from terminal.

A configuration example:

ATOS\voip\user-terminal\isdn-line-1>>show conf

Show of ATOS voip user-terminal isdn-line-1

Enable : on

Description :

Line : isdn-bri1

Call profile : italy

Echo cancellation enable : auto

Jitter buffer (msec) : 60

Call Waiting enable : on

Hold enable : on

Held Local Tone : off

Caller ID number:

In this node also available are commands to show status and statistics

```
ATOSNT\voip\user-terminal\isdn-line-1>>show status
```

```
ATOSNT\voip\user-terminal\isdn-line-1>>show statistics
```

An example of show status/statistics command

ATOS\voip\user-terminal\isdn-line-1>>show status

Status of isdn-line-1

Configuration status : enable, used into InBoundList,OutBoundList

B1 Status : IDLE

B2 Status : OUTGOING ACTIVE

Channel B1

DSP Resource : FREE

Channel B2

DSP Resource : ALLOCATED

DSP Media : OPEN

DSP Protocol : VOICE

DSP Encoder : CODE-G729_8

DSP Decoder : CODE-G729_8

Echo cancellation : ONCommand executed

Command executed

ATOS\voip\user-terminal\isdn-line-1>>show statistics

Statistics of isdn-line-1

Incoming Outgoing

Calls : 1 1

Calls Answer : 1 1

Calls Busy : 0 0

Calls No Answer: 0 0

Calls Failed : 0 0

VOICE pkts from Lines : 1456

VOICE pkts to Lines : 1457

Command executed

isdn-line-n-number – Commands

Configuration is the same as per isdn-line-n nodes. See below an example

```
ATOSNT\voip\user-terminal\isdn-line-4-071210651>>set ?

Set command parameters:
 enable                              [on|off]                        Current value: on
 description                         [description]                   Current value:
 call profile                        [call-profile]                  Current value: italy
 echo cancellation enable            [echo-cancellation]             Current value: auto
 jitter buffer (msec)                [jitter-buffer]                 Current value: 50
 sip 183 progress to isdn progress   [sip183-to-progress]            Current value: off
 plus to double zero in clip enable  [plus-to-double-zero-in-clip]   Current value: off
 hold enable                         [hold-enable]                   Current value: off
 call waiting enable                 [call-waiting-enable]           Current value: off
 call held local tone                [held-local-tone]               Current value: off
 clir outgoing                       [clir-outgoing]                 Current value: off
```

isdn-pri-line-1 – Commands

In this node, “logical” parameters, mainly related to VoIP service, can be configured for a PRI ISDN user terminal. Notice that ISDN specific parameters for the physical port (where user terminal is to be connected) are configurable in “isdn\isdn-pri1” node below the root of configuration tree.

Available commands in these nodes are the following:

```
ATOSNT\voip\user-terminal\isdn-pri-line-1>>set ?

Set command parameters:
 enable                              [on|off]                        Current value: on
 description                         [description]                   Current value:
 call profile                        [call-profile]                  Current value: italy
 echo cancellation enable            [echo-cancellation]             Current value: auto
 jitter buffer (msec)                [jitter-buffer]                 Current value: 50
 sip 183 progress to isdn progress   [sip183-to-progress]            Current value: off
 plus to double zero in clip enable  [plus-to-double-zero-in-clip]   Current value: off
 modem fax detection enable          [modem-fax-detection-enable]    Current value: on
 hold enable                         [hold-enable]                   Current value: off
 call waiting enable                 [call-waiting-enable]           Current value: off
 call held local tone                [held-local-tone]               Current value: off
 clir outgoing                       [clir-outgoing]                 Current value: off
```

***Table 21:*set**

Syntax	Description
[on|off]	Enable/disable the user terminal voip functioning
Description <string> [max 100 char]	Description of the node content. Default [empty]
call-profile [call_profile_1 | call_profile_n]	Set the active call profile. Only proposed values (defined in call-setting node) can be chosen. Default [italy]
echo-cancellation [on|off|auto]	• **on**: local echo cancellation always enabled; • **off**: local echo cancellation always disabled; • **auto**: normally enabled, but automatically disabled when a fax or a modem is detected; Default [auto]
jitter-buffer<value> [20 – 200] msec	Duration in ms of the jitter buffer used in the local reproduction of the voice. Default [50]
plus-to-double-zero-in-clip [on|off]<value> [20 – 200] msec	If the parameter is set to on and if from SIP you receive a calling number that contains the '+' as the first digit (eg +390712506566), when you send the calling number in FSK to the ISDN terminal, the '+' is replaced by 00. Default [off]
sip183-to-progress [on|off]<value> [20 – 200] msec	If the value is set to ON, at the moment of the reception of a SIP message 183 progress, it will generate a message PROGRESS towards ISDN terminal. Default [off]
plus-to-double-zero-in-clip [on|off]<value> [20 – 200] msec	If the parameter is set to on and if from SIP you receive a calling number that contains the '+' as the first digit (eg +390712506566), when you send the calling number in FSK to the ISDN terminal, the '+' is replaced by 00. Default [off]
hold-enable [on|off]	If enabled, putting an active call on hold will be possible. When one call is already active, the user can put it on hold and place a new one (intermediate call). Also, this parameter must be enbled in order to make the call waiting working. Default [off]
call-waiting-enable [on|off]	If enabled, when an incoming call (Invite) is received for the port and both B channel are in use, then a SETUP specifying “no channel” is sent. Consequent SIP signalling will be related to ISDN messages received from terminal (e.g. 180 ringing will be sent if an ALERT is received or a reinvite sendonly if a HOLD message is received). If disabled, the new incoming call is refused with a STATUS 486 busy message. Default [off]
held-local-tone [on|off]	If enabled, a local tone is generated to the user when an indication of call held is received from remote.
Caller id number [read-only]	If the isdn-line has been created specifying a number (see add ISDN line command) it is shown, otherwise the field is empty.
clir-outgoing[off|always|per-call-basis]	Modulates the decision to request or not to the relevant trunk to insert the restriction in outgoing invite (see “clir-type” parameter in trunk nodes) based its value and request from the terminal (restriction is specified in Calling number information element or the configured keypad sequence is dialed before the called number). • **Off**: restriction is never requested to trunk even if requested from terminal; • **Always**: restriction is always requested to trunk even if not requested from terminal; • **per-call-basis**: restriction is requested to trunk only when requested from terminal.

A configuration example:

ATOSNT\voip\user-terminal\isdn-pri-line-1>>**show conf**

Show of ATOSNT voip user-terminal isdn-pri-line-1

Enable : on

Description :

Line : isdn-pri1

Call profile : test

Echo cancellation enable : auto

Jitter buffer (msec) : 50

Caller ID number :

SIP 183 Progress to ISDN Progress : off

Plus to double zero in CLIP enable : off

Modem Fax Detection enable : on

Hold enable : off

Call Waiting enable : off

Call held local tone : off

Clir Outgoing : per-call-basis

In this node also available are commands to show status and statistics

```
ATOSNT\voip\user-terminal\isdn-pri-line-1>>show status
```

```
ATOSNT\voip\user-terminal\isdn-pri-line-1>>show statistics
```

An example of show status/statistics command

ATOSNT\voip\user-terminal\isdn-pri-line-1>>show statistics -s

Statistics of isdn-pri-line-1

	Incoming	Outgoing
Calls:	0	0
Calls Answer :	0	0
Calls Busy :	0	0
Calls No Answer :	0	0
Calls Failed :	0	0

Command executed

ATOSNT\voip\user-terminal\isdn-pri-line-1>>show status -s

Status of isdn-pri-line-1

Configuration status : enable, no used into call-mng

No B Channels in use.

dect-base0.n – Commands

```
ATOSNT\voip\user-terminal\dect-base0.1>>set ?

Set command parameters:
 enable                              [on|off]                        Current value: on
 description                         [description]                   Current value:
 call profile                        [call-profile]                  Current value: italy
 reminder ringing enable             [reminder-ringing-enable]       Current value: off
 jitter buffer (msec)                [jitter-buffer]                 Current value: 50
 gap compatibility enable            [gap-compatibility-enable]      Current value: off
 plus to double zero in clip enable  [plus-to-double-zero-in-clip]   Current value: off
 hold enable                         [hold-enable]                   Current value: off
 call waiting enable                 [call-waiting-enable]           Current value: off
 call held local tone                [held-local-tone]               Current value: off
 clir outgoing                       [clir-outgoing]                 Current value: off
 three party enable                  [three-party-enable]            Current value: off
```

***Table 22:*set**

Syntax	Description
[on|off]	Enable/disable the user terminal voip functioning
Description <string> [max 100 char]	Description of the node content. Default [empty]
call-profile [call_profile_1 | call_profile_n]	Set the active call profile. Only proposed values (defined in call-setting node) can be chosen. Default [italy]
reminder-ringing-enable [on|off]	If a second call on exists, both on hold or waiting, when the user goes on hook with this feature enabled, the terminal will ring to remind the user of the second call. If the feature is disabled, the second call is automatically released. Default [off] Default [auto]
jitter-buffer<value> [20 – 200] msec	Duration in ms of the jitter buffer used in the local reproduction of the voice. Default [50]
gap-compatibility-enable [on|off]	When set on, ensures the compatibility with other terminals compliant with the standard GAP (Generic Access Profile), even if the terminals are registered to another base stations. Default [off]
plus-to-double-zero-in-clip[on|off]	When set on, the "+" character contained in the field "from" of the SIP message of the incoming call, means that it is an international call, and is translated into "00". The telephone will display a number starting by "00", for example 003907123456. Instead if the parameter is set off, the "+" character is skipped. Default [off]
hold-enable [on|off]	If enabled, putting an active call on hold will be possible. When one call is already active, the user can put it on hold and place a new one (intermediate call). Also, this parameter must be enbled in order to make the call waiting working. Default [off]
call-waiting-enable [on|off]	If enabled, when an incoming call (Invite) is received for the port and both B channel are in use, then a SETUP specifying “no channel” is sent. Consequent SIP signalling will be related to ISDN messages received from terminal (e.g. 180 ringing will be sent if an ALERT is received or a reinvite sendonly if a HOLD message is received). If disabled, the new incoming call is refused with a STATUS 486 busy message. Default [off]
held-local-tone [on|off]	If enabled, a local tone is generated to the user when an indication of call held is received from remote.
clir-outgoing [off|always|per-call-basis]	Modulates the decision to request or not to the relevant trunk to insert the restriction in outgoing invite (see “clir-type” parameter in trunk nodes) based its value and request from the terminal (restriction is specified in Calling number information element or the configured keypad sequence is dialed before the called number). • **Off**: restriction is never requested to trunk even if requested from terminal; • **Always**: restriction is always requested to trunk even if not requested from terminal; • **per-call-basis**: restriction is requested to trunk only when requested from terminal.

three-party-enable [offlalways|per-call-basis]	If enabled, the user can activate the 3 party conference starting from a state with one active plus one held call. Notice that the audio mixer function is prformed inside the device and not by Central Office. Default [off]

trunk – Commands

Trunk is a general concept for voice transport which indicates a “point to point” connection. This does not mean that using a trunk you can reach a single destination only. For example a SIP trunk can be a connection with a SIP proxy which will be able to connect with the rest of the world. This is the case of SIP trunks used in ATOS Voip.

This node is intended as a container of effective trunk nodes which are dynamically created. Depending on the CPE model, it is possible to create SIP, ISDN or PSTN trunks.

Therefore no parameters are configurable on this node where only the add command (to add new trunks) is available.

```
ATOSNT\voip\trunk>>add ?

add  help :  Add a Trunk
add  usage:
 <SIP><name>
 <PSTN|ISDN><line-id>

add command parameters:
 Type     [SIP|PSTN|ISDN]
```

Table 23:add a SIP trunk

Syntax	Description
SIP	Keyword: type of trunk
name [max 11 char]	Partial name a new SIP trunk. The effective name of the created trunk will be automatically composed by the command provided name with the suffix “sip-“.

Table 24:add an ISDN trunk

Syntax	Description
ISDN	Keyword: type of trunk
isdn-line-n	Partial name a new ISDN trunk. The effective name of the created trunk will be automatically composed by the command provided line name with the suffix “te-“.

Table 25: add a PSTN trunk

Syntax	Description
PSTN	Keyword: type of trunk
pstn-line-n	Name of a new PSTN trunk. The effective name of the created trunk will be automatically composed by the command provided line name with the suffix “pstn-“.

```
ATOSNT\voip\trunk>>del ?


Available nodes:
                     sip-0289279022
                     sip-9200
                     sip-9201
```

```
                    te-isdn-bri1
                    te-isdn-bri2
                    pstn-fxo1
del  help :  Delete a Trunk
del  usage:
 <name>

del command parameters:
 Name     [sip-0289279022|sip-9200|sip-9201|te-isdn-bri1|te-isdn-bri2|pstn-fxo1]
```

sip-trunk_name_n – Commands

In this node, you can configure all parameters of a a SIP trunk.
If a trunk defines a SIP profile, all of its general parameters will be hidden (see “sip-profile” parameter) and only the subset of parameters necessary to define a SIP account (username, password…) will be taken into account.

If, as opposite, a trunk does not define a SIP profile, then its own general parameters (identical to sip profile ones) will work.

Available commands in this node are the following:

```
ATOSNT\voip\trunk\sip-0289279022>>set ?


Set command parameters:
 enable
[on|off]                                          Current value: on
 description
[description]                                     Current value:
 authentication password
[authentication-password]                         Current value: 1012
 authentication user id
[authentication-user-id]                          Current value: 1012
 user name
[user-name]                                       Current value: 1012
 display name
[display-name]                                    Current value: 1012
 codec type priority
[codec-type]                                      Current value: G.729a
 G.711Alaw G.711Ulaw
 codec rate (g.729a,g.711alaw,g.711ulaw,g.722,g.726) (msec)  Note (*)
          [codec-rate]                                      Current
value: 20 20 20 20 20
 rfc3325 preferred outgoing user defined string(sip uri username)
[rfc3325-preferred-outgoing-user-defined-string]  Current value:
my_username@my_domain.com
 rfc3325 asserted outgoing user defined string(sip uri username)
[rfc3325-asserted-outgoing-user-defined-string]   Current value:
 sip profile
[sip-profile]                                     Current value:
```

```
 srv record
[srv-record]                                    Current value:
 proxy host
[proxy-host]                                    Current value:
0.0.0.0
 sip registration
[sip-registration]                              Current value: on
   registrar host
[registrar-host]                                Current value:
0.0.0.0
   registration retry timer (sec)
[registration-retry-timer]                      Current value: 600
   registration retry random interval (sec)
[registration-random-interval]                  Current value: 0
   registration expiry (sec)
[registration-expiry]                           Current value: 600
   expire time percentage
[expire-time-percentage]                        Current value: 70
   register uri
[register-uri]                                  Current value:
Registrar-host
   automatic deregister
[automatic-deregister]                          Current value: on
 sip domain
[sip-domain]                                    Current value:
 port
[port]                                          Current value: 5060
 fax mode
[fax-mode]                                      Current value:
t38-reinvite,g711-reinvite
   declare t.38 on first invite
[declare-t38-on-first-invite]                   Current value: off
   fax passtrough before t38 reinvite
[fax-pass-trough-before-t38]                    Current value: on
 dtmf mode
[dtmf]                                          Current value:
rfc2833
   rfc2833 payload type
[rfc2833-payload-type]                          Current value: 101
 rfc4040 clearmode enable
[rfc4040-enable]                                Current value: off
   rfc4040 payload type
[rfc4040-payload-type]                          Current value: 97
 rfc3325 incoming
[rfc3325-incoming]                              Current value: off
 rfc3325 preferred outgoing type
[rfc3325-preferred-outgoing-type]               Current value: off
```

```
 rfc3325 asserted outgoing type
[rfc3325-asserted-outgoing-type]                  Current value: off
 hold type
[hold-type]                                       Current value:
RFC2543
 clir type
[clir-type]                                       Current value:
anonymous
 privacy content type
[privacy-content-type]                            Current value: id
 enable prack
[enable-prack]                                    Current value: off
 username from field
[username-from-field]                             Current value:
start-line
 ringing cw string
[ringing-cw-string]                               Current value:
 rx server internal error
[rx-server-internal-error]                        Current value:
congestion-tone
 rx ringing no sdp after 183 prog
[rx-ringing-no-sdp-after-183prog]                 Current value:
no-action
 sending 183 progress enable
[send-183-progress]                               Current value: off
 not escaped charset
[not-escaped-charset]                             Current value:
include'#'
 overlap timer (sec)
[overlap-timer]                                   Current value: 12
 voice activity detector
[voice-activity-detector]                         Current value: off
 max sip request retransmission time (sec)
[max-retransmission-time]                         Current value:
Default(32)
 provisional keep alive
[provisional-keep-alive]                          Current value: on
 send 503 no isdn channel available
[send-503-no-ISDN-channel]                        Current value: off
 session timers support
[session-timers-support]                          Current value: accept
```

Note (*) only available on CPE models with DECT iterfaces

Table 26: set

Syntax	Description
[on|off]	Enable/disable the trunk functioning
Description [string] [max 100 char]	Description of the node content. Default [empty]
authentication-password [string] [max 80 char]	Assign the password of the trunk SIP account. Used both for registration and Invite authentication.
authentication-user-id [string] [max 40 char]	Assign the authentication user id of the trunk SIP account. Used both for registration and Invite authentication.
user-name [string] [max 32 char]	Assign the username of the trunk SIP account Typically, but not necessarily, this is a phone number for compatibility with the traditional telephone network.
display-name [string] [max 32 char]	Assign an additional string to better show the identity associated to username (e.g. a personal name) inside SIP messages. It is optional.
codec-type [list of up to 3 codec] [G.729A, G.711Alaw, G.711Ulaw, G.722, G.726]	Priority list of audio codec. One to three of them can be listed separated by space. All listed codec will be inserted in the same order in outgoing Invite, and used for match with codec contained in incoming requests. Note: G.722 and G.726 are only available on CPE models with DECT interfaces. Default [G.729a G.711Alaw G.711Ulaw]
codec-rate [list of 3 codec rate] [10|20|30]	Codec rate assigned to each of the three supported codec G.729a G.711Alaw G.711Ulaw (**in this order**). Even if less than 3 codec are assigned to codec-type parameter, all 3 values must be assigned in codec-rate command. Default [20 20 20]
rfc3325-preferred-outgoing-user-defined-string (sip uri username) [max 32 char]	Preferred identity is included in outgoing INVITE and its content is defined by the user in an string such as <sip:my_username@my_domain.com> where: sip: identifies a URI SIP <username> : defines the SIP user <domain>: is the DNS domain (eg:my_domain.com) or an IP address (eg:192.168.0.1)
rfc3325-asserted-outgoing-user-defined-string (sip uri username) [max 32 char]	Header asserted identity is included in outgoing INVITE and its content is defined by the user in an string such as <sip:my_username@my_domain.com> where: sip: identifies a URI SIP <username> : defines the SIP user <domain>: is the DNS domain (eg:my_domain.com) or an IP address (eg:192.168.0.1)
sip-profile[list of defined sip profiles]	If a not empty value is defined all parameters listed here below will be ignored and corresponding parameter values set in the sip profile will be used instead. Local parameters will not be even visible with show conf/work command of this trunk.

srv-record [_service._protocol.domainname]	If the parameter is configured, DNS resolution (mydomainname.com) is made through an srv_query; in practice an srv-query message is sent to a server encharged to answer the queries for a given service which in turn is specified in the parameter; in our case SIP is the service and UDP is the protocol used. Typically the response to the query contains the proxies addresses (IP format or DNS) to which the REGISTER messages are sent. There may also be several proxies addresses with different priorities; in this case the address with highest priority is used as a primary proxy and the others as secondary proxies. Obviously, in case of srv_query, proxies (primary and secondary) statically configured, will not be used; instead those received in response to the query will be used. SRV records are commonly used by SIP clients to discover the IP address and port of the SIP server.
proxy-host [ip-address|string]]	Assign the address of Proxy host. All SIP messages excepted registration are sent to this host. In case it would be not defined, the Registrar address is used for all SIP messages. • **ip-address**: In the form aa.bb.cc.dd is the actual IP address of the outbound proxy host. • **string**: is the URL associated to outbound proxy host to be resolved via DNS. A DNS server is to be defined on the device to make this configuration working.
sip-registration [on|off|on-light]	• **on**: the trunk account is registered versus registrar. • ***""off:****no registration is performed. This functioning mode can only work in a point to point scenario (trunk) or if the IP address of the device is statically assigned and known by SIP Proxy.* • **On-light**: the trunk account is registered versus registrar, but when refreshing registration, credentials obtained in the first registration are reused (instead of sending a REGISTER message without credential then receiving 401 and finally a new REGISTER with credentials) in order to minimize network congestion. Default [on]
registrar-host [ip-address|string]]	Assign the address of Registrar host. Messages relevant to SIP registration are sent to this host. In case it would be not defined, the Outbound Proxy address is used for registration too. • **ip-address**: In the form aa.bb.cc.dd is the actual IP address of the registrar host. • **string**: is the URL associated to registrar host to be resolved via DNS. A DNS server is to be defined on the device to make this configuration working.
registration-retry-timer [5 – 1200] sec	Set the time interval after which the device retry the registration in the case it has failed. Notice that a registration is considered as failed after the number of message repetition (11) specified by SIP protocol. It is advisable to wait for a while before trying again, in order to avoid a useless “avalanche” effect in the network in case of registrar failure (all CPEs would continuously transmit REGISTER messages…).
registration-random-interval [0 - 1200] sec	If different from 0, a random time, from 0 to its value, is added each time to registration-retry-timer before trying again a registration after a failure.
registration-expiry [1-3600] sec	Is the time a registration to registrar remains valid. Before it expires, registration must be refreshed. Notice that this is the value proposed by device to registrar which could, in its answer, change it. Default [600]
expire-time-percentage [1–100] %	Set at which percentage of registration expiry timer the registration is refreshed. Default [70] Example: if registration-expiry is 600 sec and expire-time-percentage is 50%, registration is refreshed after 300 sec.

register-uri [Registrar-host|SIP-domain]	This parameter allows to put in the URI Request, the registrar-host address or the SIP domain. • **Registrar-host**:registrar host ip address is used in Register URI • **SIP-domain**: sip-domain is used in Register URI
automatic-deregister [on|off]	This parameter is used to ignore the changes of the interface state when an account is registered. • **ON**:when the interface goes down, the account will be considered unregistered. This means that if the user pick up the phone to make a call, he will receive the congestion tone. • **OFF**:when the interface goes down, the account ignores the change and continues to be registered. Obviusly with the physical interface down, if the user tries to make a call, this should not be successful, the user would hear a congestion tone but not immediately, just at the end of the SIP transaction (32 seconds) . Default: on
sip-domain[string] [max 128 char]	If a string is set for sip domain, it is substituted to Proxy/Registrar IP address in URI contained in: Request Line, To and From header, in INVITE and REGISTER messages.
port [0-65535]	Set the used UDP port for SIP protocol. Default [5060]
fax-mode [g711-reinvite| g711-no-reinvite| t38-no-reinvite| t38-reinvite,g711-reinvite| t38-reinvite,g711-no-reinvite]	Set the working mode when a local fax answering a call (CED tone) is detected. In any case transmission codec is immediately switched from G.729 (compressed) to G.711, echo cancellation disabled (if relevant parameter is set to auto) and Voice Activity Detection disabled (if supported). All this is done while waiting for actions below. Default[t38-reinvite,g711-reinvite] • **g711-reinvite** : a reinvite indicating G.711 only (not G.729) is sent to peer; • **g711-no-reinvite**: no additional actions are performed; • **t38-no-reinvite**:transmission switches to T38 without renegotiating; • **t38-reinvite-g711-reinvite** : a reinvite indicating T38 is sent to peer. If a positive answer is received, transmission switches to T38, otherwise a further reinvite is sent indicating G.711; • **t38-reinvite-g711-no-reinvite** : a reinvite indicating T38 is sento to peer. If positive answer is received, transmission switches to T38, otherwise no other actions are performed (transmission is already G.711).
declare t.38 on first invite [on|off]	If fax mode supports T.38, set declare t.38 on first invite on Default [off]
fax-passtrough-before-t38 [on|off]	If a local fax tone is recognized and the parameter is set: • **ON**: the device switches to G.711. • **OFF**: the device closes the transmission channel and waits for a negotiation (T.38 or G.711) to reopen the channel. In this situation there is no packets tramsmission between the recognition of G.711 fax tone and the end of the SIP negotiation. Default: on
dtmf [info|inband|rfc2833]	Set the transport mode for DTMF tones: Default [rfc2833] • **info**: DTMF are locally detected, and notified to remote peer using “INFO” SIP message. Notice that outgoing audio is as soon as the tone is detected in order not to overlap with “logical” information; • **rfc2833** : DTMF are locally detected, and notified to remote peer using special RTP packet according to RFC 2833 [1]. Notice that outgoing audio is as soon as the tone is detected in order not to overlap with “logical” information; • **inband** : no operations are performed on DTMF tones which are transported as normal audio signal.
rfc2833-payload-type [96-127]	Set the payload type value to be used in SIP/RTP for DTMF relay when using rfc2833. Default [101]

rfc4040-enable [on|off]	If set, RFC 4040 [2] is used to negotiate (in SIP messages) a clear channel. Used for example to transport on SIP an Unrestricted Digital (UDI) call from a ISDN port. Negotiation of RFC 4040 [2] for outgoing calls is automatically activated when a UDI call is detected.
rfc4040-payload-type [77-127]	Set the payload type value to be used in SIP/RTP for clear channel transport. Default [97]
rfc3325-incoming [off|preferred-prior|asserted-prior]	• **off:**neither “asserted identity” nor “preferred identity” header are taken into account to establish the caller identity; • **preferred-prior:** RFC3325 header are taken into account when establishing caller identity. Priority is given to “preferred identity” if both are present; • **asserted-prior :** RFC3325 header are taken into account when establishing caller identity. Priority is given to “asserted identity” if both are present.
rfc3325-preferred-outgoing-type [off|use-from|from-trunk|user-defined]	• **off:**header “preferred identity is not included in outgoing INVITE; • **use-from:**header “preferred identity is included in outgoing INVITE and its content is copied from “from” header. Notice that it could differ from trunk username (see trunk OPTION, “username” parameter); • **from-trunk :** preferred identity is included in outgoing INVITE and its content is built using the trunk username. • **user-defined:** preferred identity is included in outgoing INVITE and its content is defined by the user in an string set on "rfc3325-preferred-outgoing-user-defined-string" parameter.
rfc3325-asserted-outgoing-type [off|use-from|from-trunk|user-defined]	• **off :** asserted identity is not included in outgoing INVITE; • **use-from :** asserted identity is included in outgoing INVITE and its content is copied from “from” header. Notice that it could differ from trunk username (see trunk OPTION, “username” parameter); • **from-trunk :** header “asserted identity is included in outgoing INVITE and its content is built using the trunk username. • **user-defined**: header asserted identity is included in outgoing INVITE and its content is defined by the user in an string set on "rfc3325-asserted-outgoing-user-defined-string" parameter.
hold-type [RFC2543|RFC3264]	Set the reference RFC based on which the hold request is performed. Default [RFC2543]
clir-type [none|anonymous|keypad| privacy]	Specifies how to translate in SIP the identity restriction required by a user terminal (see “clir-outgoing” parameter in user terminal nodes) • **none**: no restriction, in any form, is contained in outgoing INVITE even if requested from user terminal; • **anonymous**: standard SIP “anonymous” syntax is used. “privacy id” header is also included; • **keypad**: the keypad string specified by “clir-on-call-code” parameter value in active call profile is prepended to called number in outgoing INVITE; • **privacy:** the “privacy” header is included in outgoing INVITE.
enable-prack [off|supported|required|]	• **off**: Provisional Reliable (PRACK) is not supported; • **supported**: Provisional Reliable (PRACK) is supported but interoperability with peers not supporting PRACK is granted; • **required**: Provisional Reliable (PRACK) is supported and interoperability is granted with PRACK supporting peers only.

privacy-content-type	This parameter is only applied if clir-type is set to "privacy". List of up to 6 items chosen from: • header • user • session • critical • history • id
username-from-field [start-line|to]	Specifies where to get the called number from in incoming INVITE when there is an ambiguity between start-line (request URI) and “to” field
ringing-cw-string [Any value(0-80 char) | [http://127.0.0.1/Beep2 http://127.0.0.1/Beep2]]	Specifiesthe string to be recognized in incoming “Alert info” header in 180 ringing message, in order to understand that the outgoing call has been put in waiting. One of proposed string can be chosen or a user defined string can be set.
rx-server-internal-error [special-tone|congestion-tone]	Specifiesthe behaviour in case a 503 Server Internal Error message is received as an answer to outgoing INVITE. A special (tri-tone) or congestion tone can be selected.
rx-ringing-no-sdp-after-183prog[local-ring|no-action]	Specifiesthe behaviour in case a 180 ringing without SDP is received after a 183 progress with SDP (so audio channel with remote is open). • **no-action**: the channel is left open. • **local-ring**: channel with remote is closed and ringback tone is locally generated.
send-183-progress[on|off]	If enabled, a 183 Progress SIP message is sent: • **With SDP** when from ISDN a Call Proceeding or Progress or SetupAck or Alerting message with Progress Indicator equal 1 or 8 is received;[/font] • **Without SDP** when from ISDN a Call Proceeding or Progress message without Progress Indicator or with Progress Indicator different from 1 and 8 is received;
not-escaped-charset [exclude'#'|include'#']	Somenot numeric characters, when included in the request URI or “to” field could be “escaped” (as their hexadecimal value). For example ‘#’ char could, or not, be translated in ‘0x23’. Character “included” in not escaped list are not translated in hexadecimal. Currently only ‘#’ char is managed. Default [include'#']
overlap-timer[0 – 15] sec	This timer is started when receiving a STATUS 404 or 484 as a response to an outgoing INVITE. If the timer expires, the call is considered as failed and congestion tone is sent to user. If the user press more digits before expiration, the timer is stopped and new digits will be queued to previous ones and a new INVITE will be transmitted according to interdigit timer rules. Default: [12]
voice-activity-detector[on|off]	Enable/Disable the Voice Activity Detection feature. If enabled, silences in the speech are detected and suppressed. Special packets are sent in order to notify remote side about silence. Also Comfort Noise is generated when receiving silence notifications from remote.
max-retransmission-time (sec) [3-30|Default(32)]	Sets the maximum retransmission time in seconds of SIP request messages to the proxy before taking any action (i.e. proxy redundancy activation) because the proxy is no longer reachable.This timer matches RFC 3261 SIP timers B and F. Default: [32]

provisional-keep-alive [on|off]	Enables or disables the provisional keep alive functionality. • **on**: the provisional responses (180 or 183 ringing progress) to an INVITE message received from the network would be repeated every 60 seconds until the call goes to active state. • **off**: the provisional response would be sent just once time. Default: [on]
send-503-no-ISDN-channel [on|off]	Only applicable if ISDN terminals are connected to the CPE. • on the disconnection cause "ISDN 34 no-channel-available", is mapped into SIP message as 503 "Service Unavailable". • off the disconnection cause "ISDN 34 no-channel-available", is mapped into SIP message as 486 "User busy" Default: [off]
session-timers-support [originate|accept|refuse]	Enables a session expiration mechanism with periodic refreshes to keep the session active, and to avoid "hanging" calls when the connection is interrupted. **session-timers** parameter supports RFC 4028. It is known that SIP does not define a keepalive mechanism for the sessions it establishes. User agents may be able to determine whether the session has timed out by using session specific mechanisms, but proxies will not be able to do so. The result is that call stateful proxies will not always be able to determine whether a session is still active. The refresher is responsible for sending polling messages to the other peer whenever the refresh timer expires. Both, the refresher and the peer that is receiving the refresh, activate a timer that lasts twice the refresh timer; the timer is reset whenever there is an exchange of keep-alive messages. If the timer expires before this exchange took place, it means that the call is no longer active, and both peers will cut down the call. The parameter can be configured with 3 possible values: • originate In outgoing calls, SIP declares in the header field of the message (supported:timer) that supports the feature . In incoming calls, SIP answers offering to work as a refresher and add a Session Expires header field. • accept In outgoing calls, the behaviour is passive and SIP does not declare that supports the feature. In incoming calls, instead SIP accepts the feature activation, whenever is proposed. • refuse The feature is not activated but the CPE responds to the refresh messages in any case Default: [accept]

```
ATOSNT\voip\trunk\sip-0289279022>>add ?


                                                                    add
  help:  Add a SIP Trunk Option or Range list

add  usage:
```

```
<OPTION><Option-name><Display-name><Username>[default
 Display-name][default Username]
 <RANGE><Start-number><End-number>[Start-alias]


add command parameters:

   OPTION

 RANGE
```

***Table 27:*add RANGE command**

Syntax	Description
RANGE	Keyword: add a new range to the trunk. Is used to manage the GNR (or DDI) scenario: While registering only a single username (often a radix number ending with a '*' is used) towards the registrar, on provisioning basis, the account can manage one or more groups of contiguous numbers (ranges) for incoming or outgoing calls. See parameters of this command and description of Username field of OPTION for further details.
Start-number [1-20 decimal digits preceded by +]	First number of the group. An initial + can optionally be prepended.
End-number [1-4 decimal digits]	Defines the final number of the group. Only final digits with differ from the first one must be included. For example, to add the range [0719999001 – 0719999555], 0719999001 must be specified as start number, while just 555 must be specified as end number.
Start-alias [1-20 decimal digits preceded by +]	First number of the alias group. An initial + can optionally be prepended. End number is not specified because automatically calculated: the alias group must be composed of the same amount of number as the basic one. This optional field is used when numbers on user side (user terminals) must be different from numbers used on trunk side (e.g. because of difficulties in reconfiguring a PBX). See description of Username field of OPTION command for further details.

***Table 28:* add OPTION command**

Syntax	Description
OPTION	Keyword: add a new set of options
name <string> [max 16 char]	Name of the new set of options
Display-name [Any value|from-trunk]	• **Any value**: If a value different from "from trunk" is set, and this option is specified in an outbound rule using current trunk, ougoing INVITEs will contain this value as display field in "from" header. • **From-trunk:**the display name defined for the trunk is used (same behaviour when default option is specified in outbound rule)
Username [Any value|from-trunk|range| range-auth]	• **Any value**: If a value different from "from trunk" is set, and this option is specified in an outbound rule using current trunk, ougoing INVITEs will contain this value as "calling" username in "from" header. • **From-trunk:**the display name defined for the trunk is used (same behaviour when default option is specified in outbound rule) • **Range**: This value makes sense only if at least one range is added for the trunk.It affects bothoutgoing and incoming calls. For **outgoing calls** originated from a ISDN port, the calling number contained in the received SETUP is checked against defined ranges: if it matches it is used as "calling" number in outgoing INVITE ("from" header); if it doesn't, the username of the trunk is used instead, unless it is terminated by a '*'. In this case the first number of the first range is used.

	For **calls incoming** from trunk, when the “called” number (start line or “to” header) does not match with trunk username, it is also checked against defined ranges: if it matches the calls is accepted for the trunk and forwarded to user terminal using (if ISDN) the checked number as called number in SETUP message; otherwise it is refused (unless it is acceptable for other trunks). • **Range-auth**: the same as for Range value with the only difference that, for outgoing calls, the checked number is also used in “authorisation” header as username value instead of the value of “authentication-user-id” parameter of the trunk.
default Display-name [max 32 char]	To be used as default display (instead of trunk display) when an unrecognized Calling number is received from ISDN port and range value has been set.
default Username [max 32 char]	To be used as default identity (instead of trunk username) when an unrecognized Calling number is received from ISDN port and range value has been set.

```
ATOSNT\voip\trunk\sip-0289279022>>del ?

del  help :  Delete a SIP Trunk Option or Range list
del  usage:
 <OPTION><Option-name>
 <RANGE><Range-name>

del command parameters:
 OPTION
 RANGE
```

For parameters explanation refer to add tables.

A configuration example:

ATOS\voip\trunk\sip-potsline1>>**show conf**
Show of ATOS voip trunk sip-potsline1
Enable : on
Description :
Authentication password : 9401
Authentication user ID : 9401
User name : 9401
Display name : 9401
Codec type priority : G.729a G.711Alaw
Codec rate (G.729a,G.711Alaw,G.711Ulaw) (msec) : 20 20 20
Sip profile :
SRV Record:
Proxy Host :
Sip Registration : on-light
Registrar Host : 192.168.31.222
Registration Retry Timer (sec) : 15
Registration Retry Random Interval (sec) : 0
Registration Expiry (sec) : 60
Expire Time Percentage : 70
Sip Domain :
Port : 5060
Fax Mode : t38-reinvite,g711-reinvite
Dtmf mode : rfc2833
RFC2833 Payload Type : 101
RFC4040 Clearmode enable : off
RFC4040 Payload Type : 97
RFC3325 Incoming : off
RFC3325 Preferred Outgoing Type : off
RFC3325 Asserted Outgoing Type : off
Hold type : RFC2543
CLIR type : anonymous
Enable PRACK : off
Username from field : start-line
Ringing CW string :
Rx server internal error : congestion-tone
Rx Ringing no SDP after 183 Prog : no-action
Sending 183 Progress Enable : off
Not escaped charset : include'#'
LIST OF SIP-TRUNK OPTIONS
OPTION-NAME DISPLAY-NAME USERNAME
default from-trunk from-trunk
my-option from-trunk range
LIST OF SIP-TRUNK RANGES-ALIAS
RANGE ALIAS
0719999001-999 719999001-999

In this node also available are commands to show status and statistics.

```
ATOSNT\voip\trunk\sip-0289279022>>show status

ATOSNT\voip\trunk\sip-0289279022>>show statistics
```

An example of show status/statistics command

ATOS\voip\trunk\sip-potsline1>>show status

Status of sip-potsline1

Configuration status : enable

Registrar Host : 192.168.31.200

Proxy Host : 192.168.31.200

Interface status : eth0 up

Registration status : Registered (Refresh Time = 307 sec)

Logical status : used into InBoundList,OutBoundList

Message waiting : No

Connections:

Direction Remote-User Codec

Outgoing to 9401 g729

Command executed

ATOS\voip\trunk\sip-potsline1>>show statistics

Statistics of sip-potsline1

Incoming Outgoing

Calls : 0 1

Calls Answer : 0 1

Calls Busy : 0 0

Calls No Answer : 0 0

Calls Failed : 0 0

Direction Remote-User DurationRECV: Pack Lost (%) Jitter SEND: Pack Lost (%) Jitter

Outgoing to 9401 01:51:53 0000335884 0000000000 (00%) 000000 0000335894 0000000000 (00%) 000000

Command executed

isdn-trunk_name_n – Commands

In this node, you can configure the ISDN trunk parameters.

Available commands in this node are the following:

```
ATOSNT\voip\trunk\te-isdn-bri1>>set ?

Set command parameters:
 enable                            [on|off]                  Current value: off
 description                       [description]             Current value:
 overlap sending   timer (sec)     [overlap-send-timer]      Current value: 12
 overlap receiving timer (sec)     [overlap-recv-timer]      Current value: 0
 clir type                         [clir-type]               Current value: none
 clir on call basis code           [clir-on-call-code]       Current value: *31*
 send 34 no isdn channel available [send-34-no-ISDN-channel] Current value: off
```

Table 29: **set**

Syntax	Description
onloff	Enables/disables the trunk functioning
Description <string> [max 100 char]	Description of the node content. Default [empty]
overlap-send-timer (sec) [0-15]	Assigns the value of the overlap sending timer. This timer is started at receiving a DISCONNECT with cause UNALLOCATED NUMBER or INVALID NUMBER FORMAT as response to outgoing SETUP, instead of considering aborted the call and sending congestion tone. If the user selects many digits before the timer expires, a new SETUP (after Interdigit timer expiration), containing all the selected digits (also digits selected before DISCONNECT), will be sent. At the timer expiration, if no additional digits have been selected, the call will be released. Default: [12]
overlap-recv-timer (sec) [0-15]	Assigns the value of the overlap receiving timer. When the timer expires, an outgoing SETUP is sent to the network - If the value is set to 0, the SETUP received from network is sent immediately to the terminal. - If the value is X (not 0): • if SETUP contains Sending Complete Info Element, it is sent immediately to the terminal • if SETUP does not contain Sending Complete Info Element, the CPE waits X seconds in order to collect more digits (INFO messages) before forwarding SETUP to the terminal. Timer is restarted after each digit received. Default: [0]
clir-type [noneletsilkeypad]	Specifies how to translate in ISDN the identity restriction required by a user terminal (see “clir-outgoing” parameter in user terminal nodes) • **none:**no restriction, in any form, is contained in outgoing SETUP even if requested from user terminal; • **etsi:**in outgoing SETUP the CLIR request is formatted according to standard ETSI. • **keypad:**in outgoing SETUP the keypad string specified by “clir-on-call-code” parameter value is sent as keypad information element. Default: [none]
clir-on-call-code [max 6 decimal digits,#,*]	the code string used to request CLIR on call basis. Default: *31*
off]	• **on**: when receiving a SETUP from network and both B channels are being used, the “Cause Code” provided to indicate the reason why the call is rejected is "34" that means "No channel available to progress the call" • **off**: when receiving a SETUP from network and both B channels are being used, the “Cause Code” provided to indicate the reason why the call is rejected is "17" that means "User Busy" Default: [off]

```
ATOSNT\voip\trunk\te-isdn-bri1>>add ?

add  help :  Add an ISDN Trunk Option or Range list
add  usage:
 <OPTION><Option-name><Calling>
 <RANGE><Start-number><End-number>[Start-alias]

add command parameters:
 OPTION
 RANGE
```

Table 30: **add RANGE command**

Syntax	Description
RANGE	Keyword: add a new range to the trunk.
Start-number [1-20 decimal digits preceded by +]	First number of the group. An initial + can optionally be prepended.
End-number [1-4 decimal digits]	Defines the final number of the group. Only final digits with differ from the first one must be included. For example, to add the range [0719999001 – 0719999555], 0719999001 must be specified as start number, while just 555 must be specified as end number.
Start-alias [1-20 decimal digits preceded by +]	First number of the alias group. An initial + can optionally be prepended. End number is not specified because automatically calculated: the alias group must be composed of the same amount of number as the basic one. This optional field is used when numbers on user side (user terminals) must be different from numbers used on trunk side (e.g. because of difficulties in reconfiguring a PBX).

Table 31: **add OPTION command**

Syntax	Description
OPTION	Keyword: add a new option
name <string> [max 16 char]	Name of new option
Username [Any value|from-trunk|range]	**Any value**: If a value different from “from trunk” is set, and this option is specified in an outbound rule using current trunk, outgoing SETUP messages will contain this value as “calling number” . **From-trunk:**the calling number defined for the trunk (node isdn\isdn-bri-n) is used (same behaviour when default option is specified in outbound rule) **Range**: This value makes sense only if at least one range is added for the trunk.It affects bothoutgoing and incoming calls. For **outgoing calls**originated from a ISDN port, the calling number contained in the received SETUP is checked against defined ranges: if it matches it is used as “calling number" in outgoing SETUP; if it doesn’t, the calling number of the trunk (see above) is used instead, if defined. For **incoming calls** from trunk, when the “called” number (start line or “to” header) does not match with trunk username, it is also checked against defined ranges: if it matches the calls is accepted for the trunk and forwarded to user terminal using (if ISDN) the checked number as called number in SETUP message; otherwise it is refused (unless it is acceptable for other trunks).

```
ATOSNT\voip\trunk\sip-0289279022>>del ?

del  help :  Delete a SIP Trunk Option or Range list
del  usage:
 <OPTION><Option-name>
 <RANGE><Range-name>

del command parameters:
 OPTION
 RANGE
```

For parameters explanation refer to add tables.

pstn-trunk_name_n – Commands

In this node you can configure a PSTN trunk using the following commands and parameters.

```
ATOSNT\voip\trunk\pstn-fxo1>>set ?

Set command parameters:
 enable        [on|off]        Current value: off
 description   [description]   Current value:
 clir type     [clir-type]     Current value: none
 alias number  [alias-number]  Current value: 0
```

Table 32: set

Syntax	Description
[on|off]	Enables/disables the trunk functionality
Description [max 100 char]	Description of the node content. Default [empty]
clir-type [none|keypad]	Specifies how to translate in PSTN the identity restriction required by a user terminal (see “clir-outgoing” parameter in user terminal nodes). • **none** no restriction, in any form, is contained in outgoing SETUP even if requested from user terminal. • **keypad** in outgoing SETUP the keypad string specified by “clir-on-call-code” parameter value is sent as keypad information element. Default: none
alias-number [1-32 decimal digits,#,*]	Alias number parameter allows to set the called number for incoming calls coming from a trunk fxo. In practice, if a call comes from the outside world to a trunk fxo, the call is sent to the user terminal specified in the inbound rules inserting as a called number the “alias-number” value.

```
ATOSNT\voip\trunk\pstn-fxo1>>show work
Show of ATOSNT voip trunk pstn-fxo1
Enable       : on
Description  :
Line         : fxo1
CLIR type    : keypad
Alias number : 190
```

Hints for DDI (italian GNR) or MSN management

Direct Dial In (DDI)

Indicates a service where the user has been assigned a block of continuous numbers to directly access single lines. When offering this service using VoIP trunk, usually a single number, often the commom radix of number ended by ‘*’ is registered. The whole group of number is intended silently registered on provisioning base.

Let’s assume the range of number: 071999901-99 registrable using 0719999* username. In this case incoming INVITE will arrive indicating specific numbers of the range (e.g. 071999955) and the CPE must accept them. Also outgoing INVITE should indicate as calling number (“from” header) specific numbers of the range if provided by (ISDN) terminal.

Finally could be requested to use different numbers on ISDN and SIP sides (for example because of a fixed configuration of PBX). In this case, for example, the leading 0 could be omitted.

This requirement can be managed as follows:

1 Add a SIP trunk with the user name to be registered (0719999*) plus authentication user id and password;

2 add a range with relevant alias for distinguish SIP and ISDN numbers:

```
ATOS\voip\trunk\sip-trunk1>>add RANGE 071999901 99 71999901
Command executed
```

Note: more then one range can be added to a single trunk

3 Add a proper OPTION for the trunk:

```
ATOS\voip\trunk\sip- trunk1>>add OPTION my-option from-trunk range
Command executed
```

4 Add an OUTBOUND rule in call-mng node:

```
ATOS\voip\call-mng>>add OUTBOUND isdn-line-1 ALL-NUMBER 0 NO-PREPEND sip-trunk1 my-option
Command executed
```

5 Add an INBOUND rule in call-mng node:

```
ATOS\voip\call-mng>>add inBOUND sip-trunk1 RANGE 071999901-99 isdn-line-1
Command executed
```

Note: a terminal group can be indicated instead of a single user terminal.

Multiple Subscriber Number (MSN) :

In legacy ISDN service a ISDN line subscriber could have more then one number associated to a single ISDN line. Normally these number (up to 8) where not contiguous.

When providing this service on VoIP, usually numbers must be individually registered; if the provider would implement a single registration with implicit registration of additional number, then the case could be managed in the same way as for DDI management above: single number will be added as additional ranges composed each one of a single number.

Otherwise (every number must be registered individually), in order to manage, as an example, a MSN service with 3 different numbers (071999901 071888850 071777799 on SIP side and 71999901 71888850 71777799 on ISDN side) the following procedure must be followed:

1 Add 3 SIP trunks with using each one a SIP number (071999901 071888850 071777799), plus authentication user id and password;

2 Add 3 ISDN user terminal with ISDN numbers associated:

```
ATOS\voip\user-terminal>>add ISDN isdn-bri1 71999901

ATOS\voip\user-terminal>>add ISDN isdn-bri1 71888850

ATOS\voip\user-terminal>>add ISDN isdn-bri1 71777799
```

Note: 3 terminals named isdn-line-1-71999901, isdn-line-1-71888850 and isdn-line-1-71777799 will be created. All of them are “logical” terminal on isdn-line-1 port (see “user terminal” chapter).

3 Add 3 INBOUND and 3 OUTBOUND rules using each one a trunk with relevant user terminal. For example:

```
ATOS\voip\call-mng>>add OUTBOUND isdn-line-1-71999901 ALL-NUMBER 0 NO-PREPEND sip-071999901 default
```

```
ATOS\voip\call-mng>>add INBOUND sip-071999901 ALL-NUMBERisdn-line-1-71999901
```

With this configuration incoming INVITE directed to 071999901 will be forwarded to isdn 1 physical port (user terminal isdn-line-1-71999901) setting a called number 71999901 in SETUP.

In opposite direction, a SETUP coming from isdn 1 physical port with a calling number 71999901 will originate an outgoing INVITE indicating in the “from” header as calling number 071999901.

If no number translation is needed between ISDN and SIP, logical ISDN terminal must be created using same SIP number. Then, same procedure above will apply.

Call-mng – Commands

In the subnode it is possible to define a number of rules for managing incoming and outgoing calls. It is important to notice that in case of absence of suitable rules it will be impossible to make or receive phone calls even if a valid account for one or more trunk has been correctely configured and registered.

```
ATOSNT\voip\call-mng>>set ?

Nodes not available.
Set command parameters:
 level of log               [loglevel]            Current value: 1
 call detail record number  [call-detail-number]  Current value: 10
```

Table 33:set

Syntax	Description
loglevel <value>	Set the detail level used by ATOS to log the events of the VoIP, from the less detailed one (0) to the more detailed one (5). [default: 1]
call-detail-number [5-50]	Number of entries shown by “show statistics” command (see below) which contain details of last calls. Default [10]

```
ATOSNT\voip\call-mng>>add ?

add  help :  Add an OutBound or InBound list
add  usage:
 <OUTBOUND><source-terminal><dial-mode><strip><prepend><trunk-name><option>
 <INBOUND><source-trunk><incoming-number><destination>

add command parameters:
 OUTBOUND
 INBOUND
```

Table 34:**add OUTBOUND**

Syntax	Description
OUTBOUND	Keyword: add a rule for outgoing calls
source-terminal [ALL-TERMINAL|ALL-POTS-TERMINAL|pots-line-1|…|pots-line-n| ALL-ISDN-TERMINAL|ALL-ISDN-LINE-1-TERMINAL|isdn-line-1|… |isdn-line-n|isdn-line-x-number|ALL-DECT-BASE0-TERMINAL |ALL-DECT-TERMINAL|dect-base0.1|… |dect-base0.6|ring-gr-1|…|ring-gr-n|]	Specifies the source user terminal the rule is valid for. • **all-terminal**: rule is valid for all user terminals; • **all-pots-terminal:**rule is valid for all POTS user terminals; • **pots-line-x:**rule is valid for the specific POTS user terminal • **all-isdn-terminal:**rule is valid for all ISDN user terminals; • **all-isdn-line-1-terminal:**Obsolete and equivalent to "isdn-line-x". Kept for compatibility with older software versions. • **isdn-line-x:** rule is valid for all terminal on specified port: both numbered or not numbered. • **isdn-line-x-number**: rule is valid for calls coming from isdn port 'x' and containing (in SETUP message) the calling number "number" matching with the number of the specified "numbered" terminal. • **all-dect-base0-terminal** : rule is valid for all DECT user terminals registered to the main base station (by default is base0) • **all-dect-terminal**: rule is valid for all DECT user terminals registered to any base station • **dect-base0.x**: rule is valid for a specific DECT user terminal or handset (with x equal to 1,2,3,4,5 or 6) • **Ring-gr-x:**rule is valid for the specific terminal group (i.e. all terminal belonging to terminal group)
dial-mode [ALL-NUMBER|SEL-PREFIX]	Give the possibility to associate outgoing calls to this rule (and consequently to relevant trunk) based on called number: • **ALL-NUMBER**: any called number matches the rules • **SEL-PREFIX**: only called number including a prefix matching the specified one (see below) will be associated to this rule.
prefix [1-20 decimal digits]	Accepted only if SEL-PREFIX has been specified: Variable-length prefix to match. If SEL-PREFIX is not selected, this parameter is not to be inserted.
strip [0 – 20]	Number of initial digits to be stripped from called number
prepend [PREPEND|NO-PREPEND]	Give the possibility to add to the called number a variable length specified prefix (see below). • **PREPEND**: the prefix specified immediately after will be prepended to called number; • **NO-PREPEND**: no prefix is prepended to called number.
Prepend number [1-10 decimal digits, eventually preceded by +]	Accepted only if PREPENDhas been specified: Variable-length prefix to prepend. If NO PREPEND is selected, this parameter is not to be inserted.

trunk-name [sip-trunk_name1|pstn-trunk_name2|isdn_trunk_name3|…]	SIP, PSTN or ISDN trunk to be used for outgoing calls matching this rule. Only proposed names can be selected.
option [default | option_name1| … option_namen]	Name of the OPTION associated to specified trunk to be used. Only proposed names can be selected.

Table 35: **add INBOUND**

Syntax	**Description**
INBOUND	Keyword: add a rule for incoming calls
source-trunk [ALL-TRUNK|ALL-PSTN-TRUNK|pstn-trunk_name1|ALL-SIP-TRUNK|sip-trunk_name2| ALL-ISDN-TRUNK|te-isdn-trunk_name3|....]	Trunk incoming calls are directed to. Only proposed names can be selected. • **all-trunk**: calls directed to any trunk are acceptable for this rule; • **pstn-trunk_name_n**:only calls directed to the specified trunk are acceptable for this rule. Incoming calls would be only presented to the user if at least one of the user terminals specified in the inbound rules is capable to receive the call. In case any user-terminal would be in 'idle' state, the FXO interface will hold the line off-hooked to indicate the busy state. • **sip-trunk_name_n**: only calls directed to the specified trunk are acceptable for this rule. • **te-isdn-trunk_name_n**:only calls directed to the specified trunk are acceptable for this rule.
incoming-number [ALL-NUMBER|NUMBER]	* **ALL-NUMBER**: incoming calls directed to any called number matche the rules • **NUMBER**: only calls directed to the specified called number (see below) will be associated to this rule.
[number] [1-20] decimal digits	Accepted only if NUMBER has been specified as incoming number: called number to match. If ALL-NUMBER is selected, this parameter is not to be inserted.
destination [pots-line-1|pots-line-n|isdn-line-1|… |isdn-line-n|dect-base0.1|… |dect-base0.6| terminal_group_1| … terminal_group_n]	Set the user terminal (pots-line-x, isdn-line-x, dect-base0.x) or terminal group which will receive (ring) the call matching this rule.

```
ATOSNT\voip\call-mng>>del ?

del  help :  Delete an OutBound or InBound list
del  usage:
  <OUTBOUND><source-terminal><dial-mode><trunk-name>
  <INBOUND><source-trunk><incoming-number>

del command parameters:
  OUTBOUND
  INBOUND
```

For parameter explanation refer to add command tables.

A configuration example:

ATOS\voip\call-mng>>**show conf**

Show of ATOS voip call-mng

Call Detail Record number : 10

LIST OF OUTBOUND

SOURCE-TERMINAL DIALLING-MODE SELECTION-PREFIX STRIP PREPEND PREPEND-NUM DEST-TRUNK OPTION-LIST

pots-line-1 ALL-NUMBER 0 NO-PREPEND sip-potsline1 default

pots-line-2 ALL-NUMBER 0 NO-PREPEND sip-potsline2 default

LIST OF INBOUND

SOURCE-TRUNK INCOMING-MODE NUMBER DESTINATION

all-trunk NUMBER 401 pots-line-1

all-trunk NUMBER 402 pots-line-2

Command executed

An example of show statistics command

ATOS\voip\call-mng>>**show statistics**

Statistics of Call-mng

SOURCE DESTINATION START END DURATION DISPOSITION ACTIVE

9401 pots-line-3 2011-01-01 03:34:14 2011-01-01 03:43:57 583 ANSWERED 581

9401 pots-line-3 2011-01-01 03:44:24 2011-01-01 03:44:36 12 ANSWERED 10

9401 pots-line-3 2011-01-01 03:44:53 2011-01-01 03:46:21 88 ANSWERED 86

isdn-line-1 9401 2011-01-01 03:48:02 2011-01-01 05:46:43 7121 ANSWERED 7118

Command Executed

terminal-group – Commands

This node is intended as a container of effective terminal group nodes which are dynamically created.

No parameters are configurable on this node where only the add command (to add new terminal groups) is available.

```
ATOSNT\voip\terminal-group>>add ?

add  help:  Add a Terminal Group
add  usage:
 <number><User-terminal name>[timer-prio-no-answer]

add command parameters:
 Number    [max 3 decimal digits]
```

Table 36: **add**

Syntax	Description
number [max 3 decimal digits]	Numeric identifier for a new terminal group. The actual name of the dynamic node will be automatically composed using this number as a suffix of the common radix “ring-gr-”
User-terminal name [pots-line-1|pots-line-2]	First terminal name to add to the list of terminals included in the group.
timer-prio-no-replay [value] [5 - 120] sec	Optional. When hunting mode (see ring-gr-xxx commands) is set to “PRIO-NO-ANSWER, is the timer the system waits for a non answering user terminal before passing the call to the next user terminal. Default[20]

ATOSNT\voip\terminal-group>>del ?

```
del  help:  Delete a Terminal Group
del  usage:
 <Terminal-Group name>

del command parameters:
 Name      [Empty list]
```

ring-gr-xxx – Commands

A ring group (or terminal group) is a list of user terminal which share incoming call related to one or more inbound rules specifying the terminal group itself as “destination”. Calls are distributed to different terminals based on the value of hunting-mode and priority list parameters.

It is important to underline that a singular user terminal can be used at the same time stand alone in one or more inbound rules and included in one or more terminal groups in one ore more other inbound rules.

Available commands in these nodes are the following:

ATOSNT\voip\terminal-group\ring-gr-1>>set ?

Nodes not available. Set command parameters:

```
 description    [description]    Current value:
 call profile   [call-profile]   Current value: italy
 hunting mode   [hunting-mode]   Current value: CIRCULAR
 priority list  [priority-list]  Current value: pots-line-1
```

Table 37: **set**

Syntax	Description
Description <string> [max 100 char]	Description of the node content
call-profile [call_profile_1 | call_profile_n]	Set the active call profile. Only proposed values (defined in call-setting node) can be chosen. Default [italy]
hunting-mode [CIRCULAR|PRIO-BUSY| BROADCAST|PRIO-NO-ANSWER]	Set the distribution rules of incoming calls to different user terminal of the group: • **CIRCULAR:**incoming calls are uniformly distributed to terminal of the group based on a round robin algoritm, in the order terminals are added to the group (note that in this case priority list is unused); • **PRIO-BUSY**: the call is offered to the first not busy terminal in the priority list; • **BROADCAST:**the call is simulaneously offered to all terminal of the group; • **PRIO-NO-ANSWER**: similar to PRIO-BUSY functioning, but, in the case the selected terminal wouldn't reply for a specific timer, the call is transferred to the next terminal in the priority list.

priority-list [list of pots-line_1 … pots-line_n]	In case of hunting mode parameter set to PRIO-BUSY or PRIO-NO-ANSWER this list represents the order of preference in which terminals receive incoming calls. In case hunting mode parameter is set to other values, this parameter has no effects.

```
ATOSNT\voip\terminal-group\ring-gr-1>>add ?

add  help :  Add a Ring Group element
add  usage:
 <USER-TERMINAL><name>[timer-prio-no-answer]

add command parameters:
 USER-TERMINAL
```

Table 38: **add**

Syntax	Description
USER-TERMINAL	Keyword: add a new user terminal to the group
name [pots-line_1 | …|potsl-line_n|isdn-line-1|...|isdn-line-n|dect-base0.1|...|dect-base0.n|]	Name of user terminal to be added to group. Can only be chosen from the proposed list, which contains all terminals not yet added.
timer-prio-no-replay [value] [5 - 120] sec	Optional. When hunting mode is set to “PRIO-NO-ANSWER, is the timer the system waits for a non answering user terminal before passing the call to the next user terminal. Default [20]

```
ATOSNT\voip\terminal-group\ring-gr-1>>del ?

del  help :  Del a Ring Group element
del  usage:
 <USER-TERMINAL><name>

del command parameters:
 USER-TERMINAL
```

For parameter explanation refer to add command tables.

A configuration example:

ATOS\voip\terminal-group\ring-gr-402>>show conf

Show of ATOS voip terminal-group ring-gr-402

Description :

Call profile : italy

Hunting Mode : BROADCAST

Priority List : pots-line-2 pots-line-1

LIST OF USER-TERMINALS

Command executed

An example of show statistics command

ATOS\voip\terminal-group\ring-gr-402>>show statistics

Statistics of ring-gr-402

Incoming

Calls : 8

Calls Answer : 6

Calls Busy : 1

Calls No Answer: 1

Calls Failed : 0

Command executed

Index

References

[1] http://tools.ietf.org/html/rfc2833
[2] http://tools.ietf.org/html/rfc4040

ManVrRp

Virtual Router Redundancy Protocol

Overview

The VRRP (Virtual Router Redundancy Protocol) implementation allows, on LAN interface, router backup functionality. It selects, among virtual routers running with VRRP on the same LAN, a router MASTER that controls the IP address(es) associated with a virtual router and forwards packets sent to these IP addresses.

Backup functionality among routers follows RFC2338.

VRRP application is similar to Cisco Systems, Inc. proprietary protocol named Hot Standby Router Protocol (HSRP) and to a Digital Equipment Corporation, Inc. proprietary protocol named IP Standby Protocol.

VRRP - Commands

In **vrrp** node you can use set, add and del commands to configure the following parameters

```
ATOSNT\vrrp>>set ?

Nodes not available.
Set command parameters:
 level of log  [loglevel]  Current value: 1
```

Table 1: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the VRRP INSTANCE events. Default: 1

```
ATOSNT\vrrp>>add ?

add  help :  Add a new VRRP IP or IPv6 instance
add  usage:
 <INSTANCE>[name[id-value]]
 <INSTANCE-IPV6>[name[id-value]]

add command parameters:
 INSTANCE
 INSTANCE-IPV6
```

```
ATOSNT\vrrp>>del ?

del  help :  Remove a VRRP instance
del  usage:
 <INSTANCE><name>
 <INSTANCE-IPV6><name>

del command parameters:
 INSTANCE
 INSTANCE-IPV6
```

Table 2: add/del a new VRRP INSTANCE

Syntax	Description
INSTANCE	Keyword for a VRRP IP instance
INSTANCE-IPV6	Keyword for VRRP IPv6 instance
name [max 16 char]	Add/del the name of the VRRP instance. It's allowed to add up to 8 VRRP instances. The “add” command without “name” creates a VRRPn instance where n = 1-8 and vrid = 1-255.
id-value [1-255]	Configure the vrid value used by the vrrp instance. The “add” command without “vrid” creates a VRRP instance where id value (vrid) = 1-255.

VRRP - Nodes

When you add a VRRP IP INSTANCE a new subnode appears; if no name is specified, the system will assigned the name vrrp followed by a progressive number, look at the examples below

```
ATOSNT\vrrp>>add INSTANCE
Command executed

ATOSNT\vrrp>>tree
vrrp                    vrrp0                   authentication
```

```
ATOSNT\vrrp>>add INSTANCE-IPV6
Command executed

ATOSNT\vrrp>>tree
vrrp                    vrrp-ipv6-0
```

VRRPname - Commands

In **vrrpname** node you can use set, add and del commands to configure the following parameters.

```
ATOSNT\vrrp\vrrp0>>set ?

Available nodes:
                       authentication

Set command parameters:
 enable                                [on|off]                      Current value: on
 vrrp interface                        [vrrp-interface]              Current value: eth0
 local address or ifc name             [local-address-or-ifc-name]   Current value: eth0
 vrid                                  [vrid]                        Current value: 1
 priority                              [priority]                    Current value: 100
 preemption                            [preemption]                  Current value: true
 startup delay until preemption (sec)  [delay-until-preemption]      Current value: 0
 handle virtual mac address            [handle-virtual-mac-address]  Current value: true
 advertisement interval (sec)          [advertisement-interval]      Current value: 1
 gratuitous arp delay (sec)            [gratuitous-arp-delay]        Current value: 5
 gateway interface                     [gateway-interface]           Current value:
 network group                         [network-group]               Current value:
 priority decrement                    [priority-decrement]          Current value: 0
 priority increment                    [priority-increment]          Current value: 0
```

```
ATOSNT\vrrp\vrrp-ipv6-0>>set ?

Nodes not available.
Set command parameters:
 enable                                [on|off]                      Current value: on
 vrrp interface                        [vrrp-interface]              Current value:
 local address or ifc name             [local-address-or-ifc-name]   Current value: ::
 vrid                                  [vrid]                        Current value: 1
 priority                              [priority]                    Current value: 100
```

```
preemption                          [preemption]                Current value: true
startup delay until preemption (sec) [delay-until-preemption]    Current value: 0
handle virtual mac address          [handle-virtual-mac-address] Current value: true
advertisement interval (sec)        [advertisement-interval]    Current value: 1
gratuitous arp delay (sec)          [gratuitous-arp-delay]      Current value: 5
gateway interface                   [gateway-interface]         Current value:
network group                       [network-group]             Current value:
priority decrement                  [priority-decrement]        Current value: 0
priority increment                  [priority-increment]        Current value: 0
```

Table 3: set a VRRP IP or a VRRP IPv6 instance

Syntax	Description
on|off	Enables/disables the VRRP instance. Default: off.
vrrp-interface <name>	Configures the interface having the VRRP protocol active. Default: no interface.
local-address-or-ifc-name [aa.bb.cc.dd|loopback0|eth0|eth0-ppp0]	Default IP for binding vrrpd is the primary IP on interface. If you want to hide location of vrrpd, use this IP as src_addr for multicast vrrp packets.
vrid <value>	Configures the virtual router identifier. Range: 1-255. Default: a progressive value from 1 up to 8.
priority <value>	Configures a priority value for the router, the highest priority value identifies the MASTER router. Range: 1-255. Default: 100.
preemption <true|false>	Enables/disables the preemption condition in the election mechanism for the MASTER router. “True” value for preemption means that a router having the highert priority has the precedence on routers having lower priority. “False” value for preemption means that the preemption is always allowed, independently from the router priority.Default value: true.
delay-until-preemption (sec) [0-1000]	Seconds after startup until preemption (if not disabled by "nopreempt"). Range: 0 to 1000. Default:0
advertisement-interval <value>	Time, in seconds, between two ADVERTISEMENT messages. Range: 1-255 sec. Default: 1 sec..
handle-virtual-mac-address <true|false>	“True” value means that the virtual MASTER router uses the virtual MAC address router 00-00-5E-00-00-{VRID} defined by IEEE 802 MAC Address. Default value: true.
gratuitous-arp-delay (sec) [1-255]	“Delay for gratuitous ARP after transition to MASTER. Range: 1 to 255 Default:5
Gateway-interface <name>	Set the gateway interface that define the router behavior in the network: as MASTER router if this interface is UP, as BACKUP router if this interface is down.
network-group	Sets the association between a network group and the VRRP instance . The network group cab be defined as a profile in **Network Groups** node or in **Network groups – Node** section of "IP" node.
priority-increment [0-254]	Sets the priority of the VRRP instance in case of failure of the Gateway or the NETWORK-GROUP configured in the following way: work_priority = conf_priority + (priority-increment - priority-decrement). Obviously, if the value is out of range (1 ~ 255) it will be reported into the range of validity.Default: 0.
priority-decrement [0-254]	Sets the decrement of the router priority in case of failure of the Gateway or the NETWORK GRUOUP. Default: 0..

```
ATOSNT\vrrp\vrrp0>>add ?

add  help :  Add a new Address
add  usage:
 <address>
```

```
add command parameters:
 address         [aa.bb.cc.dd]

ATOSNT\vrrp\vrrp0>>del ?

del  help :  Remove an Address
del  usage:
 <address>

del command parameters:
 address         [aa.bb.cc.dd]
```

```
ATOSNT\vrrp\vrrp-ipv6-0>>add ?

add  help :  Add a new Address
add  usage:
 <address>

add command parameters:
 address         [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]

ATOSNT\vrrp\vrrp-ipv6-0>del ?

del  help :  Remove an Address
del  usage:
 <address>

del command parameters:
 address         [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]
```

Table 4:add/del an IP or an IPv6 address

Syntax	Description
address [aa.bb.cc.dd]	Add/del an IP address from the list of addresses controlled by the MASTER router
address [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]	Add/del an IPv6 address from the list of addresses controlled by the MASTER router

VRRPname – Nodes

Under **vrrp0** node there is available "authentication" subnode

```
ATOSNT\vrrp\vrrp0>>tree
vrrp0                   authentication
```

Authentication - Commands

```
ATOSNT\vrrp\vrrp0\authentication>>set ?

Nodes not available.
Set command parameters:
 type      [type]      Current value: no

ATOSNT\vrrp\vrrp0\authentication>>set type ?

 type  [no|password|ah]

 Current value:    no
 Default fw value: no
```

Table 5: set

Syntax	Description
type [no|password|ah]	Sets the authentication type used in the “Authentication Data” field for the ADVERTISEMENT : • no • password • ah Default: no
password [max 8 char]	String used for a password authentication type. Default: null string.

This example shows how to create a VRRP instance IP on eth0 interface. The VRRP instance, in order to evaluate if the router is a MASTER or a BACKUP one, uses the default gateway interface defined in the router configuration

ATOSNT\vrrp\vrrp1>>**conf**

add vrrp INSTANCE vrrp1

add vrrp vrrp1 1.2.3.4

set vrrp vrrp1 on

set vrrp vrrp1 vrrp-interface eth0

set vrrp vrrp1 vrid 2

set vrrp vrrp1 authentication type ah

ATOSNT\vrrp\vrrp1>>**show work**

Show of ATOSNT vrrp vrrp1

Enable : on

VRRP interface : eth0

Local address or ifc name : 0.0.0.0

VRId : 2

Priority : 100

Preemption : true

Startup delay until preemption (sec) : 0

Handle virtual MAC address : true

Advertisement interval (sec) : 1

Gratuitous arp delay (sec) : 5

Gateway interface :

Network group :

Priority decrement : 0

Priority increment : 0

LIST OF ADDRESSES

Addresses

1.2.3.4

Show of ATOSNT vrrp vrrp1 authentication

Type : ah

Password :

Command executed

Index

ManWEB

WEB

Web node allows to manage **web servers** and **web proxies** installed in the CPE.

The CPE comes out from factory with a web server inside that allows the local and remote management of the device using a web browser.
Under the web node, there is a default subnode named server0.

WEB – General and Operating Commands

Look at the available general and operating commands on web node.

```
ATOSNT\web>>?

Available nodes:
                        server0
Available commands:
up                      Move one step up from the current node
top                     Back to the root of the tree
quit                    Exit from CLI session
set                     Set 'web' options
add                     Add a new SERVER or PROXY
del                     Remove a SERVER or PROXY
conf                    Show the configuration in CLI command format
full-conf               Show full configuration in CLI command format
show                    Show 'web' settings
delete                  Delete statistics
tree                    Show the tree structure of CLI interface
help                    Help of item
info                    Show the system informations
```

```
date                    Show or setting system date and time
save                    Save configuration data
restart                 Restart device
telnet                  Open telnet client session
ssh                     Open SSH2 client session
ping                    Send an ICMP ECHO request
atmping                 Send an ATM loopback cells
tracert                 Display a trace of packet
mtrace                  Display a path for a multicast group
resolve                 Resolve a IP address or IP name
log                     Log Management
show-logging-level      Show logged level
banner                  Edit pre and post login banners

import-site             Import site on node ATOSNT\web>>
remove-site             Remove site on node ATOSNT\web>>
```

Import-site command permits to import an Aethra certified site package containing web page and files.
Remove-site command permits to remove a site from the list of available sites.

```
ATOSNT\web>>import-site ?

import-site  help :  Import site
import-site  usage:
 <TFTP><remote file name>[server-name][on storage type][site-name]
 <FTP><remote file name>[server-name[:port]][on storage type][site-name]
 <SCP><remote path/file-name>[server-name[:port]][on storage type][site-name]
 <HTTP><[username:password@]URL/file-name[:port]>[on storage type][site-name]
 <FROM-DISK><local source-file name>[on storage type][site-name]

import-site command parameters:
 protocol              [TFTP|FTP|HTTP|SCP|FROM-DISK]
```

Table 1: import-site

Syntax	Description
TFTP FTP SCP HTTP FROM-DISK	Protocol type to use for import-site
remote file name [max 128 char]	File name of the signed package containing the web site page and files
server-name	Optional name or IP address of the host where the TFTP/FTP server is located.
on storage type [internal| List disk unit]	Sets the file destination. To save the file select one of the optional storage types: • “internal” to save the file into the internal device file system • select a Disk Unit from the list of connected external devices such as memory cards or usb keys. Default: Internal

site-name	Optional name of the web site. Default: remote filename (without extension)

Remove-site command allows to remove a web site from the available web sites list

```
ATOSNT\web>>remove-site ?

remove-site  help :  Remove site
remove-site  usage:
 <REMOVE-SITE>[name]

remove-site command parameters:
 site name             [Empty list]
```

Table 2: remove-site

Syntax	Description
REMOVE-SITE	Keyword
name	the web site name to be removed from the list

Import-site Configuration Example

This example shows how to import a web site named "webprova" from a remote server (IP address is 192.168.110.20) using TFTP protocol and to donwload the package containing the web site information (file name is WebClientApp.mips32r2) in a USB key (local disk F)

ATOSNT\web>>**import-site** TFTP WebClientApp.mips32r2 ?

import-site command parameters:

server Name [max 128 char]

on storage [internal|Z:]

site name [max 24 char]

<cr>

ATOSNT\web>>import-site TFTP WebClientApp.mips32r2 192.168.110.20 ?

import-site command parameters:

on storage [internal|Z:|F:]

site name [max 24 char]

<cr>

ATOSNT\web>>import-site TFTP WebClientApp.mips32r2 192.168.110.20 F: ?

import-site command parameters:

site name [max 24 char]

<cr>

ATOSNT\web>>import-site TFTP WebClientApp.mips32r2 192.168.110.20 F: WebProva

Starting...

Downloading 'WebClientApp.mips32r2' using TFTP protocol

```
WebClientApp.mips32 100% |*****************************| 190k 0:00:00 ETA
Checking bundle...
Received file is a valid bundle. Installing...
Installing AUTHENTICATION
Installing bin/
Installing bin/WebClient.sh
Installing bin/WebClientOnNotify.sh
Installing bin/web-deactive
Installing bin/web-active
Installing bin/WebClientCaptivePortal.sh
Installing etc/
Installing etc/manifest.xml
Installing var/
Installing var/www/
Installing var/www/contents.sfs
Command executed
```

Set command allows to configure the global enabled web services. For more details, look at below

```
ATOSNT\web>>set ?

Available nodes:
                      server0

Set command parameters:
 enable        [on|off]    Current value: on
 level of log  [loglevel]  Current value: 1
```

Table 3: set

Syntax	Description
on|off	Activates/deactivates all web services. Default: on
loglevel [0-5]	Sets the detail level used by ATOS to record web services events. Default: 1

Add command permits to add a new **web server** or **proxy**.

```
ATOSNT\web>>add ?

add  help :  Add a new SERVER or PROXY
add  usage:
 <SERVER>[name]
 <PROXY>[name]

add command parameters:
 SERVER
 PROXY
```

```
ATOSNT\web>>add SERVER ?

add command parameters:
 name     [max 16 char]
 <cr>
ATOSNT\web>>add SERVER
Command executed

ATOSNT\web>>set ?

Available nodes:
                       server0
                       server1

ATOSNT\web>>add PROXY ?

add command parameters:
 name     [max 16 char]
 <cr>

ATOSNT\web>>add PROXY
Command executed

ATOSNT\web>>tree
web                     server0
                        server1
                        proxy0
```

Table 4: add SERVER or PROXY

Syntax	Description
SERVER	Keyword
PROXY	Keyword
name [max 16 char]	Name of the SERVER or PROXY to add, if the name is not specified, a web server or proxy node will be created with index sequence (server1, server2…proxy0, proxy1...).

Del command permits to delete a web SERVER or PROXY, default web servers installed on factory can not be deleted.

```
ATOSNT\web>>del ?

del  help :  Remove a SERVER or PROXY
del  usage:
 <SERVER><name>
 <PROXY><name>

del command parameters:
```

```
SERVER
PROXY
```

Table 5: del

Syntax	Description
SERVER	Keyword
PROXY	Keyword
name [max 16 char]	Name of the SERVER or PROXY to delete

WEB - Nodes

Web Server Configuration Commands

Set command allows to configure the **web server** parameters.

```
ATOSNT\web\server0>>set ?

Nodes not available.
Set command parameters:
 enable               [on|off]              Current value: on
 level of log         [loglevel]            Current value: 1
 local binding        [local-binding]       Current value: all
 local ipv6 binding   [local-ipv6-binding]  Current value: all
 http port            [http]                Current value: DEFAULT
 https port           [https]               Current value: DEFAULT
 contents             [contents]            Current value: webgui
```

Table 6: set

Syntax	Description
on|off	Activates/deactivates the web server. Default: on
loglevel [0-5]	Sets the detail level used by ATOSNT to record web server events. Default: 1
local-binding [aa.bb.cc.dd|all|none|loopback0|eth0]	Sets the IP address or the interface to access the web server. Option "all" means to enable the "web server" service on all configured interfaces and ports. Default: all
local-ipv6-binding [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx|all|none|loopback0|eth0]	Sets the IPv6 address or the interface to access the web server. Option "all" means to enable the "web server" service on all configured interfaces and ports. Default: all
http [1-65534|OFF|DEFAULT]	Sets http port for the web server. DEFAULT option means to use the same port as configured in system/interfaces. When configured as DEFAULT, "show work" command allows to see the current used port. Default: OFF

https [1-65534|OFF|DEFAULT]	Sets https port for the web server. DEFAULT option means to use the same port as configured in system/interfaces. When configured as DEFAULT, "show work" command allows to see the current used port. Default: OFF
contents [<cr>|webcli|webgui]	Set contents for the web server, select a site from the list of available sites. Default: webcli

Web Proxy Configuration Commands

Set command allows to configure a **web proxy** parameters.

```
ATOSNT\web\proxy0>>set ?

Nodes not available.
Set command parameters:
 enable                [on|off]              Current value: on
 level of log          [loglevel]            Current value: 1
 local binding         [local-binding]       Current value: all
 local ipv6 binding    [local-ipv6-binding]  Current value: all
 http port             [http]                Current value: OFF
 https port            [https]               Current value: OFF
 contents              [contents]            Current value:
 captive portal        [captive-portal]      Current value: off
 default action        [default-action]      Current value: deny
```

Table 7: set

Syntax	Description
on|off	Activates/deactivates the web proxy. Default: on
loglevel [0-5]	Sets the detail level used by ATOSNT to record web proxy events. Default: 1
local-binding [aa.bb.cc.dd|all|none|loopback0|eth0]	Sets the IP address or the interface on which the web proxy is working. Option "all" means to enable the "web proxy" service on all configured interfaces and ports. Default: all
local-ipv6-binding [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx|all|none|loopback0|eth0]	Sets the IPv6 address or the interface on which the web proxy is working. Option "all" means to enable the "web proxy" service on all configured interfaces and ports. Default: all
http [1-65534|OFF|DEFAULT]	Sets http port for the web proxy. DEFAULT option means to use the same port as configured in system/interfaces. When configured as DEFAULT, "show work" command allows to see the current used port. Default: OFF
https [1-65534|OFF|DEFAULT]	Sets https port for the web proxy. DEFAULT option means to use the same port as configured in system/interfaces. When configured as DEFAULT, "show work" command allows to see the current used port. Default: OFF

contents [<cr>|webcli|webgui]	Set contents for web proxy, choose a site from the list of available sites, a custom internal or external path/url (max 64 char) or empty string (use internal default page). Default: empty
captive- portal [on|off]	Activates/deactivates captive portal for web proxy. Default: off
default-action [deny]	Sets the proxy default action for URLs that don't match the rules table. Default: deny

Add Web Proxy Rules

In order to define the proxy rules, you should use add command.

Add command allows to add a rule in the web proxy

```
ATOSNT\web\proxy0>>add ?

add  help :  Add a new RULE
add  usage:
 <RULE><match-url><action-type>[prefix-len]

add command parameters:
 RULE
```

Table 8: add RULE

Syntax	Description
RULE	keyword
match-url [max 128 char]	Sets the url, domain, IP address...etc to be matched by the proxy.
action-type [permit|bypass]	Sets the proxy action or rule: • **permit** the "match url" goes through the proxy and is permited to pass • **bypass** the proxy is transparent and the "match url" bypass the proxy completely .
prefix-len [0-32]	Sets the subnet mask (IPv4) and prefix lenght (IPv6) when the match-url is set to an IP address.

del command allows to delete a rule in the web proxy

```
ATOSNT\web\proxy0>>del ?

del  help :  Remove a RULE
del  usage:
 <RULE><match-url>

del command parameters:
 RULE
```

Table 9: del RULE

Syntax	Description
RULE	keyword
match-url [max 128 char]	Sets the url, domain, IP address...etc to be deleted .

Example of Web Configuration and Status

Show conf command allows you to see the sites table

ATOSNT\web>>**show conf**

Show of ATOSNT web

Enable : on

Level of log : 1

SITE NAME	STORAGE TYPE	INFORMATION
webcli	internal	Aethra Built-In Site
webgui	internal	Aethra Built-In Site
WebClientApp	internal	Aethra Custom Site V_5_7_X@r14566, Size 176.5k

Show of ATOSNT web server0

Enable : on

Level of log : 1

Local binding : all

Local ipv6 binding: all

Http port : 80

Https port : 443

Contents : webgui

Show of ATOSNT web proxy0

Enable : on

Level of log : 1

Local binding : all

Local ipv6 binding: all

Http port : OFF

Https port : OFF

Contents : webcli

Captive portal : on

Default action : deny

MATCH-URL	ACTION-TYPE	PREFIX-LEN
www.aethra.com	permit	
192.168.111.123	permit	
www.google.com	bypass	20

Show of ATOSNT web server1
Enable : on
Level of log : 1
Local binding : all
Local ipv6 binding: all
Http port : 8080
Https port : 8443
Contents : webcli
Command executed

Show status command allows you to see the list of the configured web sites

ATOSNT\web>>**show status**
List of configured web servers
server0
Status: Active
Contents: webgui
Binding Address: all
Binding6 Address: all
Http Port: 80
Https Port: 443
server1
Status: Active
Contents: webcli
Binding Address: all
Binding6 Address: all
Http Port: 8080
Https Port: 8443
List of configured web proxies
proxy0
Status: Not Active
Contents: webcli
Binding Address: all
Binding6 Address: all
Captive Portal: on
Http Port: 8080
Https Port: 8443
Command executed

ManWiFi

Wireless – WLAN0 interfaces

Wireless technology (WLAN, IEEE 802.11 standard) is used to realize an inexpensive and scalable local area network that uses high-frequency radio waves rather than wires. ATOSNT1can be configured as an AP2, implements IEEE 802.11n (2009), IEEE 802.11g (2003) and IEEE 802.11b (1999) standards.

Both 802.11b and 802.11g standards use the DSSS3modulation, a transmission technology where each bit is trasmitted as a redundant sequence of bits (called chip).

From 802.11, 802.11b and 802.11g standars inherit AP access and authentication methods and data cryptography with either WEP4or WAP5.

Like traditional networks, the maximum number of contemporary customers that a single AP can support depends on amount and type of data to transfer.

WLAN0 – Commands

This is the list of Wireless LAN chipset compliant with **IEEE 802.11n/b/g** supported by ATOSNT:

IEEE 802.11n

- Atheros Communications, Inc. - **AR9287**
- Lantiq - **Wave300**

IEEE 802.11 b/g

- Atheros Communications, Inc. - **AR5007G**

At the **wlan0** node, based on the chipset mounted on the 2.4 GHz WLAN miniPCI module or on the printed circuit board, the user can set the following parameters:

```
ATOSNT\wlan0>>set ?
Available nodes:
                       security
                       ap

Set command parameters:
 level of log           [loglevel]              Current value: 1
 enable                 [on|off]                Current value: on
 rf mode                [RF-mode]               Current value: b-g-n
 ssid                   [ssid]                  Current value: ATOS-NT:wlan0
 nick                   [nick]                  Current value: ATOS-NT:wlan0-NICK
 antenna                [antenna]               Current value: diversity*
 tx power (dbm)         [tx-power]              Current value: 18dBm
 rts threshold  (byte)  [rts-threshold]         Current value: 2346
 fixed tx rate  (mbps)  [tx-rate]               Current value: auto
 bc tx rate     (mbps)  [bc-tx-rate]            Current value: auto(*)(***)
 frag threshold (byte)  [frag-threshold]        Current value: 2346(*)(***)
 channel width          [chan-width]            Current value: 40-above**
 guard interval         [guard-interval]        Current value: short**
 wifi multimedia        [wmm]                   Current value: on**
```

```
Commands legend:
* only available on Atheros AR9287 chipset
** available on Atheros AR9287 and Lantiq Wave300 chipset
*** not available on Lantiq Wave300 chipset
```

Table 1:**set**

Syntax	Description
loglevel <0-5>	Set the detail level used by ATOSNT to log the events of the Wireless physical interface, from the less detailed one (0) to the more detailed one (5). [default: 1]
on|off	Enable/disable the wireless interface.
RF-mode [b-g-n | b-g | n]	***available on Atheros - AR9287 and Lantiq - Wave300*** Configure the RF mode of the AP *Access Point*: • b-g-n select IEEE 802.11n G-band, IEEE 802.11b(1999)and IEEE 802.11g (2003) • b-g select IEEE 802.11b (1999) and IEEE 802.11g (2003) • n select only IEEE 802.11n [default: b-g-n]
RF-mode [b-only | g-only | mixed]	***available on Atheros - AR5007G*** • b-only only IEEE 802.11b is active • g-only only IEEE 802.11g is active • mixed both IEEE 802.11b and 802.11g are active at the same time [default: mixed]
ssid [6] [max 32 char]	*Service set identifier* Configure the network name, it is used to identify cells belonging to the same net [default: ATOS-NT]
nick [max 32 char]	Configure the work station's nickname [default: ATOS-NT]
antenna [diversity|antenna1|antenna2]	Define the antenna receiving mode. The *divesity* option selects in real time, the antenna to use with the better signal/noise ratio. This functionality allows to solve the reflection problem selecting quickly and automatically the antenna that receives the best quality signal [default: diversity]
tx-power (dbm) [4dBm|6dBm|8dBm|10dBm|12dBm|14dBm|16dBm|18dBm]	Define the antenna transmitting power [default: 18dBm]
rts-threshold [0-2346]	Define the packet size in bytes, after which an RTS [7]/CTS [8] packet is sent [default: 2346]
tx-rate [auto]	Define in Mbps the transmitting rate of the AP. It automatically selects the better rate for each client [default: auto] In case of "set rf-mode ng" or "set rf-mode b-g-n", it is not possible to set a different value of auto.
bc-tx-rate [auto|1|2|5.5|11]	***not available on Lantiq Wave300*** Define in Mbps the broadcast transmitting rate of the AP. It automatically selects the better rate for each client [default: auto]

frag [9]-threshold [256-2346]	***not available on Lantiq Wave300*** Define in bytes the packet fragmentation threshold to improve performances in case of RF interference. This option allows to split big size files before sending and to reassemble them at the AP [default: 2346]
chan-width [20|40-above|40-below]	***available on Atheros-AR9287 and Lantiq-Wave300*** Set the channel width. This option allows to double the channel bandwith to 40 MHz which results in slightly more than double the data rate. With the width option you can specify the bandwidth to use: • 20 Chosing 20 sets the channel width to 20 MHz • 40-above Chosing 40-above sets the channel width to 40 Mhz with the extension channel above the control channel • 40-below Chosing 40-below sets the channel width to 40 MHz with the extension channel below the control channel. [default: 40-above] *This command is available when ' set rf-mode ng' or 'set rf-mode b-g-n'*
guard-interval [short|long]	***available on Atheros-AR9287 and Lantiq-Wave300***. Set the guard interval. The 802.11n guard interval is the period in nanoseconds between packets. Two settings are available: short (400ns) and long (800ns). A short guard interval increases the PHY rate by 11%. A shorter 400 ns interval boosts a single spatial stream operating at 20 MHz from 65 to 72.2 Mbps, and from 135 to 150 Mbps when operating at 40 MHz. [default: short] *This command is available when ' set rf-mode ng' or 'set rf-mode b-g-n'*
wmm [on|off]	***available on Atheros-AR9287 and Lantiq-Wave300*** Enable or disable Wi-Fi Multimedia (WMM). This feature provides QoS of the Multimedia applications in a Wi-Fi network and enables the AP to prioritize traffic and sharing network resources among the different applications. [default: on]

```
ATOSNT\wlan0>>add ?

Available nodes:
                        ap
add  help :  Add a SSID
add  usage:
 <SSID>[name]

add command parameters:
 SSID

ATOSNT\wlan0>>add SSID 2
Command executed
ATOSNT\wlan0>>add SSID 3
Command executed
ATOSNT\wlan0>>add SSID 4
SSID list full
Command not executed
```

Table 2:add

Syntax	Description
SSID	Keyword
name [max 1 decimal digits]	Sets the name of the SSID. Up to three different SSID can be configured

A new node has been created, see below

```
ATOSNT\wlan0>>tree
wlan0                    security
                        ap                          mac-filter
                        ssid1                       security
                                                    mac-filter
```

```
ATOSNT\wlan0>>del ?

Available nodes:
                        ap
                        ssid1
                        ssid2
                        ssid3
del  help :  Delete a SSID
del  usage:
 <SSID><Name>

del command parameters:
 SSID
```

How WMM works

WMM works by dividing traffic into 4 access categories: Voice, Video, Best Effort and Background. QoS policy (different handling of access categories) is applied on transmitted packets, therefore the AP decides which data streams are most important and assign them a higher traffic priority.

AP classifies packets based on priority assigned to them, according to the bellow table:

At layer 2, priority is based on the VLAN tag (802.1Q); instead at Layer 3, priority is based on TOS field of the IP packet.

When priority is given by Layer 2 (PCP) and Layer 3 (TOS) simultaneously, it is used the highest of both them.

Access Category	Description	Layer 2 VLAN PCP (802.1p priority)	Layer 3 Atheros AR9287 TOS	Layer 3 Lantiq Wave300 TOS
WMM Voice Priority	Highest priority Allows multiple concurrent VoIP calls, with low latency and toll voice quality	7,6	0xb8, 0x88, 0xe0, 0x30	192 or 224
WMM Video Priority	Prioritize video traffic above other data traffic One 802.11g or 802.11a channel can support 3-4 SDTV streams or 1 HDTV streams	5,4	0x28, 0xa0	128 or 160
WMM Best Effort Priority	Traffic from legacy devices, or traffic from applications or devices that lack QoS capabilities (non IP traffic) Traffic less sensitive to latency, but affected by long delays,such as Internet surfing	0,3	Other	0 or 96
WMM Background Priority	Low priority traffic (file downloads, print jobs) that does not have strict latency and throughput requirements	2,1	0x08, 0x20	32 or 64

WMM provides prioritized media access based on the Enhanced Distributed Channel Access (EDCA) method (the higher the AC, the higher the probability to transmit). The collision resolution algorithm is responsible for trafic prioritation and depends on two timing parameters that vary for each AC:

- the minimum interframe space, or Arbitrary Inter-Frame Space Number (AIFSN)
- the Contention Window (CW), sometimes referred to as the Random Backoff Wait

Both values are smaller for high-priority traffic. For each AC, a backoff value is calculated as the sum of the AIFSN and a random value from zero to the CW. The AC with the lowest backoff value gets the Transmit Opporunity (TXOP). As frames with the highest AC tend to have the lowest backoff values, they are more likely to get a TXOP.

In the following table there is the set of parameters fixed (not configurable at the moment), that have been used to define the 4 traffic classes in the Wi-Fi network:

Access Category	CW min	CW max	AIFSN	Max TXOP
Voice (AC_VO)	2	4	1	1.504 ms
Video (AC_VI)	3	4	1	3.008 ms
Best Effort (AC_BE)	4	6	3	0
Background (AC_BK)	4	10	7	0

WLAN0 – Nodes

Under **wlan0** you can see these subnodes.

```
ATOSNT\wlan0>>tree
wlan0                   security
                        ap                      mac-filter
                        ssid1                   security
                                                mac-filter
```

SSID - Commands

```
ATOSNT\wlan0\ssid1>>set ?

Available nodes:
                       security
                       mac-filter

Set command parameters:
 level of log     [loglevel]  Current value: 1
 enable           [on|off]    Current value: on
 ssid             [ssid]      Current value: ATOS-NT:wlan0[0]
 nick             [nick]      Current value: ATOS-NT:wlan0-NICK[0]
 broadcast ssid   [bc-ssid]   Current value: on
 wifi multimedia  [wmm]       Current value: on
```

Table 3: set

Syntax	Description
loglevel [0-5]	Sets the detail level used by ATOSNT to record the SSID events. Default: 1
on|off	Enables/disables the wireless interface.
ssid [max 32 char]	Sets the "Service set identifier" name, it is used to identify cells belonging to the same net
nick [max 32 char]	Sets the work station's nickname
bc-ssid [on|off]	Sets the broadcast ssid. Default: on
wifi multimedia [on|off]	Enables or disables Wi-Fi Multimedia (WMM). Default: on

```
ATOSNT\wlan0\ssid1>>add ?

Available nodes:
                       mac-filter

ATOSNT\wlan0\ssid1>>mac-filter
```

Mac-filter - Commands

```
ATOSNT\wlan0\ssid1\mac-filter>>set ?

Nodes not available.
Set command parameters:
 association control  [association-control]  Current value: disable
```

Table 4: set

Syntax	Description
association-control [disable|default-permit|default-deny]	Enables/disables the association control defined by the mac addresses list. When the association control is active, you can choose between “default-permit” or “default-deny”: • **default-deny –** it means that the mac-address present in the list without any right (default) or not present at all, don’t have the permission to work with AP • **default-permit –** it means that the mac-address present in the list without any right (default) or not present at all, have the permission to work with AP

```
ATOSNT\wlan0\ssid1\mac-filter>>add ?

add  help :  Add mac address to filter
add  usage:
 <mac address>[permit|deny]

add command parameters:
 mac addr          [aa-bb-cc-dd-ee-ff]
```

Table 5: add

Syntax	Description
<mac address>[permit|deny]	Defines the mac address allowed or denied in the AP MAC Address List. If any right is select, “default” value is associated to the entry. In this case, the “association-control default-right” defines the permission to work with the AP.

Security - Commands

```
ATOSNT\wlan0\ssid1\security>>set ?

Set command parameters:
 mode  [mode]  Current value: disable

ATOSNT\wlan0\ssid1\security>>set mode ?

 mode  [disable|wep-dot1x|wpa-psk|wpa-dot1x]

 Current value:    disable
 Default fw value: disable
```

Table 6: set

Syntax	Description
Mode [disable|wep-dot1x|wpa-psk|wpa-dot1x]	Disable: disable the security protocol (default value); wep-dot1x: enable WEP-dot1x encryption and create the dot1xsubnode dinamically; wpa-psk: enable WPA-PSK encyption and create the wpasubnode dinamically;. When "set wlan0 security mode wpa-psk", the wlan0/ap/mac-filter node, is not available. wpa-dot1x: enable WPA-dot1x encyption and create wpa and dot1x subnodes dinamically.

AP - Commands

```
ATOSNT\wlan0\ap>>set ?

Available nodes:
                      mac-filter

Set command parameters:
 broadcast ssid             [bc-ssid]        Current value: on
 rf channel                 [rf-channel]     Current value: auto
 beacon period (msec)       [beacon-period]  Current value: 100
 dtim period (beacon-unit)  [dtim-period]    Current value: 1
```

Table 7: set

Syntax	Description
bc-ssid 10<on|off>	Default value (on), allows clients to use the access point without the SSID configuration.
rf11-channel <value>	1|2|3|4|5|6|7|8|9|10|11|12|13] • When 'set rf-mode ng' or 'set rf-mode b-g-n' the values depend on the 'set channel width [20|40-above|40-bellow]' command: 'set channel width 20' [auto|1|2|3|4|5|6|7|8|9|10|11|12|13] 'set channel width 40-above' [auto|1|2|3|4|5|6|7|8|9] 'set channel width 40-bellow' [auto|5|6|7|8|9|10|11|12|13]
beacon-period <value>	A beacon is a special packet sent from the AP to notify its availability. The "beacon-period" indicates the time (sent in the beacon packet) between each beacon. Admitted values are 20-1000 ms, default is 100 ms.
dtim[12]-period <value>	Indicate, in beacon packet unit, the activation time of the stations in standby. Default value is 1ms, admittes values are 1-255.
ap-protection <on|off>	Enable/disable the feature that notify to 802.11b client when a 802.11g client is transmitting. This feature is usefull expecially when there are more then an AP that use the same RF channel. [Default: on].

AP - Nodes

Mac-filter - Commands

```
ATOSNT\wlan0\ap\mac-filter>>set ?

Nodes not available.
Set command parameters:
 association control  [association-control]  Current value: disable
```

Table 8: set

Syntax	Description
association-control <disable|default-permit|default-deny>	Enable/disable the association control defined by the mac addresses list. When the association control is active, you can choose between “default-permit” or “default-deny”: • **default-deny –** it means that the mac-address present in the list without any right (default) or not present at all, don’t have the permission to work with AP • **default-permit –** it means that the mac-address present in the list without any right (default) or not present at all, have the permission to work with AP [Default: disable]

```
ATOSNT\wlan0\ap\mac-filter>>add ?

add  help :  Add mac address to filter
add  usage:
 <mac address>[permit|deny]

add command parameters:
 mac addr          [aa-bb-cc-dd-ee-ff]
```

Table 9: add

Syntax	Description
<mac address>[permit|deny]	Define the mac address allowed or denied in the AP MAC Address List. If any right is select, “default” value is associated to the entry. In this case, the “association-control default-right” defines the permission to work with the AP.

Security - Commands

```
ATOSNT\wlan0\security>>set ?

Set command parameters:
 mode  [mode]  Current value: disable
```

Table 10: set

Syntax	Description
Mode <disable|wep|wep-dot1x| wpa-psk|wpa-dot1x>	• Disable: disable the security protocol (default value); • wep: enable WEP encryption and create the wepsubnode dinamically; • wep-dot1x: enable WEP-dot1x encryption and create the dot1xsubnode dinamically; • wpa-psk: enable WPA-PSK encyption and create the wpasubnode dinamically;. When "set wlan0 security mode wpa-psk", the wlan0/ap/mac-filter node, is not available. • wpa-dot1x: enable WPA-dot1x encyption and create wpa and dot1x subnodes dinamically.

Security – Nodes

Wep – Commands

WEP, Wired Equivalent Privacy, is a ciphering protocol that belongs to the 802.11b standard and is used to protect wireless communications. It uses the stream cipher algorithm named RC4[13]. Thanks to a combination of 64 or 128 bit keys, WEP provides to network access control and trasmission data ciphering. Each wireless client needs to use the same 64, 128 or 256 bit key to decode a trasmission.

Enabling WEP protocol, "wep" subnode will be dinamiccaly created from security node.

WEP weakness is that the protocol uses a static key to initiate encryption and that it lacks a means of authentication.

```
ATOSNT\wlan0\security>>set mode wep
Command executed

ATOSNT\wlan0\security\wep>>set ?

Nodes not available. Set command parameters:

 authentication  [authentication]  Current value: open-system
tx key          [tx-key]          Current value: key1
key 1 value     [key1]            Current value: 11111111111111111111111111
key 2 value     [key2]            Current value: 22222222222222222222222222
key 3 value     [key3]            Current value: 33333333333333333333333333
key 4 value     [key4]            Current value: 44444444444444444444444444
```

Table 11: set

Syntax	Description
authentication <open-system|shared-key|both>	Tree options are available for the authentication:Tree options are available for the authentication: • **open-system**, where the Access Point accepts connections from any station, without a check identity; • **shared-key**, that uses a shared key auhtentication; • **both**, accepts the two above modes [default: open-system]
tx-key <key1|key2|key3|key4>	Select one of the four keys used for the authentication.
key1/4 <string hex character>	Define the key value in string of 26 or 10 characters (hexadecimal format), that uses a 128 or 64 bits protection system respectively. Each key has a default value (see example below).

The MAC address is the only parameter used to filter the *open system* authentication.

```
ATOSNT\wlan0\security\wep>>show conf
Show of ATOSNT wlan0 security wep
Authentication : open-system
Tx key : key1
Key 1 value : 11111111111111111111111111
Key 2 value : 22222222222222222222222222
Key 3 value : 33333333333333333333333333
Key 4 value : 44444444444444444444444444
```

Wep-dot1x – Commands

In "Wep-dot1x" mode, WEP enhances security using the 802.1X standard authentication with EAP 14. 802.1X is a network access control method that supplies an authentication framework using a RADIUS server.

```
ATOSNT\wlan0\security>>set  mode wep-dot1x
Command executed

ATOSNT\wlan0\security\dot1x>>set ?

Nodes not available.
Set command parameters:
 aaa profile name  [aaa-profile]  Current value:
```

Table 12: set

Syntax	Description
aaa-profile <string>	Name of the AAA profile previously created (see Authentication, Authorization, Accounting chapter), max 32 digits.

AAA-profile configuration must include a RADIUS group with a predefined RADIUS server .

Wpa-psk – Commands

The Wireless Protected Acces, compatible with the previous WEP standard, belongs to the IEEE 802.11i standard [15] and it is implemented in 802.11g devices.

The WPA-psk (Pre Shared Key) uses a psk that a devices will give to each equipment in the network. This mode guarantees a high security level, cause of the lack of an authentication server; everyone, discovering the psk, can access the network. WPA encryption protocols are:

- **TKIP**[16], that uses an encryption algorithm with a 128 bit dynamic key (instead of a 40 bit static key used by WEP);
- **AES** [17], that uses a block encryption algorithm.

Both algorithms can be enabled in the same device.

```
ATOSNT\wlan0\security>>set mode wpa-psk ?

Command complete (enter cr)
```

Automatically a new subnode named **wpa** appears under "security" node.

```
ATOSNT\wlan0\security\wpa>>set ?

Nodes not available.
Set command parameters:
 version           [version]     Current value: wpa1&2
 encryption type   [encryption]  Current value: tkip&aes-ccmp
 key value         [key-value]   Current value: ATOS-WPA-PASSPHRASE
```

Table 13: set

Syntax	Description
version <wpa1|wpa2|wpa1&2>	Select the wpa version to use: wpa1, wpa2 or both wpa1&2.
Encryption <tkip|aes-ccmp|tkip&aes-ccmp>	Select the encryption protocol: • tkip (Temporal Key Integrity Protocol), • aes-ccmp (Aes Counter-Mode/CBC-Mac Protocol) or • both (tkip&aes-ccmp). [default: tkip&aes-ccmp].
key-value <string><8-64 characters>	Configure the key value, that can include from 8 to 64 digits. Devices in the same network must use the same key. [default: ATOS-WPA-PASSPHRASE]

Wpa-dot1x – Commands

In "WPA-dot1x" mode, WPA enhances security using the 802.1X standard authentication with EAP. 802.1X is a network access control method that supplies an authentication framework using a RADIUS server.

```
ATOSNT\wlan0\security>>set mode wpa-dot1x
Command executed

ATOSNT\wlan0\security>>tree
security               dot1x
                       wpa

ATOSNT\wlan0\security>>dot1x
ATOSNT\wlan0\security\dot1x>>set ?

Nodes not available.
Set command parameters:
 aaa profile name  [aaa-profile]  Current value:
```

Dot1x – Nodes

```
ATOSNT\wlan0\security\dot1x>>set ?

Nodes not available.
Set command parameters:
 aaa profile name  [aaa-profile]  Current value:
```

Table 14: set

Syntax	Description
aaa-profile	Name of the AAA profile previously created (see Authentication, Authorization, Accounting chapter), max 32 digits.

WPA – Node

```
ATOSNT\wlan0\security\wpa>>set ?

Nodes not available.
Set command parameters:
 version          [version]     Current value: wpa1&2
 encryption type  [encryption]  Current value: tkip&aes-ccmp
```

Table 15: set

Syntax	Description
version <wpa1|wpa2|wpa1&2>	Select the wpa version to use: • wpa1, • wpa2 or • both wpa1&2 [default: wpa1&2]
Encryption <tkip|aes-ccmp|tkip&aes-ccmp>	Select the encryption protocol: • tkip (Temporal Key Integrity Protocol), • aes-ccmp (Aes Counter-Mode/CBC-Mac Protocol) or • both (tkip&aes-ccmp) [default: tkip&aes-ccmp].

Wlan0 - Configuration Example

Here an example to enable Wlan0 interface with WPA-PSK encryption mode, naming the SSID "wlan0" Show of ATOSNT wlan0

Level of log : 1

Operation Mode : ap

Enable : on

RF Mode : b-g-n

SSID : ATOS-NT:wlan0

Nick : ATOS-NT:wlan0-NICK

Antenna : diversity

Tx power (dBm) : 18dBm

RTS threshold (byte) : 2346

Fixed Tx rate (Mbps) : auto

BC Tx rate (Mbps) : auto

Frag threshold (byte) : 2346

Channel width : 40-above

Guard interval : short

WiFi Multimedia : on

Show of ATOSNT wlan0 security

Mode : wpa-psk

Show of ATOSNT wlan0 security wpa

Version : wpa1&2

Encryption type : tkip&aes-ccmp

Key value : ATOS-WPA-PASSPHRASE

Show of ATOSNT wlan0 ap

Broadcast SSID : on

RF channel : auto

Beacon period (msec) : 100

DTIM period (beacon-unit) : 1

Example about how to create a new Wireless subinterface and set IP address 192.168.5.1, mask 255.255.255.0:

add interfaces iFC wlan0 192.168.5.1/24

ATOSNT>>show interfaces wlan0 conf

Show of ATOSNT interfaces wlan0

Level of log : 1

Description :

Enable : on

Encapsulation : 802.3

Show of ATOSNT interfaces wlan0 ip

Level of log : 1

IP address : 192.168.5.1

Netmask : 255.255.255.0

Default router : 0.0.0.0

MTU value : 1500

Wlan0 Status and statistics

Here 2 examples of Wlan0 status and statistics one is referred to "Atheros Communications" Wireless card and the second one is referred to Lantiq - Wave300 Wireless card:

ATOSNT>>info
ATOS Version: 6.0.0.rc1 (14@BVMEDtjuukbpjWcwovv)
ATOS Date: 21/05/2014 11:24
ATOS License: ETH1+TR069+AdvancedPlus_0SW000852
Hardware: SV1242EW - 2378A
Product Code: 708190297
Serial Number: 000078
eth0 MAC Address: 00:D0:D6:49:CA:EE
Wireless card: **Atheros Communications, Inc. - AR9227 Wireless Network Adapter**
Command executed

Status of wlan0\AP\ATOSNT

Access-Point stations database contents							
STATION ADDRESS	AID	RSSI	Avg Tx Rate	STATION STATE	PS	802	PREAMBLE
80:86:F2:30:13:58	0001	-37 dBm	0 Mbps	AUTHENTICATED	OFF	11n	SHORT

Command executed

ATOS\wlan0>>show statistics -s

statistics of wlan0 interface ******* upstream direction *******
packets : 1274
bytes : 213388
errors : 0
drops : 0
****** downstream direction ****** packets : 755
bytes : 98622
multicast : 0
errors : 0
drops : 0

Command executed

ATOSNT>>info
ATOS Version: 6.0.0.rc1 (15@BVMEDtjuukbpjWcwovv)
ATOS Date: 21/05/2014 11:29
ATOS License: FullFeatures
Hardware: BG7420FW - 250-544300-603
Product Code: 708190292
Serial Number: 00001F
eth0 MAC Address: 00:D0:D6:49:92:96
Wireless card: **Lantiq - Wave300 PSB 8221 PCI**
Command executed

ATOSNT>>show wlan0 status -s

Status of wlan0\AP\BG7420_lo

Access-Point stations database contents				
STATION ADDRESS	**RSSI**	**Tx Rate**	**Rx Rate**	**802**
80:86:F2:30:13:58	-35 dBm	144 Mbps	130 Mbps	11n

```
Command executed
ATOS\wlan0>>show statistics -s
statistics of wlan0 interface
******* upstream direction *******
packets : 0
bytes : 0
errors : 0
drops : 0
****** downstream direction ******
packets : 181
bytes : 17233
multicast : 0
errors : 0
drops : 0
Command executed
```

WPS - Wi-Fi Protected Setup Configuration

Wi-Fi Protected Setup **(WPS)** is a feature that makes the set up of the wireless network easy. If you have client devices such as wireless printers that have WPS button, use this method to connect them to the router.

WPS is only available with wpa-psk security mode.

WPS - Push Button Configuration

Depending on the router model, you can turn on and turn off WiFi with a short press of the button. You should start the procedure with one of the following steps:

- Locate and press the **WPS** button on the router, if available (i.e.BG7420) or
- Push the **reset** botton of the router for a time period of 6.5 to 10 seconds (i.e SV6044xx Bgxxx)
- With the CLI, set **wps wlan0 security wpa pbc** command and within 120 seconds, click the **WPS** button on the client device or in alternative click the **PBC** button in the Configuration Utility software provided with the 802.11n USB key on the WPS tab.

WPS - PIN Code Configuration

Start the procedure opening the 802.11n USB key Configuration Utility and click the **PIN** button on the WPS tab.

The client will propose a random pin code. You should capture and insert it in the CLI **wps wlan0 security wpa pin <pin code>** command within 120 seconds.

Notes

1In Aethra devices with wireless card.

2Access Point.

3Direct Sequence Spread Spectrum.

4Wired Equivalent Privacy, protocol that uses the RC4 cypher algorithm for security and the CRC-32 for data integrity check.

5Wireless Application Protocol

6Service Set IDentifier.

7Request To Send.

8Clear To Send.

9Short for fragmentation.

10BroadCast- Service Set IDentifier.

11Radio Frequency.

12Delivery Traffic Indication Map.

13Rivest's Code, from Ron Rivest, the inventor of the algorithm used.

14Extensible Authentication Protocol.

15Temporal Key Integrity Protocol.

16Temporal Key Integrity Protocol.

17Advanced Encryption Standard.

Index

ManW3Gphy

WWAN physical interfaces

WWAN identifies the node where physical WWAN parameters can be managed.

Multiple WWAN interfaces can be created

Logical interfaces are abstract interfaces built on top an WWAN interface (for more details see "Interfaces" paragraph)

WWAN – Commands

```
ATOSNT\wwan>>set ?

Nodes not available

Set command parameters:
 level of log  [loglevel]  Current value: 1
```

Table 1: set

Syntax	Description
loglevel <value>	Set the detail level used by ATOS to log the events

Creating a new wwan interface

```
ATOSNT\wwan>>add ?

add  help :  Add a WWAN
add  usage:
 <WWAN>[name]

add command parameters:
 wwan
ATOSNT\wwan>>add wwan 1
```

```
Command executed
ATOSNT\wwan>>set ?

Available nodes:
                        wwan0
                        wwan1
```

```
ATOSNT\wwan>del ?

del  help :  Delete a WWAN
del  usage:
 <WWAN><Name>

del command parameters:
 wwan
```

Table 2: add/del

Syntax	Description
WWAN	keyword
name	Max 4 decimal digits for naming wwan interface

The example shows how to create a new wwan interface

ATOSNT\wwan>>add WWAN 1

Command executed

Then there is a new subnode named “wwan1” available.

```
ATOSNT\wwan\wwan1>>set ?

Set command parameters:
 level of log    [loglevel]      Current value: 1
 description     [description]   Current value:
 device id       [device-id]     Current value: auto
 phone number    [phone-number]  Current value:
 apn             [apn]           Current value:
 pin code        [pin-code]      Current value:
 cgdcont         [cdg]           Current value: 1
 mode pref       [mode]          Current value: auto
```

Table 3: set

Syntax	Description
loglevel <value>	Set the detail level used by ATOSNT to log the routing events.
Description	255 chars for description
Device id [device-id]	ID to select specific USB dongle. Default: auto. Show status command in the WWAN node shows the currents installed dongle
Phone number [phone-number]	Phone number to dial-up
Apn [apn]	Access Point Name
Pin code [pin-code]	SIM pin code
cgdcont [cdg]	Context Activation Number in the CGDCONT AT command. Value:0-60000 Default:1
Mode pref mode [mode]	Preferable mode: • 3Gpref • 3Gonly • GPRSpref • GPRSonly

List of 3G USB dongle compatible with Aethra CPEs

This is the list of the 3G USB dongle keys supported :

- HUAWEI E1692
- HUAWEI E220
- HUAWEI K4505H
- HUAWEI K3765
- HUAWEI K4510H
- HUAWEI EC156 e E372
- ZTE/ONDA K3765Z
- ZTE/ONDA MF622
- ZTE/ONDA MF626
- ZTE/ONDA MF628
- ZTE/ONDA MF636
- PIRELLI ID 1266:1000
- DIGICOM ID 1c9e:9605
- TP-LINK MA180

WWAN Status

```
ATOSNT\wwan>>show status
Info of attached WWAN devices

Device {0:06:12D1:14CB:@01:1-1}: HUAWEI K4510H USB 3GModem on USB bus at 1-1

SIM Status :   SIM is waiting a PIN
Manufacturer : Vodafone (Huawei)
Model :        K4510
Revision :     11.810.09.16.11
```

```
IMEI :          356616041377287
IMSI :          222105602836344
```

SIM Status : <xxxxx> may be

- SIM is ready
- SIM is waiting a PIN,
- SIM is waiting a PUK
- SIM is waiting a password **YYYY**

YYY may be:

- PH-SIM PIN

  MT is waiting phone-to-SIM card password to be given

- PH-FSIM PIN

  MT is waiting phone-to-very first SIM card password to be given

- PH-FSIM PUK

  MT is waiting phone-to-very first SIM card unblocking password to be given

- SIM PIN2

  MT is waiting SIM PIN2 to be given (this <code> is recommended to be returned only when the last executed command resulted in PIN2 authentication failure (i.e. +CME ERROR: 17); if PIN2 is not entered right after the failure, it is recommended that MT does not block its operation)

- PH-NET PIN

  MT is waiting network personalization password to be given

- PH-NET PUK

  MT is waiting network personalization unblocking password to be given

- PH-NETSUB PIN

  MT is waiting network subset personalization password to be given

- PH-NETSUB PUK

  MT is waiting network subset personalization unblocking password to be given

- PH-SP PIN

  MT is waiting service provider personalization password to be given

- PH-SP PUK

  MT is waiting service provider personalization unblocking password to be given

- PH-CORP PIN

  MT is waiting corporate personalization password to be given

- PH-CORP PUK

  MT is waiting corporate personalization unblocking password to be given

- **Manufacturer** : <xxxx>

  string to identify the w3g device manufacturer

- **Model** : <xxxx>

  string to identify the w3g device model

- **Revision** : <xxxx>

  string to identify the w3g device version

- **IMEI** : <xxxxx>

  International Mobile station Equipment Identity string , identifying dongle

- **IMSI** : <xxxxx>

  International Mobile Subscriber Identity string identifying the individual SIM card

WWAN0 Status

```
ATOSNT\wwan\wwan0>>show status
Show link status of Device 0:06:12D1:14CB:@01:1-1

Signal power : ............ -87 OK
Signal quality(BER) : ..... unknown
Network Operator : ........ vodafone IT
Protocol : ................ UMTS
Network registration : .... registered
QOS up down rate and delay : ...... 5824 kbit/s  8640 kbit/sec  1000 ms
QOS traffic class and priority : .. interactive 1
```

Signal power : .... <xxxx>

received signal strength indication rssi (in dBm)from -111 to -51 dBm

Signal quality(BER) : ..... <xxx>

channel bit error rate (in percentage %): 0,14-0,28-0,57-1,13-2,26-4,53-9,05-18,10.

Network Operator : .... <xxxx>

Network Operator in use in alphanumeric or numeric format

Protocol : ..... <xxx>

access technology in use, it may be:“GSM” , “GSM Compact" ,"UMTS","GSM /EGPRS" ,"HSDPA" ,"HSUPA" , "HSDPA and HSUPA","HSPA+"

Network registration : .... <xxx>

network registration status , it may be:

- "searching an operator"

  not registered, MT is not currently searching an operator to register to

- "registered"

  registered, home network

- "trying to attach",

  not registered, but MT is currently trying to attach or searching an operator to register to

- "registration denied"

  registration denied

- "registered(roaming)",

  registered, roaming

- "registered for SMS only",

  registered for "SMS only",home network

- "registered for SMS only (roaming)",

  registered for "SMS only", roaming

- "attached for emergency services"

  attached for emergency bearer services only

QOS up down rate and delay : ..... <up rate > <down rate ><delay>

- <up rate>

  the maximum number of kbits/s delivered to UMTS (up-link traffic)at a SAP

- <down rate>

  a numeric parameter that indicates the maximum number of kbits/s delivered by UMTS (down-link traffic) at a SAP.

- <delay>

  the targeted time in milliseconds between request to transfer an SDU at one SAP to its delivery at the other SAP.

QOS traffic class and priority : .... <class><priority>

- <class>

  conversational

  streaming

  interactive

  background

Traffic Class	Conversational (Real Time)	Streaming (Real Time)	Interactive (Best Effort)	Background (Best Effort)
Characteristics	Preserve time relation (variation)between information entities of the stream. Conversational pattern, therefore, very low delay and jitter	Preserve time relation (variation) between information entities of the stream. Delay and jitter requirements are not as strict as with the conversational class	Request/response pattern. Retransmission of payload content in-route	Destination is not expecting the data with a stringent time. Retransmission of payload content in-route might occur
Example Applications	Voice over IP	Streaming audio and video	Web browsing	Downloading email
Diffserv Class / Map to DSCP	Expedited Forwarding Class	Assured Forwarding 2 Class	Assured Forwarding 3 Class	Best Effort

- <priority>

  a numeric parameter (1,2,3....) that specifies the relative importance for handling of all SDUs belonging to the UMTS bearer compared to the SDUs of other bearers

Index

ManxDsl

xDSL – VDSL2, ADSL2+

xDSL (Digital Subscriber Line) is a term that covers several forms of DSL technology, including Asymmetric DSL (**ADSL/ADSL2/ADSL2+**), Single-pair High-speed Digital Subscriber (**SHDSL**), and Very High Bit Data Rate DSL2 (**VDSL2**).

This chapter is focused on VDSL2 and ADSL/ADSL2+ configurations.

Depending on Aethra's model, the devices can operate either in VDSL2 or ADSL2+ mode.

XDSL0 – Commands

```
ATOSNT\xdsl0>>set ?

Set command parameters:
 enable         [on|off]    Current value: on
 level of log   [loglevel]  Current value: 1
 mode           [mode]      Current value: adsl_auto_xa

ATOSNT\xdsl0>>set mode ?

 mode  [adsl_auto_xa|adsl_xa|adsl_g_dmt_xa|adsl_t1_413|adsl2_xa|adsl2plus_xa|
       adsl_auto_xm|adsl2plus_xm|adsl_auto_xb|adsl_xb|adsl2_xb|adsl2plus_xb]

 Current value:    adsl_auto_xa
 Default fw value: adsl_auto_xa

ATOSNT\xdsl0>>bitpertone
```

Table 1: set, set mode, bitpertone

Syntax	Description
<onloff>	Enable/disable the xdsl chipset modem. [default on]
loglevel <value>	It sets the detail level used by ATOSNT to record the xDSL events (0 – 5) [default 1]
adsl_auto_xa	Select the (ANSI | ITU) parameter automatically (ADSL2+/ADSL2/ReADSL/ADSL) according to the DSLAM configuration, for annex A standard .
adsl_xa	Select the (ANSI | ITU) parameter automatically (ADSL1), according to the DSLAM configuration, for annex A standard
adsl_g_dmt_xa	Select the ITU G.DMT ADSL1 parameter for annex A standard
adsl_t1_413	Select the ANSI T1.413 ADSL1 parameter for annex A standard
adsl2_xa	Select the (ANSI | ITU) parameter automatically (ADSL2), according to the DSLAM configuration, for annex A standard
adsl2plus_xa	Select the (ANSI | ITU) parameter automatically (ADSL2+), according to the DSLAM configuration, for annex A standard
adsl2plus_xm	Select the (ANSI | ITU) parameter automatically (ADSL2+ annex M/ADSL2+/ADSL2/ReADSL/ADSL) according to the DSLAM configuration, for annex A standard

adsl_auto_xb	Select the (ANSI | ITU) parameter automatically (ADSL2+/ADSL2/ADSL according to the DSLAM configuration, for annex B standard
adsl_xb	Select the (ANSI | ITU) parameter automatically (ADSL), according to the DSLAM configuration, for annex B standard
adsl2_xb	Select the (ANSI | ITU) parameter automatically (ADSL2), according to the DSLAM configuration, for annex B standard
adsl2plus_xb	Select the (ANSI | ITU) parameter automatically (ADSL2+), according to the DSLAM configuration, for annex B standard
auto_over_pots	Select the (ANSI | ITU) parameter automatically (VDSL2/ADSL2+/ADSL2/ReADSL/ADSL) according to the DSLAM configuration, for annex “over pots” standard
auto_over_isdn	Select the (ANSI | ITU) parameter automatically (VDSL2/ADSL2+/ADSL2/ReADSL/ADSL) according to the DSLAM configuration, for annex “over isdn” standard
vdsl2_over_pots	Select the VDSL2 parameter according to ITU-T G.993.2 “over pots” standard.
Bitpertone	**Bitpertone** command specifies which tones are being transmitted and which they are not. When the tone is present, it specifies the number of the transmitted bits that the tone is carrying on, as well as the Upstream (USx) or Downstream (DSx) band to which the tone belongs to. In VDSL2, it can be up to 4 bands in Down and Upstream (x = 0,1,2,3) and the total tones number is 4096. In ADSL/2/2+, there is only one band Up and Downstream (US0 and DS0. The total tones number is 256 in ADSL and 512 in ADSL2+. Span information is also provided. In ADSL/2/2+ and VDSL2 profiles from 8a to 17a, the bandwith tone is 4.3125kHz. In VDSL2 profile 30a, the bandwith tone is 8.625kHz . To determine the total bandwith occupied, you have to multiply the span to the total number of tones.

Example of the Bitpertone Command for a VDSL2 profile 17a

```
ATOSNT>>xdsl0
ATOSNT\xdsl0>>bitpertone
bit per tone: vdsl span=4.3125kHz
inv,0
inv,0
.....
DS0,8
.....
DS0,9
......
DS0,10
......
DS0,9
......
DS0,11
.......
DS0,13
......
DS0,14
.....
inv,0
......
US0,7
US0,8
......
DS1,14
.......
US1,13
......
DS2,10
.......
US2,11
```

inv,0 means that the tone is not present

How to check the xDSL status

In the xDSL0 node the **show status** command is available: **Example for VDSL2 interface down**

```
ATOSNT\xdsl0>>show status
********** xdsl0 status **********
link status : down
line up count : 0
```

Example for VDSL2 interface up

```
ATOSNT\xdsl0>>show status
**************** xdsl0 status ****************
link status : up
line up count : 1
line up time : 0h 00m 39s
operational mode: VDSL2 G.993.2 Annex B
profile type : 17a
band plan type : -
TC layer : EFM
peer id : 0xB500 'IFTN' 0xA4B2 (Siemens Infineon)
power state : L0
upstream downstream
bitrate ch B0-L0: 40312 83400 kbps
attain. bitrate : 44057 128856 kbps
delay ch B0-L0: 8.0 4.0 ms
INP path L0: 2.0 2.0 DMTSymbols
noise margin : 8.8 14.2 dB
band0: 6.1 12.5 dB
band1: 8.7 14.8 dB
band2: 9.0 14.8 dB
line attenuation: - 4.0 dB
band0: 0.1 2.2 dB
band1: 2.8 3.6 dB
band2: 5.4 6.0 dB
signal attenuat.: - 3.1 dB
band0: 0.1 2.2 dB
band1: 2.8 3.5 dB
band2: 5.4 6.0 dB
tx power : 9.6 11.5 dBm
tx power density: - - dBm/Hz
```

Example for ADSL interface up

ATOSNT\xdsl0>>show status
********** xdsl0 status **********
link status : up
line up count : 1
line up time : 0h 37m 04s
operational mode: ADSL G.992.1 Annex A
TC layer : ATM
peer id : 0xB500 'TSTC' 0x0000 (Texas Instruments)
power state : L0
upstream downstream
bitrate ch B0-L0: 320 1504 kbps
attain. bitrate : 812 5504 kbps
delay ch B0-L0: 8.0 16.0 ms
INP path L0: 1.3 2.4 DMTSymbols
noise margin : 18.0 24.6 dB
line attenuation: 21.0 35.6 dB
signal attenuat.: 21.0 34.2 dB
tx power : 12.2 18.5 dBm
tx power density: - - dBm/Hz

How to check the xDSL statistics

In the xDSL0 node the **show statistics** command is available:

Example for VDSL2 statistics when the interface is up

```
ATOSNT\xdsl0>>show statistics
****************** xdsl0 statistics ******************
far-end near-end
FEC events B0-L0: 19228 0
CRC errors B0-L0: 0 0
errored seconds : 0 0
LOS ES : 0 0
LOF ES : 0 0
severely ES : 0 0
unavailable ES : 69 63
------------------- PTM counters -------------------
far-end near-end
CRC_n err.B0-L0: 0 0
CRC_np err.B0-L0: 0 0
CV_p B0-L0: 0 0
CV_np B0-L0: 0 0
----------------- line path counters -----------------
tx rx
frames ok : 37 74
octets ok : 3235 6475
FCS errors : - 0
alignment errors: - 0
frames int.err. : 0 0
pause frames : 0 0
frames too long : - 0
frames too short: - 0
---------------- system ifc counters -----------------
tx rx
frames ok : 74 37
octets ok : 6475 3235
single coll.fr. : 0 -
multi coll.fr. : 0 -
FCS errors : - 0
alignment errors: - 0
frames int.err. : 0 0
pause frames : 0 0
frames too long : - 0
frames too short: - 0
802.3ah CRC err.: 0 -
802.3ah align er: 0 -
```

Example for ADSL statistics when the interface is up

ATOSNT\xdsl0>>show statistics

********** xdsl0 statistics **********

---------- DSL counters ----------

far-end near-end

FEC events B0-L0: 0 0

CRC errors B0-L0: 0 0

errored seconds : 0 0

LOS ES : 0 0

LOF ES : 0 0

severely ES : 0 0

unavailable ES : 0 0

---------- ATM counters ----------

far-end near-end

rx user cells : 0 42

rx total cells : 0 159456

tx user cells : 0 42

tx idle cells : 0 33885

HEC errors B0-L0: 0 0

idle cell BitErr: 0 0

SHDSL.bis

Aethra devices with **SHDSL.bis** (Single-pair High-speed Digital Subscriber) line interfaces permit to deliver either Ethernet in the First Mile **EFM** or Asynchronous Transfer Mode **ATM** services.
Annex F and G allow symmetrical bandwidth and data rates up to 5696 kbps for each pair used. Using the bonding technique, a CPE with 4 copper pairs, can provide line data rates up to 22 Mbps.

To configure the relevant ShDSL parameters, you should go to **shdsl0** node:

```
ATOSNT>>shdsl0

ATOSNT\shdsl0>>
```

SHDSL0 – Commands

The following configuration commands are available in the **shdsl0** node:

```
ATOSNT\shdsl0>>set ?

Nodes not available.

Set command parameters:

level of log [loglevel]  Current value: 1

mode [mode]  Current value: cpe
```

Table 1: set

Syntax	Description
loglevel [value]	Sets the detail level used by ATOSNT to record the events of the ShDSL operations. [Default: 1]
mode [cpelco]	Sets the ShDSL interface mode: • CPE = it works as a CPE Customer Premises Equipment (e.g. for handshake phase). In this mode it is possible to set either ATM or EFM Phys; • CO = it works as a CO Central Office (e.g. like a DSLAM ShDSL port). In ATOS version 5.4.0, in this mode, only ATM Phys can be set. **Note:** it is not possible to have a mix of ATM and EFM Phys . After changing the operation mode, a disconnection of all Phy is necessary to activate the new mode.

```
ATOSNT\shdsl0>>add?

add help: Add an shdsl phy

add usage:

[phy][numeric_suffix_name][pairs][tc]

add command parameters:

PHY
```

```
ATOSNT\shdsl0>>del?

del help: Delete an shdsl phy

del usage:

[phy][name]
```

Table 2: add

Syntax	Description
phy	Keyword. It sets a new ShDSL physical interface composed by the pairs number specified [pairs number] and tc layer defined in [tc]
numeric_suffix_name[0|1]	It can be 0 or 1 and identifies the suffix for the ATM or PTM port (PTM in case of EFM layer is selected). If 0 is selected, the port will be named “shdsl0.0” (in case of EFM mode, only “0” suffix is allowed); If 1 is selected, the port will be named “shdsl0.1 (only in ATM mode is available).

pairs [pair1|pair2|pair3| pair4|pair1-2|pair1-3| pair1-4|pair3-4]	Define the pair number to use in the created phy. pair1= only Line 1 is used pair2= only Line 2 is used pair3= only Line 3 is used pair4= only Line 4 is used pair1-2= Line 1 and Line 2 are used pair1-3= Line 1, Line 2 and Line 3 are used pair1-4= Line 1, Line 2 Line 3 and Line 4 are used pair3-4= Line 3 and Line 4 are used.
tc[ATM|EFM]	Select the ShDSL layer you want to use. ATM = ATM mode ITU-T 991.2 (2005) EFM = EFM mode ITU-T 991.2 (2005) **Note**: if tc= ATM, when 2 pairs are selected, MPAIR or 4 wire is automatically switched, depending of the CO configuration. If tc = EFM, only EFM bonding works

Table 3: del

Syntax	Description
phy	Keyword. It deletes the ShDSL phy specified in “name” field.
name	ShDSL phy name you want to delete (e.g. shdsl0.0 or shdsl0.1).

SHDSL0\shdsl0.x – Commands

The following configuration commands are available as soon as a new phy is created:

```
ATOSNT\shdsl0\shdsl0.0>>set ?

Set command parameters:
max rate [maxrate] Current value: 89
min rate [minrate] Current value: 3
annex [annex] Current value: bg
rate 2312 [rate2312] Current value: off
four wire mode [four-wire-mode] Current value: auto
tc pam [tc-pam] Current value: auto
force shdsl capabilities [force-shdsl] Current value: off
force capabilities style [force-cap-style] Current value: off
rate adaptive [adaptive] Current value: off
snr margin [margin] Current value: 6
latency [latency] Current value: normal
up shift snr [up-shift-snr] Current value: 0
up shift time  [up-shift-time] Current value: 0
up shift max rate  [up-shift-maxrate]  Current value: 89
down shift snr  [down-shift-snr]  Current value: 0
down shift time  [down-shift-time]  Current value: 0
down shift min rate  [down-shift-minrate]  Current value: 3
```

Table 4: set

Syntax	Description
maxrate <3-89>	Sets the maximum ShDSL rate in terms of number of nx64 kbit. [default 89]
minrate<3-89>	Sets the minimum ShDSL rate in terms of number of nx64 kbit. [default 3]
annex <bg|af>	Sets ITU G.991.2 Annex type: af = Annex AF (ShDSL and ShDSL.bis American standard); bg = Annex BG (ShDSL and ShDSL.bis European standard). [default bg].
rate2312 <on|off>	If maxrate = 36 and four-wire-mode = OFF, this parameter enables/disable an SHDSL connection to reach a 2312 kbps rate. [default off].
four-wire-mode <auto|standard|enhanced>	Sets the behaviour in case of 4 wire connection mode is selected: **auto**: it is automatically selected the standard or enhanced 4 wire connection mode. Enhanced is used if the other ShDSL side has a Globespan firmware precedent to R1.10 or comprise from 2.0 to 2.5; **standard**: it always use standard 4 wire connection mode; **enhanced**: it always use GSPN Enhanced proprietary 4 wire connection mode. [default auto]. **Note:** This command operates only if tc is ATM mode and the phy is composed by 2 pairs.
tc-pam <auto|32|16>	Sets the PAM mode: **16:**it is only PAM 16 (the rate can be from 192 to 3840 kbps), **32:**is only PAM 32 (the rate can be from 768 to 5696 kbps), **auto:**The PAM is automatically selected . [default auto].
force-shdsl <on|off>	**On**: it enables the compatibility with old G.shdsl standard (up to 2312 Kbit). **Off**: it disables the compatibility with old G.shdsl standard (only ShDSL.bis is used) [default off].
force-cap-style <off|full|shdsl|cpe-auto|cpe-auto-tc>	Sets the capabilities list style used during the handshake phase. **off:**using this option, the capabilities list style are not sent. **full**: The support of complete caplist, code points for EFM and extended data rates will be exchanged. **shdsl**: The support of caplist according to G.shdsl (old standard), codepoints up to 2312 are only exchanged , **cpe-auto**: Automatic caplist detection , (applicable to cpe mode only) **cpe-auto-tc**: Automatic TC detection (applicable to cpe mode only). In this case the full capabilities will be generated . [default off].
adaptive <off|on|auto>	It manages the line probing feature to search the right rate, depending on the selected target noise margin. (Current Condition Target Margin Down). **off**: line probing disable [default] **on**: line probing enable (standard mode) **auto**: line probing enable and compatible with Globespan firmware 2.5.x and 3.0.x . [Default: auto]
margin <0-20>	It selects the “Current Condition Target Margin Down” in dB used during line probing phase. [default 6]

medium|low	Sets the latency of the ShDSL line. [default normal]
up-shift-snr <0-21>	Sets a preconfigured value of the Minimum Upshift Noise Margin. In “rate renegotiating” operating mode, it allows to renegotiate the line speed upwards when the current Noise Margin is superior to the Minimum Up shift Noise Margin for a period of time that is superior to the Minimum Upshift Time Interval. [default 0]
up-shift-time <0-7200>	Sets a preconfigured value of the Minimum Upshift Time Interval. In “rate renegotiating” operating mode, it allows to renegotiate the line speed upwards when the current Noise Margin is superior to the Minimum Upshift Noise Margin for a period of time that is superior to the Minimum Upshift Time Interval. When the value is 0, the upwards rate renegotiating operating mode is disable [default 0]
up-shift-maxrate <3-89>	Sets the maximum ShDSL rate in terms of number of nx64 kbit in upwards rate renegotiating operating mode. [default 89]
down-shift-snr <0-21>	Sets a preconfigured value of the Minimum Downshift Noise Margin. In “rate renegotiating” operating mode, it allows to renegotiate the line speed downwards when the current Noise Margin is inferior to the Minimum Downshift Noise Margin for a period of time that is superior to the Minimum Downshift Time Interval . [default 0]
down-shift-time <0-7200>	Sets a preconfigured value of the Minimum Downshift Time Interval. In “rate renegotiating” operating mode, it allows to renegotiate the line speed downwards when the current Noise Margin is inferior to the Minimum Downshift Noise Margin for a period of time that is superior to the Minimum Downshift Time Interval. When the value is 0, the downwards rate renegotiating operating mode is disable. [default 0]
down-shift-minrate <3-89>	Sets the minimum ShDSL rate in terms of number of nx64 kbit in downwards rate renegotiating operating mode. [default 3]

SHDSL0.0 – Status

This is an example of the device status when the 4-pair SHDSL lines are connected

ATOSNT\shdsl0\shdsl0.0>>show status
Phy shdsl0.0 is up
Connection time: 474 sec
Phy is: in sync
PAF fragment size: 256 byte
PAF in use

Pair 1 is in sync
Pair 2 is in sync
Pair 3 is in sync
Pair 4 is in sync

Pair 1
Rate : 5696 Kbit/sec
Transmission power : 8.5 dB
Annex : Annex B/G
PAM : PAM 32
Used capabilities : new or automatic
SNR margin : 18 dB
Loop attenuation : 1 dB
Power Back-Off : 6 dB

Pair 2
Rate : 5696 Kbit/sec
Transmission power : 8.5 dB
Annex : Annex B/G
PAM : PAM 32
Used capabilities : new or automatic
SNR margin : 18 dB
Loop attenuation : 1 dB
Power Back-Off : 6 dB

Pair 3
Rate : 5696 Kbit/sec
Transmission power : 8.5 dB
Annex : Annex B/G
PAM : PAM 32
Used capabilities : new or automatic
SNR margin : 18 dB
Loop attenuation : 1 dB
Power Back-Off : 6 dB

Pair 4
Rate : 5696 Kbit/sec
Transmission power : 8.5 dB
Annex : Annex B/G
PAM : PAM 32
Used capabilities : new or automatic
SNR margin : 18 dB
Loop attenuation : 1 dB
Power Back-Off : 6 dB

Remote side

Pair 1
Transmission power : 8.5 db
SNR margin : 19 dB
Loop attenuation : 1 dB
Power Back-Off : 6 dB

Pair 2
Transmission power : 8.5 db
SNR margin : 19 dB
Loop attenuation : 1 dB
Power Back-Off : 6 dB

Pair 3
Transmission power : 8.5 db
SNR margin : 20 dB
Loop attenuation : 1 dB
Power Back-Off : 6 dB

Pair 4
Transmission power : 8.5 db
SNR margin : 19 dB
Loop attenuation : 1 dB
Power Back-Off : 6 dB

SHDSL0.0 – Statistics

ATOSNT\shdsl0\shdsl0.0>>show statistics
Phy 'shdsl0.0' is up
Time : 546290 ms
Tx frames : 0
Rx frame : 0
Rx fcs error : 0
Rx alignment error: 0
Rx frame too long : 0
Rx frame too short :0
Rx internal error :0
Tx failed :0

debug statistics .....
PAF received frames from rate matching : 0
PAF received frames from rate matching with error marker set :
0
PAF transmitted fragments for link 0 : 0
PAF transmitted fragments for link 1 : 0
PAF transmitted fragments for link 2 : 0
PAF transmitted fragments for link 3 : 0
PAF transmitted fragments with activated TX_ERR signal : 0
PAF received fragments : 0
PAF forwarded fragments from queues to PAF function : 0
PAF transmitted frames to rate matching : 0
PAF transmitted frames with RX_err asserted/garbage frames: 0
PAF dropped frames due to buffer overflow : 0
Clause 45 TC_PAF_LostEnd counter : 0
Clause 45 TC_PAF_LostStart counter : 0
Clause 45 TC_PAF_LostFragment counter : 0
Clause 45 TC_PAF_BadFragmentReceived counter : 0
Clause 45 TC_PAF_Overflow counter : 0
Clause 45 TC_PAF_FragmentTooLarge counter : 0
more...[y][n]?

Clause 45 TC_PAF_FragmentTooSmall counter : 0
Clause 45 TC_PAF_RxErrorReceive counter : 0
Received 64/65 frame with crc error : 0
Received 64/65 frame frame with code violation : 0

xMII statistics: aFramesTransmittedOK : 0
aSingleCollisionFrames : 0
aMultipleCollisionFrames: 0
aFramesReceivedOK : 0
aFrameCheckSequenceErrors : 0
aAlignmentErrors : 0
aFramesLostDueToIntMACXmitError : 0
aFramesLostDueToIntMACRcvError : 0
aPAUSEMACCtrlFramesTransmitted : 0
aPAUSEMACCtrlFramesReceived : 0
aFrameTooLongErrors : 0
aFrameTooShortErrors : 0

Pair 1
Link loss : 0
Shdsl frame error : 0
ES : 0
SES : 0
LOSWS :0
UAS :0

Pair 2
Link loss : 0
Shdsl frame error : 0
ES : 0
SES : 0
LOSWS :0
UAS :0

Pair 3
Link loss : 0
Shdsl frame error : 0
ES : 0
SES : 0
LOSWS :0
UAS :0

Pair 4
Link loss : 0
Shdsl frame error : 0
ES : 0
SES : 0
LOSWS :0
UAS :0

Remote side

Pair 1
Shdsl frame error : 1
ES : 1
SES : 1
LOSWS :1
UAS :1

Pair 2
Shdsl frame error : 1
ES : 1
SES : 1
LOSWS :1
UAS :1

Pair 3
Shdsl frame error : 1
ES : 1
SES : 1
LOSWS :1
UAS :1

Pair 4
Shdsl frame error : 1
ES : 1
SES : 1
LOSWS :1
UAS :1

SHDSL0\shdsl0.x – Trubleshooting Commands

The following troubleshooting commands are available in the **shdsl0\shdsl0.x** subnode:

Table 5: troubleshooting commands

Syntax	Description
connect	It allows to force a shdsl connection for the selected bundle (e.g. after a “disconnect” command).
disconnect	It allows to force a shdsl disconnectionfor the selected bundle. If this command has been sent, to start again a shdsl training, a “connect” command must be used.
loop <offlinelsystem>	Activate a loop in the line side. In any case the physical layer must be up. Off disable the loop if active line active a loop only in the “line” direction. Received ATM cells from the remote side are looped to the network. system active a loop in both “line” and “user” side. . Received ATM cells from the remote side are looped to the network , User traffic are looped to the “user” interface (e.g. Ethernet port).

EOC RESPONSE

Discovery Response Information Field

Octet #	Contents	Data Type	Aethra Response
1	129	Message ID	
2	Hop Count	unsigned char	
3 bits 7..4	Reserved		
3 bits 3..0 -11	Vendor ID (ordered identically to bits in G.994.1 Vendor ID)		‘Aethra’
12	Vendor EOC Software Version	unsigned char	0
13	SHDSL Version #	unsigned char	0
14 bit 7..1	Reserved		0
14 bit 0	Forward LOSW indication, EOC unavailable	bit	0 0 = Available

Inventory Response Information Field

Octet #	Contents	Data Type	Aethra Response
1	130	Message ID	
2	SHDSL Version #	unsigned char	
3 - 5	Vendor List #	3 octet string	‘000’
6 – 7	Vendor Issue #	2 octet string	‘00’
8 - 13	Vendor Software Version	6 octet string	Atos version
14-23	Unit Identification Code (CLEI)	10 octet string	‘A.TLC’
24 bits 7..4	Reserved		
24 bits 3..0 - 32	Vendor ID (ordered identically to bits in G.994.1 Vendor ID)		‘Aethra’
33-44	Vendor model #	12 octet string	‘SV6044S’
45-56	Vendor serial #	12 octet string	serial number

57-68	Other vendor information	12 octet string	Hardware version

Index