SpeedTouch™

610/610i/610s/610v

Business DSL Router

Remote Management

600 SERIES

THOMSON MULTI MEDIA

speedtouch™ ALCATEL

SpeedTouch™ 610

Remote Management

Application Note Ed. 01

speedtouch™ ALCATEL

Status	Released
Change Note	PeckelbeenS
Short Title	AppNote_RemoteManagement R4.1 Ed. 01
Copyright	

speedtouch™ ALCATEL

Contents

1 Introduction

Overview

Abstract

Being a key component of your business network, a good operation of the SpeedTouch™610 is essential to gain maximum performance of your DSL connections.

Continuous management and diagnosis of the SpeedTouch™610 should be performed to ensure a faultless operation of the SpeedTouch™610, 24 hours a day, 7 days a week.

As such, the SpeedTouch™610 can be perfectly embedded in high quality networks, covered by Service Level Agreements (SLAs).

This application note describes how to remotely manage the SpeedTouch™610 Business DSL Router.

This application note focusses on the diagnosis and management of the SpeedTouch™610 from the Wide Area Network (WAN) side, i.e. remotely "over" the DSL line. Nevertheless, most if not all topics described can be equally performed from the local LAN.

Applicability

This application note applies to the following SpeedTouch™ Business DSL Routers:

- The SpeedTouch™610 ADSL/POTS Business DSL Router
- The SpeedTouch™610i ADSL/ISDN Business DSL Router
- The SpeedTouch™610s SHDSL Business DSL Router
- The SpeedTouch™610v VDSL Business DSL Router.

2 SpeedTouch™610 Remote Access

Introduction

The application note SpeedTouch™610 Operation and Maintenance described some of the standard access methods the SpeedTouch™610 provides to allow users to perform configurations and/or - if needed- the required procedures for maintaining and optimizing SpeedTouch™610 operation and performance.

While that application note described what tools are provided by the SpeedTouch™610 and how to use them via the SpeedTouch™610's local interface(s) (Ethernet and ATMF-25.6Mb/s), this section will describe how you can use the very same tools via its DSL interface, i.e. from the remote side of the Packet service connection.

Resumé of SpeedTouch™610 access methods

Before going deeper into the specific changes needed to allow certain monitoring or management, a listing of the methods to access the SpeedTouch™610 is provided:

- SpeedTouch™610 web interface access (HTTP/HTML)
- SpeedTouch™610 CLI access (TCP/IP-Telnet)
- SpeedTouch™610 FTP access (TCP/IP-FTP).

Note For more information on the SNTP, Syslog and SNMP management tools, see the respective sections in this application note.

2.1 The SpeedTouch™610 Firewall

Introduction

All traffic from, to, or via any of the SpeedTouch™610 interfaces is subjected to its powerful programmable firewall.

For a full description of the SpeedTouch™610 programmable firewall see the application note The SpeedTouch™610 and Firewalling.

In the scope of Remote management however, the following topics provide some essential information to understand the operation of the SpeedTouch™610 firewall.

Default firewall configuration

By default a set of rules is provided for basic firewalling.

Defining LAN as your local network, SpeedTouch™610 as the SpeedTouch™610's IP host, and WAN as the "outside" network (i.e. any IP connection configured over the SpeedTouch™610 DSL line), the combination of the firewall rules make sure that IP packets migrating:

- from WAN to LAN are allowed (Rule 1)
- from LAN to WAN are allowed (Rule 2)
- from LAN to SpeedTouch™610 are allowed (Rule 3)
- from SpeedTouch™610 to LAN are allowed (Rule 4)
- from SpeedTouch™610 to WAN are dropped, except DNS and DHCP (Rule 5)
- from WAN to SpeedTouch™610 are dropped, except DNS and DHCP (Rule 6)
- from WAN to WAN are dropped (Rule 7).

Rules 1 and 2 can be considered as "DSL Gateway rules": these assure that the SpeedTouch™610 can act as DSL Gateway for your local network.

Rules 3 and 4 can be defined as "Local Management rules": these two rules enable direct communication between the local network and the SpeedTouch™610 IP host (be it for http, ftp or telnet access) possible.

Rules 5, 6 and 7 could be defined as the "Security and Remote Management rules": these rules ensure that by default no one from the WAN has IP access with the SpeedTouch™610 device itself.

Implementation of the default firewall rules

In the following an extract is given of the default firewall rules.

- Sink chain firewall rules applying to traffic destined for the SpeedTouch™610 IP host (sink hook):

```
chain=sink index=0 srcintf="eth0" srcbridgeport=!1 action=drop
chain=sink index=1 srcintfgrp=!wan action=accept
chain=sink index=2 prot=udp dstport=dns action=accept
chain=sink index=3 prot=udp dstport=bootpc action=accept
chain=sink index=4 prot=udp dstport=sntp action=accept
chain=sink index=5 prot=udp dstport=snmp log=yes action=count
chain=sink index=6 prot=udp dstport=rip log=yes action=count
chain=sink index=7 action=drop
```

  The first rule indicates the firewall to allow only incoming traffic to the SpeedTouch™610 IP host if it comes from the Ethernet interface, but not from a WAN hardware bridge port. The second rule indicates to accept any traffic coming from any not-WAN interface.
  Some specific UDP ports are opened for correct functioning of the SpeedTouch™610. SNMP and RIP packets are logged.
  All other packets to the SpeedTouch™610 IP host are dropped.

- Source chain firewall rules applying to traffic generated by the SpeedTouch™610 IP host (source hook)::

```
chain=source index=0 dstintfgrp=!wan action=accept
chain=source index=1 prot=udp dstport=dns action=accept
chain=source index=2 prot=udp dstport=bootps action=accept
chain=source index=3 prot=udp dstport=sntp action=accept
chain=source index=4 prot=udp dstport=syslog action=accept
chain=source index=5 prot=udp dstport=rip log=yes action=count
chain=source index=6 prot=udp dstport=snmptrap log=yes action=count
chain=source index=7 prot=udp srcport=snmp log=yes action=count
chain=source index=8 action=drop
```

  The first rule indicates that there is no restriction for traffic towards the LAN. Again some specific UDP ports are opened for correct functioning. SNMP and RIP packets are logged.
  All other packets generated by the SpeedTouch™610 IP host are dropped.

When adding rules to the source and sink chains, always make sure to insert the rules before the last rule, as all traffic subjected to this last rule will be dropped.

Firewalling in the scope of remote management

Allowing remote management and monitoring of the SpeedTouch™610 from the WAN actually means creating specific holes in the firewall to allow dedicated WAN traffic directly to and from the SpeedTouch™610 IP host.

Otherwise stated, if you want to allow remote management and monitoring, the firewall rules applying to source and sink have to be changed that way that all traffic (DNS and DHCP not included) between SpeedTouch™610 is dropped as before, except traffic specifically belonging to one or more kinds of remote management and monitoring.

In the following, the changes are described per remote access method.

Note All of following examples start from the default set of firewall rules.

2.2 Remote SpeedTouch™610 Web Interface Access

Appropriate firewall rules

To allow remote access to the SpeedTouch™610 web pages from the WAN, you must add following rules:

- To the sink chain:

```
[firewall rule]=>
create chain=sink index=2 prot=tcp dstport=www-http action=accept
```

The rule allows incoming traffic from the WAN to the SpeedTouch™610 web host.
The rule is inserted after the first two rules (index=0 and index=1) as none of the two rules apply to traffic coming from any WAN interface. However, make sure (as in the example) to insert the rule before the last rule (which drops all traffic not blocked by any preceding rule).

Note If you want to allow remote access to the SpeedTouch™610 web pages in a Bridged Ethernet Packet Service scenario, you must add the rule mentioned above with index=0 (i.e. the added rule becoming the first one) to avoid that the traffic coming from the WAN Bridge port and destined for the SpeedTouch™610 web host is dropped.

- To the source chain:

```
[firewall rule]=>
create chain=source index=1 prot=tcp srcport=www-http action=accept
```

The rule allows outgoing traffic from the SpeedTouch™610 web host to the WAN. It is added after the first rule concerning all traffic towards the LAN as it has no concern with it, but before the last rule (which drops all traffic not blocked by any preceding rule).

The added rules will allow any user on the WAN to contact the SpeedTouch™610 web pages and browse them after authentication.

Refinements of the rules

However, if needed, the rules can be fine-tuned to allow only traffic coming from/going to a particular Packet Service interface, or even (additionally) restrict allowed traffic to a range of IP addresses.

The example below shows the rules to add in case a separate management PVC (called IPoA) is used with the Routed IPoA Packet Service configuration in the 192.6.11.x/24 range of IP addresses. In this setup only remote hosts with an IP address in the range of 192.6.11.1 to 192.6.11.254 with an IP connection to the SpeedTouch™610 via the IPoA WAN interface are allowed to contact the SpeedTouch™610 web pages.

```
[firewall rule]=>
create chain=sink index=2 srcintf=IPoA src=192.6.11.1/24 prot=tcp
       dstport=www-http action=accept

[firewall rule]=>
create chain=source index=1 dstintf=IPoA dst=192.6.11.1/24 prot=tcp
       srcport=www-http action=accept
```

For more information on the complete CLI command parameters, see the SpeedTouch™610 CLI Reference Guide.

2.3 Remote SpeedTouch™610 Telnet Access

Appropriate firewall rules

To allow remote access to the SpeedTouch™610 Command Line Interface (CLI) via a Telnet session from the WAN to the SpeedTouch™610, you must add following rules:

- To the sink chain:

```
[firewall rule]=>
create chain=sink index=2 prot=tcp dstport=telnet action=accept
```

The rule allows incoming traffic from the WAN to the SpeedTouch™610 Telnet server.
The rule is inserted after the first two rules (index=0 and index=1) as none of the two rules apply to traffic coming from any WAN interface. However, make sure (as in the example) to insert the rule before the last rule (which drops all traffic not blocked by any preceding rule).

Note If you want to allow remote access to the SpeedTouch™610 CLI via Telnet in a Bridged Ethernet Packet Service scenario, you must add the rule with index=0 (i.e. the added rule becoming the first one) to avoid that the traffic coming from the WAN Bridge port and destined for the SpeedTouch™610 Telnet server is dropped.

- To the source chain:

```
[firewall rule]=>
create chain=source index=1 prot=tcp srcport=telnet action=accept
```

The rule allows outgoing traffic from the SpeedTouch™610 Telnet server to the WAN. It is added after the first rule concerning all traffic towards the LAN as it has no concern with it, but before the last rule (which drops all traffic not blocked by any preceding rule).

The added rules will allow any user on the WAN to open a Telnet session to the SpeedTouch™610 and accessing the CLI after authentication.

Refinements of the rules

However, if needed, the rules can be fine-tuned to allow only traffic coming from/going to a particular Packet Service interface, or even (additionally) restrict allowed traffic to a range of IP addresses.

The example below shows the rules to add in case a same management setup as in "2.2 Remote SpeedTouchTM610 Web Interface Access" on page 8 is applied. Again, in this setup only remote hosts with an IP address in the range of 192.6.11.1 to 192.6.11.254 with an IP connection to the SpeedTouch™610 via the IPoA WAN interface are allowed to contact the SpeedTouch™610 Telnet server.

```
[firewall rule]=>
create chain=sink index=2 srcintf=IPoA src=192.6.11.1/24 prot=tcp
       dstport=telnet action=accept

[firewall rule]=>
create chain=source index=1 dstintf=IPoA dst=192.6.11.1/24 prot=tcp
       srcport=telnet action=accept
```

For more information on the complete CLI command parameters, see the SpeedTouch™610 CLI Reference Guide.

2.4 Remote SpeedTouch™610 FTP Access

Appropriate firewall rules

To allow remote access to the SpeedTouch™610 File System via an FTP session from the WAN to the SpeedTouch™610, you must add two rules per chain: one rule for the FTP control channel and one for the FTP data channel:

- To the sink chain:

```
[firewall rule]=>
create chain=sink index=2 prot=tcp dstport=ftp action=accept
[firewall rule]=>
create chain=sink index=3 prot=tcp dstport=ftp-data action=accept
```

  The first rule allows users from the WAN to contact the SpeedTouch™610 FTP server. The second rule allows data coming from the WAN to the SpeedTouch™610 file system.
  The rules are both inserted after the first two rules (index=0 and index=1) as none of the two rules apply to traffic coming from any WAN interface. However, make sure (as in the example) to insert the rule before the last rule (which drops all traffic not blocked by any preceding rule).

Note If you want to allow remote access to the SpeedTouch™610 CLI via Telnet in a Bridged Ethernet Packet Service scenario, you must add the rules with index=0 respectively index=1 (i.e. becoming the first two rules) to avoid that the traffic coming from the WAN Bridge port and destined for the SpeedTouch™610 FTP server, or file system is dropped.

- To the source chain:

```
[firewall rule]=>
create chain=source index=1 prot=tcp srcport=ftp-data action=accept
[firewall rule]=>
create chain=rule index=2 prot=tcp srcport=ftp-data action=accept
```

  The first rule allows control messages generated by the SpeedTouch™610 FTP server to pass through to the WAN. The second rule allows data coming from the SpeedTouch™610 file system and FTP server to pass through to the WAN. Both rules are added after the first rule concerning all traffic towards the LAN as it has no concern with it, but before the last rule (which drops all traffic not blocked by any preceding rule).

The added rules will allow any user on the WAN to open an FTP session to the SpeedTouch™610 and accessing the file system after authentication.

Note The access rights which apply to the SpeedTouch™610 file system are not controlled by the firewall. I.e. you can not change the access rights to the file system root directory, nor to the /dl and /active subdirectories.
For more information on the access rights that apply to the SpeedTouch™610 file system, see the application note SpeedTouch™610 Operation and Maintenance.

2.5 SpeedTouch™610 Controlled Access

Introduction

In sections "2.2 Remote SpeedTouchTM610 Web Interface Access" on page 8, "2.3 Remote SpeedTouchTM610 Telnet Access" on page 9 and "2.4 Remote SpeedTouchTM610 FTP Access" on page 10 the methods for allowing remote management of the SpeedTouch™610 by a remote host or network on the WAN are described.

Generally the method existed of changing or adding firewall rules to which the packets arriving at or leaving from the SpeedTouch™610 from/to the WAN are checked against

Regarding the local network no restrictions exist at all by default.

However, in many cases where the SpeedTouch™610 is remotely managed it is useful to restrict access to the device from the local network to avoid potential mis-configuration and/or interference with remote management tasks.

The SpeedTouch™610 firewall provides various means to restrict access from the LAN.

Default Firewall configuration vs LAN

No restriction apply at all for packets arriving at the SpeedTouch™610 IP host from the local network due to following two primary rules in the sink chain:

```
chain=sink index=0 srcintf="eth0" srcbridgeport=!1 action=drop
chain=sink index=1 srcintfgrp=!wan action=accept
```

Equally, no restrictions apply for packets leaving the SpeedTouch™610 IP host to the local network due to following primary rule in the source chain:

```
chain=source index=0 srcintfgrp=!wan action=accept
```

Restricting all SpeedTouch™610 access for the local network

Forbidding all contact between the SpeedTouch™610 IP host and the local network can be simply done by deleting these three rules.

Note Do not perform this operation via a Telnet session, or via the SpeedTouch™610 web pages, as deleting the rules will have immediate effect: all direct IP conectivity will be lost. Therefore, make sure to perform this operation only from CLI access via the serial Console port.

Doing so will not affect the forwarding and routing functionality of the SpeedTouch™610, but local hosts will no longer be able to ping, ftp and telnet the SpeedTouch™610 or browse its web pages.

However, before the local users will experience the same behaviour of the services delivered by the SpeedTouch™610 two internal SpeedTouch™610 should be made available for the "outside" again:

For the good operation of the SpeedTouch™610 DNS server towards the local network, following rule must be added to the source chain:

```
chain=source index=1 prot=tcp srcport=dns action=accept
```

This rule makes sure that name resolvings by the SpeedTouch™610 can be propagated to the requesting (local) host.

In case you use the SpeedTouch™610 DHCP server for automatic IP configuration for the hosts on your local network, DHCP requests from local hosts will no longer be accepted to arrive at the SpeedTouch™610 IP host (i.e. its DHCP server), and equally, DHCP replies will no longer be accepted to leave the SpeedTouch™610 IP host towards the local LAN.

To solve this, you can add following firewall rules:

```
chain=sink index=3 srcintfgrp=lan prot=udp dstport=bootps action=accept
chain=source index=3 dstintfgrp=lan prot=udp srcport=bootpc action=accept
```

The first rule makes sure that DHCP requests are accepted to pass the SpeedTouch™610 DHCP server's BootP-Server UDP port; the second that DHCP replies in answer to the DHCP requests are accepted to pass the DHCP server's BootP-Client UDP port.

Of course, in case your local network uses fixed IP adresses or another DHCP server than the SpeedTouch™610's, there is no need for these rules.

Syslog messages

When restricting access as described in " Restricting all SpeedTouchTM610 access for the local network" on page 11 no communication between any host and the SpeedTouch™610 IP host is possible.

However, to provide minimal management, syslog messages are allowed to pass the firewall towards the LAN or WAN via following rule in the source chain:

```
chain=source index=4 prot=udp dstport=syslog action=accept
```

Still, to allow a host's syslog deamon to receive SpeedTouch™610 syslog messages, a syslog rule for that host must be configured via the SpeedTouch™610 web pages or the CLI.

Allowing restricted access

Once you denied all access leaving from or ariving at the SpeedTouch™610 IP host, you are able to allow service by service to the LAN by adding specific firewall rules for the sink and source chains.

The rules are very similar to the rules added for remote management except that now the "gate" must be opened for the LAN instead of the WAN.

3 SpeedTouch™610 Syslog

Introduction

Syslog is a basic, uncomplicated, yet powerful method to administer a network device as the SpeedTouch™610. By sending syslog messages, the SpeedTouch™610 is able to inform network managers about the general state of the device and to record events which can be retrieved for later analysis and diagnosis.

This section describes how to use the SpeedTouch™610 Syslog server.

SpeedTouch™610 SNMP service

Next to Syslog the SpeedTouch™610 supports SNMP for extended device management.

For more information on SNMP, see "4 The SpeedTouchTM610 SNMP" on page 21.

SpeedTouch™610 SNTP client

Because it is not only important to know what events occurred on the SpeedTouch™610 or its services, but also when, the SpeedTouch™610 features an SNTP client to allow synchronization of the internal clock with one of Internet's many real-time NTP servers.

For more information on the SpeedTouch™610 SNTP client, see The SpeedTouch™610 Orientation Guide.

3.1 The SpeedTouch™610 Syslog Daemon

What is Syslog

Syslog is a message generating tool that can be implemented in any network device. The intention of the tool is to send messages over the network indicating status, actions, possible problems, etc. from the device.

Although the syslog protocol is widely spread and evolved to a de-facto standard, only recently some first Internet drafts and informational Request For Comments (RFC) became available to describe the existing protocol and some proposal for enhancements.

The SpeedTouch™610 Syslog daemon

For the SpeedTouch™610, the syslog daemon conforms to the proposed standards as much as possible.

Syslog messages

Syslog messages consist of a message header called Priority and a message body containing the message itself.

Via the Priority identification it is possible to determine the severity and facility of a message, hence allows to diversify the messages according their importance. Each severity and each facility can be identified by a numerical value. The sum of the numerical values of the severity and the facility indicates (the numerical value of) the priority.

In the following all severities and facilities are listed with respective notation and numerical values.

Syslog priority severities

Following priority severities are possible for a syslog message generated by the SpeedTouch™610 The severities are listed by descending priority:

Severity	Notation	Code
Emergency conditions, system unusable	emerg	0
Alert conditions, immediate action is needed	alert	1
Critical conditions	crit	2
Error conditions	err	3
Warning conditions	warning	4
Normal but significant conditions	notice	5
Informational messages	info	6
Debug-level messages	debug	7

Syslog priority facilities

Following priority facilities are possible for a syslog message generated by the SpeedTouch™610. The facilities are listed by descending priority:

Priority	Notation	Code
Kernel messages	kern	0
User-level messages	user	8
Mail system	mail	16
System daemons	daemon	24
Authorization messages	auth	32
Syslog daemon messages	syslog	40
Line printer subsystem	lpr	48
Network news subsystem	news	56
UUCP subsystem	uucp	64
Clock daemon	cron	72
Security messages	security	80
FTP daemon	ftp	88
NTP subsystem	ntp	96
Log audit	audit	104
Log alert	alert	112
Clock daemon	clock	120
Local use messages	local0 local1 local2 local3 local4 local5 local6 local7	128 136 144 152 160 168 176 184

Syslog message bodies

The SpeedTouch™610 syslog daemon is internally responsible for collecting and administering messages generated by one or more of its subsystems. Following of the SpeedTouch™610 subsystems are able to trigger a message:

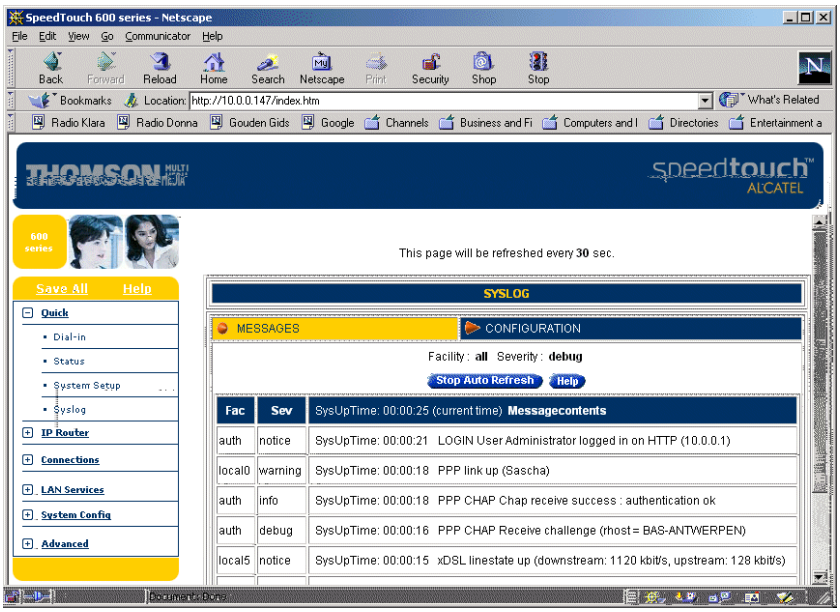
- The PPP dial-in client
- The PPPoA-to-PPTP relaying facility
- The DHCP server and DHCP client
- The SNTP client
- The RIP module
- The login authentication module
- The NAPT module
- The Firewall module
- The SpeedTouch™610 kernel module.

Depending on the triggering event, fixed messages are generated. For a complete listing of the possible syslog messages, see The SpeedTouch™610 CLI Reference Guide.

3.2 Syslog via the Web Pages

The SpeedTouch™610 Syslog web page

The SpeedTouch™610 Syslog web page allows users to view all or a selection of syslog messages the SpeedTouch™610 generated. Simply browse to the SpeedTouch™610 web pages at http://10.0.0.138 and click Syslog in the Quick Tasks menu:



The advantage of offering the syslog web page, is that any authenticated user on the local network is able to browse the SpeedTouch™610 web pages, hence the syslog page to view the latest event loggings, without the need for additional syslog software.

Syslog configuration

Via the SpeedTouch™610 Syslog page, you can also configure the SpeedTouch™610 syslog daemon to send syslog messages to one or more particular host IP addresses. This allows dedicated syslog software on the host to collect SpeedTouch™610 syslog messages for immediate notification, future reference, and event archiving.

For more information on the configuration of the syslog daemon via the SpeedTouch™610 web pages, see The SpeedTouch™610 Orientation Guide.

3.3 Syslog via the CLI

The Syslog CLI command group

The SpeedTouch™610 CLI syslog command group basically provides the same possibilities as provided on the SpeedTouch™610 syslog web page:

```
=>syslog help
Following commands are available :

config           : Set/Display configuration
ruleadd          : Add a new rule to the syslog configuration.
ruledelete       : Delete a rule in the syslog configuration
flush            : Flushes syslog rules.
list             : List the current syslog configuration

Following command groups are available :

msgbuf

=>syslog msgbuf help
Following commands are available :

show             : Show messages in the syslog message buffer.
send             : Send messages to remote syslog server.

=>
```

For more information on the syntax and use of the CLI syslog command group commands, see The SpeedTouch™610 CLI Reference Guide.

3.4 Remote Syslog Notification

Introduction

As described before the SpeedTouch™610 can be configured to send all or a selection of generated syslog messages to a host on the local or a remote network IP address.

This section describes how to configure the SpeedTouch™610 syslog daemon for sending messages to a particular host.

Preconditions

The host to send the syslog messages to, should have syslog daemon software installed for capturing the messages, and a known, fixed IP address.

Syslog host on the local network

By default, no traffic restrictions apply for the local network. Simply add a syslog rule via the SpeedTouch™610 syslog configuration web page or the CLI. Specify the IP address of the host, and optionally refine the set of syslog messages to send.

Note You can specify one or a selection of (comma-seperated) or all facilities. Specifying a severity actually means specifying to send syslog messages with a severity as specified, and all messages with a higher severity.
For a priority listing see " Syslog priority severities" on page 14.

The following example shows the configuration via the CLI for a syslog host on the local "Net10" network with fixed IP address 10.0.0.1 to send all generated syslog messages (all facilities, with severity debug and higher) to:

```
=>syslog ruleadd
fac = all
sev = debug
dest = 10.0.0.1
:syslog ruleadd fac=all sev=debug dest=10.0.0.1
=>saveall
=>
```

Syslog host on a remote network

The default firewall rules do allow traffic from the SpeedTouch™610 syslog daemon towards the WAN due to following firewall rule in the source:

```
:firewall rule create chain=source index=4 prot=udp dstport=syslog action=accept
```

Therefore, no additional firewall configuration is needed in case you want to configure a syslog host on a remote network

The example below shows the syslog rule to add for a syslog host with IP address 192.6.11.1, accessible via the separate management PVC with the Routed IPoA Packet Service configuration in the 192.6.11.x/24 range of IP addresses. The local syslog host (10.0.0.1), configured before (See " Syslog host on the local network") will receive all generated syslog messages; the remote syslog host only receives syslog messages from all facilities with severity warning, error, critical, alert or emergency (all facilities, with severity warning and higher):

```
=>syslog ruleadd fac=all sev=warning dest=192.6.11.1
=>
=>syslog list
1: all.debug                    10.0.0.1
2: all.warning                  192.6.11.1
=>
=>saveall
=>
```

4 The SpeedTouch™610 SNMP

Introduction

Simple Network Management Protocol (SNMP) is a widely spread method for managing networks. Based on a client /server concept, the SNMP server (the SNMP manager) gets or sets the values of objects defined in a Management Information Base (MIB) kept by the SNMP client (the SNMP agent). In addition the SNMP agent is also able to autonomously initiate an action by sending a trap to the SNMP manager.

This section describes the SpeedTouch™610 SNMP implementation and how to use it.

SNMP in the SpeedTouch™610

SNMP has become the de-facto standard for network management. Especially the monitoring aspect has become important: network administrators want to be notified when things go wrong in their network. In addition, to prevent problems, they also want to be able to do network load and trend analysis.

SNMP allows the user to access data about the SpeedTouch™610 as defined in several MIBs. This way the SpeedTouch™610 can perfectly fit in a managed network, monitored by SNMP.

Today, three versions of SNMP exist: SNMP v1, SNMP v2 and SNMP v3. However currently, the SpeedTouch™610 SNMP agent only supports the SNMP v1 protocol.

Management Information Base

The Management Information Base, or MIB, is a tree-like structure containing SNMP objects, instances of these objects and their corresponding values. Parts of this tree have been standardized, other parts may be specific to a device.

For the SpeedTouch™610 a set of MIBs is provided on the SpeedTouch™610 Setup CD-rom, some being identical to the standard MIBs, others specifically made for the SpeedTouch™610 functionality.

The available data covers statistics of the traffic through an interface, errors and setup information. For details of what information is available consult the MIB definitions at "4.2 SpeedTouchTM610 MIBs" on page 24.

Community Names

Reading MIBs is harmless - unless security parameters could be read (get) -, however, writing (set) can have severe consequences.

It is not possible to set any behavior changing objects using SNMP. If a malicious user were to have access to the SNMP interface he would not be able to cause any serious damage, although - potentially sensitive - statistical and set up information on the managed device could be learnt.

Therefore, SNMP offers a possibility to restrict access to sensitive MIBs by means of SNMP 'Community Names'.

To have specific kinds of access to these MIBs, the SNMP manager has to know the correct Community Name. A Community Name serves as password and authentication. On agent-side, a community name is associated with a specific MIB-view (which MIB objects can be seen by a manager using that community name) and an access policy (read-only or read-write).

By default, the SpeedTouch™610 uses the default SNMP Community names for read-only (public) and read-write (private). It is recommended however that the user should change the default community names thus improving security.

4.1 SpeedTouch™610 SNMP configuration

SNMP Configuration

There are a few settleable options covering the SNMP functionality. If no traps, spontaneous messages sent from the SpeedTouch™610 to a manager, are required then all of the default options will be sufficient to access information in the SpeedTouch™610 from the LAN.

All SNMP settings must be changed or viewed using the CLI.

By default the SpeedTouch™610 SNMP configuration is as follows:

```
=>snmp config

Read-write SNMP community name  :  private
Read-only  SNMP community name  :  public
SNMP System Contact     : Service Provider
SNMP System Name        : SpeedTouch 610
SNMP System Location    : Customer Premises
All SNMP traps  : DISABLED
Delay, in secs before first trap is sent        : 90
=>
```

The ": snmp config" command can also be used to change the following variables:

- Read only and read write community names.
- MIB II RFC1213 contains a number of fundamental read and writable objects called the system group. Some of these values can be set, they are system contact, system name, and system location.
- Traps can be enabled and disabled.
- The delay before the first trap is sent can be set. If traps are sent before the DSL connection is up or the connection session is connected, e.g. Routed PPP connections, they will be lost. Therefore a delay, set at a default of 90 seconds, before sending the first trap is observed. Changing this value may result in the first traps being lost.
- The SpeedTouch™610 buffers traps so that there is never a flood of messages sent to the manager which may worsen a faulty or congested connection. The minimum time between traps can be set to between 0 seconds (no gaps inbetween) and 60 seconds (default value).

If traps are required, the address of the SNMP manager must be specified. These can be added, up to nine different SNMP manager addresses, using the “:snmp trapadd” command. The IP address must be entered, and, if the port is different to the normal default, 162 port, a port number can be specified. The port number will very rarely need to be entered. Use “:snmp trapdelete” to delete such an entry.

The “:snmp get” command allows to Get, GetNext or Walk from a MIB’s object ID.

SNMP and the default SpeedTouch™610 Firewall

Towards the local network, no restrictions apply on behalf of the firewall rules. However, regarding the WAN, any traffic on destination UDP ports 161 (SNMP) and 162 (SNMP-trap) generated by the SpeedTouch™610 will be counted and logged to Syslog:

```
:firewall rule create chain=source index=6 prot=udp dstport=snmp
     log=yes action=count
:firewall rule create chain=source index=7 prot=udp dstport=snmptrap
     log=yes action=count
```

Any traffic arriving from the WAN sourced on UDP port 162 towards the SpeedTouch™610 is counted and logged as well:

```
:firewall rule create chain=sink index=6 prot=udp dstport=snmp
     log=yes action=count
```

Subsequently the SNMP packets are dropped by the drop-all rules of the firewall:

```
:firewall rule create chain=source index=8 action=drop
:firewall rule create chain=sink index=7 action=drop
```

Allowing remote SNMP

To allow a remote SNMP manager to monitor the SpeedTouch™610 you must add following firewall rules:

```
:firewall rule create chain=source index=7 prot=udp dstport=snmp
     action=accept
:firewall rule create chain=sink index=7 prot=udp dstport=snmp
     action=accept
```

To allow the remote SNMP manager to receive SNMP traps generated by the SpeedTouch™610, additional firewall rule must be added (next to enabling traps for the remote manager via a ":snmp trapadd"), assuming the default snmp trap UDP port (162) is used:

```
:firewall rule create chain=source index=9 prot=udp dstport=snmptrap
     action=accept
```

As a result, any WAN traffic coming from or going to the SpeedTouch™610 SNMP agent, will still be counted and logged to Syslog, but will be accepted.

Note As for all remote management methods the possibility exist to refine the firewall rules to restrict access to a certain range of, or a single IP address - optionally over a specific WAN interface.

4.2 SpeedTouch™610 MIBs

Introduction

As mentioned in " Management Information Base" on page 21 both the SpeedTouch™610 SNMP agent and the SNMP manager rely on Management Information Base (MIB) files containing all relevant SNMP objects.

In the following, all MIBs important for the SpeedTouch™610 are described. Additionally some of the most important and/or interesting SNMP counters are shortly highlighted.

Standard MIBs

Following MIBs are common standard MIBs that are relevant to monitoring the SpeedTouch™610. All MIB manager implementations should provide these MIBs by default. Therefore, these are not provided on the SpeedTouch™610 CD-rom.

- RFC1213 MIB-II
  MIB-II is defined by IETF Full Standard RFC1231 and is the foundational MIB for TCP/IP based Internets, describing objects available from devices which run the Internet suite of protocols. The MIB is fundamental to SNMP and is referenced by many other MIB modules.
  It contains management information and statistics on the IP, ICMP, TCP, and UDP protocols.
- RFC2863 IF-MIB
  The IF-MIB is an extension and replacement of the interface table in MIB-II. It contains statistics on the number of bytes and packets transported across the represented interfaces, including errors.

SpeedTouch™610 specific MIBs

Most of the following MIBs are commonly supported by most MIB manager implementations. Updated copies of the MIBs have been provided on the SpeedTouch™610 CD-rom. It is advised to load the copies provided on the CD-rom to your SNMP manager, instead of using the SNMP manager's provided MIBs.

- RFC1493 Bridge MIB
  The Bridge-MIB contains management information on the Bridge port(s). It contains statistics on, for example, alignment errors, collisions and MAC transition errors.
- IANAifType MIB
  This required MIB module is for adminitrational use by for the other MIBs only. It defines the IANAifType Textual Convention, and thus the enumerated values of the ifType object defined in MIB-II's ifTable.
- RFC2665 Ethernet-like MIB
  The Ethernet MIB contains management information on the Ethernet interface(s). It contains statistics on, for example, alignment errors, collisions and MAC transition errors.

ADSL and SHDSL MIBs

Following two MIBs are specific per SpeedTouch™610 variant (ADSL or SHDSL variants). You should only load the appropriate one, although loading both will not harm functionality. To retrieve maximum SNMP information it is imperative to use the MIB provided on the CD-rom, and not the one supported (if so) by the SNMP manager.

- RFC2662 ADSL MIB (containing ADSL-LINE-MIB and ADSL-TC-MIB)
  The ADSL MIB is in fact a bundle of three MIBs: the ADSL-LINE-MIB, the ADSL-TC-MIB and additionally the PerfHist-TC-MIB. It contains management information about the ADSL line such as Signal-to-Noise Ratio (SNR), output power and attainable bit rate.
- HDSL2-SHDSL-LINE MIB (containing SNMP-FRAMEWORK-MIB)
  The SHDSL MIB contains management information about the SHDSL line such as Signal-to-Noise Ratio (SNR), Loop attenuation, PSD regional setting, line rate and line status.

SpeedTouch™610 specific MIBs

Following MIBs are specifically designed for the SpeedTouch™610:

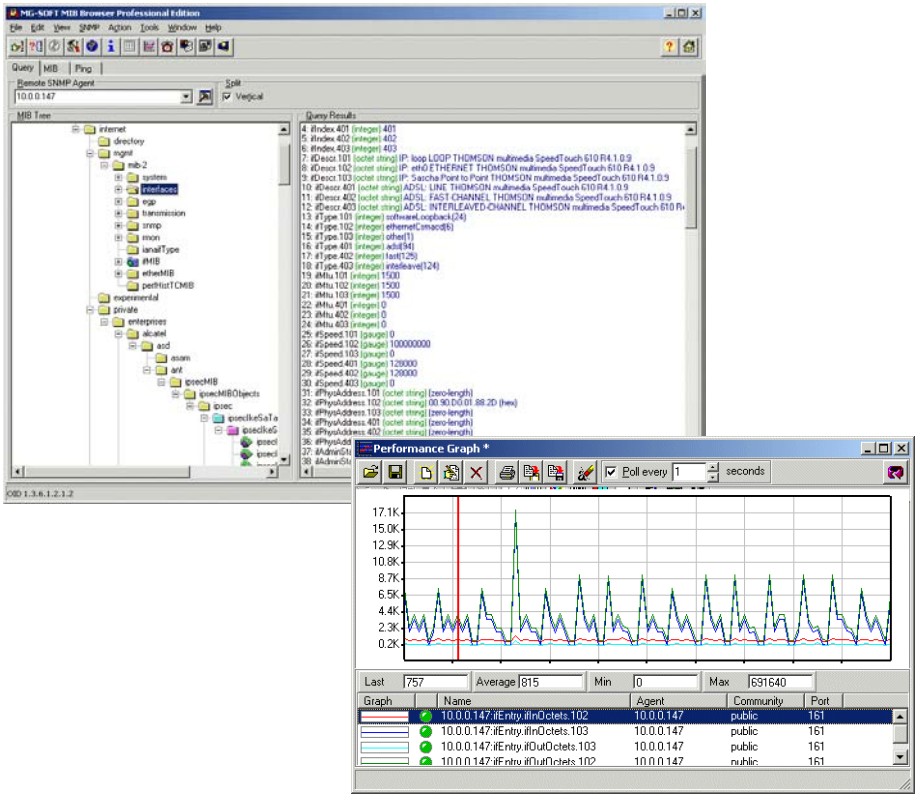
- System MIB (Enterprise specific branch MIB)
  This required MIB is for adminitrational use by the other MIBs only. It provides the object IDs (OID) from the SpeedTouch™610 specific MIBs and defines the Enterprise specific object identifier.
- IPSec MIB (Product specific)
  The SpeedTouch™610 specific IPSec MIB contains management information about the IPSec protocols (in case IP VPN IPSec functionality has been enabled via the appropriate SpeedTouch™610 software key). Details are given of Security associations, tunnel statistics and errors.

Example of MIB browsing

Using a MIB manager (sometimes equally referred to as MIB browser) network administrators are able to walk through MIB objects in order to view current of historical values of the managed device, and get or set specific values of MIB objects.

Many implementations of SNMP managers are available from the Internet. For the convenience of the user most of them provide GUI-driven MIB browsing and graphical tools for intuitive comprehension of MIB values. To be able to use the Enterprise specific MIBs, all MIB manager software includes a MIB compiler to compile the MIBs into a format readable for the manager.

In the following example the MGSoft MIB Browser is used to show an extract of SpeedTouch™610 relevant MIB object counters. This MIB browser can be obtained from http://www.mg-soft.com/:



www.speedtouch.com

600
SERIES

Built for excellence

speedtouch™
ALCATEL