SPEED TOUCH 570

User's Guide

3EC 17766 AAAA TCZZA Ed. 03

Status Released

Change Note BD F aa 33622

Short Title CD−UG AST570 1.0

Contents

1 Speed Touch Quick Guide 11
1.1 Get Acquainted with your Speed Touch 12
1.2 Speed Touch Installation 14
1.2.1 What you Need 15
1.2.2 AST570 Connections 16
1.2.3 Check your Service Provider's Offering 19
1.2.4 Select an AST570 Packet Service 20
1.2.5 Configure your AST570 (If Necessary) 21
1.2.6 Surf the Internet 22
1.2.7 Detailed AST570 Information 23
2 Wiring Guide – Wired LAN 27
2.1 LAN Cables 28
2.2 Connecting Ethernet 29
2.2.1 The Ethernet Port on your AST570 30
2.2.2 Single PC Ethernet Wiring 31
2.2.3 LAN Ethernet Wiring 32
3 Wiring Guide – DSL and Power 33
3.1 Locating Ports 34
3.2 Connecting the DSL Port 35
3.3 Connecting the Power Adapter 36
4 WLAN Guide – Wireless LAN 39
4.1 Wireless LAN Connectivity 40
4.1.1 Wireless Networking Basics 41
4.1.2 First-Time Wireless Client Connectivity 42
4.1.3 Connecting other Wireless Clients 44
4.2 Wireless Configuration 46
4.3 Wired Ethernet vs. Wireless Ethernet 53
5 Configuration and Use – Packet Services 57
5.1 Supported Packet Services 58
5.2 Packet Services at a Glance 59
5.3 Selection Criteria 62
6 Configuration and Use – Transparent Bridging 63
6.1 Preparatory Steps 64
6.2 Using Bridging 65
6.3 Bridging Configuration 66
6.4 Bridge Data 69

7 Configuration and Use – Routed Ethernet 71
7.1 Preparatory Steps 72
7.2 Using Routed Ethernet 73
7.3 Routed Ethernet Configuration 74
8 Configuration and Use – Bridged PPPoE 77
8.1 Preparatory Steps 78
8.2 Using Bridged PPPoE 79
8.3 Bridged PPPoE Configuration 80
9 Configuration and Use – Routed PPPoE 81
9.1 Preparatory Steps 82
9.2 Using Routed PPPoE 83
9.3 Routed PPPoE Configuration 85
9.4 Detailed Configuration 87
9.4.1 'PPPoE' Configurations 88
9.4.2 'Routing' Configurations 89
9.4.3 'Other' Configurations 90
9.4.4 'Stats' During a Routed PPPoE Session 91
10 Configuration and Use – Relayed PPPoA 93
10.1 Preparatory Steps 94
10.2 Using Relayed PPPoA 95
10.2.1 Preparing the PC for PPTP Tunneling 96
10.2.2 Using PPTP towards your AST570 97
10.3 Example : MS Windows 98 Dial-Up Networking 98
10.3.1 Create a New Dial-Up Networking Icon 99
10.3.2 Open a Dial-Up Session 102
10.3.3 Close a Dial-Up Session in Use 104
10.4 Relayed PPPoA Configuration 105
11 Configuration and Use – Routed PPPoA 109
11.1 Preparatory Steps 110
11.2 Using Routed PPPoA 111
11.3 Routed PPPoA Configuration 114
11.4 Detailed Configuration 118
11.4.1 'Routing' Configurations 119
11.4.2 'Other' Configurations 123
11.4.3 'Stats' During a Routed PPPoA Session 127
12 Configuration and Use – CIP & IP Routing 129
12.1 Preparatory Steps 130
12.2 CIP Configuration for a LIS 131
12.2.1 General CIP Configuration Procedure 132

12.2.2 Retrieving LIS Parameters 133
12.2.3 Implicit Assignment Mechanism 134
12.2.4 Explicit Assignment Mechanism 135
12.2.5 Configuring the AST570 for CIP 136
12.2.6 Adding Appropriate Routes to the Routing Tables 137
12.2.7 Example Configuration 139
12.3 Using CIP & IP Routing 141
12.4 CIP Configuration 142
13 Networking – ATM 149
13.1 The ATM Packet Switching Technology 150
13.1.1 ATM Parameters 151
13.1.2 ATM and the AST570 152
13.1.3 ATM and Interfaces 153
13.2 The Speed Touch Phonebook 154
13.2.1 The AST570 'Phonebook' Page 155
13.2.2 Using the Phonebook 159
13.2.3 AutoPVC and the Phonebook 161
14 Networking Services – IP 163
14.1 Speed Touch and IP 164
14.2 Packet Services and IP 166
14.2.1 Transparent Bridging 167
14.2.2 Relayed PPPoA 168
14.2.3 Routed Packet Services 169
14.3 Speed Touch Addresses 171
14.3.1 AST570 IP Address Types 172
14.3.2 Static IP Address Configuration 175
14.4 Speed Touch DHCP 178
14.4.1 AST570 DHCP Pages 179
14.4.2 The AST570 DHCP Server 180
14.4.3 The AST570 DHCP Client 185
14.5 Speed Touch Routing 188
14.5.1 The AST570 IP Router 189
14.5.2 Configuring the AST570 IP Routing Table 192
15 Networking Services – DNS 197
15.1 Speed Touch DNS Resolving 198
15.2 Configuring the Speed Touch DNS Server 200
16 Security Services – NAT & PAT 205
16.1 Speed Touch and NA(P)T 206
16.2 Packet Services and NA(P)T 207
16.3 The Speed Touch 'NAT' Page 211
16.4 NA(P)T Configuration Example 215

17 Security Services – Firewalling 217
17.1 Operation of the Firewall 218
17.2 Firewall Model 219
17.3 Firewall Actions 221
17.4 Firewall Criteria 222
17.5 Firewalling and NAPT 224
17.6 Firewall Configuration 225
17.7 Firewall Configuration Examples 226
18 Maintenance – Speed Touch Software 231
18.1 Software Upload from the local (W)LAN 232
18.2 Software Download from the DSL WAN 237
19 Maintenance – Speed Touch Password 239
20 Maintenance – Speed Touch To-Defaults 241
20.1 Ping-of-Life 242
20.2 Speed Touch Reset 245
20.2.1 Browse-to-Defaults 246
20.2.2 Ping-to-Defaults 247
20.2.3 Switch-to-Defaults 248
21 Maintenance – Speed Touch Web Interface 249
21.1 Web Interface Preconditions 250
21.1.1 Disabling Proxy Servers 251
21.1.2 Disabling Proxying for Local IP Addresses 252
21.2 Browsing to the Speed Touch Pages 253
21.3 Speed Touch Page Structure 254
22 Maintenance – Speed Touch CLI 257
22.1 CLI via the Speed Touch Pages 258
22.2 Native CLI Access 261
22.2.1 CLI through a Telnet Session 262
22.2.2 CLI Command Basics 264
Abbreviations 269
AppendixA Speed Touch Troubleshooting 273
AppendixB Wall Fixing Assembly 275
AppendixC Speed Touch Upcoming Features 277
AppendixD Speed Touch Specifications 279
AppendixE Speed Touch Default Assignments 289
AppendixF Safety and Agency Regulatory Notices 293

Alcatel Speed Touch™ 570

Introduction

The **Alcatel Speed Touch™570** Wireless ADSL router provides high-speed access to the Internet and Corporate networks for small office and fastidious home users and high-speed inter office LAN-to-LAN connections.

With the **Alcatel Speed Touch™570** Alcatel combines two cutting-edge technologies: DSL and the Wireless LAN (WLAN). With this answer to the increasing popularity of both technologies users can join your (Wireless) Local Area Network (LAN) and surf the Internet at high-speed without the need of any expensive wiring installation. For the safety of your data MAC-based filtering and encryption tools, and a physical authentication mechanism secure your WLAN from unauthorized access.

For optimal LAN and WLAN performance the **Alcatel Speed Touch™570** includes a comprehensive set of features, as there are a DHCP server, DNS server, NAT&PAT, CIDR and VLSM to name a few. On top, a programmable firewall allows you to shield your local network from the Wide Area Network (WAN) and to protect your resources from intruders.

Moreover, the **Alcatel Speed Touch™570** Wireless ADSL router is ready to be upgraded towards:

- Extended management: Simple Network Management Protocol (SNMP) and Syslog
- IP Virtual Private Network (VPN) based on IPSec Protocol Suite technology
- Routing Information Protocol (RIP) Routing Protocols.

Note: See appendix C for more information on these upcoming features.

Terminology

For readability, the **Alcatel Speed Touch™570** will be referred to as **AST570** in this User's Guide.

Safety instructions

Prior to connecting the **Alcatel Speed Touch™570**, read the Safety Instructions in appendix F.

CAUTION

WARNING

The following words and symbols mark special messages throughout this document:

WARNING: indicates that failure to follow the directions could cause bodily harm or loss of life.

CAUTION: indicates that failure to follow the directions could result in damage to equipment or loss of information.

Trademarks

The following trademarks are used in this document:

- Speed Touch™ is a trademark of the Alcatel Company
- Netscape® and Netscape Navigator® are registered trademarks of Netscape Communications Corporation
- Windows™ and Internet Explorer™ are trademarks of Microsoft Corporation
- Apple® and Mac®OS are registered trademarks of Apple Computer Inc.
- UNIX® is a registered trademark of UNIX System Laboratories, Inc.
- Ethernet™ is a trademark of Xerox Corporation.

Other products may be trademarks or registered trademarks of their respective manufacturers.

Service Provider

For readability, the term Service Provider (SP) will be used to designate all organizations which provide either DSL connectivity, Internet access or Corporate access, for example an Internet Service Provider (ISP).

PC, workstation, terminal, ...

For readability, PC will refer to all involved computer devices which are able to interact with the **AST570**, i.e. Personal Computer (PC), Portable PC (PPC), Macintosh computer, workstation, (remote) terminal, etc.

LAN, network, WLAN

For the **AST570** there is no difference between Wired LAN connectivity and Wireless LAN (WLAN) connectivity. Therefore, both will be referred to as (W)LAN.

Disclaimer

All examples throughout this User's Guide refer to :

- "Net 10" IP addresses for local network configurations
- VPI 0 or VPI 8 to identify the Virtual Path (VP) on the DSL line.

However, your SP might prefer other values.

User's Guide updates

Due to the continuous evolution of the Alcatel DSL technology, existing products are regularly upgraded. Alcatel documentation changes accordingly.

For more information on the newest technological changes and documents, please consult the Alcatel web site at following Uniform Resource Locator (URL):

http://www.alcatel.com

http://www.alcateldsl.com

1 Speed Touch Quick Guide

Aim of this Quick Guide

Use this chapter to quickly connect your **AST570** to the Internet.

In this chapter

Topic	See
Get Acquainted with your **AST570**	1.1
AST570 Installation	1.2

1.1 Get Acquainted with your Speed Touch

Delivery check

Check your **AST570** package for the following items:

- The **Alcatel Speed Touch™570**
- If applicable, 1 or 2 WLAN adapters with installation software
- 1 Power supply adapter with 2m (6.56ft.) connecting cable
- 2m Cat.5 straight-through Ethernet cable (RJ45/RJ45)
- 2m DSL cable (RJ11/RJ11, RJ14/RJ14)
- 1 Wall mounting assembly with Velcro sticker
- 2 Screws and 2 wall plugs for the wall mounting assembly
- This User's Guide, in hard copy format.

Damaged or missing items

In the event of damaged or missing items, contact your local product dealer for further instructions.

Other materials

Your **AST570** shipping carton may also include release notes, safety and conformity declarations and other materials.

Wall mounting

Part of the packaging is a wall mounting assembly with accompanying screws and wall plugs.

For instructions to prepare the **AST570** and wall mounting assembly for use, refer to appendix B.

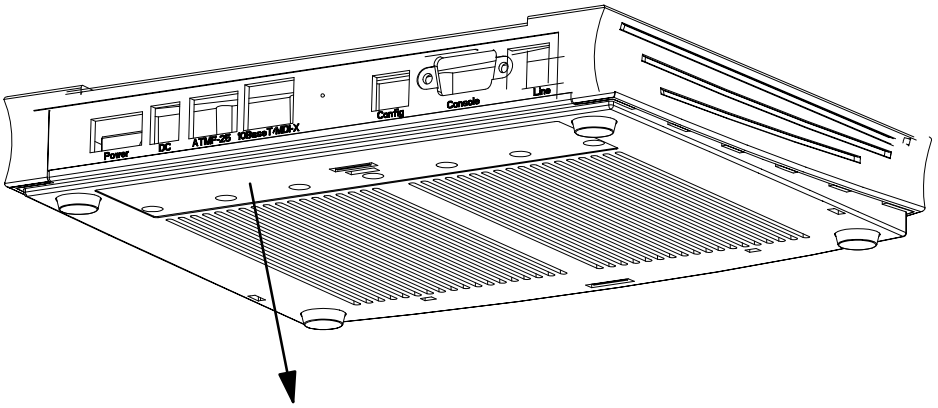
The AST570

The **AST570** is presented in a slim line box:

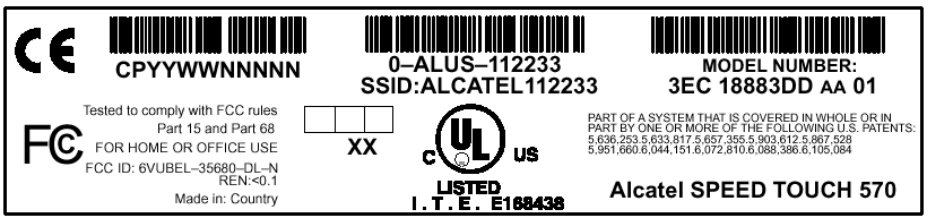
For detailed information, refer to appendix D.

Identify your AST570

You can identify your **AST570** via the marking label on the bottom:



The marking label for the North-American market is similar to the example below:



CAUTION

Marking Label Information

Do not remove the marking label from the bottom, nor cover it with another label.

Next to other important information, it contains the default SSID for your **AST570** WLAN configuration, needed for initial Wireless connectivity.

1.2 Speed Touch Installation

Aim of this section

Execution of the steps in this section will bring you on the Internet in no time.

In this section

Topic	See
What you Need	1.2.1
AST570 Connections	1.2.2
Check your SP's Service Offerings	1.2.3
Select an **AST570** Packet Service	1.2.4
Configure your **AST570** (If Necessary)	1.2.5
Surf the Internet	1.2.6
Detailed **AST570** Information	1.2.7

1.2.1 What you Need

DSL service

Asymmetric Digital Subscriber Line (ADSL) service must be enabled on your telephone line.

As both Plain Old Telephone Service (POTS) and ADSL service are simultaneously available from the same copper pair you need a central splitter or distributed filters for decoupling ADSL and telephone signals.

Contact your SP for more information.

Wireless networking

For WLAN connectivity:

- The (portable) PCs, intended to be connected via the **AST570** need a WLAN networking adapter (WLAN-NIC).

Each WLAN adapter must be:

- Compliant to 802.11b Direct Sequence Spread Spectrum (DSSS)
- WECA Wi-Fi certified to ensure smooth interoperability.

Wired networking

To use the Ethernet port you need at least:

- One PC with an Ethernet 10Base-T PC-Network Interface Card (NIC) installed
- For local networking, a 10Base-T hub and the necessary connection cables.

Accessing the AST570

For local configuration via HTTP/HTML, you need:

- A TCP/IP protocol suite
- A Web browser.

1.2.2 AST570 Connections

You must wire

- The Ethernet Port (10Base-T), if needed
- The DSL Port (Line)
- The Power Port (DC).

After performing these steps you can turn on your **AST570**. Proceed then with connecting:

- Your WLAN clients.

Ethernet port (10Base-T), if needed

Use the included LAN cable to wire your PC's Ethernet port to **AST570**' Ethernet interface.

Note: In case no wired Ethernet connections have to be made, you can omit this step and continue with wiring the DSL port.

Refer to section 2.2 for more information.

DSL port (Line)

Use the included DSL cable to wire the **AST570**' Line port to your DSL wall outlet.

Refer to section 3.2 for more information.

Power port (DC)

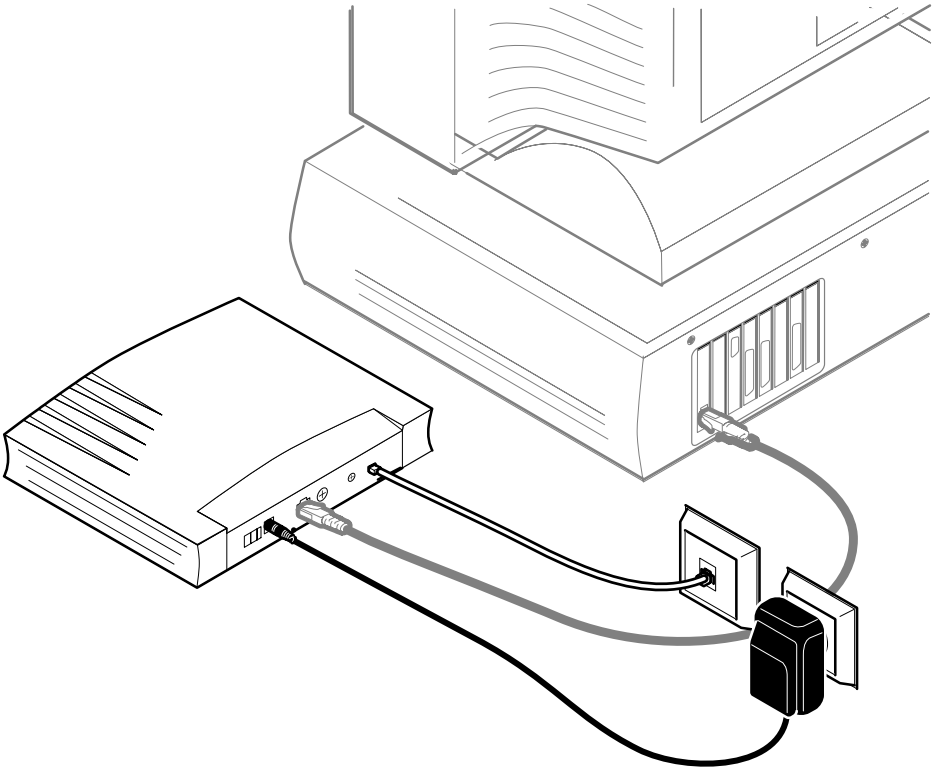
Firstly check whether the included mains adapter suits the local power specifications. If you are not sure of the regional power conditions, check the adapter's specifications in section D.5 and contact your local power company.

Plug the adapter's coaxial jack into the **AST570**' receptacle marked 'DC'.

Refer to section 3.3 for more information.

Check your wiring

Once all connections are made the result should look similar as below:



The grey shaded wired Ethernet connection only implies in case the Ethernet port is used for connecting a PC.

Turn on your AST570

Once all previous steps are completed, turn on your **AST570**.

The **AST570** is ready for service as soon as the start-up procedures are completed, the Power On Self Test (POST) is passed and both *Power/Alarm* and *Line Sync* LEDs on the front panel are constantly lit green.

Refer to section D.2 for more information.

Connecting WLAN clients

- **Preconditions**:

  Make sure your **AST570** is turned on and finished its Power On Self Test (POST).

  The (portable) PCs, intended to be connected to the **AST570**, must have a WLAN adapter readily installed and should be configured as DHCP client or configured with a fixed "Net10" IP address.

- **Joining the AST570 WLAN network**

  Some WLAN adapters are able to detect the presence of the **AST570** Wireless network. For others you have to preset the SSID.

  When first using the **AST570**:

  1. On the WLAN adapter configure the **Service Set ID (SSID)** with the **AST570** default SSID printed on the marking label, found on the bottom of the **AST570**.

     This default SSID exists of the word "Alcatel" followed by (directly concatenated) the 6 last characters of the **AST570** WLAN access point MAC address.

  2. To register the WLAN client, push the *'Association'* button on the **AST570**' back panel while the WLAN adapter tries to join the **AST570** WLAN network.

  3. Repeat this procedure for each (portable) PC you want to associate the **AST570** WLAN network.

See chapter 4 for more information.

Note There is no difference between wired and wireless LAN connections for the **AST570**, i.e. all network configurations are equally valid for both.

Therefore, both are referred to as (W)LAN.

1.2.3 Check your Service Provider's Offering

Service Offering

The SP provides at least the following information:

- The ***VPI/VCI*** of the Virtual Channel (VC) to use on the DSL line
- The ***Connection Service*** supported on this VC
- The ***Encapsulation Method*** (if different from the Connection Service's default encapsulation).

Example:

- VPI/VCI = 0/35
- Connection Service = ETHoA (RFC1483/Br)
- Encapsulation Method : ETHoA default, i.e. LLC/SNAP.

Your **AST570** supports multiple simultaneous VCs on the DSL line. If your SP exploits this capability, he will provide this information *per* VC.

Default AST570 VPI/VCI settings

The VPI/VCI value of the default configured VCs are listed in Appendix E.

In the event that the provided VPI/VCI differ with the **AST570** defaults, you can change VC settings via the **AST570** pages.

See section 13.2 for more information.

1.2.4 Select an AST570 Packet Service

Connection service

As soon as you know the Connection Service on a VC, you can attach a Packet Service to it.

Following combinations are possible:

Connection Service	Protocol(s)	Packet Service
ETHoA	RFC1483 Bridging	Transparent Bridging
		Routed Ethernet
		Bridged PPPoE (*)
		Routed PPPoE
PPPoA	RFC2364	Relayed PPPoA (**)
		Routed PPPoA
		PPP-to-DHCP Spoofing
IPoA	RFC1483 Routing RFC1577/RFC2225 CIP	CIP & IP Routing

(*) A PPPoE Client application must be installed on your PC.
(**) A PPTP Dial-Up application must be installed on your PC.

Selection criteria

For more information on the criteria to prefer one Packet Service over the other, see chapter 5.

1.2.5 Configure your AST570 (If Necessary)

AST570 access

In most cases your **AST570** provides instant Internet connectivity as it features well chosen defaults

In exceptional cases additional or advanced configurations are desired, the **AST570** offers various access methods:

- Its Web interface (See chapter 21)
- The Command Line Interface (See chapter 22).

AST570 configuration

Configure the **AST570** via its web interface.

Most **AST570** topics have a dedicated page, e.g. for Bridging, PPP, CIP, NAT, DHCP, Wireless etc. Context related Help pages provide detailed information.

For profound configurations use the Command Line Interface (CLI).

1.2.6 Surf the Internet

Finishing setup

After wiring, joining the wireless network (and optionally configuring) the **AST570**, you are ready to surf the Internet.

Access methods

Depending on the selected packet service(s), there is:

- Always-On Access
- Dial-In Access.

Always-on access

With *Transparent Bridging, Routed Ethernet* and *CIP & IP Routing*, no connection procedure is needed. Turn on the **AST570** and you are online.

Note: Although no access procedure is needed, some SPs require authentication before granting accesss to their resources.

Dial-in access

A main feature of the **AST570** is support for traditional Dial-in connectivity to a Remote Access Server (RAS) via its *Bridged PPPoE, Routed PPPoE, Relayed PPPoA* and *Routed PPPoA* packet services.

Manually establish a connection via the **AST570** pages or via Operating System (OS) dependent dial-in applications.

Most dial-in procedures require a user name and password for identification and authentication.

1.2.7 Detailed AST570 Information

The AST570 is more than "just" a WLAN DSL router

Use the following parts to explore **AST570**' advanced features:

Alcatel Speed Touch™ Quick Guide	1

Alcatel Speed Touch™ Wiring Guide	
Wired LAN	2
DSL and Power	3

Alcatel Speed Touch™ WLAN Guide	
Wireless LAN	4

Alcatel Speed Touch™ Configuration and Use	
Packet Services	5
Transparent Bridging	6
Routed Ethernet	7
Bridged PPPoE	8
Routed PPPoE	9
Relayed PPPoA	10
Routed PPPoA	11
CIP & IP Routing	12

Alcatel Speed Touch™ Networking	
ATM	13
IP	14
DNS	15

Alcatel Speed Touch™ Security	
NAT & PAT	16
Firewalling	17

Alcatel Speed Touch™ Maintenance	
Alcatel Speed Touch™ Software	18
Alcatel Speed Touch™ Password	19
Alcatel Speed Touch™ To-Defaults	20
Alcatel Speed Touch™ Web Interface	21
Alcatel Speed Touch™ CLI	22

Alcatel Speed Touch™ Appendices	
Abbreviations	
Alcatel Speed Touch™ Troubleshooting	A
Alcatel Speed Touch™ Wall Fixing Assembly	B
Alcatel Speed Touch™ Upcoming Features	C
Alcatel Speed Touch™ Specifications	D
Alcatel Speed Touch™ Default Assignments	E
Alcatel Speed Touch™ Safety and Regulatory Notices	F

Alcatel
Speed Touch™570

Wiring Guide

2 Wiring Guide – Wired LAN

Introduction

To allow the **AST570** to be used as an extension of a traditional wired networking environment it features a 10Base-T MDI-X Ethernet port on the back panel.

This chapter will guide you through the wiring of the **AST570** Ethernet port.

Note: In case your complete network is wireless you can omit this chapter.

In this chapter

Topic	See
LAN Cables	2.1
Connecting Ethernet	2.2

2.1 LAN Cables

Included LAN cable

In your **AST570** package, a full wired straight-through RJ45/RJ45 cable, further referred to as LAN cable is included.

Using LAN cables

You can use *LAN cables* other than the one provided in the box, e.g. crossover LAN cables. However, make sure that these have the correct layout.

See section D.6 for more information on how to identify straight-through and crossover LAN cables.

LAN cable types vs. port types

Determine the LAN cable type from the following table:

Speed Touch™	Other equipment	Type of LAN cable	Symbol
MDI-X	MDI-X	Crossover	
	MDI	Straight-through	

Equipment and ports

The **AST570** Ethernet port is of type MDI-X.

PC Ethernet ports are always of type MDI.

Ethernet hub ports are of type MDI-X.

Note: You may use the (switchable) “uplink” or “cascade” MDI port which is sometimes present on Ethernet hubs. However, make sure to use the correct cable type.

2.2 Connecting Ethernet

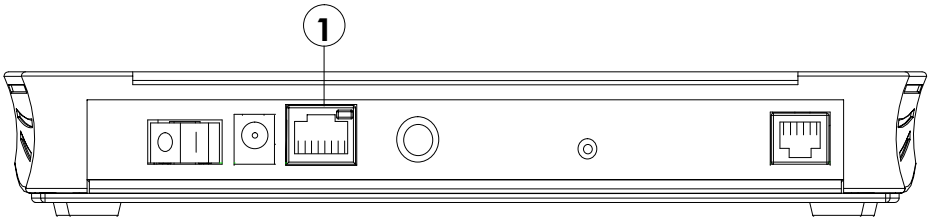
In this section

Topic	See
The Ethernet Port on your **AST570**	2.2.1
Single PC Ethernet Wiring	2.2.2
LAN Ethernet Wiring	2.2.2

2.2.1 The Ethernet Port on your AST570

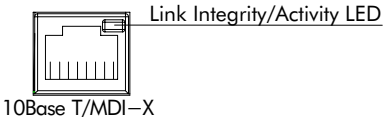
Ethernet interfaces

The **AST570** Ethernet port (1) is a 10Base-T *Half Duplex* Ethernet interface of type MDI-X:



Ethernet port LED

The Ethernet port on the back panel has a LED:



Indicator			Description
Name	**Color**	**State**	
Integrity **Activity**	Green	Off	No connection on the Ethernet port.
		On	Ethernet link up. No activity on the Ethernet port.
		Flashing	Data is flowing from/to the Ethernet port.

If the **AST570** and other wired LAN device(s) are properly connected and powered on, the green LED lights up.

CAUTION

10Base-T Half Duplex Interfacing

Make sure the 10Base-T port(s) of your PC(s) are configured for either Auto Negotiation or Half Duplex.

Never configure the 10Base-T Ports for Full-Duplex !

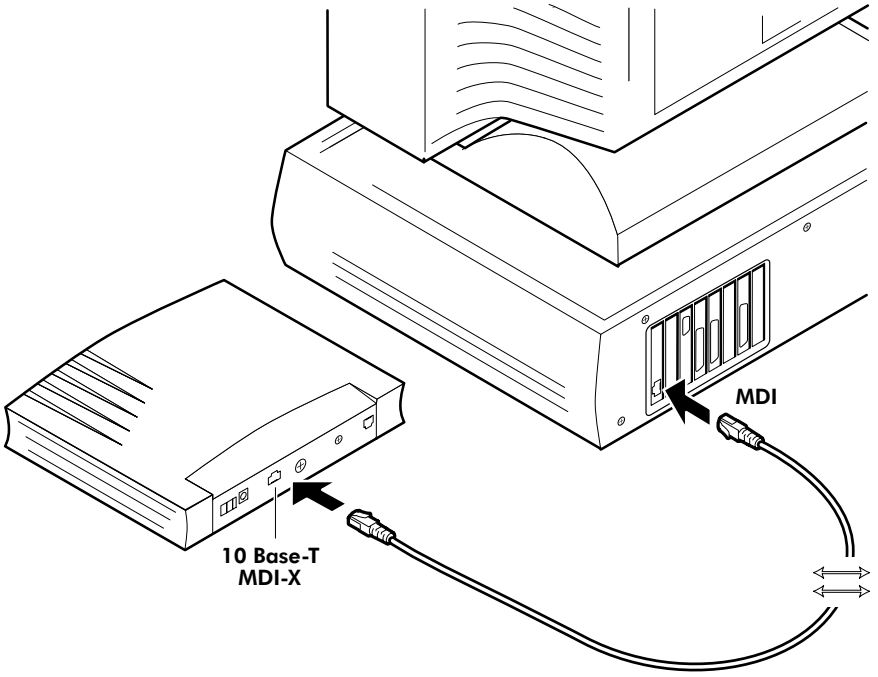
2.2.2 Single PC Ethernet Wiring

Single PC configuration

In this configuration the **AST570** is connected to a single PC. Your wired "LAN" consists of only one PC and the **AST570**.

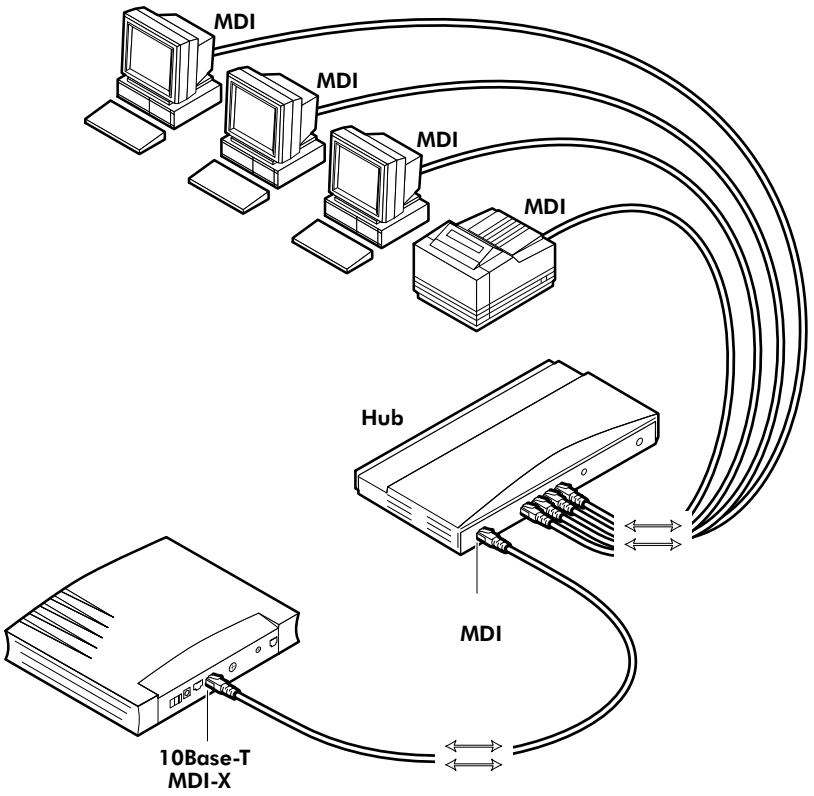
Procedure

Proceed as indicated in the following figure to connect your **AST570** to a single PC:



2.2.3 LAN Ethernet Wiring

Procedure Proceed as indicated in the following figure to make the connections for a LAN:



CAUTION

Cascading Repeating Hubs

You may cascade up to four repeating hubs in your LAN (limitations of Repeating Ethernet V2.0/IEEE802.3 hubs). In case more hubs need to be cascaded, you must use switching hubs.

MDI vs. MDI-X hub ports and the AST570

In the above figure the MDI "uplink" port on the hub connects to the **AST570**. Therefore, a straight-through LAN cable can be used, e.g. the one included in the **AST570** package.

Note: In case a hub's MDI-X port is used to wire the **AST570** you must use a crossover LAN cable.

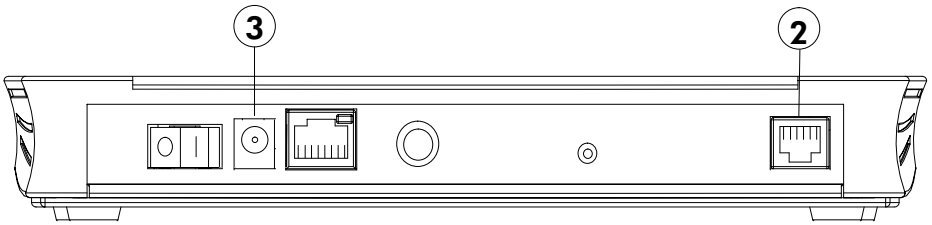
3 Wiring Guide – DSL and Power

In this chapter

Topic	See
Locating Ports	3.1
Connecting the DSL Port	3.2
Connecting the Power Adapter	3.3

3.1 Locating Ports

Port description



Following ports are used:

- (2): *DSL line port*, marked “LINE”
- (3): *Power socket*, market “DC”.

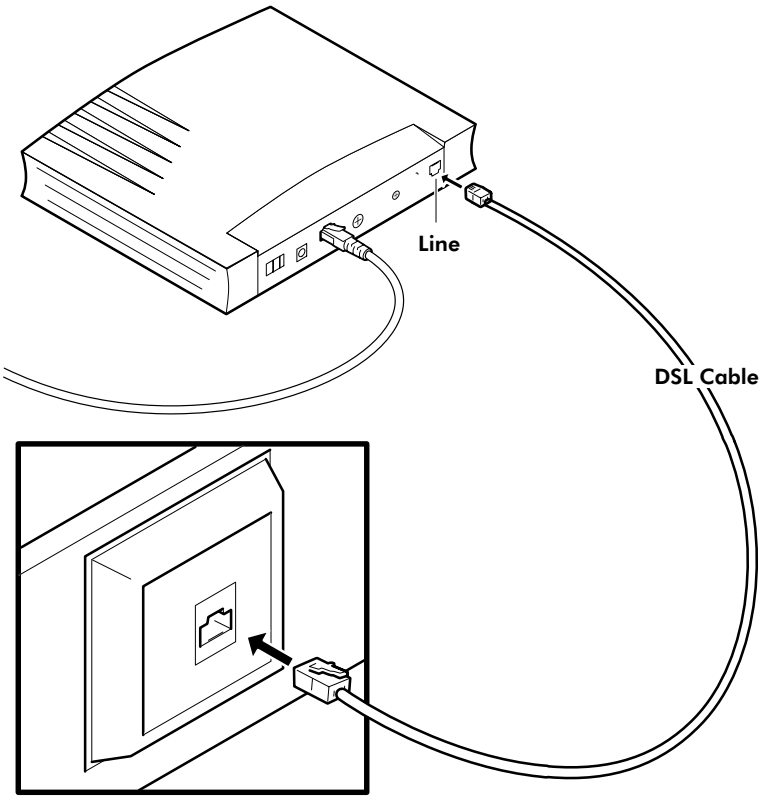
3.2 Connecting the DSL Port

Preconditions prior to connecting

A **central splitter** or **distributed filters** for decoupling DSL and POTS signals must be installed on your telephone line or telephone wall outlets. In some cases crossover adapters might be required.

Procedure

Proceed as indicated in the following figure to connect the **AST570** to the DSL line using the included black DSL cable:



3.3 Connecting the Power Adapter

Introduction

The **AST570** is delivered with a modular external power adapter converting the AC mains to $9V_{DC}$/1A unregulated output voltage.

Power adapter types

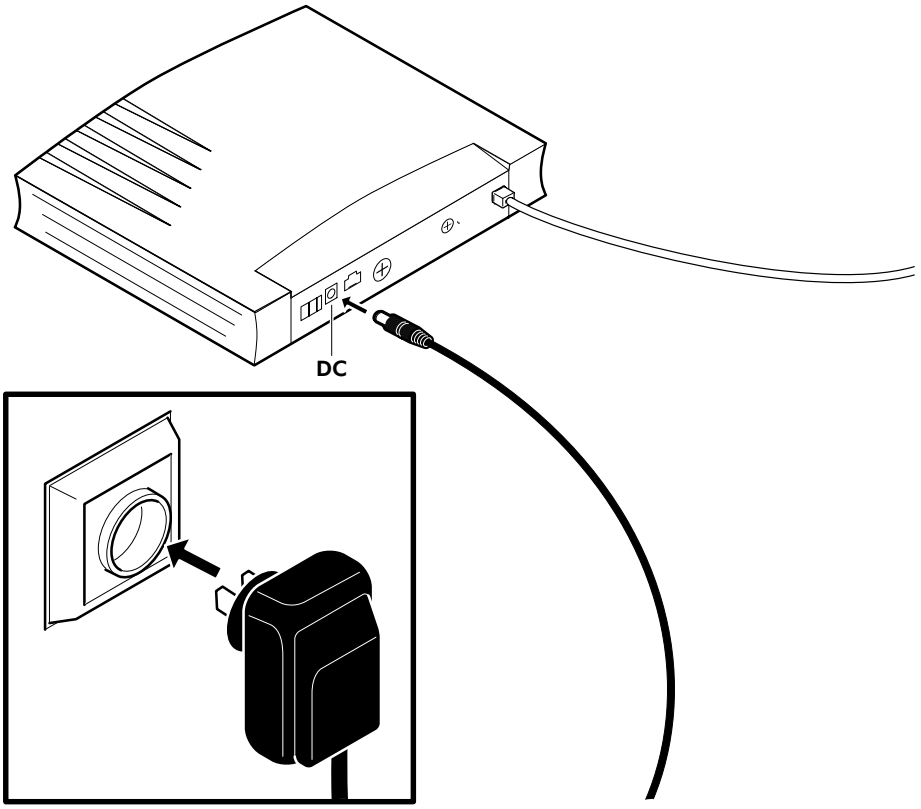
Check if the power adapter included in the **AST570** package is compatible with your local electrical power specifications.

See section D.5 for connector layout and output specifications.

If you are not sure of the specifications of your local mains power, contact your local product dealer for more information.

Procedure

Proceed as follows to connect the power supply adapter :



Alcatel
Speed Touch™570

WLAN Guide

4 WLAN Guide – Wireless LAN

In this chapter

Topic	See
Wireless LAN Connectivity	4.1
Wireless LAN Configuration	4.2
Wired LAN vs. Wireless LAN	4.3

4.1 Wireless LAN Connectivity

Introduction

Next to the single Ethernet port, enabling wired LAN connectivity, the **AST570** contains a Wireless LAN (WLAN) Access Point.

This WLAN Access Point behaves as a hub and allows wireless connectivity of several devices to the local (W)LAN and – via the **AST570** DSL router – to the public network, e.g. the Internet.

The same technology enables these devices to communicate with each other in a locally mobile fashion, without the need of a wired environment.

In this section

Topic	See
Wireless Networking Basics	4.1.1
First-Time Wireless Client Connectivity	4.1.2
Connecting other Wireless Clients	4.1.3

4.1.1 Wireless Networking Basics

The wireless network

The WLAN's 'radio' link is a shared medium. A wireless Access Point like the **AST570**, can be seen as a hub between WLAN clients. As no physical connection exists between the **AST570** and these clients, you must name your **AST570**' WLAN network. This is done by the Service Set ID (SSID). WLAN clients must be part of this SSID environment in order to be able to communicate with other clients of the (W)LAN – including the **AST570**.

The IEEE802.11b standard for WLANs allows for several WLAN networks using different radio channels to be co-located. Several channels are available for use which are associated to a slightly different frequency in the allowed range. The **AST570** supports operation on all allowed channels.

Wireless client requirements

Only WLAN client adapters compliant to IEEE802.11b DSSS, will be able to communicate with the **AST570**, and hence, with other members of the **AST570** WLAN environment.

It is advisable that the WLAN client adapter is Wireless Ethernet Compatibility Alliance (WECA) Wi-Fi™ (*) certified to ensure smooth interoperability.

(*) Wireless Fidelity (Wi-Fi)

4.1.2 First-Time Wireless Client Connectivity

Initial AST570 configuration

When the **AST570** leaves the factory and after every Ping-to-Defaults or Push-to-Defaults, the **AST570** Wireless configuration returns to its initial default settings.

These settings are as follows:

- **Service Set ID (SSID)**

  The default SSID is printed on the marking label which can be found on the bottom of your **AST570**. This unique SSID exists of the word "Alcatel" followed by (directly concatenated) the 6 last characters of the **AST570** WLAN access point MAC address.

- **Direct Sequence Spread Spectrum (DSSS) channel number**

  The channel number possible values are dependent of the regulatory domain where you purchased the **AST570** (FCC 1 to 11 and ETSI 1 to 13). By default the **AST570** DSSS channel number is 11.

- **Wired Equivalent Privacy (WEP) Algorithm**

  WEP encryption is by default turned OFF.

- **WLAN Client Access Control**

  Access Control is by default turned ON.

Therefore, the WLAN client must be appropriately configured and authenticated for initial Wireless connectivity to the **AST570** WLAN environment.

Preconditions

Make sure that:

- Your **AST570** is powered on and finished its POST
- The WLAN adapter is readily installed on your PC
- The PC's WLAN adapter is configured as DHCP client or has a fixed "Net 10" IP address
- The WLAN adapter is correctly configured for the default **AST570** SSID.

Connecting First-time WLAN client

Proceed as follows:

1. Make sure that all preconditions mentioned above are met.
2. On the WLAN adapter configure the SSID with the default **AST570** SSID.

   Note: The **AST570** allows also WLAN clients configured with an empty SSID to associate.
3. To register the WLAN client, push the *'Association'* button on the **AST570**' back panel while the WLAN adapter tries to join the **AST570** WLAN network.
4. Make sure that the WLAN client is correctly associated. Depending on your WLAN adapter the following message could pop up:

   "Successfully joined Wireless network Alcatel012345."

   Note: In fact this step allows your WLAN to be secure: without the physical authentication, i.e. pushing the *'Association'* button, while your WLAN client tries to join your WLAN, no connectivity will be enabled between the WLAN client and the **AST570** WLAN.
5. You should now be able to contact the **AST570**, e.g. by pinging 10.0.0.138 or by browsing to the **AST570** pages.

Configuration of your WLAN network

As soon as you have initial connectivity with the **AST570** you are able to configure the **AST570** WLAN parameters via its *'Wireless'* page.

Reconfiguration of your WLAN parameters is useful for securing your WLAN environment from possible WLAN client access by others.

See section 4.2 for more information on **AST570**' WLAN configuration.

Note: After reconfiguring the **AST570** WLAN parameters, Wireless contact may be lost and WLAN clients might need reconfiguration and re-authentication to rejoin **AST570**' WLAN environment.

4.1.3 Connecting other Wireless Clients

AST570 and WLAN client configuration

In the case you reconfigured the **AST570** WLAN parameters via the *'Wireless'* page, the joining procedure for WLAN client to **AST570**' WLAN might be different from the first-time joining procedure, explained in subsection 4.1.2.

The following parameters could influence the way how to allow WLAN clients to join the **AST570** WLAN:

- The **AST570** DHCP Server configuration
- The configured SSID
- Whether WEP encryption is used or not
- Whether the Association Control mechanism is used or not.

See section 4.2 for more information on these configuration possibilities.

Procedure

1. Make sure the **AST570** is turned on and finished its POST.
2. Make sure you have all needed information:
   - The SSID
   - In case of WEP encryption, the 40-bits WEP key

     Note: If the WEP encryption is enabled on the **AST570**, it is necessary to configure the same WEP key on the WLAN adapter in order to be able to access the **AST570** WLAN.
3. On the WLAN adapter configure the SSID as configured on the **AST570** *'Wireless'* page.

   Note: This could be the default **AST570** SSID.
4. In case **AST570**' Association Control is enabled, you must press the *'Association'* button on the back panel of the **AST570** or click Associate on the *'Wireless'* page (via an authenticated WLAN client or a wired Ethernet connection).
5. Make sure that the WLAN client is correctly associated. Depending on your WLAN adapter the following message could pop up:

   "Successfully joined Wireless network Alcatel012345."

   Note: In fact this step allows your WLAN to be secure: without the physical authentication, i.e. pushing the (virtual) *'Association'* button, while your WLAN client tries to join your WLAN, no connectivity will be enabled between the WLAN client and the **AST570** WLAN.
6. You should now be able to contact the **AST570**, e.g. by pinging its IP address (per default 10.0.0.138) or by browsing to the **AST570** pages.

4.2 Wireless Configuration

Introduction

After having initial WLAN connectivity, you can configure your **AST570** WLAN parameters via the *'Wireless'* page.

Additional configuration of your WLAN network settings might be required in case, e.g. another Access Point with a similar WLAN configuration is located nearby.

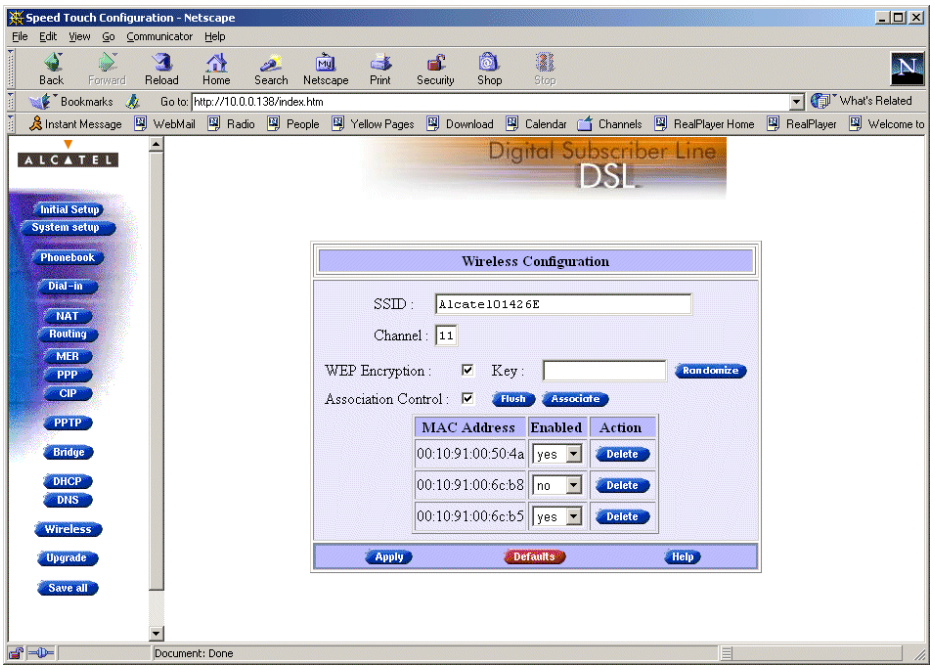
The *'Wireless'* page allows also to configure WEP encryption and Association Control for security and privacy of your WLAN network.

In this section

- The **AST570** *'Wireless'* Page
- The *'Wireless Configuration'* Table
- *'Wireless Configuration'* Table Components
- Configuring Wireless LAN Parameters
- Configuring WEP Encryption
- Configuring the Association Control Mechanism
- The *'Access Control'* Table
- Allowing or Rejecting a WLAN Client
- Removing a WLAN Client from the *'Access Control'* Table
- Resetting the Wireless LAN Configuration.

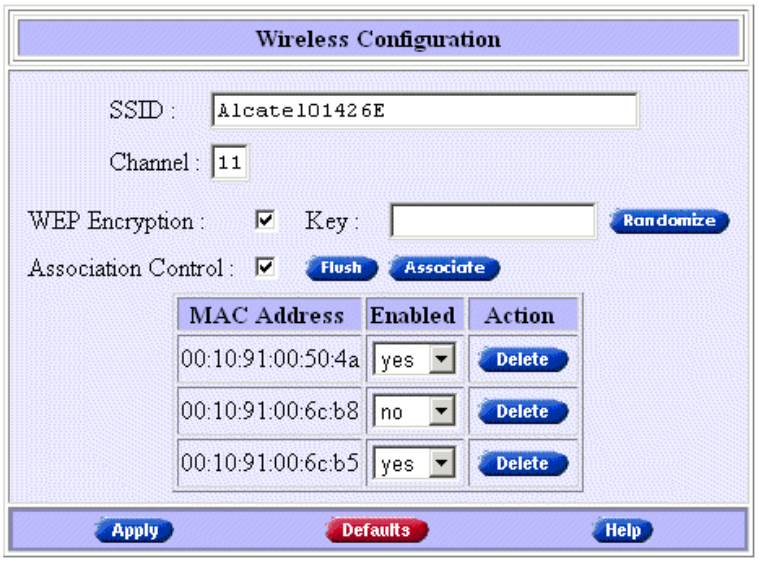
The 'Wireless' page

Click Wireless in the left pane of the **AST570** pages to pop up the *'Wireless'* page (See section 21.2 for more information):



The 'Wireless Configuration' table

The following figure shows the *'Wireless Configuration'* table:



'Wireless Configuration' table components

Field	Description
SSID	The Service Set ID (SSID) allows you to uniquely identify your **AST570** WLAN in the radio environment. This can be useful in case multiple WLAN networks are present nearby your location. The default **AST570** SSID is printed on the marking label found on the bottom of your **AST570**. It consists of the word "Alcatel" followed by (directly concatenated) the last six characters of the **AST570**' Access Point MAC address.
Channel	The Direct Sequence Spread Spectrum (DSSS) channel number is an identifier for the frequency on which your WLAN connectivity is enabled in the WLAN network. Changing the default channel number to another value can be useful in case you know another wireless equipment runs nearby yours, e.g. another **AST570** WLAN network. This way you can avoid sharing the channel bandwidth with other WLANs by selecting different channel numbers for concurrent WLANs. Although the configurable DSSS channel number range is from 1 up to 13, restrictions apply depending on the country where the **AST570** is used: • FCC: channels 1 to 11 • ETSI: channels 1 to 13
WEP Encryption	This checkbox allows you to enable (✓) or disable the Wired Equivalent Privacy (WEP) encryption mechanism the **AST570** provides for privacy, i.e. encryption of all wireless frames migrating from or towards the **AST570** access point.
Key	Allows to enter manually a fixed 40-bits WEP key (in hexadecimal notation) or will show the generated 40-bits WEP key after clicking Randomize Before proceeding you must write down the entered or generated key and keep the information on a save place. Clicking Apply applies the key and will hide it, i.e. the '*Key*' field is filled with a random amount of asterisks. You can NEVER retrieve the 40-bits WEP key from the **AST570** once you have applied it !
Association Control	This checkbox allows you to enable (✓) or disable association control of WLAN client adapter based on their MAC address. Next to WEP encryption which provides privacy for each WLAN client, the Association Control mechanism controls the authorization of WLAN clients to join the **AST570** WLAN. Via the '*Access Control*' table you can allow or reject WLAN adapters.

Configuring Wireless LAN parameters

Proceed as follows:

1. Browse to the *'Wireless'* page.
2. Enter an SSID of your choice to identify your WLAN. Make sure not to use a name which already exists in your WLAN environment neighborhood.
3. Enter a DSSS channel number for your WLAN radio environment. Preferably use a channel which is not occupied by another WLAN in your neighborhood.
4. Click Apply to save your changes and finish the procedure.

   Note: You do not need to click Save all to save changes. This button has no effect on the Wireless LAN configuration.

Configuring WEP encryption

Proceed as follows:

1. Browse to the *'Wireless'* page.
2. The 40-bits WEP key can be:
   - Generated by the **AST570**. Therefor, click Randomize
   - Manually configured by yourself in the *'Key'* field.

     Enter the key in hexadecimal notation, e.g. **`1a:2c:3e:4f:05`**.
3. Write down this WEP key and keep it on a save place. You will need this key to allow future WLAN clients to join the WLAN.

   Note: It is advisable to change the WEP key regularly for enhanced security.
4. Click Apply. As a result the *'Key'* field is filled with a random number of asterisks, the *'WEP Encryption'* checkbox is checked and previous WLAN connectivity lost.
5. Activate the WEP on your WLAN client by configuring the same 40-bits WEP key.
6. Verify connectivity of the WLAN clients by letting them browse to the **AST570** pages.

Configuring the Association control mechanism

Proceed as follows:

1. Browse to the *'Wireless'* page.
2. Association Control is by default enabled. The *'Access Control'* table lists all associated WLAN clients: authorized clients (Enabled column states *'Yes'*) as well as non-authorized clients (Enabled column states *'No'*).
3. Via the *'Association Control'* checkbox you can:
   - Enable the Association Control mechanism by checking (✓) the box
   - Disable the Association Control mechanism by clearing the box.
4. Click Apply .In case of enabling the Association Control mechanism previous WLAN connectivity might be temporary lost.
5. Verify connectivity of the WLAN clients by letting them browse to the **AST570** pages.

The 'Access Control' table

In case the Association Control mechanism is disabled, the *'Access Control'* table lists all currently joined WLAN client adapters.

In case MAC filtering is enabled, it lists all WLAN client adapters which are authorized to traffic the WLAN as well as the WLAN client adapters which are not allowed to join the WLAN:

MAC Address	Enabled	Action
0:10:91:0:6e:1e	yes	Delete
0:90:4b:0:6a:e2	no	Delete

In the example above the WLAN client adapter with MAC address **`00:10:91:00:6e:1e`** is authorized to join, the WLAN adapter with MAC address **`00:90:4b:00:6a:e2`** is not.

Allowing and rejecting a WLAN client

To enable future association for a currently joined WLAN client:

1. In the *'Access Control'* table select the authorization status **Yes** for the WLAN client from the *'Enabled'* pop-down list next to the WLAN client adapter's MAC address.

   Future joining will be allowed for this client without the need of using the *'Associate'* button every time

2. Click Apply to finish the procedure.

To reject a WLAN client, listed in the *'Access Control'* table:

1. Select the authorization status **No** for the WLAN client from the *'Enabled'* pop-down list next to the WLAN client adapter's MAC address.

   A rejected WLAN client will never be allowed to traffic the **AST570** WLAN network, even when Associate is clicked or the *'Association'* button is pressed.

2. Click Apply to finish the procedure.

Removing a WLAN client from the 'Access Control' list

To remove a WLAN client from the list you click Delete next to the WLAN client adapter's MAC address you want to delete the authorization for.

As a result the WLAN client is removed from the *'Access Control'* list. It is not able to traffic the **AST570** WLAN anymore. To re-join, you must click Associate again or press the *'Association'* button.

Removing a WLAN client from the *'Access Control'* table is not advised in case future joining of this client is not desired, as in this case a future re-association might be possible in case Associate is clicked or the *'Association'* button is pressed. Rather disable future association possibilities by rejecting the WLAN client.

Note: You can also flush the complete *'Access Control'* list, i.e. delete all joined WLAN clients. Therefor, click Flush.

Resetting the Wireless configuration

To reset all **AST570** Wireless settings and return to the factory default WLAN configuration, proceed as follows:

1. Browse to the *'Wireless'* page.
2. If you are sure to reset the **AST570** WLAN configuration, click Defaults.
3. The **AST570** will ask to confirm the reset:

4. Click OK if you are sure. Otherwise click Cancel. All WLAN parameters are reset to their factory default. Therefore, WLAN connectivity will be lost.
5. If you previously changed the **AST570** SSID, you must configure the WLAN adapter(s) SSID with the default **AST570** SSID.
6. Re-authenticate the WLAN client(s), using the *'Association'* button.
7. Verify connectivity of your WLAN client(s), e.g. by pinging the **AST570** IP address.

4.3 Wired Ethernet vs. Wireless Ethernet

Wireless vs. Wired LANs

The **AST570** makes no difference between wired Ethernet and joined WLAN clients. All connected PCs, whether these are connected via the **AST570** Ethernet port or connected via joining the WLAN SSID, share the same (sub)network. All are equally valid.

AST570 network configurations

The **AST570** allows local network management via:

- An IP router (See section 14.5)
- A DHCP server (See section 14.4)
- A DNS server (See chapter 15)
- NAPT abilities (See chapter 16)
- A programmable Firewall (See chapter 17)

All **AST570** configurations for these management tools, are equally valid for both wired Ethernet clients and WLAN clients upon configuration.

AST570 ADSL configurations

All **AST570** configurations for DSL connectivity, are equally valid for both wired Ethernet clients and joined WLAN clients upon configuration.

AST570 configuration examples

This User's Guide contains numerous examples and exemplary figures.

For clarity, all network connections, i.e. both wired Ethernet and WLAN client connections, are visualized as if all were wired.

Alcatel
Speed Touch™570

Configuration and Use

5 Configuration and Use – Packet Services

In this chapter

Topic	See
Supported Packet Services	5.1
Packet Services at a Glance	5.2
Selection Criteria	5.3

5.1 Supported Packet Services

What is a packet service ?

*Packet services are the core functions of the **AST570**. They provide that frames or packets get forwarded from the LAN side towards the DSL line and vice versa.*

Seven packet services

- Transparent Bridging
- Routed Ethernet
- Bridged PPPoE
- Routed PPPoE
- Relayed PPPoA
- Routed PPPoA
- Classical IP & IP Routing.

Multiprotocol

All examples in this User's Guide are based on the Internet Protocol (IP) suite.

However, the **AST570** DSL router is a true multiprotocol device: it can easily handle most other popular protocol suites

Examples in this User's Guide

This User's Guide presents typical configurations but as an experienced user you are free to experiment and find an optimal configuration.

5.2 Packet Services at a Glance

Access methods

The **AST570** supports two access methods:

- **Direct access**
  Once initial configuration is done, continuous and immediate access is available via the DSL line.

  For direct access use either of:
  - Transparent Bridging
  - Routed Ethernet
  - CIP & IP Routing.
- **Dial-in access**
  In this mode access must be explicitly established, e.g. by "dialing" into a Remote Access Server (RAS).

  For dial-in access use either of:
  - Bridged PPPoE
  - Routed PPPoE
  - Relayed PPPoA
  - Routed PPPoA.

Forwarding methods

As their names imply the packet services can be differentiated in two groups:

- Forwarding packet services:
  - Transparent Bridging
  - Bridged PPPoE
  - Relayed PPPoA.

  These packet services forward frames unmodified.
- Routing packet services:
  - Routed Ethernet
  - Routed PPPoE
  - Routed PPPoA
  - CIP & IP Routing.

  These packet services, combined with NA(P)T allow to share a single IP address amongst multiple users on the (W)LAN.

Transparent Bridging

The **AST570** *IEEE802.1D Transparent Bridging* packet service (further referred to as *Bridging*) offers complete protocol transparency and has inherent configuration simplicity. Yet it provides excellent forwarding performance.

Routed Ethernet

The **AST570** *RFC1483 Routed Ethernet* packet service (also referred to as *MAC Encapsulated Routing (MER)*) relies on standard IP Routing for its forwarding. However, prior to output IP packets on the DSL line they are wrapped in Ethernet frames.

By doing so there is no apparent difference for the remote access server between frames sourced by a bridge and those sourced by the **AST570** MER entity.

PPPoE

PPPoE is one of two popular mechanisms to get in touch with the SP.

- **Bridged PPPoE**
  By installing a PPPoE client application (provided by your SP.) on your PC(s) and by using the **AST570**' bridge, connectivity can be established.
- **Routed PPPoE**
  PPPoE SP access can equally be accomplished by the embedded PPPoE client of the **AST570**.

PPPoA

The other method to get in touch with the SP over the DSL line is PPPoA.

- **Relayed PPPoA**
  Similar to Bridged PPPoE this requires installation of a PPTP dial-in application (*) on your PC(s).
- **Routed PPPoA**
  PPPoA SP access can equally be accomplished by the embedded PPPoA dial-in client of the **AST570**.

(*) Most popular OSs have a PPTP dial-in application installed, e.g. Microsoft Dial-Up Networking.

CIP & IP Routing

The **AST570** IP router can also be combined with *Classical IP (CIP*).

Classical IP is a mature technique for creating classical IP networks on top of ATM technology. It is widely supported by most, if not all remote access routers.

Although not the original aim of *Classical IP* it is mostly used for connecting routers over wide area point-to-point links.

Packet services resumé

All **AST570**' packet services can be summarized as follows:

Port	Packet Service	User/VC	IP Address	Protocol
(W)LAN interface(s)	Bridging	n	1 per user	Multiprotocol
	Routed Ethernet	n	1 (via NAPT)	IP Suite
	Bridged PPPoE	n	1 per user	Multiprotocol (*)
	Routed PPPoE	n	1 (via NAPT)	IP Suite
	Relayed PPPoA	1	1 per user	Multiprotocol (*)
	Routed PPPoA	n	1 (via NAPT)	IP Suite
	CIP	n	1 (via NAPT)	IP Suite

(*) The supported protocol(s) depend on the provisioning by the session client application, e.g. IP, IPX and NETBEUI for Microsoft's Dial-Up Networking application for Relayed PPPoA.

Detailed packet service use description

For more information on the configuration and use of all of the **AST570** packet services, see for:

- Transparent Bridging: chapter 6
- Routed Ethernet: chapter 7
- Bridged PPPoE: chapter 8
- Routed PPPoE: chapter 9
- Relayed PPPoA: chapter 10
- Routed PPPoA: chapter 11
- CIP & IP Routing: chapter 12.

5.3 Selection Criteria

In this section

- Selection Criteria
- Simultaneous Use of Packet Services.

Selection criteria

The criteria below can help you to select the most appropriate packet service for your application:

- The configuration required by your SP
- The application protocol you wish to use (within the boundaries of the remote end)
- The access method: an “Always-On” connection or a connection that is established when needed, i.e. “Dial-In”
- Connectivity to a single or multiple remote networks
- Security features such as identification, authentication, encryption, NA(P)T and Firewalling
- DSL modem vs DSL gateway model.

Simultaneous use of packet services

All packet services can be active at the same time without any restriction. The **AST570** can manage any combination of the packet services simultaneously up to a maximum number of 12 configured virtual connections.

Note: For Transparent Bridging (including Bridged PPPoE) the maximum number of configured Bridging ports is four.

6 Configuration and Use – Transparent Bridging

Introduction

Transparent Bridging is the packet service of your choice as it:

- Is platform and OS independent
- Is true multiprotocol
- Has no performance limitations in the Alcatel implementation
- Has almost no constraints on the number of attached users.

See also

Routed Ethernet packet service in chapter 7.

In this chapter

Topic	See
Preparatory Steps	6.1
Using Bridging	6.2
Bridging Configuration	6.3
Bridge Data	6.4

6.1 Preparatory Steps

Needed information

- **VPI/VCI** value of the VC(s) to use on the DSL line
- **ETHoA (RFC1483/Bridged) connection service** must be supported on these VCs
- **Encapsulation** method (LLC/SNAP)
- The PC's IP configuration: static or dynamic (DHCP).

Note: The RFC1483 is updated by RFC2684. The **AST570** fully complies with the relevant sections in both RFCs.

Multiple destinations

You can attach up to four connections (VCs) to the bridge.

To conserve DSL upstream bandwidth do not attach more connections than needed.

PC(s)

Bridging does not impose specific requirements to your PC's protocol layers. However, make sure that these are properly installed and configured.

In all subsequent examples, TCP/IP will be used.

TCP/IP

For TCP/IP, your SP will assign either static IP parameters or will ask to enable DHCP (per PC).

CAUTION

Transparent Bridging and DHCP

If the SP requires you to use DHCP on your local PC(s), you must disable the **AST570** DHCP server.

This is to avoid conflicts between two DHCP servers.

See section 14.4 for more information.

6.2 Using Bridging

Bridging configuration

There are no default Bridging entries.

Therefore, configure an appropriate entry as follows:

1. If needed, add an ETHoA phonebook entry with the correct VPI/VCI on the *'Phonebook'* page.
2. On the '*Bridge*' page, select this phonebook entry from the '*Address*' pop-down list.
3. For this entry, select the correct encapsulation method from the *'Encapsulation'* pop-down list.
4. Click Add.

See section 6.3 for more information.

Using Bridging

Make sure your **AST570** is turned on first.

Turn on your PC(s), start your Web browser and you are on the Internet or have Corporate Intranet access.

Although the access method of the bridge is 'Always-on', the remote organization might ask for a user name and password.

6.3 Bridging Configuration

Introduction

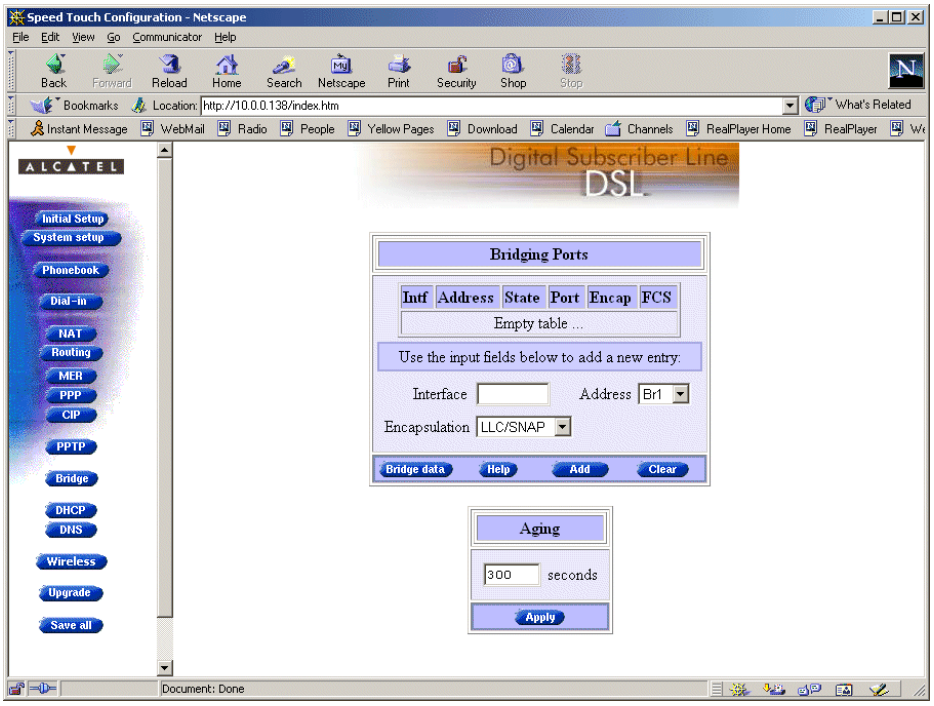
This section describes the use of the **AST570** *'Bridge'* page.

In this section

- The *'Bridge'* Page
- The *'Bridging Ports'* Table
- *'Bridging Ports'* Table Components
- The *'Aging'* Box
- Adding Entries
- Deleting Entries.

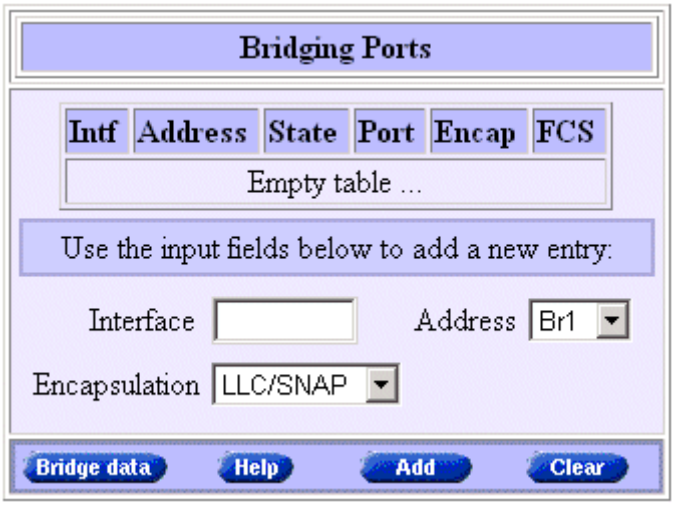
The 'Bridge' page

Click Bridge in the left pane of the **AST570** pages to pop up the *'Bridging'* page (See section 21.2 for more information):



The 'Bridging Ports' table

The following figure shows the *'Bridging Ports'* table:



'Bridging Ports' table components

Field	Description
Intf *Interface*	Indicates the interface name for the Bridging entry. **Note**: In most cases, the interface name will be the same as the phonebook entry name.
Address	Indicates the phonebook entry used by the Bridging entry.
State	Indicates the state of the Bridging entry. **Note**: Unless the interface is created via the CLI, Bridging entries are always in state connected, i.e. attached to a Bridge port.
Port	Indicates the name of the Bridge port on the WAN side: wan0, wan1, wan2, ...
Encap *Encapsulation*	Indicates the applied encapsulation method for Ethernet frames(*) on the VC. The **AST570** supports both the LLC/SNAP method (default) and the VC-MUX method.
FCS	Indicates whether the last four bytes of the Ethernet frames are preserved or not. By default the FCS is set to **NO**. **Note**: You can set the FCS to **YES** via the CLI.

(*) Ethernet frames are also referred to as Medium Access Control (MAC) frames or IEEE802.3 frames.

The 'Aging' box

The following figure shows the *'Aging'* box:

It indicates the aging timer of the bridge internal database.

If the aging time of a MAC entry has expired this entry will be removed from the database.

Only in exceptional cases the default value of 300 seconds (5 minutes) needs to be modified. The allowed range is from 10 seconds to 12 days.

Adding entries

Proceed as follows:

1. Browse to the *'Bridge'* page.
2. If needed, click New.
3. Select the phonebook entry from the *'Address'* pop-down list.

   Note: In case the presented phonebook entries do not suite your desired configuration, you must firstly create a correct phonebook entry. See section 13.2 for more information.
4. Select the encapsulation method for the Bridging port from the *'Encapsulation'* pop-down list (per default set to LLC/SNAP).
5. Optionally, enter a name for the Bridge interface in the *'Interface'* field.
6. Click Add and Save all to finish the procedure.

Deleting entries

On the *'Bridge'* page, click  next to the Bridging entry you want to delete. As a result your selection is highlighted.

Click Delete and Save all.

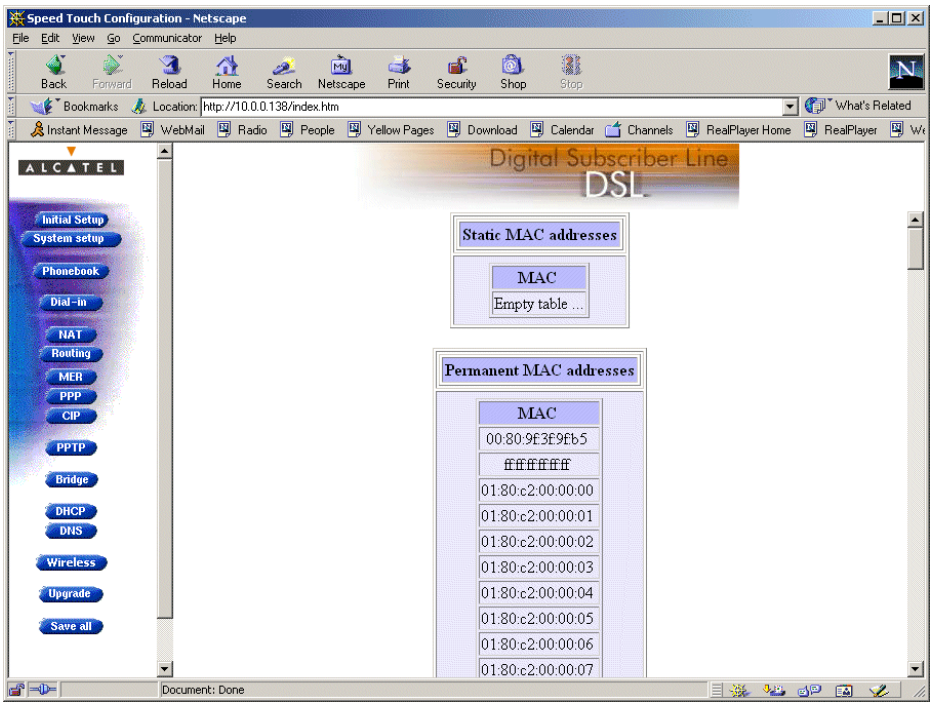
6.4 Bridge Data

Introduction

Transparent Bridging completely relies on its filtering database for its frame forwarding through the bridge. This filtering database is accessible via the *'Bridge'* page and allows you to overview all current MAC entries.

The 'Bridge Data' page

Click **Bridge data** on the *'Bridge'* page to pop up the *'Bridge Data'* page:



Available 'Bridge Data' tables

All MAC entries are spread over 3 tables:

- The *'static MAC addresses'* table
- The *'permanent MAC addresses'* table
- The *'dynamic MAC addresses'* table.

Static MAC addresses

This table lists the MAC addresses you have added to the filtering database via the CLI. These MAC addresses will never be aged by the bridge.

In principle, no static MAC addresses are to be configured.

Permanent MAC addresses

These are the MAC addresses that must always be resident inside the bridge, as stipulated in the IEEE802.1D standard:

- The **AST570**' own Ethernet MAC address:
  e.g. 00–80–9F–01–02–03
- The Broadcast MAC address:
  FF–FF–FF–FF–FF–FF
- The bridge group MAC address:
  01–80–C2–00–00–00
- The 16 reserved MAC addresses of IEEE802.1D:
  From 01–80–C2–00–00–01
  up to 01–80–C2–00–00–0F
- The all LANs bridge management group MAC address:
  01–80–C2–00–00–10

Dynamic MAC addresses

This table lists all MAC entries added by the learning process of the Bridge.

If the aging time of a MAC entry has expired, i.e. its age equals the time indicated in the *'Aging'* box, this entry will be removed from the list.

7 Configuration and Use – Routed Ethernet

Introduction

Routed Ethernet(*) is the packet service of your choice as it:

- Is instantly replaceable with an IEEE Transparent Bridge
- Provides Always-on type of connections and is auto-configurable if DHCP is enabled
- Allows multiple users to share a single IP address if NA(P)T is enabled
- Allows your local network to be shielded from the Internet via **AST570**' programmable Firewall.

(*) Is also referred to as MAC Encapsulated Routing (MER).

In this chapter

Topic	See
Preparatory Steps	7.1
Using Routed Ethernet	7.2
Routed Ethernet Configuration	7.3

7.1 Preparatory Steps

Needed information

- **VPI/VCI** value of the VC(s) to use on the DSL line
- **ETHoA (RFC1483/Bridged) connection service** must be supported on this VC
- **Encapsulation** method (LLC/SNAP)
- Whether IP configuration is static or dynamic (DHCP).

Multiple destinations

The **AST570** can manage up to 12 Routed Ethernet connections simultaneously.

Note: Check with your SP or corporate whether multiple end-to-end connectivity is enabled.

PC(s)

In order to use the Routed Ethernet mode of the **AST570**, the OS on your PC(s) must support TCP/IP.

See chapter 14 for more information on IP.

7.2 Using Routed Ethernet

Routed Ethernet configuration

There are no default Routed Ethernet entries.

Therefore, configure an appropriate entry as follows:

1. If needed, add an ETHoA phonebook entry with the correct VPI/VCI on the '*Phonebook*' page.
2. On the '*MER*' page, select this phonebook entry from the '*Address*' pop-down list.
3. For this entry, select the correct encapsulation method from the '*Encapsulation*' pop-down list.
4. DHCP is per default on (✓). If needed, uncheck it and enter IP information manually.
5. Click Add.

See section 7.3 for more information.

Using Routed Ethernet

Make sure your **AST570** is turned on first.

Turn on your PC(s), start your Web browser and you are on the Internet or have Corporate Intranet access.

Although the access method of Routed Ethernet is 'Always-on' the remote organization might ask for a user name and password.

7.3 Routed Ethernet Configuration

Introduction

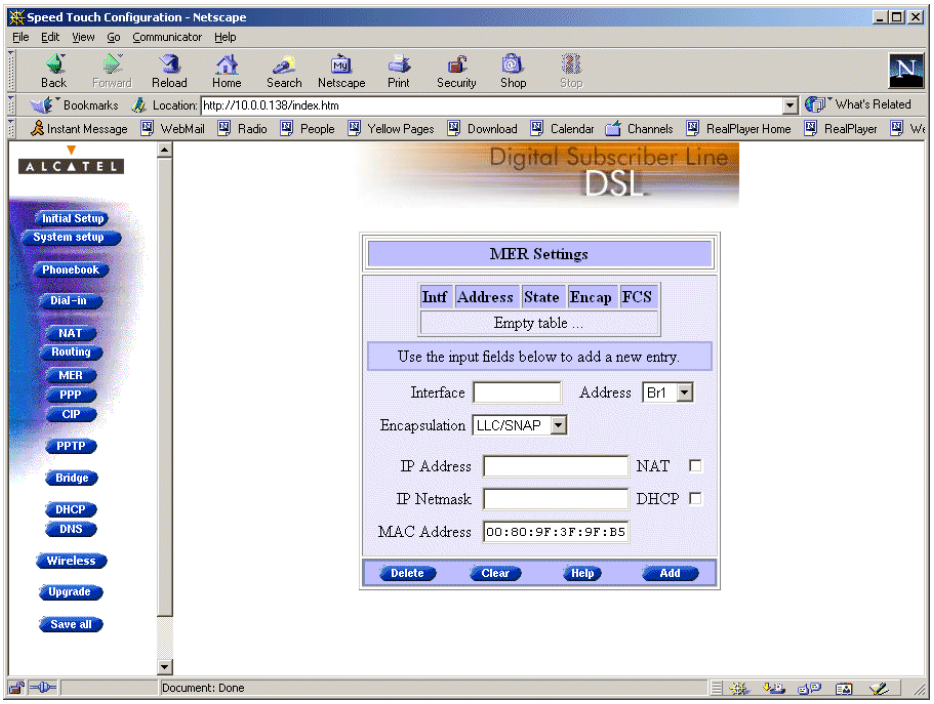
This section describes the use of the **AST570** *'MER'* page.

In this section

- The *'MER'* Page
- The *'MER Settings'* Table
- *'MER Settings'* Table Components
- Adding Entries
- Deleting Entries.

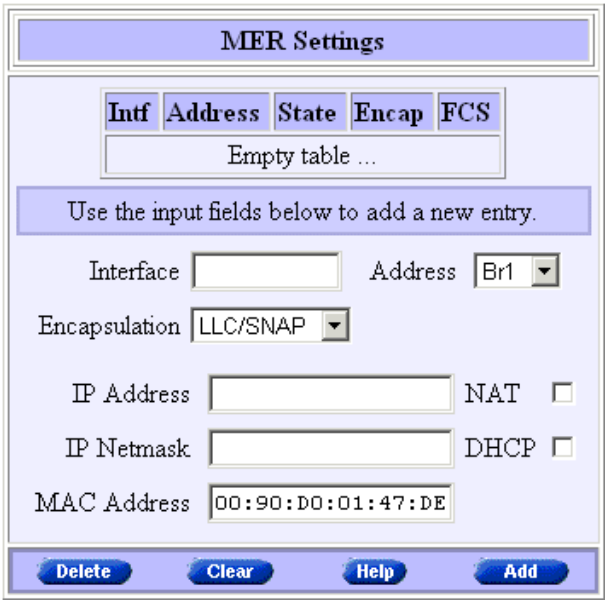
The 'MER' page

Click MER in the left pane of the **AST570** pages to pop up the *'MER'* page (See section 21.2 for more information):



The 'MER Settings' table

The following figure shows the *'MER Settings'* table:



'MER Settings' table components

Field	Description
Intf *Interface*	Indicates the interface name for the Routed Ethernet entry. **Note**: In most cases, the interface name will be the same as the phonebook entry name.
Address	Indicates the phonebook entry used by the Routed Ethernet entry.
State	Indicates the state of the Routed Ethernet interface. **Note**: Unless the interface is created via the CLI, Routed Ethernet entries are always in state *connected*.
Encap *Encapsulation*	Indicates the applied encapsulation method for Ethernet frames(*) on the VC. The **AST570** supports both the LLC/SNAP method (default) and the VC-MUX method.
FCS	Indicates whether the last four bytes of the Ethernet frames are preserved or not. By default the FCS is set to **NO**. **Note**: You can set the FCS to **YES** via the CLI.
IP Address *IP Netmask*	Indicates the negotiated IP address and netmask used by the Routed Ethernet entry. In case DHCP is checked (✓) this IP address is dynamically assigned by the remote DHCP server. If DHCP is unchecked, you must enter a static IP address for the local side of the Routed Ethernet connection.

Field	Description
MAC Address	Indicates the MAC address for the Routed Ethernet entry. **Note**: In case no MAC address is entered manually, the source MAC address of the Ethernet frames is the **AST570** Ethernet MAC address.
NAT	Indicates whether NA(P)T is used (✓) or not on the IP address of the Routed Ethernet entry.
DHCP	Indicates whether DHCP is used (✓) or not for the Routed Ethernet entry.

(*) Ethernet frames are also referred to as Medium Access Control (MAC) frames or IEEE802.3 frames.

Adding entries

Proceed as follows:

1. Browse to the *'MER'* page.
2. If needed, click New.
3. Select the phonebook entry from the *'Address'* pop-down list.

   Note: In case the presented phonebook entries do not suite your desired configuration, you must firstly create a correct phonebook entry. See section 13.2 for more information.
4. Select the encapsulation method for the Bridging port from the *'Encapsulation'* pop-down list (per default set to LLC/SNAP).
5. Optionally, enter the appropriate configuration in one, or more of the following fields:
   - The *'Interface'* field
   - The *'IP Address'* and *'IP Netmask'* fields
   - The *'MAC Address'* field.
6. Optionally, check one or more of the following checkboxes:
   - The *'NAT'* checkbox
   - The *'DHCP'* checkbox.
7. Click Add and Save all to finish the procedure.

Deleting entries

On the *'MER'* page, click  next to the entry you want to delete. As a result your selection is highlighted.

Click Delete and Save all.

8 Configuration and Use – Bridged PPPoE

Introduction

The **AST570** transparent bridge can be used in combination with a PPP over Ethernet (PPPoE) client installed on your PC.

The resulting *Bridged PPPoE* packet service provides similar dial-in experience as found on point-to-point connections.

See also

Routed PPPoE packet service in chapter 9.

In this chapter

Topic	See
Preparatory Steps	8.1
Using Bridged PPPoE	8.2
Bridged PPPoE Configuration	8.3

8.1 Preparatory Steps

Needed information

- **VPI/VCI** value of the VC(s) to use on the DSL line
- **ETHoA (RFC1483/Bridged) connection service** must be supported on this VC
- **Encapsulation** method (LLC/SNAP)
- Remote access server must be a **PPPoE server**
- **PPPoE client** to be installed
- User name and password for your **user account**.

Multiple destinations

Up to four simultaneous Bridged PPPoE sessions can be active.

Note: Per active Bridged PPPoE session a dedicated Bridging entry must be made available on the **AST570**. See section 8.3 for more information.

PC(s)

To use Bridged PPPoE, a PPPoE client must be installed on your PC.

The SP will provide the PPPoE client software. Contact him for more information.

8.2 Using Bridged PPPoE

Creating and using a PPPoE session instance

Via the PPPoE client, you will be able to create PPPoE session icons, representing all the connection parameters, just like creating Dial-Up icons with Microsoft's Dial-Up Networking application.

All you need is your user name and password for your account; although sometimes also a Service Name and/or Access Concentrator is required.

Check with your SP which Service Name and/or Access Concentrator to choose, if any.

For further details on how to fill in these parameters and use additional functionality, consult the User's Guide of your PPPoE client or follow the instructions of your SP.

8.3 Bridged PPPoE Configuration

Introduction

As the Bridged PPPoE packet service implies nothing more than using the **AST570** Transparent Bridging packet service, no specific configuration for Bridged PPPoE is required on the **AST570**.

However, you may need to configure the *Transparent Bridging* packet service of the **AST570** in order to meet the requirements of your SP regarding VC(s) and encapsulation.

Bridging configuration

There are no default Bridging entries.

Therefore, configure an appropriate entry as follows:

1. If needed, add an ETHoA phonebook entry with the correct VPI/VCI on the '*Phonebook*' page.
2. On the '*Bridge*' page, select this phonebook entry from the '*Address*' pop-down list.
3. For this entry, select the correct encapsulation method (per default set to LLC/SNAP).
4. Click Add.

See section 6.3 for more information.

9 Configuration and Use – Routed PPPoE

Introduction

Routed PPPoE(*) is the packet service of your choice as it:

- Provides the dial-in access method over a virtual Ethernet segment
- Requires no PPPoE client on the PC(s), avoiding special installation procedures
- Allows multiple users to share a single IP address if NA(P)T is enabled
- Allows your local network to be shielded from the Internet via **AST570**' programmable Firewall.

(*) Routed PPPoE is also referred to as Embedded PPPoE.

In this chapter

Topic	See
Preparatory Steps	9.1
Using Routed PPPoE	9.2
Routed PPPoE Configuration	9.3
Detailed Configuration	9.3

9.1 Preparatory Steps

Needed information

- **VPI/VCI** value of the VC(s) to use on the DSL line
- **ETHoA (RFC1483/Bridged) connection service** must be supported on this VC
- **Encapsulation** method (LLC/SNAP)
- Remote access server must be a **PPPoE server**
- User name and password for your **user account**.

Multiple destinations

The **AST570** can manage up to 12 Routed PPPoE connections simultaneously.

Note: Check with your SP or corporate whether multiple end-to-end connectivity is enabled.

PC(s)

In order to use the Routed PPPoE mode of the **AST570**, the OS on your PC(s) must support TCP/IP.

See chapter 14 for more information on IP.

9.2 Using Routed PPPoE

Routed PPPoE configuration

There are no default Routed PPPoE entries.

Therefore, configure the appropriate as follows:

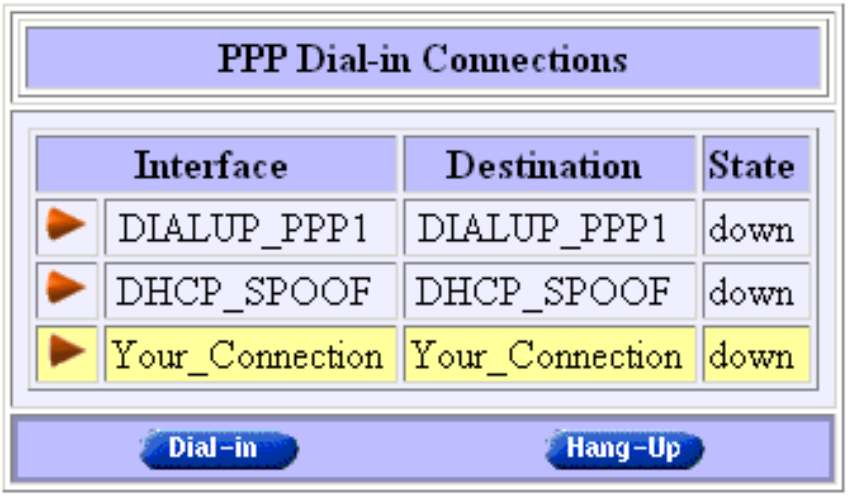
1. If needed, add an ETHoA phonebook entry with the correct VPI/VCI on the 'Phonebook' page.
2. On the '*PPP*' page, select this phonebook entry from the '*Address*' pop-down list.
3. For this entry, select PPPoE in the '*Protocol*' field.
4. Select the correct encapsulation method from the '*Encapsulation*' pop-down list.
5. Optionally, enter user name and password.
6. Click Add.
7. Optionally perform detailed configurations.

See section 9.3 for more information.

Opening dial-in PPPoE sessions

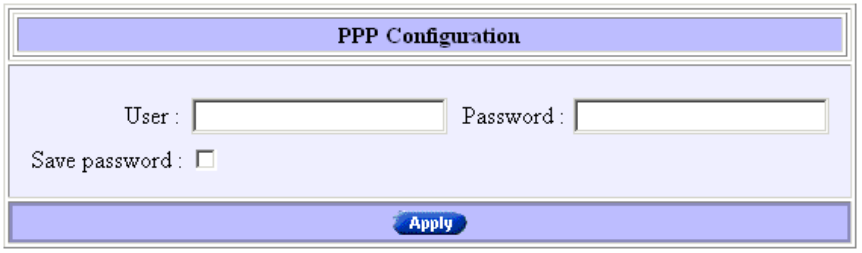
Proceed as follows (See section 21.2 for more information):

1. Click Dial-in on the **AST570** pages.
2. On the '*Dial-in*' page the following table is shown:



3. Click  next to the PPPoE entry you want to connect with. As a result your selection is highlighted (See example above).
4. Click Dial-in.

5. If applicable an *'Authentication'* table pops up:



Enter your user name and password in the appropriate fields. If you want the **AST570** to remember your credentials, check *'Save password'* (✓).

6. Click Apply.

7. After identification and authentication the *'PPP connections'* page reappears.

While the **AST570** tries to open the session '**trying**' will appear in the *'State'* field. Once the session is active the field displays '**up**'. From then you are online and you can start your application or browse the Internet.

During the session

During the time the session is up, you can overview some important connection statistics on the *'PPP'* page.

See section 9.4.4 for more information.

Closing dial-in PPPoE sessions

Proceed as follows:

1. Browse to the *'Dial-in'* page.

2. Active PPPoE sessions are indicated via **up** in the *'State'* field.

Click  next to the active PPPoE entry in the list you want to close the session for. As a result your selection is highlighted.

3. Click Hang-Up.

The session state of the PPPoE entry will change to **down**, i.e. it becomes idle.

9.3 Routed PPPoE Configuration

Introduction

This section describes the use of the **AST570** *'PPP'* page for Routed PPPoE.

Note

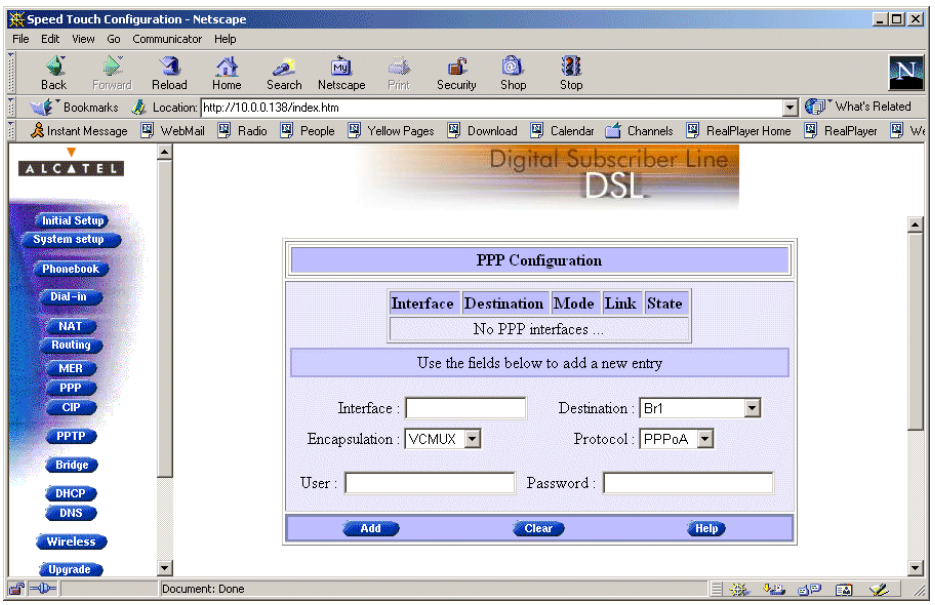
Most, if not all configurations for Routed PPPoE connections are identical to the configuration of Routed PPPoA connections. Therefore most configurational aspects in this section will be referred to the configuration sections of chapter 11.

In this section

- The *'PPP'* Page and Description
- Adding Entries
- Deleting Entries.

The 'PPP' page and description

Click PPP in the left pane of the **AST570** pages to pop up the *'PPP'* page (See section 21.2 for more information):



See section 11.3 for a description of all fields of the *'PPP Configuration'* table.

Adding entries

Proceed as follows:

1. Browse to the *'PPP'* page.
2. If needed, click New.
3. Select the PPPoE protocol from the *'Protocol'* pop-down list.
4. Select the phonebook entry from the *'Address'* pop-down list.

   You must use a ETHoA or "any type" phonebook entry for Routed PPPoE connections.

   Note: In case the presented phonebook entries do not suite your desired configuration, you must firstly create a correct phonebook entry. See section 13.2 for more information.
5. Select the encapsulation method for the Routed PPPoE entry from the *'Encapsulation'* pop-down list.
6. Optionally, enter user name and password for the Routed PPPoE entry.

   Note: In case you do not enter this information it is asked each time you open the Routed PPPoE session.
7. Optionally, enter the appropriate configurations in the *'Detailed Configuration'* table.

   See section 9.4 for more information.
8. Click Add and Save all to finish the procedure.

Detailed configuration

Prior to using the PPPoE entry you may need to enter additional configurations for the connection.

See section 9.4 for more information.

Deleting entries

On the *'PPP'* page, click  next to the PPPoE connection you want to delete. As a result your selection is highlighted.

Click Delete and Save all.

9.4 Detailed Configuration

Introduction

Additional configuration of the Routed PPPoE entry may be needed in the *'Detailed Configuration'* table.

This section describes the various PPPoE connection configurations the **AST570** offers for assuring end-to-end connectivity.

The 'Detailed Configuration' table

On the *'PPP'* page a *'Detailed Configuration'* table can be found. The contents of this table are always related to the highlighted entry in the *'PPP Configuration'* table.

The *'Detailed Configuration'* table contains three or four tabs. Three tabs, *'PPPoE'*, *'Routing'* and *'Other'* allow you to overview or configure connection related settings for the Routed PPPoE entry. The fourth tab *'Stats'* appears only if a session is running on the selected Routed PPPoE entry.

After configuration of these detailed Routed PPPoE entry aspects, press Apply and Save all to apply and save your changes.

Interaction with the AST570 IP router

Most of the configurations described in this section, influence the IP router in the **AST570**.

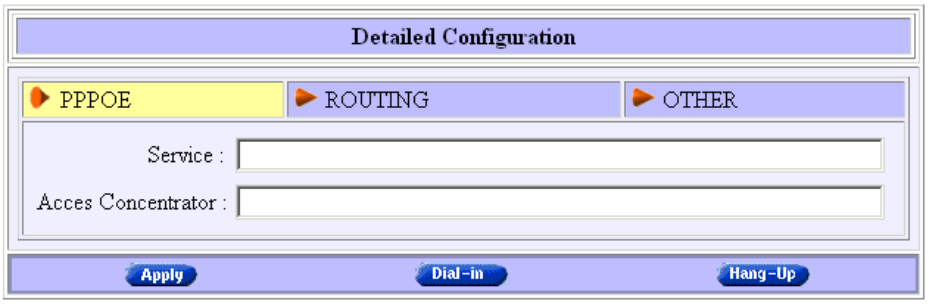
See chapter 14 for more information on IP routing aspects.

In this section

Topic	See
'PPPoE' Configurations	9.4.1
'Routing' Configurations	9.4.2
'Other' Configurations	9.4.3
'Stats' During a Routed PPPoE Session	9.4.4

9.4.1 'PPPoE' Configurations

The 'PPPoE' tab



PPPoE Service and Access Concentrator

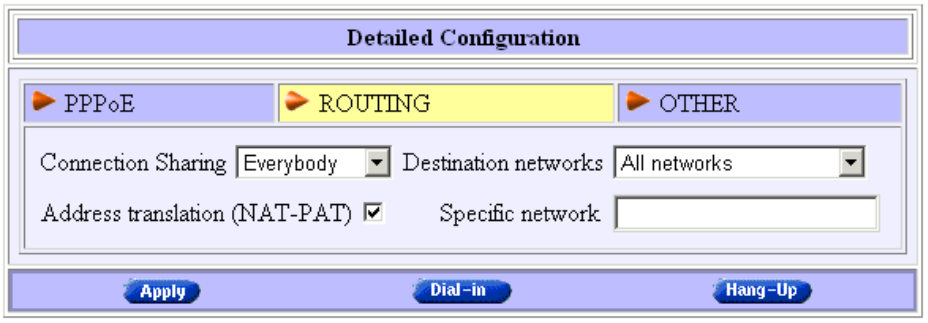
The **AST570** Routed PPPoE embedded session client allows to configure your PPPoE session for connecting for a dedicated Service via an Access Concentrator.

If applicable, both *Service* name and *Access Concentrator* will be provided by the SP.

For more information, contact your SP.

9.4.2 'Routing' Configurations

The 'Routing' tab



Configurable items

The *'Routing'* tab allows you to configure the IP routing aspects of the selected Routed PPPoE entry.

Following routing aspects are configurable:

- Connection sharing

  This field allows you to configure which (W)LAN members, besides the PC that opened the Routed PPPoE session, can use the connection.

- Destination networks / Specific network

  These fields allow you to configure which destination can be reached over the particular Routed PPPoE entry.

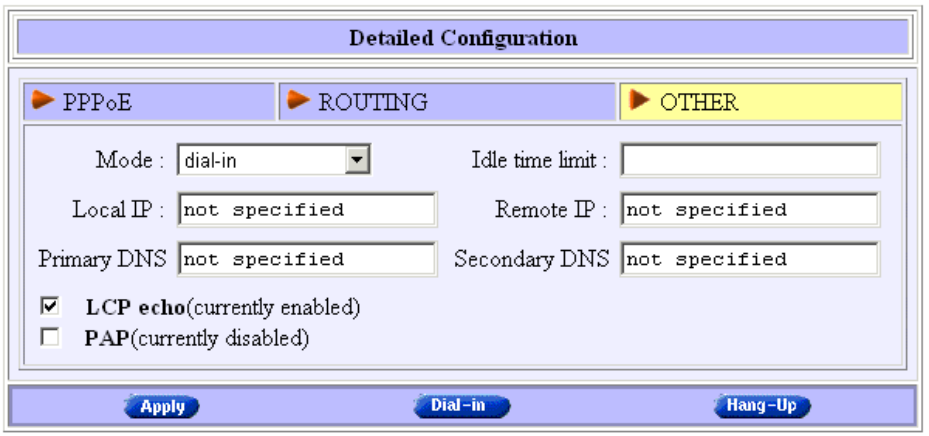
- Address translation (NA(P)T)

  Checking this checkbox allows you to share the single Routed PPPoE entry with multiple simultaneous users on your (W)LAN.

For more information on these routing aspects, see subsection 11.4.1.

9.4.3 'Other' Configurations

The 'Other' tab



Configurable items

The *'Other'* tab allows you to configure the connection related aspects of the selected Routed PPPoE entry.

Following connection aspects are configurable:

- Mode
  This field allows you to configure how the Routed PPPoE session is opened.
- Idle time limit
  For *'Dial-on-demand'* this checkbox allows you to specify the time after which a running but unused PPPoE session is closed.
- Local IP / Remote IP
  IP addresses are negotiated between the two PPP peers of the Routed PPPoE session. The *'Local IP'* and *'Remote IP'* fields influence this negotiation.
- Primary DNS / Secondary DNS
  These fields allow – optionally – to enter the IP address(es) of the primary (and optionally the secondary) DNS server(s).
- LCP echo
  This checkbox allows to turn on/off LCP echo request/replies.
- PAP
  This checkbox allows to switch between Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP), and forced PAP only.

For more information on these aspects, see subsection 11.4.2.

9.4.4 'Stats' During a Routed PPPoE Session

The 'Stats' tab

During a Routed PPPoE session a fourth tab *'Stats'* is available:

Configurable items

The *'Stats'* tab allows to overview some session statistics while a session is running on the selected Routed PPPoE entry.

Following session statistics are available:

- IP Address

  The IP address at the local peer of the current PPP link. This address can be dynamically assigned by the RAS or statically configured on the *'Other'* tab fields.

- Bytes received / Bytes sent

  The number of bytes received and sent since the Routed PPPoE session came up.

- Bytes dropped

  The number of bytes dropped, i.e. discarded due to failure since the Routed PPPoE session came up.

10 Configuration and Use – Relayed PPPoA

Introduction

Relayed PPPoA(*) is the packet service of your choice as it:

- Provides standard Dial-in PPP behavior
- Supports security via identification, authentication and encryption
- Has multiprotocol support depending on the PPTP implementation, e.g. for MS Windows: TCP/IP, IPX/SPX and NETBEUI
- Offers complete TCP/IP protocol transparency; no NA(P)T is required
- Supports concurrent access to multiple remote destinations.

(*) Relayed PPP over ATM (PPPoA) is also referred to as PPPoA-to-PPTP Relaying or PPPoA/PPTP.

See also

Routed PPPoA packet service in chapter 11.

Topics

Topic	See
Preparatory Steps	10.1
Using Relayed PPPoA	10.2
Example : MS Windows 98 Dial-Up Networking	10.3
Relayed PPPoA Configuration	10.4

10.1 Preparatory Steps

Needed information

- **VPI/VCI** value of the VC(s) to use on the DSL line
- **PPPoA (RFC2364) connection service** must be supported on this VC
- **Encapsulation** method (VC-MUX)
- Remote access server must be a **PPP(oA) server**
- User name and password for your **user account**.

Multiple destination

The **AST570** can manage up to 12 Relayed PPPoA connections simultaneously.

Note: Check with your SP or corporate whether multiple end-to-end connectivity is enabled.

PC(s)

Your PC must support Point-to-Point Protocol (PPP) and Point-to-Point Tunnelling Protocol (PPTP).

Note: All Microsoft Windows platforms support PPP and PPTP.

A PPTP Dial-Up application must be installed on your PC.

Note: All Microsoft Windows platforms have a PPTP Dial-Up application installed per default.

TCP/IP

Before you can establish PPTP tunnels, you must configure:

- A local IP address in each PC which initiates a PPTP tunnel
- A local IP address in the **AST570** which terminates the PPTP tunnel(s).

See chapter 14 for more information on IP.

10.2 Using Relayed PPPoA

Introduction

Before you can open a PPTP tunnel towards the **AST570**, firstly you must initially configure a PPTP dial-up connection on your PC. Once this PPTP dial-up connection is configured you can use it to open a Relayed PPPoA connection to the remote side of the DSL line.

Because the configuration and use of such a connection follows similar patterns for all popular OSs, this section will describe the procedures in global.

In section 10.3 an example is provided how to create and use a PPTP Dial-Up icon in MS Windows 98.

In this section

Topic	See
Preparing the PC for PPTP Tunneling	10.2.1
Using PPTP towards the **AST570**	10.2.2

10.2.1 Preparing the PC for PPTP Tunneling

Creating a PPTP connection icon

Most, if not all OSs provide a Graphical User Interface (GUI) guided procedure for the initial creation of a PPTP connection icon.

The result of such creation is in most cases an icon, or entry in a folder or a table called 'RAS', 'Dial-Up Networking', 'PPTP', 'Call sessions', etc.

PPTP connection parameters

During the initial configuration of your PPTP connection icon, you must provide the following parameters:

- A name for the PPTP connection icon
- The VPN server's IP address, or DNS hostname, i.e. the **AST570**' IP address, or DNS hostname

Optionally, you can complete this entry with the following string information:

- The VC's PPPoA phonebook name – configured on your **AST570** – to be used for this connection

  Note: Only in case multiple PPPoA or any phonebook entries are directed towards different destinations, you must add the appropriate phonebook name to the dial-string. This allows the **AST570** to open the session to the correct specific destination. In case all PPPoA and/or any phonebook entries are directed towards the same destination, it is better not to add a phonebook name to the dial-string.
- A PPTP profile name – configured via the **AST570**' CLI – to be used for this connection.

10.2.2 Using PPTP towards your AST570

PPPoA configuration

Per default, following PPPoA phonebook entries are available for Relayed PPPoA connections:

- **RELAY_PPP1** (PPPoA on 8.48)
- **RELAY_PPP2** (PPPoA on 8.49)
- **RELAY_PPP3** (PPPoA on 8.50)
- **RELAY_PPP4** (PPPoA on 8.51)
- **DIALUP_PPP3** (PPPoA on 8.66)

In case these PPPoA phonebook entries do not meet your requirements, you can configure a new one.

See section 13.2 for more information.

Opening a session

Depending on your OS, you can open a session by either double-clicking the PPTP session icon or selecting it from a RAS table and clicking 'Dial-Up' or 'Connect'.

Credentials

Before you can actually browse the Internet or contact the remote side's resources, you must supply the following credentials:

- A user name
- An associated password.

Note: Most, if not all OSs allow the credentials to be saved.

10.3 Example : MS Windows 98 Dial-Up Networking

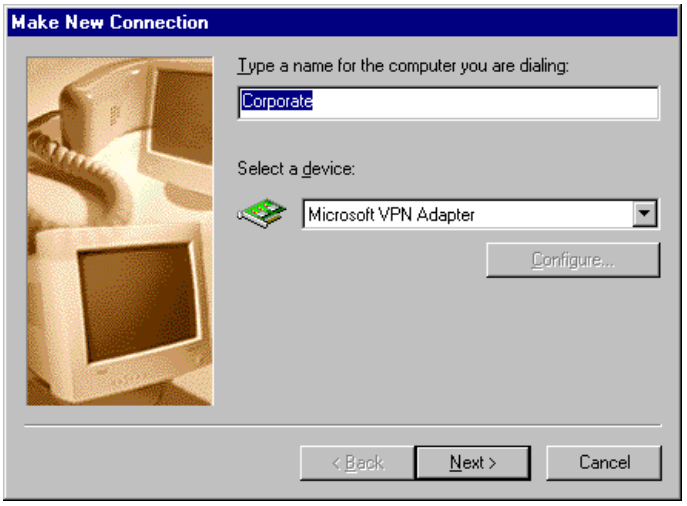
In this section

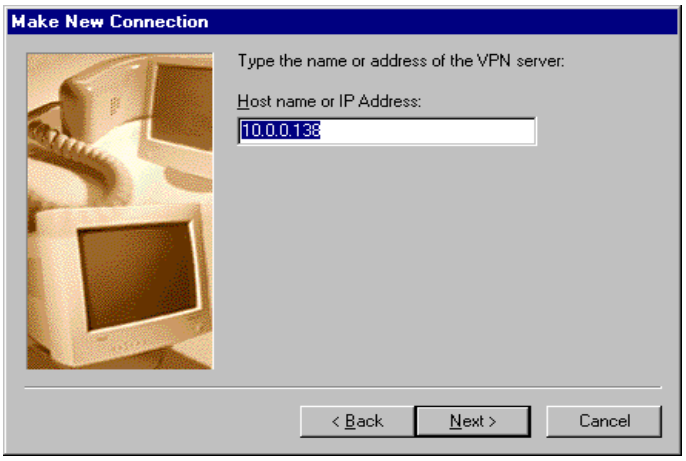
The following overview summarizes the necessary steps to setup a Microsoft Windows 98 PC for the use of Relayed PPPoA:

Step	Action	See
1	Configure a *Private* IP address on your PC	
2	Create a new Dial-Up Networking icon	10.3.1
5	Open a Dial-Up Session	10.3.2
6	Surf the Internet.	
7	Close a Dial-Up Session in Use	10.3.3

10.3.1 Create a New Dial-Up Networking Icon

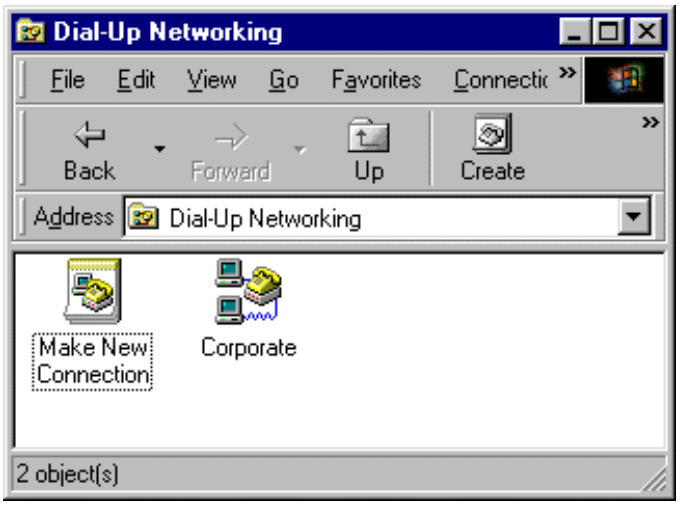
Procedure Proceed as follows:

Step	Action and Description
1	Double-click the '*My Computer*' icon on your desktop.  My Computer
2	Double-click the '*Dial-Up Networking*' icon.  Dial-Up Networking
3	Double-click the '*Make New Connection*' icon to activate the 'Make New Connection' wizard.  Make New Connection
4	If you use the Dial-Up Networking application for the first time, the 'Welcome to Dial-Up Networking' window appears. In that case, click Next >. The '*Make New Connection*' window pops up: 

Step	Action and Description
5	In the first input field of the *'Make New Connection'* window, type a name, e.g. an alias for the organization you are connecting to. **Note**: This name will appear below the Dial-Up icon at the end of this procedure.
6	In the 'Select a device' pop-down list of the *'Make New Connection'* window, you must select the *'Microsoft VPN Adapter'* for PPTP tunneling.
7	Click Next > to pop up the VPN server window: 
8	Enter the DNS hostname or IP address of the Virtual Private Network (VPN) server. **Note**: "VPN server" is another word for PPTP server which is in this case your **AST570**. The default IP address for the **AST570** is 10.0.0.138. Its default hostname is "SpeedTouch". Optionally, you can add the phonebook name to specify which VC is to be used for the connection. Optionally this phonebook name can be followed by a PPTP profile.
9	A window pops up confirming that you have successfully installed a new Dial-Up connection. Click Finish to finish the procedure.

Result

A new icon with the name of the connection you have just created will be added to your *'Dial-Up Networking'* folder:

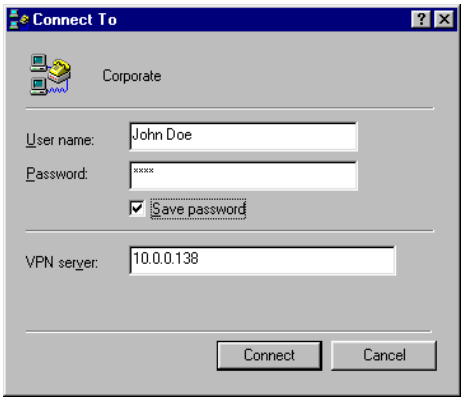


Creating multiple Dial-Up icons for multiple destinations

Per destination you can create a unique icon. To do so, repeat the steps starting with step 3 of the previous procedure.

10.3.2 Open a Dial-Up Session

Procedure Proceed as follows:

Step	Action and Description
1	Double-click the appropriate Dial-Up icon in the *'Dial-Up Networking'* folder or double-click its shortcut on your desktop.  Corporate The *'Connect To'* window pops up: 
2	Fill in your *user name* and *password*, according your user account at the SP or Corporate. **Note**: If you want the current Dial-Up connection to remember your credentials for future use, check the 'Save Password' box (✓). Make sure though that you have logged in when you boot your PC.
3	Click Connect The *'Connecting To Corporate'* window appears shortly before being minimized in the system tray: 
4	Start your application now, e.g. a Web browser.

While you are connected

Once the Dial-Up connection is established, you can find the MSDUN icon showing two PCs connected to each other in the system tray:

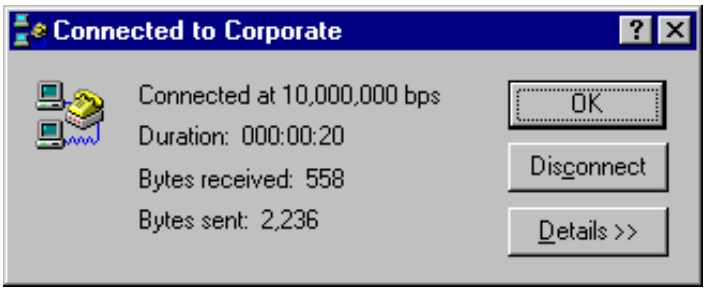
The MSDUN icon symbolizes activity on the Relayed PPPoA connection by flashing PC(s):

- A flashing “Front” PC symbolizes upstream (T_X) link activity (from your local PC towards the **AST570**)
- A flashing “Behind” PC symbolizes downstream (R_X) link activity (from the **AST570** towards your PC).

The ’Connected To’ window

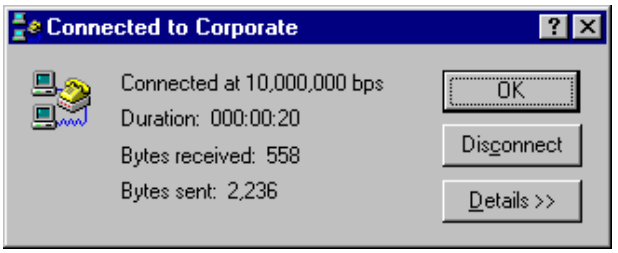
You can check the status of the connection by double-clicking the MSDUN icon in the system tray.

A *’Connected To’* window will pop up, showing the status of the connection:



10.3.3 Close a Dial-Up Session in Use

Procedure Proceed as follows:

Step	Action and Description
1	If the Dial-Up connection is minimized, click the MSDUN icon  in the system tray:  The *'Connected To'* window pops up: 
2	Click  to close the session.

Result The PPTP tunnel to the **AST570** will no longer exist. The Relayed PPPoA entry on the **AST570** is made available again for other users.

10.4 Relayed PPPoA Configuration

Introduction

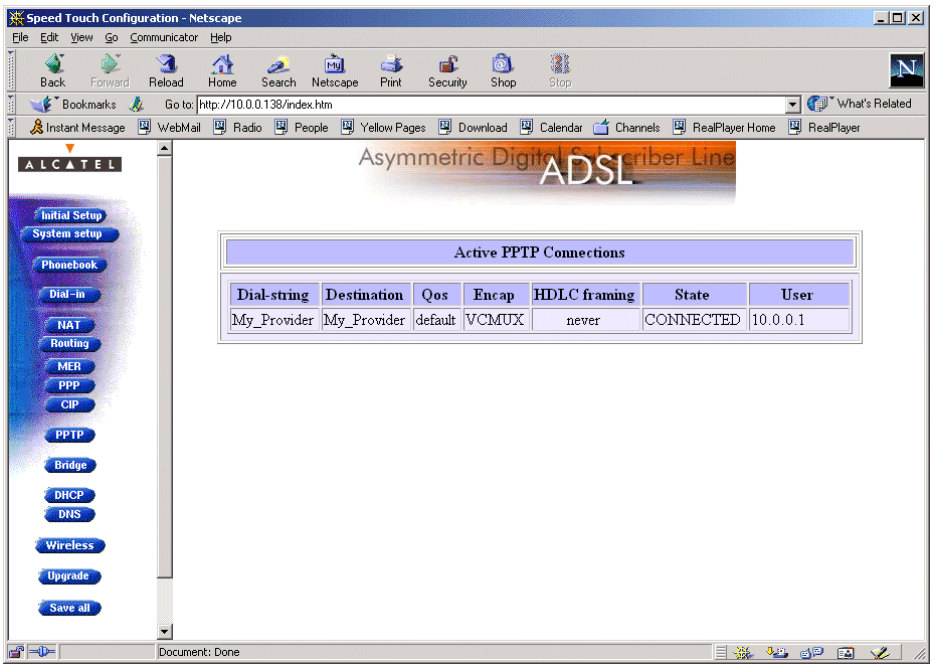
This section describes the use of the **AST570** *'PPTP'* page.

In this section

- The *'PPTP'* Page
- The *'Active PPTP Connections'* Table
- *'Active PPTP Connections'* Table Components
- Advanced Configuration
- Tunneling from behind an IP Router.

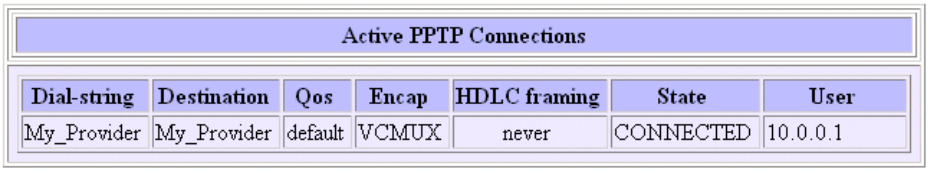
The 'PPTP' page

Click PPTP in the left pane of the **AST570** pages to pop up the *'PPTP'* page (See section 21.2 for more information):



The 'Active PPTP Connections' table

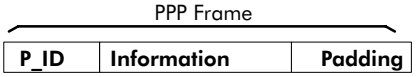
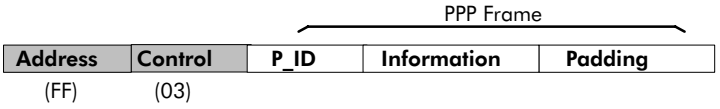
The following figure shows the *'Active PPTP Connections'* table:



Active PPTP Connections						
Dial-string	Destination	Qos	Encap	HDLC framing	State	User
My_Provider	My_Provider	default	VCMUX	never	CONNECTED	10.0.0.1

In the example one active Relayed PPPoA connection is up.

'Active PPTP Connections' table components

Field	Description
Dial-string	In your Dial-Up application you are able to specify which PPPoA entry (and PPTP profile) is to be used by adding the appropriate dial-string. This dial-string is indicated here, if applied.
Destination	Indicates the PPPoA phonebook entry name in use.
Qos	Indicates the Quality of Service (QoS) applicable for the Relayed PPPoA connection. In most cases the Qos column will indicate **`default`**. Via the CLI you can configure a specific QoS profile(*).
Encap	Indicates the applied encapsulation method for PPP frames in the VC. The **AST570** supports both the VC-MUX method (default) and the LLC/NLPID method. The encapsulation method for a Relayed PPPoA connection can be configured via the CLI.
HDLC Framing	The PPP frames arriving via a PPTP tunnel, and the PPP frames encapsulated on ATM connections, differ in format. The PPP format on AAL5 follows RFC 1661 "Point-to-Point Protocol (PPP)":  Whereas the PPP format within a tunnel follows "Point-to-Point Tunneling Protocol (PPTP)":  The latter format has two additional bytes in front of the frame (FF-03) inherited from another encapsulation i.e. RFC 1662 "PPP in HDLC-like framing".

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>HDLC Framing (continued)</td><td>In order to cope with these PPP frame differences, the AST570 adapts to the different formats on a 'per connection' base.
Additionally, the AST570 offers the following PPP/AAL5 format configuration options via the CLI if interoperability problems should arise:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>Never</td><td>The AST570 will make sure that FF-03 will never be found in front of a PPP frame encapsulated on a AAL5/ATM connection, independent of the actual format of the PPP frame in the tunnel. This setting is default, and follows RFC2364.</td></tr>
<tr><td>Always</td><td>The AST570 will make sure that FF-03 is always in front of a PPP frame encapsulated on an AAL5/ATM connection. Although not supported by RFC2364, some equipment may rely on this format.</td></tr>
<tr><td>Keep</td><td>The AST570 will not change the PPP frame arriving via a tunnel.</td></tr>
</table>
Note: This configuration possibility applies only to the upstream direction ! In the downstream direction, the AST570 will always make sure that FF-03 is in front of the frame prior to put it in a PPTP tunnel.</td></tr>
<tr><td>State
User</td><td>Indicates that the Relayed PPPoA connection is up ("CONNECTED").
As soon as a PC initiates a PPTP tunnel towards the AST570, its IP address is indicated in the 'User' field.</td></tr>
</table>

Advanced configuration

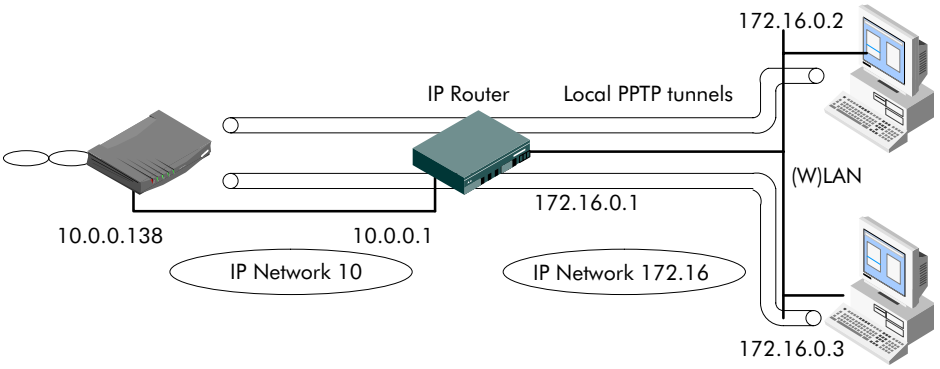
You can instruct the **AST570** to use a specific PPPoA phonebook entry by adding its phonebook name next to the **AST570**' IP address or DNS hostname in the Dial-Up application on your PC.

The phonebook name string can optionally be followed by a PPTP profile name, configured via the CLI. This PPTP profile allows you to specify:

- Encapsulation method (default = VC-MUX)
- HDLC framing (default = never)
- QoS (default = default).

Tunneling from behind an IP router

The **AST570** allows local tunneling from behind an IP router:



This requires settings in both **AST570** and PCs.

AST570

You must add a default route for the **AST570** via the *'Routing'* page (See section 14.5 for more information).

In the example of the figure above the route to be added has the following parameters:

- Destination: 0.0.0.0/0
- Source: Any
- Gateway: 10.0.0.1

PCs

For each PC, you must add a route to its internal routing table. This route must point to the **AST570**.

In the example of the figure above the route to be added to each PC's routing table has the following parameters:

- Destination: 10.0.0.138
- Gateway: 172.16.0.1

Verify connectivity

You can verify connectivity from behind the IP router by applying a ping to the **AST570**.

11 Configuration and Use – Routed PPPoA

Introduction

Routed PPPoA(*) is the packet service of your choice as it:

- Has an authenticated session concept: it supports identification, authentication and auto-configuration
- Requires no session client on the PC(s), avoiding special installation procedures
- Allows multiple users to share a single IP address if NA(P)T is enabled
- Allows your local network to be shielded from the Internet via **AST570**' programmable Firewall.

(*) Routed PPPoA is also referred to as PPP & IP Routing.

In this chapter

Topic	See
Preparatory Steps	11.1
Using Routed PPPoA	11.2
Routed PPPoA Configuration	11.3
Detailed Configuration	11.4

11.1 Preparatory Steps

Needed information

- **VPI/VCI** value of the VC(s) to use on the DSL line
- **PPPoA (RFC2364) connection service** must be supported on this VC
- **Encapsulation** method (VC-MUX)
- Remote access server must be a **PPP(oA) server**
- User name and password for your **user account**.

Multiple destinations

The **AST570** can manage up to 12 Routed PPPoA connections simultaneously.

Note: Check with your SP or corporate whether multiple end-to-end connectivity is enabled.

PC(s)

In order to use the Routed PPPoA mode of the **AST570**, the OS on your PC(s) must support TCP/IP.

See chapter 14 for more information on IP.

11.2 Using Routed PPPoA

Access methods for PPP

Three methods exist to open a Routed PPPoA session:

- **Dial-in**
  The session is opened manually
- **Always-on**
  After the **AST570** is powered and finished its POST successfully, the **AST570** automatically tries to open the session
- **Dial-on-demand**
  The session is opened automatically, triggered by the arrival of packets at a/the **AST570** Ethernet port, destined for a Routed PPPoA connection.

PPPoA configuration

Per default, following Routed PPPoA connections are preconfigured:

- **DIALUP_PPP1**: dial-in connection
- **DIALUP_PPP2**: always-on connection
- **DHCP_SPOOF**: spoofing connection.

In case these entries do not meet your requirements, you can configure a new one as follows:

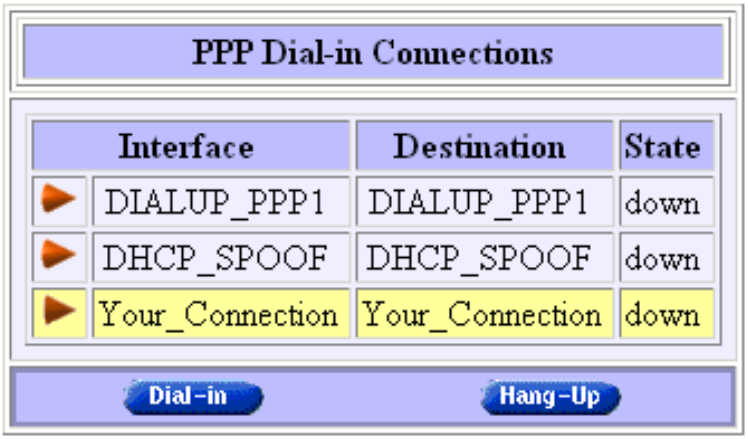
1. If needed, add an PPPoA phonebook entry with the correct VPI/VCI on the '*Phonebook*' page.
2. On the '*PPP*' page, select this phonebook entry from the 'Destination' pop-down list.
3. For this entry, select PPPoA in the '*Protocol*' field.
4. Select the correct encapsulation method from the *Encapulation*' pop-down list.
5. Optionally, enter user name and password.
6. Click Add.
7. Optionally, perform detailed configurations.

See section 9.3 for more information.

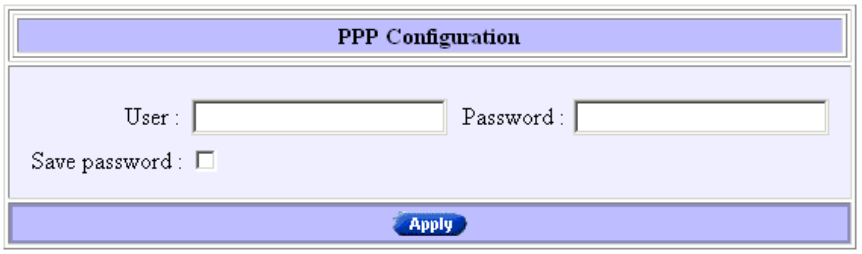
Opening dial-in sessions

Proceed as follows (See section 21.2 for more information):

1. Click Dial-in on the **AST570** pages.
2. On the *'Dial-in'* page the following table is shown:



3. Click next to the PPPoA entry you want to connect with. As a result your selection is highlighted.
4. Click Dial-in.
5. If applicable an *'Authentication'* table pops up:



Enter your user name and password in the appropriate fields. If you want the **AST570** to remember your credentials, check *'Save password'* (✓).

6. Click Apply.
7. After identification and authentication the *'Dial-in'* page reappears.

   While the **AST570** tries to open the session '**`trying`**' will appear in the *'State'* field. Once the session is active the field displays '**up**'. From then you are online and you can start your application or browse the Internet.

During the session

During the time the session is up, you can overview some important connection statistics on the *'PPP'* page.

See section 11.4.3 for more information.

Closing dial-in PPPoA sessions

Proceed as follows:

1. Browse to the *'Dial-in'* page.
2. Active PPPoA sessions are indicated via **up** in the *'State'* field.

   Click  next to the active PPPoA entry in the list you want to close the session for. As a result your selection is highlighted.
3. Click  .

   The session state of the entry will change to **down**, i.e. it becomes idle.

11.3 Routed PPPoA Configuration

Introduction

This section describes the use of the *'PPP'* page for Routed PPPoA and Routed PPPoE connectivity.

Prior to be able to use a Routed PPPoA or Routed PPPoE entry you may need to configure it. This is described in section 11.4.

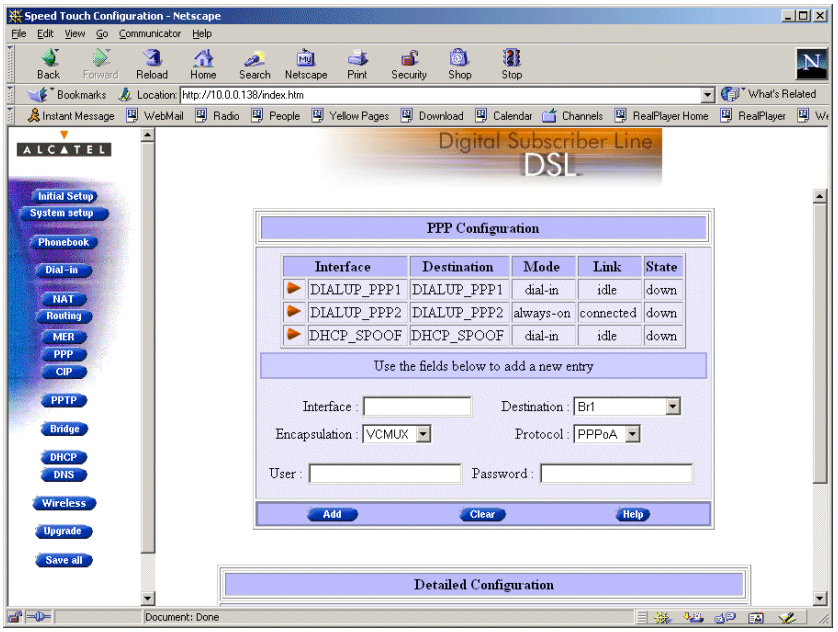
For more information on the use of the Routed PPPoE packet service of the **AST570** see chapter 9.

In this subsection

- The *'PPP'* Page
- The *'PPP Configuration'* Table
- *'PPP Configuration'* Table Components
- Adding Entries
- Deleting Entries.

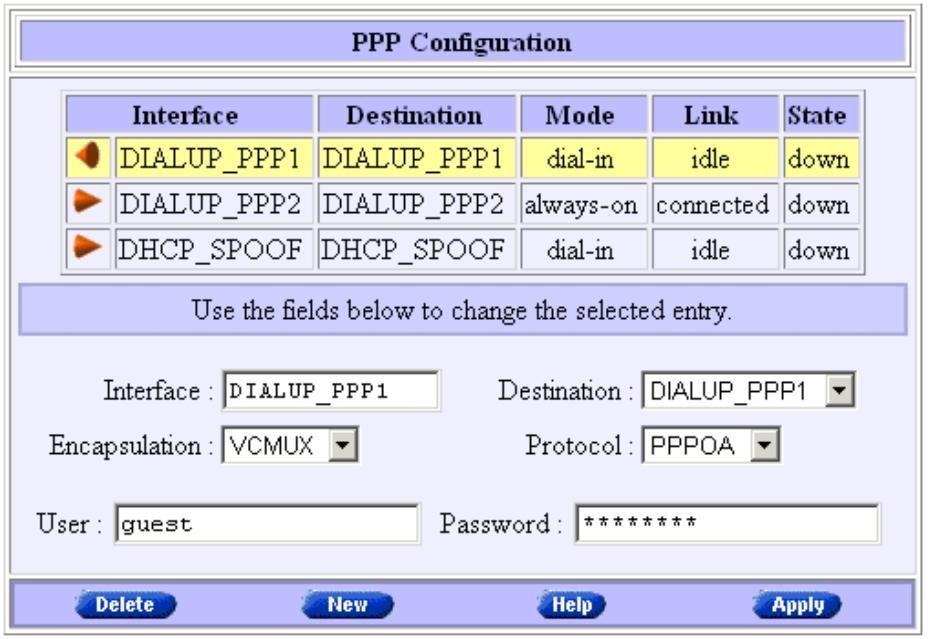
The 'PPP' page

Click PPP in the left pane of the **AST570** pages to pop up the *'PPP'* page (See section 21.2 for more information):



The 'PPP configuration' table

The following figure shows the *'PPP Configuration'* table:



'PPP Configuration' table components

Field	Description
Interface	Indicates the interface name for the PPP entry. **Note**: In most cases, the interface name will be the same as the phonebook entry name.
Destination	Indicates available phonebook entries for Routed PPPoA and Routed PPPoE. Following phonebook entries are shown: • Free PPPoA phonebook entries for PPPoA entries • Free ETHoA phonebook entries for PPPoE entries • Free "any" type phonebook entries.
Mode	Indicates whether the PPP entry is configured for: • "Always-on" connectivity • "Dial-in" session access • "Dial-on-Demand" session access. See section 11.4.2 for more information.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Link</td><td>Indicates the link state of the PPP entry.
It can take following values:
<table><tr><th>Value</th><th>Description</th></tr><tr><td>idle</td><td>The PPP entry is not activated, i.e. it does not setup a PPP connection.</td></tr><tr><td>Connected</td><td>The PPP entry is active, i.e. it tries to setup a PPP connection, or PPP connectivity is achieved.</td></tr></table></td></tr>
<tr><td>State</td><td>Indicates the active state of the PPP session.
It can take following values:
<table><tr><th>Value</th><th>Description</th></tr><tr><td>Up</td><td>The PPP session is opened and active.</td></tr><tr><td>Down</td><td>The PPP session is closed, the PPP connection is idle.</td></tr><tr><td>Trying</td><td>The PPP session is trying to reach the active state.</td></tr></table></td></tr>
<tr><td>Protocol</td><td>Indicates the packet service type for the PPP connection.
It can take following values:
<table><tr><th>Protocol</th><th>Description</th></tr><tr><td>PPPoA</td><td>The PPP connection is a Routed PPPoA connection.</td></tr><tr><td>PPPoE</td><td>The PPP connection is a Routed PPPoE connection.</td></tr></table></td></tr>
<tr><td>Encapsulation</td><td>Indicates the applied encapsulation method for the PPP frames on the VC.
The AST570 supports both the LLC/SNAP method (default for Routed PPPoE Ethernet frames) and the VC-MUX method (default for Routed PPPoA PPP frames).</td></tr>
<tr><td>User
Password</td><td>For authentication purposes a user name and password is required. These credentials are supplied by the SP.
Per default a guest account is assumed, i.e. both user name and password are “guest”. In case the SP has a guest account, you are able to open a session without having an actual subscription.</td></tr>
</table>

Adding entries

Proceed as follows:

1. Browse to the *'PPP'* page.
2. If needed, click New.
3. Select the PPPoA protocol from the *'Protocol'* pop-down list.
4. Select the phonebook entry from the *'Address'* pop-down list.

   Free PPPoA and ETHoA phonebook entries are shown as well as free "any" type phonebook entries. You must use a PPPoA or "any" type phonebook entry for Routed PPPoA.

   Note: In case the presented phonebook entries do not suite your desired configuration, you must firstly create a correct phonebook entry. See section 13.2 for more information.
5. Select the encapsulation method for the Routed PPPoA entry from the *'Encapsulation'* pop-down list (per default set to VC-MUX).
6. Optionally, enter user name and password for the Routed PPPoA entry.

   Note: In case you do not enter this information it is asked each time you open this PPPoA session.
7. Optionally, enter the appropriate configurations in the *'Detailed Configuration'* table.

   See section 11.4 for more information.
8. Click Add and Save all to finish the procedure.

Detailed configuration

Prior to using the PPPoA entry you may need to enter additional configurations for the connection.

See section 11.4 for more information.

Deleting entries

On the *'PPP'* page, click  next to the idle PPPoA entry you want to delete. As a result your selection is highlighted.

Click Delete and Save all.

11.4 Detailed Configuration

Introduction

Additional configuration of the Routed PPPoA connection may be needed in the *'Detailed Configuration'* table.

This section describes the various PPPoA connection configurations the **AST570** offers for assuring end-to-end connectivity.

The 'Detailed Configuration' page

On the *'PPP'* page a *'Detailed Configuration'* table can be found. The contents of this table are always related to the highlighted PPPoA connection in the *'PPP Configuration'* table.

The *'Detailed Configuration'* table contains three or four tabs. The first tab *'PPPoE'* is not of importance for Routed PPPoA. The second and third tab *'Routing'* and *'Other'* allow you to overview or configure connection related settings for the Routed PPPoA connection. The fourth tab *'Stats'* appears only if a session is running on the selected Routed PPPoA connection.

After configuration of these detailed Routed PPPoA entry aspects, press Apply and Save all to apply and save your changes.

Interaction with the AST570 IP router

Most of the configurations described in this section, influence the IP router in the **AST570**.

See section 14.5 for more information on IP routing aspects.

In this section

Topic	See
'Routing' Configurations	11.4.1
'Other' Configurations	11.4.2
'Stats' During a Routed PPPoA Session	11.4.3

11.4.1 'Routing' Configurations

Introduction

If a PPP session is opened successfully (either manually by the user, triggered by (W)LAN traffic or automatic at boot time) routes are automatically added to the **AST570**' routing table.

Advanced routing

For advanced users, the **AST570** allows manual configuration of permanent routes to dedicated destinations.

See section 14.5 for more information on the **AST570**' IP router.

Moreover, routes can be configured via the CLI which will only be added to the IP route table upon establishing the PPP connection.

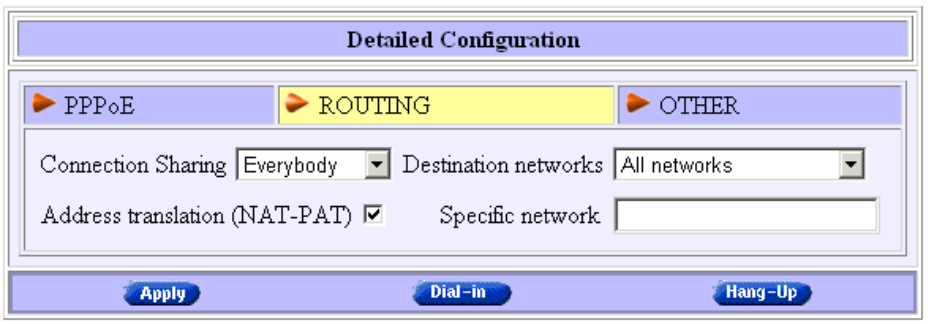
See chapter 22 for more information on the CLI.

In this subsection

- *'Routing'* Tab
- Connection Sharing
- Connection Sharing Subnet Values
- 'My net only' Configuration
- Destination Networks
- Destination Networks Subnet Values
- Address Translation.

The 'Routing' tab

The following figure shows the *'Routing'* tab:



Connection sharing

The *'Connection Sharing'* field allows you to configure which (W)LAN members, besides the PC that opened the PPP session, can use the PPP entry.

Three options are available:

- **Only Me**

  Only frames of the PC that opened the PPP session will be routed via this PPP entry.

  Suppose you opened a PPP session to your corporate and other (W)LAN members are surfing the Internet.

  Via this option you can prevent them from using the PPP entry to your corporate as their gateway to the Internet.

- **Everybody**

  All PC(s) on the local (W)LAN can forward frames over this PPP entry. This option is the exact opposite to *'Only me'*.

  If you open a PPP session to the Internet, other (W)LAN members can share the PPP entry. In this way they are not required to open a session themselves.

- **My net only**

  Only PC(s) sharing the same network and subnet number as the PC that opened the outbound PPP session can use the PPP entry.

Connection sharing subnet values

The following table lists the used classful netmasks, related to the three possible options:

Connection Sharing value	Related Source Subnet Mask	Notation
Only Me	255.255.255.255	/32
Everybody	0.0.0.0	/0
My net Only	This value depends on the subnet mask in use by the PC that opened the PPP session.	/*

'My net only' configuration

In case you want to privilege access via a particular PPP entry for specific PCs, proceed as follows:

Step	Action
1	Configure the PCs, to which you want to privilege outbound access via this PPP entry, in a particular subnet of your local (W)LAN. **Note**: Do not forget to make the **AST570** also a member of this workgroup.
2	Configure the '*Connection Sharing*' box of the particular PPP entry for '*My net only*'.
3	It is sufficient now to open the PPP session of this PPP entry from one PC of this subnet.

As a result, only the members of that particular subnet can share this PPP entry.

Destination networks

The '*Destination networks*' field allows you to configure which destination can be reached over the particular PPP entry.

Four options are available:

- **All networks**

  The **AST570** can potentially route frames to all destinations over this PPP entry. The PPP entry acts as if it was a default gateway.

- **Remote net only**

  A PPP entry configured for 'Remote net only' only forwards frames that is destined to this specific network. All other frames are blocked.

- **Remote host only**

  Only those frames with a destination IP address which matches exactly with this entry in the **AST570** routing table are forwarded over this PPP entry. In fact, only communication with the single remote host is possible.

- **Specific network defined below**

  If all previous cases do not fulfill your requirements, '*Specific network*' might help you out: you can specify which destination(s) are reachable over this PPP entry. Only if the destination IP address of a packet matches with this entry the packet is forwarded over this PPP entry.

Destination networks subnet values

The following table lists the default used classful netmasks related to the four possible options:

Connection Sharing value	Related Source Subnet Mask	Notation
All networks	0.0.0.0	/0
Remote net only	255.255.255.0	/0
Remote host only	255.255.255.255	/32
Specific network defined below	255.255.255.0.0 (default) This value is depending on the destination subnet mask.	/*

Address translation (✓)

You can apply Network Address and Port Translation (NA(P)T) on the (negotiated) PPP IP address. Per default NA(P)T are enabled.

Via this checkbox it is possible to check/uncheck the NA(P)T flag (✓).

See chapter 16 for more information.

11.4.2 'Other' Configurations

Introduction

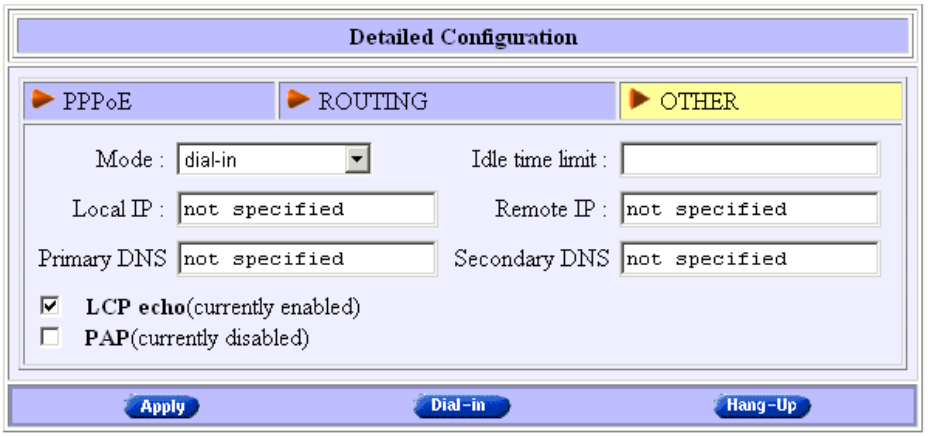
The following paragraphs explain which options that are used by a PPP entry when it opens a PPP session.

In this subsection

- *'Other'* Tab
- Mode: Triggering of a PPP Session
- Idle Time Limit
- Local and/or Remote IP: **AST570** PPP Client/Server Behavior
- Primary and Secondary DNS Server
- LCP Echo (✓) Requests
- PAP (✓): Authentication Protocols.

'Other' tab

Following figure shows the *'Other'* tab:



Mode: triggering of PPP session

The 'Mode' field allows you to configure how a PPP session is opened.

Three options are available:

- **Dial-in**

  The PPP session is opened manually by clicking Dial-in next to the PPP connection in the *'Dial-in'* page.

- **Always-on**

  After the **AST570** is powered and finished its Power On Self Test (POST) successfully, the **AST570** automatically tries to open a PPP session for the PPP entry.

- **Dial-on-demand**

  The PPP session is opened automatically for a limited period of time. The opening of the session is triggered by the arrival of packets at a/the **AST570** Ethernet port, to be sent over the PPP entry.

Note: By default one PPPoA connection is configured as *'Dial-in'* (i.e. *PPP),* another as *'Always-on'* (i.e. *PPP2*).

Idle time limit

In case you configured a PPP connection for *'Dial-on-demand',* the *'Idle Time Limit'* box allows you to specify the time after which an opened, but unused PPP session is closed.

If left free, the idle limit time is infinite (i.e. the PPP session will never be closed).

Local and/or remote IP: AST570 PPP server/client behavior

During the opening of a PPP session, IP addresses are negotiated between the two PPP peers for the PPP entry. The *'Local IP'* and *'Remote IP'* fields influence this negotiation.

Typically at the client side, the *'Local IP'* and *'Remote IP'* fields are left empty. This forces the client to ask the RAS for IP addresses.

In case you want to set up the **AST570** as PPP server, suitable values for your network configuration must be supplied:

- Setting a *local IP* address

  Forces the remote PPP client (if it allows to) to accept this IP address as the **AST570** PPP session IP address.

- Setting a *remote IP* address

  Forces the remote client (if it allows to) to accept this IP address as its PPP session IP address.

Primary and secondary DNS server

These fields allow – optionally – to enter the IP address(es) of the primary, and optionally the secondary, DNS server(s). If you supply these IP addresses the **AST570** will negotiate these addresses with the remote side of the PPP entry. If these fields are left blank the remote side will supply the IP addresses of the primary and secondary DNS servers.

See chapter 15 for more information on DNS.

LCP echo (✓) requests

If a PPP session is up, it can issue Link Control Protocol (LCP) echo requests at regular intervals and expect LCP echo replies in return.

This checkbox allows to turn on/off LCP echo request/replies by respectively checking (✓) or unchecking the *'LCP echo'* checkbox.

By default LCP echo is on (i.e. flagged ✓) allowing the local PPP peer to detect communication errors resulting in closing of the PPP session.

PAP (✓): used authentication protocol

The **AST570** features two authentication protocols to be used:

- Challenge Handshake Authentication Protocol (CHAP)
- Password Authentication Protocol (PAP).

Per default the **AST570** will negotiate CHAP with the BroadBand RAS (BBRAS) as it is the safest authentication protocol. However, PAP will be allowed, if needed.

Checking the PAP flag (✓) will force the **AST570** only to negotiate PAP with the BBRAS.

11.4.3 'Stats' During a Routed PPPoA Session

The 'Stats' tab

During a Routed PPPoA session a fourth tab *'Stats'* is available:

Configurable items

The *'Stats'* tab allows to overview some session statistics while a session is running on the selected Routed PPPoA entry.

Following session statistics are available:

- IP Address

  The IP address at the local peer of the current PPP link. This address can be dynamically assigned by the RAS or statically configured on the *'Other'* tab fields.

- Bytes received / Bytes sent

  The number of bytes received and sent since the Routed PPPoA session came up.

- Bytes dropped

  The number of bytes dropped, i.e. discarded due to failure since the Routed PPPoA session came up.

12 Configuration and Use – CIP & IP Routing

Introduction

Classical IP & IP routing(*) is the packet service of your choice as it:

- Is a third standardized method next to PPPoA and PPPoE for creating IP networks on top of ATM technology
- Is traditionally well supported by ATM access routers at the remote end of the connection
- Similar to Bridging, provides "Always-on" type of connections.

(*) In the following, Classical IP & IP Routing will be referred to as Classical IP (CIP).

In this chapter

Topic	Section
Preparatory Steps	12.1
CIP Configuration for a LIS	12.2
Using CIP & IP Routing	12.3
CIP Configuration	12.4

12.1 Preparatory Steps

Needed information

- **VPI/VCI** value of the VC(s) to use on the DSL line
- **IPoA (RFC1483/Routed) connection service** must be supported on this VC
- **Encapsulation** method (LLC/SNAP)
- For full compliancy to RFC1577 the remote access device must issue and respond to **InATMARP** messages.

Note: The RFC1577 on which Classical IP over ATM relies is updated by RFC2225. The **AST570** fully complies with both RFCs.

Multiple destinations

The **AST570** can manage up to 12 CIP connections simultaneously.

Note: Check with your SP whether multiple end-to-end connectivity is enabled.

PC(s)

In order to use the CIP & IP Routing mode of the **AST570**, the OS on your PC(s) must support TCP/IP.

See chapter 14 for more information on IP.

12.2 CIP Configuration for a LIS

Introduction

This section describes the basic procedures to enable connectivity in a Logical IP Subnet (LIS) via the ATM core network.

In this section

Topic	See
General CIP Configuration Procedure	12.2.1
Retrieving LIS Parameters	12.2.2
Implicit Assignment Mechanism	12.2.3
Explicit Assignment Mechanism	12.2.4
Configuring the **AST570** for CIP	12.2.5
Adding Appropriate Routes to the Routing Tables.	12.2.6
Example of a CIP LIS Configuration	12.2.7

12.2.1 General CIP Configuration Procedure

Decision procedure

Due to the many decisions that must be made in order to be able to configure the **AST570** to be an active member of a LIS, the procedure to be followed is best retrieved from the following decision table:

<table>
<tr><th>Step</th><th>Decision and/or Action</th><th>See</th></tr>
<tr><td>1</td><td>Are you configuring the AST570 for an existing LIS ?
<table><tr><th>Answer</th><th>Action and Description</th></tr><tr><td>Yes</td><td>You must retrieve the LIS IP parameters to which your local configuration must adhere to. See topic 'Configuration for an Existing LIS' of subsection 12.2.2.</td></tr><tr><td>No</td><td>You can create the LIS with IP parameters of your choice. See topic 'Creating a New LIS' of subsection 12.2.2.
In case you create a new LIS, you must create the LIS at both end of the DSL connection, i.e. at the local, and on the remote side.</td></tr></table></td><td>12.2.2</td></tr>
<tr><td>2</td><td>Retrieve the appropriate LIS parameters, and check on which VCs (identifiable by their VPI/VCI values) your SP enabled the IPoA connection service.</td><td>12.2.2</td></tr>
<tr><td>3</td><td>If needed, create a CIP phonebook entry, i.e. a CIP PVC in the 'Phonebook' page.</td><td>12.4</td></tr>
<tr><td>4</td><td>Is the remote access router an RFC1577/RFC2225 compliant device, e.g. another AST570?
<table><tr><th>Answer</th><th>Action and Description</th><th>See</th></tr><tr><td>Yes</td><td>The remote access router will respond to 'InATMARP' requests, thus the CIP PVC can be implicitly assigned to the CIP member.</td><td>12.2.3</td></tr><tr><td>No</td><td>The remote access router will not respond to 'InATMARP' requests submitted by the AST570, thus the CIP PVC must be explicitly assigned to the CIP member.</td><td>12.2.4</td></tr></table></td><td></td></tr>
<tr><td>5</td><td>If needed, create a CIP member in the 'CIP Interfaces' table of the 'CIP' page.</td><td>12.4</td></tr>
<tr><td>6</td><td>Add appropriate IP routes to the AST570 via the 'IP route' table on the 'Routing' page.</td><td>12.2.6</td></tr>
<tr><td>7</td><td>Add appropriate IP routes in you PC(s).</td><td>12.2.6</td></tr>
</table>

12.2.2 Retrieving LIS Parameters

LIS

The LIS is an important CIP concept. It is a group of IP machines configured as members of the same IP subnet. In other words: they share the same IP network and subnetwork numbers.

In most cases this LIS will be a corporate LAN/WAN environment, which is interconnected via the DSL/ATM network.

LIS parameters

In order to be able to properly configure your **AST570** for sharing the same logical IP subnet, you must know the following LIS parameters:

- The IP network number
- The IP subnetwork number
- The remote access router's RFC1577/RFC2225 compliancy state
- The remote access router IP address, in the case it is not RFC1577/RFC2225 compliant.

Of course, in case you know the IP address of one member of the LIS, and the associated netmask, you also have enough information.

Configuration for an existing LIS

For an existing LIS, you must configure the **AST570** CIP settings, according to the existing LIS parameters.

If the default CIP member's IP parameters, and the CIP connection's remote IP address, configured in the **AST570**, match with these parameters, nothing needs to be configured.

However, make sure that the CIP member's local IP address is not ambiguous within the LIS.

Creating a new LIS

In the case of creating a new LIS, you are recommended to use the default CIP configurations of the **AST570**. In case the remote access router is also a **AST570**, best results are assured.

Note: Both ends of the LIS must be properly configured for connectivity, inclusive the routing tables.

12.2.3 Implicit Assignment Mechanism

Implicit assignment

If the remote side is RFC1577/RFC2225 compliant, e.g. another **AST570**, your local **AST570** is able to retrieve the remote IP address of the CIP PVC, by issuing an InATMARP request on that PVC.

That way, you must not specify an IP address for the CIP PVCs you add to the *'CIP Connections'* table, it will be implicitly assigned when connecting to the LIS.

Implicit assignment example

The sequence below describes an example of an implicit assignment mechanism:

<table>
<tr><th>Phase</th><th colspan="3">Decision and Description</th></tr>
<tr><td>1</td><td colspan="3">Suppose you added a CIPPVC without supplying an IP address (e.g. CIPPVC2).</td></tr>
<tr><td>2</td><td colspan="3">The AST570 will automatically issue an InATMARP request on this PVC.</td></tr>
<tr><td rowspan="3">3</td><td colspan="3">Is the remote side is RFC1577/RFC2225 compliant ?</td></tr>
<tr><td colspan="2">Yes</td><td>No</td></tr>
<tr><td colspan="2">It responds with an InATMARP reply, containing its IP address.
The CIP's remote IP address in the 'CIP Connections' table is completed.</td><td rowspan="3">"Unresolved" will show up in the 'Remote IP Address' field.
Consequently the CIPPVC cannot be assigned and IP connectivity will not exist with the remote machine.</td></tr>
<tr><td>5</td><td colspan="2">Does the remote address share a LIS with a local CIP member ?</td></tr>
<tr><td rowspan="2">6</td><td>Yes</td><td>No</td></tr>
<tr><td>the CIPPVC is assigned to this member.
Connectivity is assured.</td><td>"Unresolved" will show up.
No connectivity exists.</td></tr>
</table>

Note

The grey shaded area of the table indicates the sequence of a correct RFC1577/RFC2225 compliant LIS interconnection.

12.2.4 Explicit Assignment Mechanism

Explicit assignment

In the case of a remote access server which is not RFC1577/RFC2225 compliant, it will not respond to InATMARP requests.

As a consequence, the **AST570** can not retrieve the remote IP address to assign the CIP PVC to the CIP member.

Therefore you must explicit assign a remote IP address to the CIP PVC.

Explicit assignment example

The default configuration of the **AST570** is an example of the explicit assignment of a CIP PVC to a CIP member:

In the *'CIP Interfaces'* table, the CIP member is configured as follows:

Intf	Local Address	Mask
cip0	172.16.1.1	255.255.255.0

In the *'CIP Connections'* table, the remote IP address is statically configured:

Nr	Dest	Remote Address
1	CIPPVC1	172.16.1.2

Consequently, *CIPPVC1* is explicitly assigned to *cip0*.

Note

Both local and remote IP addresses must fall within the same IP network and IP subnetwork, according the LIS parameters.

12.2.5 Configuring the AST570 for CIP

Introduction

After retrieving the LIS parameters, you must configure the **AST570**, according to these parameters.

This section describes in short the global procedure for configuring your **AST570** *'Phonebook'* and *'CIP'* pages.

Configuration of the AST570 'Phonebook' page

By default the **AST570** is configured for a CIP VC as used in the example of section 12.2.7. If this VC is appropriate to your, and/or the SP's needs, nothing has to be configured in the **AST570** phonebook.

If this VC does not match the requirements, three other CIP phonebook entries are available to add.

However, in the case none of the entries match, you must add a CIP phonebook entry yourself.

Adding phonebook entries is described in section 13.2.

Configuration of the AST570 'CIP' page

The default CIP phonebook entry mentioned above is by default configured for a LIS according to the example of section 12.2.7. If this LIS configuration meets your requirements, nothing needs to be configured, and your **AST570** is ready for use.

However, if additional configuration is needed, you can configure CIP members yourself.

The assignment of your CIP PVC to the CIP member can be done implicit, or explicit, according the RFC1577/RFC2225 compliancy of the remote access router.

Configuration of the **AST570** *'CIP'* page is fully described in section 12.4.

12.2.6 Adding Appropriate Routes to the Routing Tables

Introduction to routing

IP routing is a very important aspect for a LIS configuration.

This subsection describes how you can ensure end-to-end connectivity for a CIP environment.

- Configuring the **AST570** for LIS Connectivity, Basic
- Configuring the **AST570** for LIS Connectivity, Advanced
- Configuring your (W)LAN PCs for End-to-End Connectivity
- Routing Table Configuration.

Configuring the AST570 for LIS connectivity, basic

Generally, for proper CIP routing, an IP route pointing to the remote access router must exist in your **AST570**' IP routing table.

If the remote access router is RFC1577/RFC2225 compliant, no routes for LIS connectivity need to be configured by yourself for the **AST570**' IP router. This because it automatically adds two necessary routes as soon you configure the CIP member, i.e. two default gateways, thus any (0.0.0.0/0) as source address, and with:

- The LIS's local CIP member's IP address, i.e. the **AST570**' CIP interface address as destination

and

- The LIS's IP subnetwork (based on the CIP member's IP parameters) as destination.

As the RFC1577/RFC2225 compliant remote access router, falls within the same LIS as the **AST570** CIP member, it is also a member of the second route's destination IP subnetwork.

If the remote access router is not RFC1577/RFC2225 compliant, you must add this default route (with the known remote IP address) yourself.

Configuring the AST570 for LIS connectivity, advanced

The possibility exists to add routes yourself, e.g. to be more specific in the source IP address pool.

The default added routes have any as source address, meaning that all local hosts can use this gateway to connect to the LIS via the CIP interface.

However, you might want to embed restrictions in LIS access by creating a subnet in your (W)LAN, e.g. 10.0.1.x, and privilege access to the LIS – and its beyond (W)LAN – to this subnet by adding a route pointing to the remote access router (implicit, or explicit) but with now source IP address pool 10.0.1.0/24.

Of course, then the default IP routes, configured by default, must be deleted.

Configuration your (W)LAN PCs for end-to-end connectivity

In order to have end-to-end connectivity from your PCs to the remote side of the CIP connection and beyond you must add routes having the **AST570** Ethernet interface IP address as gateway.

By specifying 0.0.0.0/0 as destination and the **AST570** local Ethernet IP address as gateway the **AST570** is configured as the default gateway for all connection requests.

However, you can specify a destination IP address pool; e.g. if the remote LAN's IP subnetwork is 192.6.11.x, you can add routes in your PC's routing table with destination 192.6.11.0/32, and the **AST570** as gateway.

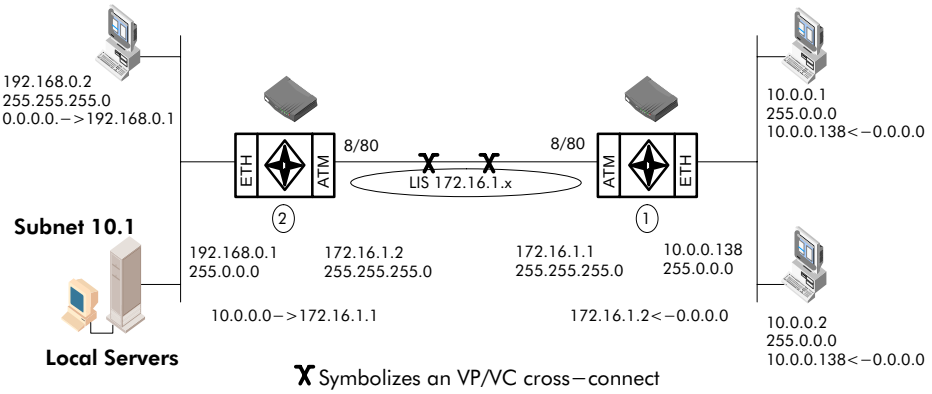
Routing table configuration

Configuring routes for the **AST570** is described in section 14.5.

12.2.7 Example Configuration

Configuration figure

The configuration of a Classical IP LIS is illustrated with the following example:



In the drawing above a LIS, 172.16.1.x, represented by the ellipse, runs between the **AST570(1)** and access router(2).

Local premisses configuration

At the local premisses an IP network, 10.x.x.x, is created.

An IP address is configured on the Ethernet port (10.0.0.138).

On the DSL side of the **AST570(1)** one CIP member is by default enabled. This CIP member is configured with IP address 172.16.1.1 and is part of the LIS 172.16.1.x.

One VC in the **AST570(1)** phonebook (CIPPVC1), is explicitly assigned to this CIP member. This VC(8/80) is cross-connected to the remote destination.

Remote premisses configuration

At the remote DSL side, the CIP LIS is terminated by access router(2) and IP packets are forwarded to local servers or the Internet and vice versa.

Here, the CIP member is configured with IP address 172.16.1.2 and is part of the same LIS 172.16.1.x.

Additionally, a VC with the same VPI/VCI values 8/80 is assigned to this CIP member (e.g. implicit assignment, because **AST570(1)** is RFC1577/RFC2225 compliant).

Routing configuration

The routing engine must be configured with routes to the final destinations.

For the given example, the configuration is as follows:

- **AST570(1)** has its default route pointing to access router(2).

  The local PCs of IP network 10.0.0.x have default gateways pointing to **AST570(1)**.

- The access router(2) has a route for "Net10" (10.0.0.0) pointing to **AST570(1)**

  The remote IP network 192.168.0.x has a default gateway pointing to access router(2).

Note

You will notice that the example relies exclusively on *Private* IP addresses. Depending the application though, other IP addresses in combination with NA(P)T can be used.

See chapter 16 for more information on NA(P)T.

12.3 Using CIP & IP Routing

CIP operation

Similar to classical LAN networking CIP & IP Routing adheres to the "always-on" concept.

IP packets sourced by local PCs, arrive via the Ethernet segment in the **AST570**. The latter makes routing decisions based on the destination IP address of the packet. If the packet ends up in the CIP member it will on its turn determine to which VC it has to output the packet.

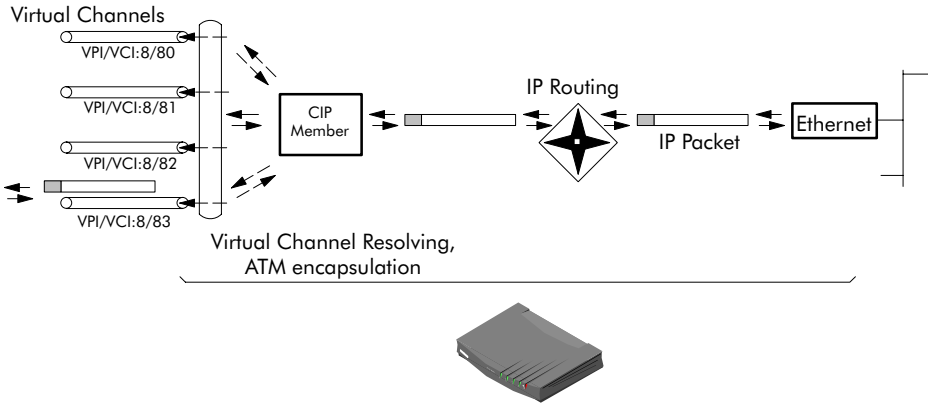
You can check IP connectivity from any PC on the local Ethernet segment. Therefor, ping the IP address at the far end of the virtual connection; e.g. for the example of subsection 12.2.7, this would be 172.16.1.2, or thus **`ping 172.16.1.2`**.

Classical IP and AST570

The IP router in the **AST570** forwards packets between the Ethernet port and the Classical IP entity sitting on top of the DSL/ATM port. In turn, the CIP entity determines which VC it has to output the packet to, prior to ATM encapsulation.

Configuration and operation example

The figure below provides an overview of the **AST570** rear-to-front end Classical IP operation:



12.4 CIP Configuration

Introduction

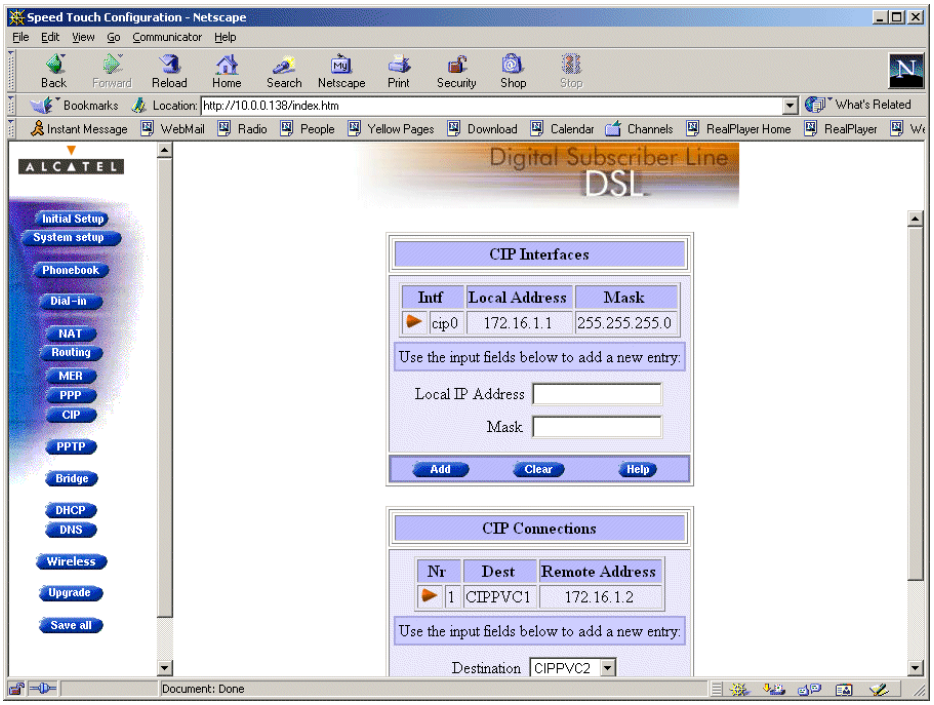
This section describes the use of the **AST570** *'CIP'* page.

In this section

- The *'CIP'* Page
- The *'CIP Interfaces'* Table
- *'CIP Interfaces'* Table Components
- The *'CIP connections'* Table
- *'CIP Connections'* Table Components
- Adding CIP members
- Assigning CIP PVCs to CIP members
- Deleting CIP Entries.

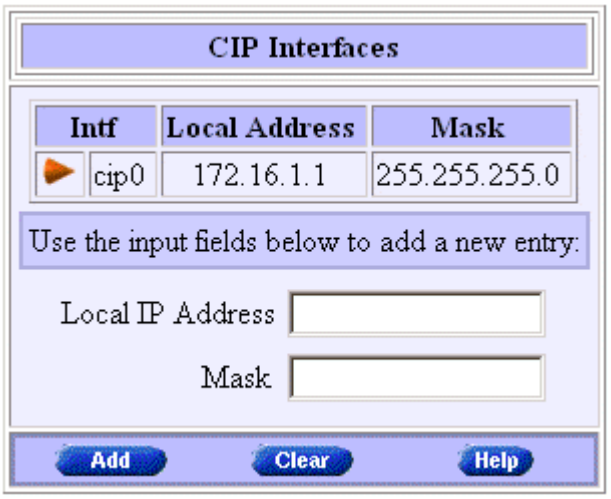
The 'CIP' page

Click CIP in the left pane of the **AST570** pages to pop up the *'CIP'* page (See section 21.2 for more information):



The 'CIP Interfaces' table

The following figure shows the *'CIP Interfaces'* table:

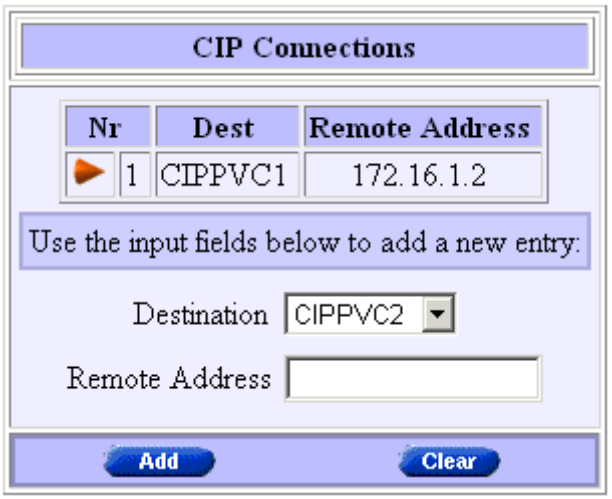


'CIP Interfaces' table components

Field	Description
Intf	Indicates the CIP member name. All CIP members are named '*cipX*', where *X* is a number.
Local Address	Indicates the IP address of the local DSL side of the LIS, i.e. the IP address of your CIP interface.
Mask	Indicates the netmask/subnetmask of the local IP address. **Note**: The netmask may be classful or classless.

The 'CIP Connections' table

The following figure shows the *'CIP Connections'* table:



'CIP Connections' table components

Field	Description
Dest	Indicates the CIP VC phonebook name.
Remote Address	Indicates the remote IP address of the remote DSL side of the LIS, i.e. the IP address of the remote CIP interface. **Note**: In case the VC is not cross-connected, or implicit assignment was not successful, this field shows *"Unresolved"*.

Adding CIP members

Proceed as follows:

1. Browse to the *'CIP'* page.

   Addition of a CIP member is performed in the *'CIP Interfaces'* table.

2. If needed, click New in the *'CIP Interfaces'* table.
3. Enter in the following CIP member parameters:
   - **Local IP address**

     The IP address of the CIP member at your local side of the LIS.
   - **Mask**

     The associated classful or classless netmask/subnetmask for this local IP address.
4. Click Add and Save all to finish the procedure.

Result

A CIP member of the LIS is created at your **AST570**' CIP interface side of the LIS. The local IP address is added to the *'IP Address'* table.

Two default routes are added to the *'IP Route'* table, both pointing to the **AST570** as gateway, but the first with the CIP member itself as destination, the second with the LIS subnetwork IP address pool as destination.

Assigning CIP PVCs to CIP members

Proceed as follows:

1. Browse to the *'CIP'* page.

   Assignment of a CIP PVC is performed in the *'CIP Connections'* table.

2. If needed, click New in the *'CIP Connections'* table.

3. Select the phonebook entry from the *'Destination'* pop-down list.

   You must use a IPoA or "any type" phonebook entry for CIP connections.

   Note: In case the presented phonebook entries do not suite your desired configuration, you must firstly create a correct phonebook entry. See section 13.2 for more information.

4. Depending the RFC1577/RFC2225 compliancy of the remote access router the following must be entered in the *'Remote address'* field:

Compliancy	Remote IP address
YES	You don't have to fill in anything; the InATMARP reply will implicitly assign the PVC to the CIP member.
NO	You must fill in the exact IP address of the remote access router; the PVC is explicitly assigned to the CIP member.

5. Click Add and Save all to finish the procedure.

Deleting CIP entries

On the *'CIP'* page, click  next to the CIP connection or CIP interface you want to delete. As a result your selection is highlighted.

Click Delete and Save all.

Alcatel
Speed Touch™570

Networking

13 Networking – ATM

Introduction

All data arriving at and departing from your **AST570** via the DSL line is carried in Asynchronous Transfer Mode (ATM) cells.

In this way, ATM is the fundamental communication “language” for the **AST570** towards the remote devices.

In this chapter

Topic	See
The ATM Packet Switching Technology	13.1
The **AST570** Phonebook	13.2

13.1 The ATM Packet Switching Technology

ATM Switching

ATM is a connection-oriented packet switching technology using fixed-size packets, called *cells*.

These cells consist of a header and a payload and are switched through a public or private ATM network depending on the contents of the header.

End-to-end connections are formed by cross-connecting individual ATM segments in ATM switches.

In this section

Topic	See
ATM Parameters	13.1.1
ATM and the **AST570**	13.1.2
ATM and Interfaces	13.1.3

13.1.1 ATM Parameters

Virtual channels

ATM uses VCs to create individual communication links between network nodes. ATM uses two types of VCs:

- Permanent Virtual Channels (PVCs) are static connections between network nodes that are configured statically. For a Permanent Virtual Channel (PVC) the nodes of the connection operate as if they are connected with a dedicated physical line.
- Switched Virtual Channels (SVCs) are similar to voice telephone network connections. These are temporary connections between any two end points on the network and are configured via signaling. A Switched Virtual Channel (SVC) is created dynamically for each session and released when the information exchange is complete.

VCs and the AST570

Currently all **AST570** ATM connections are static, i.e. of type PVC.

Channel identifiers

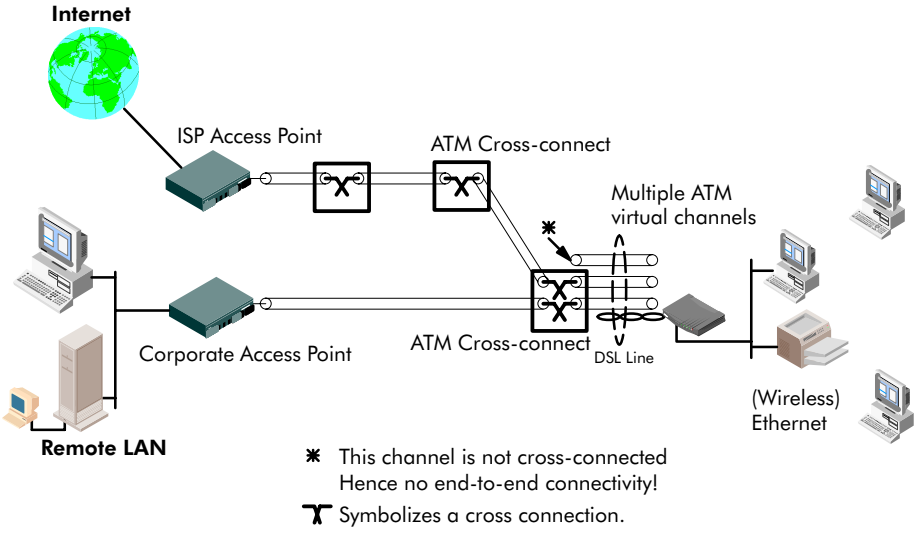
Each ATM cell carries two labels called Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) as part of its header.

An ATM channel, commonly referred to as ***Virtual Channel***, is fully identified by these two labels. Therefore, multiple ATM channels can reside on your DSL line.

13.1.2 ATM and the AST570

End-to-end ATM connectivity

The following figure provides an overview of the end-to-end architecture of the ATM connectivity; from your **AST570** to remote access devices.



AST570 vs. remote destination

Practically speaking, a number of VCs to one, or multiple remote destination(s) can start from/are terminated at the **AST570**.

By default, a number of channels are terminated in the **AST570** for end-to-end connectivity with the local (W)LAN.

ATM provision

End-to-end ATM connectivity is the responsibility of local operators. There might be regional differences in the type and number of VCs that are cross-connected.

If problems are encountered, check with your local operator for more information.

13.1.3 ATM and Interfaces

ATM traffic handling

Inside ATM VCs any protocol can be transported. However, at both endpoints – that is where the ATM channels are terminated – the same protocol must be supported. If not, there will be no end-to-end connectivity.

(W)LAN interfaces

These interfaces terminate a number of ATM connections and extract frames from arriving cells and encapsulates frames in departing cells.

Only frames recognized/supported by the **AST570** on a particular ATM connection are extracted, or encapsulated.

Currently the supported encapsulations are:

- For **Transparently Bridged** connections:

  RFC 1483, Ethernet V2.0/IEEE 802.3 bridged PDUs for both the LLC/SNAP method and VC-MUX method

- For **Routed Ethernet** connections:

  RFC 1483, Ethernet V2.0/IEEE 802.3 bridged PDUs for both the LLC/SNAP method and VC-MUX method

- For **Bridged PPPoE** connections:

  RFC 1483, Ethernet V2.0/IEEE 802.3 bridged PDUs for both the LLC/SNAP method and VC-MUX method

- For **Routed PPPoE** connections:

  RFC 1483, Ethernet V2.0/IEEE 802.3 bridged PDUs for both the LLC/SNAP method and VC-MUX method

- For **Relayed PPPoA** connections:

  RFC 2364, PPP PDUs for both the LLC/NLPID method and VC-MUX method

- For **Routed PPPoA** connections:

  RFC 2364, PPP PDUs for both the LLC/NLPID method and VC-MUX method

- For **CIP & IP Routing** connections:

  RFC 1483 LLC/SNAP method for Routed PDUs.

13.2 The Speed Touch Phonebook

Introduction

The **AST570** phonebook is like any ordinary phonebook:

"A repository for names and numbers".

However, in contrast to a standard phonebook it contains additional connectivity information.

Basic to the **AST570** operation are ATM VCs. The **AST570** phonebook is the management tool for all possible ATM connections.

This chapter describes how to use the **AST570** phonebook and consequently how to manage this VC pool.

In this section

Topic	See
The 'Phonebook' Page	13.2.1
Using the Phonebook	13.2.2
AutoPVC	13.2.3

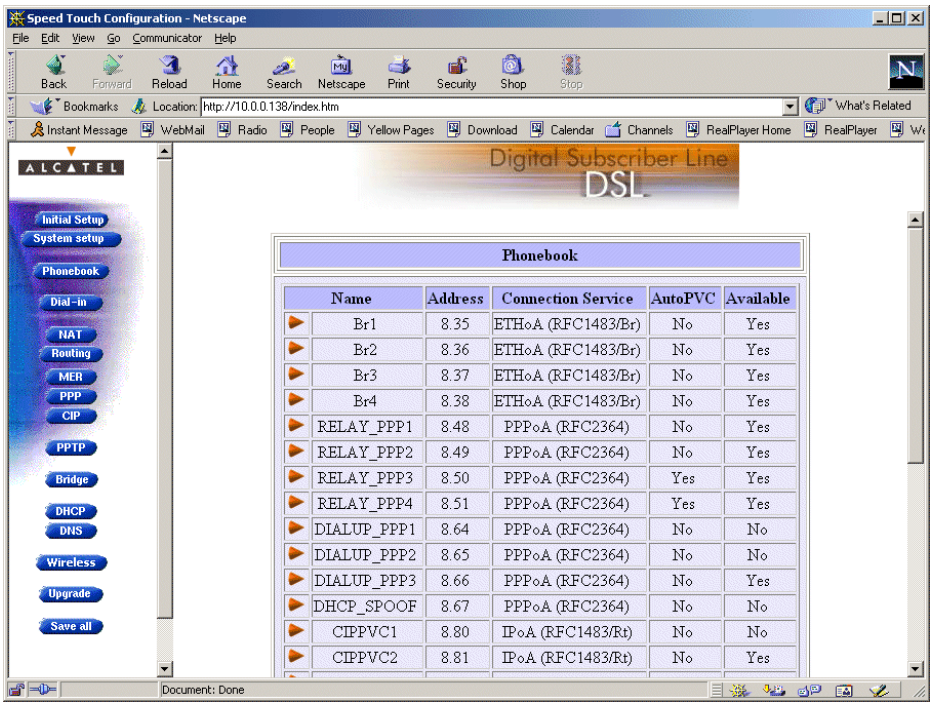
13.2.1 The AST570 'Phonebook' Page

In this subsection

- The *'Phonebook'* Page
- The *'Phonebook'* Table
- *'Phonebook'* Table Components
- Phonebook Defaults
- The *'AutoPVC'* Table.

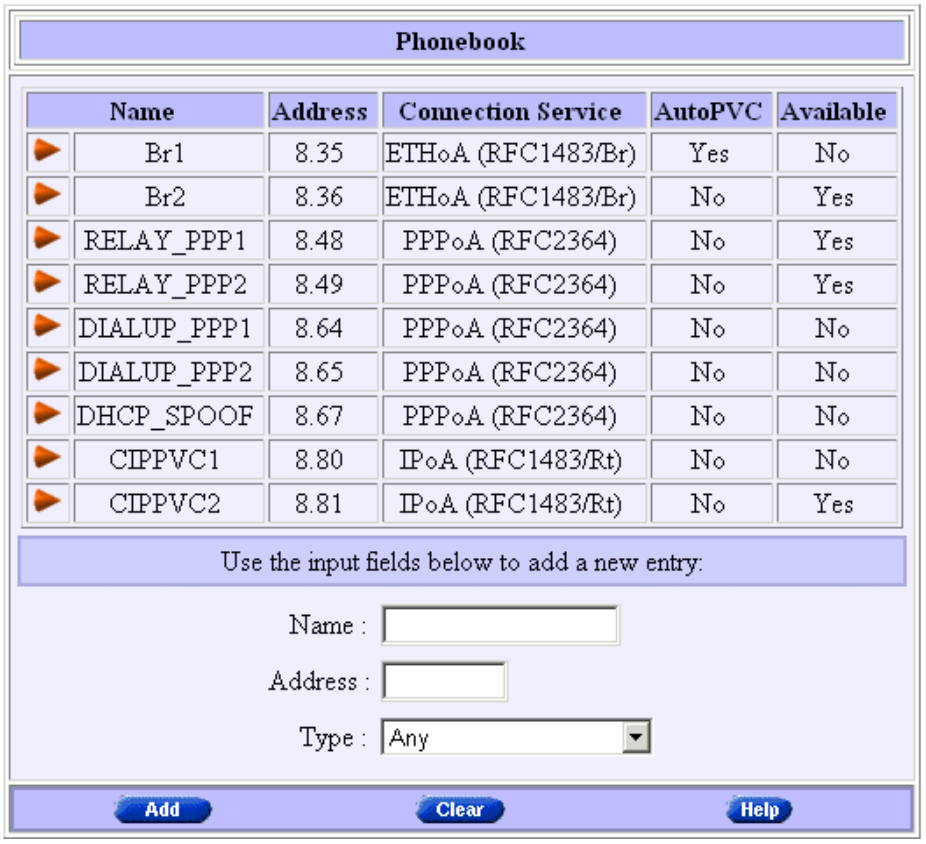
The 'Phonebook' page

Click Phonebook in the left pane of the **AST570** pages to pop up the *'Phonebook'* page (See section 21.2 for more information):



The 'Phonebook' table

The following figure shows an example of the *'Phonebook'* table of the *'Phonebook'* page:



'Phonebook' table components

Field	Description
Name	Indicates the name, or alias of the phonebook entry. Any name can be given to an entry.
Address	Indicates the VPI and VCI value of the ATM VC terminated on the DSL port for the phonebook entry. The allowed VPI range: from 0 up to 15. The allowed VCI range: from 32 up to 511.

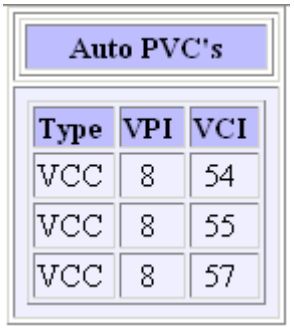
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Type</td><td>Represents the connection service supported on the ATM VC.
It can take the following values:
<table>
<tr><th>Value</th><th>Packet Service</th></tr>
<tr><td>ETHoA
RFC1483/Br</td><td>Transparent Bridging
See chapter 6 for more information.</td></tr>
<tr><td></td><td>Routed Ethernet (MER)
See chapter 7 for more information.</td></tr>
<tr><td></td><td>Bridged PPPoE
See chapter 8 for more information.</td></tr>
<tr><td></td><td>Routed PPPoE
See chapter 9 for more information.</td></tr>
<tr><td>PPPoA
RFC2364</td><td>Relayed PPPoA
See chapter 10 for more information.</td></tr>
<tr><td></td><td>Routed PPPoA
See chapter 11 for more information.</td></tr>
<tr><td>IPoA
RFC1483/Rt</td><td>CIP & IP Routing
See chapter 12 for more information.</td></tr>
<tr><td>any</td><td>Any kind of packet service is allowed.</td></tr>
</table></td></tr>
<tr><td>Auto PVC</td><td>Indicates whether the entry is listed in the 'AutoPVC' list (yes) or not (no).
See subsection 13.2.3 for more information.</td></tr>
<tr><td>Available</td><td>Indicates the availability of the VC phonebook entry. An entry is available if it is not configured in any AST570 packet service page, or not in temporary use by a packet service.</td></tr>
</table>

Phonebook defaults

The phonebook entries configured by default are listed in appendix E.

The 'AutoPVC' table

The following figure shows an example of the *'AutoPVC'* table:



Auto PVC's

Type	VPI	VCI
VCC	8	54
VCC	8	55
VCC	8	57

Any PVC, identified by its VPI/VCI and communicated via AutoPVC is added to the *'AutoPVC'* table. If AutoPVC is not supported at the remote side, i.e. the Digital Subscriber Line Access Multiplexer (DSLAM), the *'AutoPVC'* table stays empty.

See subsection 13.2.3 for more information.

13.2.2 Using the Phonebook

Introduction

The main function of the **AST570** phonebook is to present an instant overview of all possible entries and their status.

Another important function is that it helps you to navigate through the various **AST570** VC connection possibilities.

In this subsection

- Restrictions for Adding Phonebook Entries
- Adding Entries
- Deleting Entries.

Restrictions for adding phonebook entries

Although you are free to give any name to a phonebook entry, a few restrictions apply:

- You may not provide an entry with a name which already is supplied in the *'Phonebook'* table.
- Phonebook entries, which are intended to be used for the Relayed PPPoA packet service may not start with a capital 'P' or a capital 'T'.
- In case you want to use the **AST570** PPP-to-DHCP Spoofing feature the name of the PPP entry you intend to use with this feature must start with 'DHCP', e.g. DHCP_Spoof1, DHCP_2, etc.

Each entry in the **AST570** phonebook must have a unique VC, i.e. a unique VPI/VCI combination. Adding a phonebook entry with a VPI/VCI, which is already used in the *'Phonebook'* table will result in an error message.

Adding phonebook entries

Proceed as follows:

1. Browse to the *'Phonebook'* page.
2. If needed, click New.
3. Enter a name of your choice to identify the new phonebook entry in the *'Name'* field.
4. Enter the VC's VPI.VCI values in the *'Address'* field.

   Note: In most cases these values are provided by your SP.
5. Select the Connection Service of your choice, or choose any from the *'Type'* pop-down list.
6. Click Add and Save all to finish the procedure.

Deleting phonebook entries

On the *'Phonebook'* page, click  next to the phonebook entry you want to delete. As a result your selection is highlighted.

Click Delete and Save all.

CAUTION

Phonebook entries which are currently in use by a packet service (*'Available'* field = No) cannot be deleted.

In the case you want to delete a configured phonebook entry, firstly you must delete the entry on the related packet service web page.

E.g. for a configured IPoA phonebook entry, you must firstly delete the entry from the *'CIP connections'* table on the *'CIP'* page, prior to be able to delete the phonebook entry on the *'Phonebook'* page.

13.2.3 AutoPVC and the Phonebook

AutoPVC

The default VCs, can be remotely modified via the *AutoPVC* feature of the **AST570**. AutoPVC operates only in conjunction with the Alcatel DSLAM – often referred to as ATM Subscriber Access Multiplexer (ASAM) – and offers the functionality that user VCs that are to be terminated on the Ethernet port, can be notified by the **AST570**.

Operation of AutoPVC

Basically the following steps are executed:

1. The SP configures VCs on the DSLAM.
2. Via AutoPVC the VPI/VCI values are communicated to the **AST570**.
3. AutoPVC messages are subsequently processed by the **AST570**, according to the two criteria listed below.

Criterion 1

Any PVC, i.e. VPI/VCI, communicated via AutoPVC is added to the *'AutoPVC'* list on the *'Phonebook'* page.

If AutoPVC is not supported by the DSLAM, this list is empty.

Criterion 2

If the VPI/VCI value is used in the phonebook, the *'AutoPVC'* column will show **Yes** next to the corresponding phonebook entry.

Example Suppose the SP configures one of the **AST570'** default terminated VCs, e.g. 8/35 on the DSLAM.

VPI/VCI 8/35 will end up in the *'AutoPVC'* list:

Auto PVC's

Type	VPI	VCI
VCC	8	35

As this VC matches with the Bridging entry *Br1,* the *'AutoPVC'* field of this phonebook entry will indicate *"Yes"*:

Phonebook

Name	Address	Connection Service	AutoPVC	Available
Br1	8.35	ETHoA (RFC1483/Br)	Yes	No
Br2	8.36	ETHoA (RFC1483/Br)	No	Yes
Br3	8.37	ETHoA (RFC1483/Br)	No	Yes

In this way the user can distinguish an activated VC from dummy phonebook entries.

14 Networking Services – IP

Introduction

For Internet access and home networking, IP(*) plays a crucial role. Due to the flexibility and the multitude of IP features, numerous configurations are possible.

(*) Although not the same, IP is often referred to as Transmission Control Protocol (TCP)/IP.

Aim of this chapter

This chapter highlights some general IP parameters and some possible IP configurations for the below purposes:

- Internet access via your SP
- Private LAN-to-LAN interconnections over the DSL/ATM network
- Local IP connectivity towards other PCs on your (W)LAN.

In this chapter

Topic	See
AST570 and IP	14.1
Packet Services and IP	14.2
AST570 Addresses	14.3
AST570 DHCP	14.4
AST570 Routing	14.5

14.1 Speed Touch and IP

Introduction

In this section all IP features of the **AST570** are shortly described.

AST570 IP addressing

The **AST570** has a preconfigured “Net10” address: 10.0.0.138 which may not be deleted.

As the **AST570** IP layer supports logical multi-homing (one interface supporting multiple IP addresses), multiple manually configured IP addresses and multiple dynamically assigned IP address(es) can be active at the same time.

AST570 DHCP

The **AST570** features a DHCP server.

Dynamic Host Configuration Protocol (DHCP) allows the PC(s) on your local network to retrieve automatically an IP address from an “IP address leasing” server, i.e. a DHCP server.

See subsection 14.4 for more information.

AST570 IP router

The **AST570** features an IP router.

In general, IP routing allows hosts to contact other hosts which reside in other (sub)networks.

For the **AST570** the main function of the IP router is to route IP packets from the local network to the remote networks over the ATM/DSL connections and vice versa.

See section 14.5 for more information.

AST570 NAT & PAT

The **AST570** features a combination of Network Address Translation (NAT) and Port Address Translation (PAT) called NA(P)T.

Combined with the **AST570** IP router, NA(P)T allows multiple PCs to share a single public IP address.

See chapter16 for more information.

VLSM, CIDR Supernetting and Aggregation

Next to traditional classful IP addressing, (sub)netmasking and routing the **AST570** features also the following new IP standards:

- **Variable Length Subnet Masking** (**VLSM**)

  VLSM refers to the fact that one network can be configured with different contiguous masks. This offers the capability to allocate subnetworks with variable numbers of hosts, thus allowing a better utilization of address space.

- **Classless Inter Domain Routing** (**CIDR**)

  In CIDR, an IP network is represented by a prefix, which is the IP address of a network, followed by a slash and, lastly, an indication of the number of leftmost contiguous bits corresponding to the network mask to be associated with that network address.

- **Supernetting**

  A network is referred to as Supernet when a prefix netmask boundary contains fewer bits than a network's natural – classful mask.

- **Route Aggregation**

  Route Aggregation refers to the way CIDR and its prefix notation can be used to advertise multiple IP networks with one aggregate Supernet route indication.

Therefor, the **AST570** is compliant to all relevant sections in RFC1338, RFC1518 and RFC1519

See these RFCs for more information.

14.2 Packet Services and IP

Introduction

In this section the interaction between IP addresses and packet services is described.

Apart from Bridging, all packet services require the IP suite, and even the Bridging packet service will in most cases be used in combination with IP addressing.

In this section

Topic	See
Transparent Bridging	14.2.1
Relayed PPPoA	14.2.2
Routed Packet Services	14.2.3

14.2.1 Transparent Bridging

IP vs. Bridging

Basically, Bridging does not require any IP address at all: neither in your PC(s), nor in your **AST570**.

However, in case of Internet access, private IP networking or in case the Bridging packet service is used for Bridged PPPoE, your PC(s) must be configured for TCP/IP.

Typical Bridging Setup

In most cases, your SP will require you to use DHCP for your PC. In this case the DHCP server is at the remote side of the DSL connection. Therefore, your **AST570**' DHCP server must be disabled.

Using TCP/IP and Bridging

Your SP may:

- Provide you with an IP address
- Require you to use DHCP.

Local IP communication

Alternatively, a second but *Private* IP address can be manually configured for local IP communication. It depends on your OS whether it supports this combination.

e.g. Microsoft supports Logical Multihoming via Registry keys.

CAUTION

Bridging & DHCP Service

The **AST570** DHCP server is by default **enabled** (via Auto DHCP).

In case you use your **AST570** in Bridging mode and your ISP requires you to enable DHCP in your PC(s), you **must** disable the DHCP server inside the **AST570** to avoid conflicts between two DHCP servers being active at the same time.

See section 14.4 for more information on the **AST570** DHCP server.

14.2.2 Relayed PPPoA

IP vs. Relayed PPPoA

Prior to using PPTP, local IP addresses must be configured. The use of these IP addresses is limited to the local network.

Private IP addresses

You are free to choose any IP address as long as it is compatible with your local network and is unique in that same network.

As the **AST570** has a preconfigured "Net10" address (10.0.0.138), you should configure IP addresses like 10.0.0.1, 10.0.0.2, ... on your PCs.

Note: IP addresses can be configured automatically via **AST570**' DHCP server. See section 14.4 for more information.

Public IP addresses

A second set of (Public) IP addresses having end-to-end scope will automatically be negotiated via the PPP protocol inside your PC(s).

Simultaneous use of public & private IP

Both Public and Private IP addresses are active simultaneously because of tunneling. In fact two "nested" IP layers exist: the *Public* IP layer which is carried within the *Private* IP layer on the local (W)LAN.

PPP IP address negotiation

By default the PPTP tunnel application automatically negotiates the Public IP address.

In case your SP instructs you to use a static IP address for Relayed PPPoA, most dial-in applications allow a static IP address to be supplied.

14.2.3 Routed Packet Services

IP routing and IP addresses

Local IP addresses must be configured prior to use IP routing.

AST570 IP addresses

As the **AST570** has a preconfigured "Net10" address (10.0.0.138), you can configure IP addresses like 10.0.0.1, 10.0.0.2, ... in your PCs, or use the **AST570** DHCP server.

In case another IP address is required, you can set **AST570**' IP address via the **AST570** pages or via a *Ping-of-Life*™.

See sections 14.3 and 20.1 for more information.

PC IP address configuration

The PC IP address can be configured statically (no DHCP) or dynamically (**AST570** as DHCP server).

Default gateway for the PCs

In addition, configure the **AST570**' IP address as default gateway in your PCs.

Routed Ethernet

At the DSL side of the **AST570** IP router, the Routed Ethernet connection will receive an IP address from the RAS. However, you can also configure a static IP address for the connection on the *'MER'* page. In this case, the **AST570** will negotiate the acceptance of this IP address with the remote side.

Routed PPPoE and Routed PPPoA

At the DSL side of the **AST570** IP router, PPP automatically negotiates an IP address with its remote PPP peer.

You can configure the PPP local IP address of the **AST570**. In special circumstances you can configure a remote IP address for the PPP connection.

See subsection 11.4.2 for more information.

CIP & IP Routing

As it name implies Classical IP & IP Routing relies on basic IP addressing and routing for its packet forwarding.

i.e. Both local as remote users on either side of the DSL connection experience the LIS environment as if they are sharing one single network.

The configuration and use of all IP specific issues for a Classical IP environment is profoundly described in chapter 12.

14.3 Speed Touch Addresses

Introduction

Like any other member of a (W)LAN the **AST570** must be locally identified by an IP address to be able to communicate with other local (W)LAN devices.

This section deals with the IP address configuration of the **AST570** for local communication only.

In this section

Topic	See
AST570 IP Address Types	14.3.1
Static IP Address Configuration	14.3.2

14.3.1 AST570 IP Address Types

Assigning IP addresses to the AST570

IP addresses can be assigned to the **AST570** in several ways. Summarized, following IP address types exist:

- The default IP address: 10.0.0.138
- IP addresses assigned via the *'Initial Setup'* page
- IP addresses assigned via a *'Ping-of-Life™*
- IP addresses assigned via the *'Routing'* page
- IP addresses assigned via the *'DHCP Client'* page
- IP addresses configured and/or negotiated by connections.

AST570 and multiple IP addresses

As the **AST570** IP layer supports logical multi-homing (one interface supporting multiple IP addresses), both statically and dynamically configured IP address(es) can be active at the same time.

CAUTION

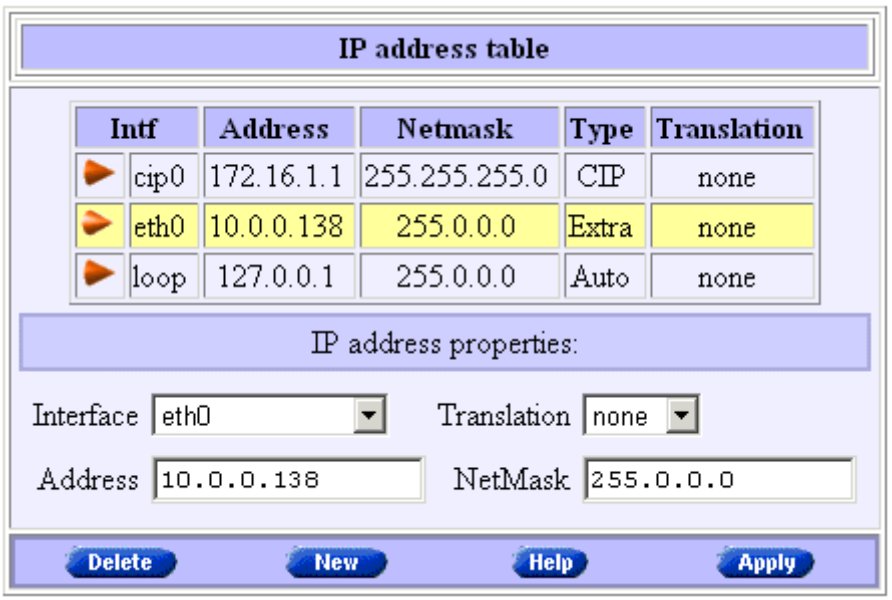
Default and Internal IP Addresses

The 10.0.0.136 and 10.0.0.138 "Net10" IP addresses are reserved.

Never delete, add nor change the default 10.0.0.138 and 10.0.0.136 IP addresses as these are required for the **AST570**' internal communication between Wired and Wireless Ethernet interfaces.

'IP address' table

On the **AST570** *'Routing'* page the *'IP address'* table summarizes all IP addresses configured on any of the **AST570** interfaces:



'IP address' table components

Field	Description
Intf	Indicates the interface (Intf) to which the IP parameter set was assigned to. It can take several values depending on the packet services that are active. Among others the Ethernet (eth0) and the Loopback (loop) are always present.
Address	Indicates the IP address of the interface.
Netmask	Indicates the netmask of the interface.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Type</td><td>Indicates the origin of the IP parameters.
It can take following values:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>Auto</td><td>Implies that the parameters were acquired automatically through DHCP, or are typical standard IP addresses (e.g. 'loop').</td></tr>
<tr><td>User</td><td>Implies that an additional IP parameter set was added through the 'Initial Setup' page.</td></tr>
<tr><td>Extra</td><td>Implies that an additional IP parameter set was added through the 'Routing' page. The default IP address 10.0.0.138 is also of this type.</td></tr>
<tr><td>Temp</td><td>Implies that this (additional) IP parameter set was added via a Ping-of-Life™.</td></tr>
</table></td></tr>
<tr><td>Transl</td><td>Indicates the translation performed.
It can take following values:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>None</td><td>No address translation can be performed on this address.</td></tr>
<tr><td>PAT</td><td>NA(P)T can be (or is) performed on this address.</td></tr>
</table></td></tr>
</table>

14.3.2 Static IP Address Configuration

Default AST570 IP address

In case you add the **AST570** to an existing (W)LAN, it could be that you must configure a "User Defined" IP address other than the default "Net 10" address, appropriate for the (W)LAN's IP settings.

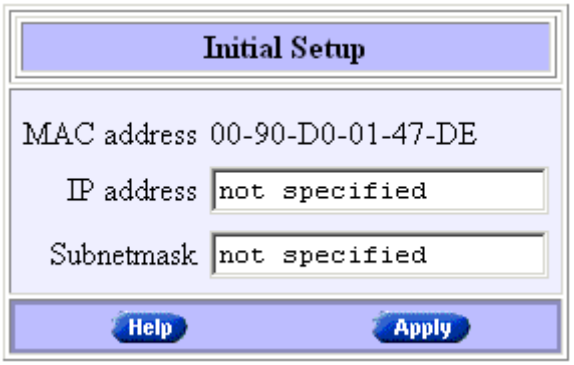
In this subsection

- Setting an IP Address via the *'Initial Setup'* Page
- Setting an IP Address via the *'Routing'* Page.

Setting an IP address via the 'Initial Setup' page

Proceed as follows:

1. Click Initial Setup in the left pane of the **AST570** pages to pop up the 'Initial Setup' page (See section 21.2 for more information). On this page the following table is shown:



2. Enter an IP address in the *'IP Address'* field.
3. You must configure a netmask for applying subnetting in your network in the *'Subnetmask'* field.
4. Click Apply. As a result the new IP settings are applied:

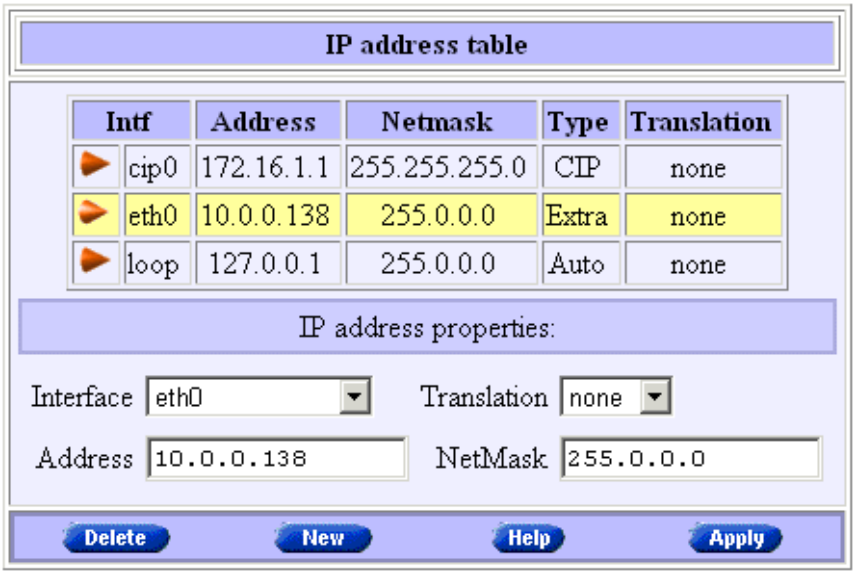
   RESULT : the IP settings have been applied. Change the IP settings on your own machine (if needed) and point your browser at the new address (http://10.0.0.151/) to verify connectivity with the new configuration. Use 'Save all' to make it permanent.

5. To verify connectivity, point your Web browser to the new IP address. Make sure though that your PC shares the same subnet.
6. Click Save all to store the applied IP settings to permanent storage.

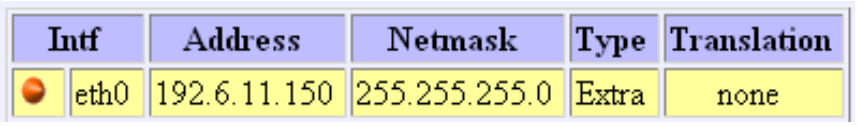
Setting an IP address via the 'Routing' page

Proceed as follows:

1. Click Routing in the left pane of the **AST570** pages to pop up the *'Routing'* page (See section 21.2 for more information). On this page the following table can be found:



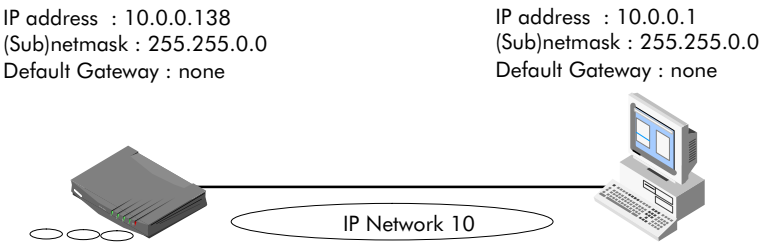
2. In this table If needed, click New.
3. Enter the following information:
   - Select *eth0* from the *'Intf'* pop-down list
   - Enter an IP address in the *'IP Address'* field, e.g. 192.6.11.150
   - Enter an associated (sub)netmask in the *'Netmask'* field, e.g. 255.255.255.0
   - Select whether NA(P)T must be applied (pat) or not (none) for this IP address from the *'Translation'* pop-down list.
4. Click Add. As a result the new IP settings are applied:



5. To verify connectivity, point your Web browser to the new IP address. Make sure your PC shares the same subnet.
6. Click Save all to store the applied IP settings to permanent storage.

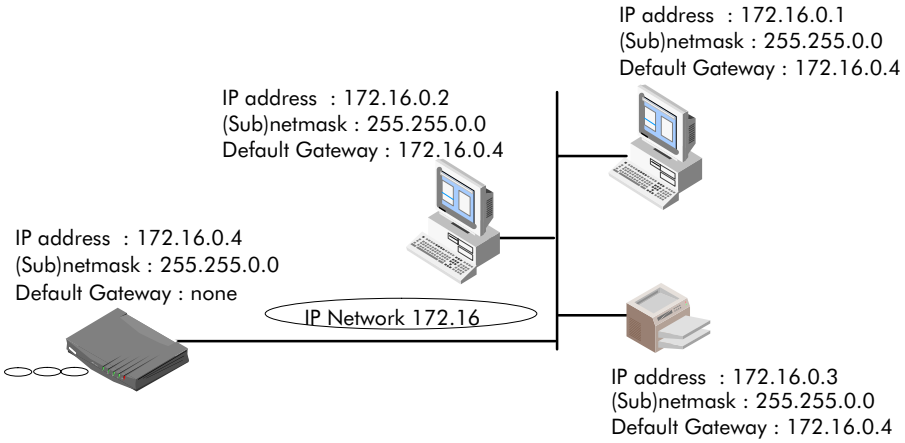
Sample configuration: single PC

In the below figure, a simple configuration is given: One PC is attached to the **AST570**:



Sample configuration: small workgroup

You can setup a local workgroup around the **AST570** as shown in the figure below:



Note: Notice that the default gateways in the PCs point to the **AST570**.

14.4 Speed Touch DHCP

DHCP

Depending on the size and complexity of your network, a few DHCP configurations can be envisaged:

(W)LAN Type	DHCP Mode	Argumentation
Simple	No	All few members of the small (W)LAN have static IP addresses, including the **AST570**.
Medium sized	Server	For small home (W)LANs it might be worthwhile to configure all of your (W)LAN devices as DHCP client and the **AST570** as the DHCP server. In this configuration each time a compute start it will obtain its IP configuration from the **AST570**.
Advanced	Client	For advanced networks, the role of DHCP server might be performed by an IP node other than the **AST570** on the local (W)LAN. Typically such functions are attributed to home gateways: computers having better networking capabilities than the other PC(s) on the home (W)LAN. All local PCs remain configured as DHCP clients, including the **AST570**.

Default AST570 DHCP

Both the **AST570** DHCP server and DHCP client are enabled by default: *AutoDHCP.*

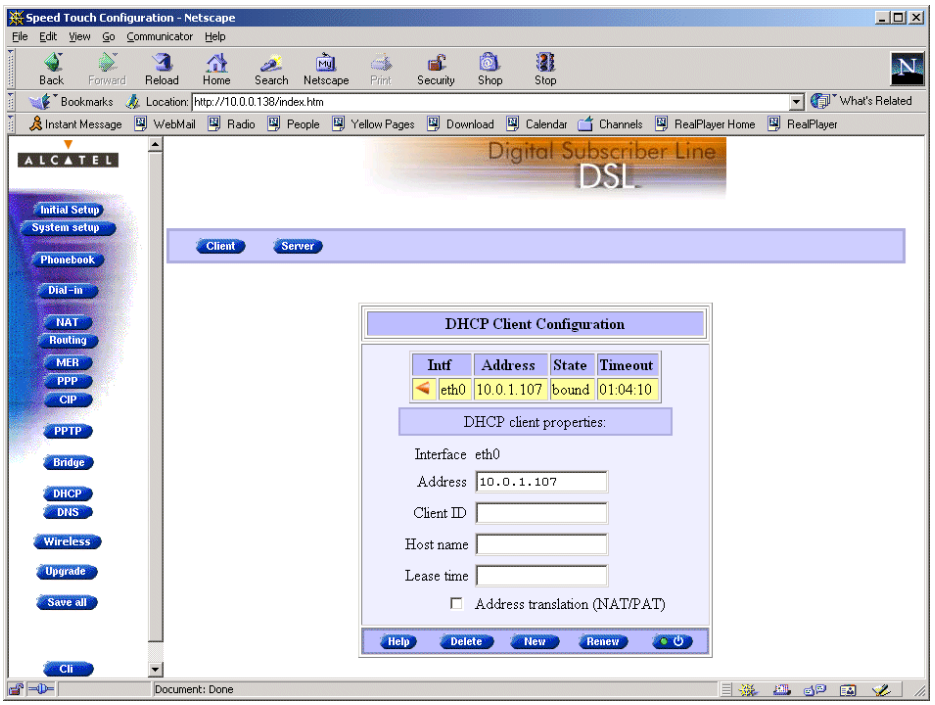
In this section

Topic	See
The **AST570** DHCP Pages	14.4.2
The **AST570** DHCP Server	14.4.2
The **AST570** DHCP Client	14.3.2

14.4.1 AST570 DHCP Pages

The 'DHCP' pages

Click DHCP in the left pane of the **AST570** pages to pop up the 'DHCP' pages (See section 21.2 for more information):



By default the *'DHCP client'* page is shown.

DHCP page selection

Two buttons on the DHCP pages allow to switch between the *'DHCP client'* page and *'DHCP server'* page:

Click this button ...	To ...	See
Server	To pop up the *'DHCP Server'* page.	14.4.2
Client	To pop up the *'DHCP Client'* page.	14.4.3

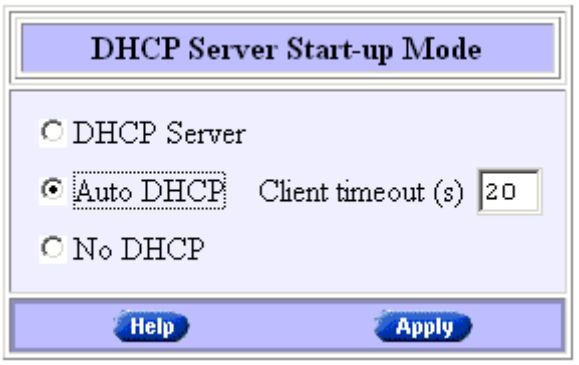
14.4.2 The AST570 DHCP Server

In this subsection

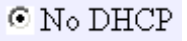
- The *'DHCP Server Start-up Mode'* Table
- Configuring the **AST570** for (W)LANs without DHCP Server
- Configuring the **AST570** as DHCP Server
- Configuring the **AST570** for Auto DHCP
- The **AST570** as DHCP client
- *'DHCP Server Configuration'* Table
- Address Pool Configuration
- PPP Spoofing Configuration
- *'DHCP Server Lease'* Table
- Adding Leases Manually.

'DHCP Server Start-up Mode' table

On the **AST570** *'DHCP Server'* page the *'DHCP Server Start-up Mode'* table allows to configure the **AST570** DHCP server behavior:



Configuring the AST570 for a (W)LAN without DHCP

To setup the **AST570** without DHCP, tick  .

In this configuration it is assumed that all members, the **AST570** included, have static IP addresses.

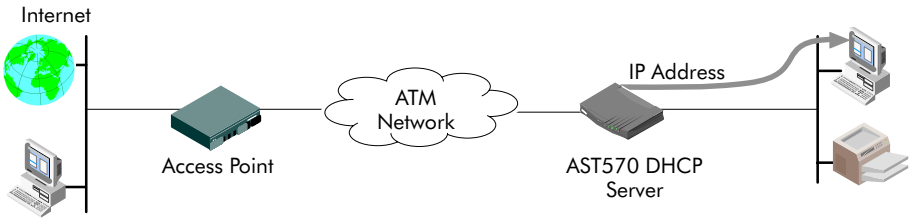
See subsection 14.3.2 for static IP addressing of the **AST570**.

Note: This configuration might be required in case you use the Transparent Bridging packet service.

Configuring the AST570 as DHCP server

To setup the **AST570** as DHCP server, tick ◉ DHCP Server .

Via the *'DHCP Server Configuration'* table you can configure the **AST570** DHCP server settings.



Note: This setting might cause side effects with Bridging. See section 14.2.1 for more information.

Configuring the AST570 for Auto DHCP

One of the **AST570** features is that it can automatically revert from DHCP client to DHCP server.

At boot time the **AST570** probes the (W)LAN for a specified time limit (*'Client timeout'*) to check whether another DHCP server is available on the network. If so, it will act as a DHCP client. If no response is received within the specified time, the **AST570** becomes a DHCP server.

To allow the **AST570** to act as Auto DHCP client/server, tick ◉ Auto DHCP on the *'DHCP Server'* page.

Additionally, you can configure the *'Client timeout'* in seconds: Client timeout (s) 20 .

Via the *'DHCP server configuration'* table, you can configure the **AST570** DHCP server settings.

Automatic IP addressing

OSs supporting *'Automatic IP Addressing'*, might initially not establish IP connectivity with the **AST570**. This is because the IP address they assimilated is not within the **AST570** *'Auto DHCP'* server range.

To prevent this problem, please power on your (W)LAN devices after the AST570 has come online.

Indeed, when the **AST570** is in 'Auto DHCP' it will first operate as a DHCP client. After the client timeout exceeded, it switches to DHCP server mode, but this might be to late as some clients will already selected an automatic IP address.

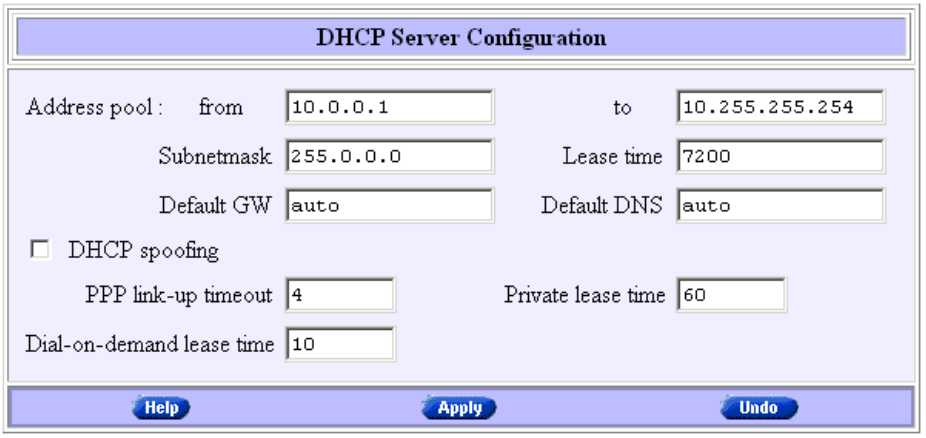
Dynamic IP addressing is a feature allowing DHCP clients to assign themselves an IP address.

This happens when there is no DHCP server on the network, or when the server is temporarily down. After automatic assignment, the DHCP client will issue DHCP requests at regular instances.

If the DHCP server is back online, the client will now lease an IP address from the server, after discarding its temporary automatic IP address.

The 'DHCP server configuration' table

On the *'DHCP Server'* page the *'DHCP Server configuration'* table allows you to configure the **AST570** DHCP server settings:



Address pool configuration

You can configure following DHCP server parameters:

Field	This configures ...	Default
Addresses through ...	The range of addresses the DHCP server can choose an IP address from for lease.	"Net10"
Subnet Mask	The subnetting applied to the local network, scoped by the DHCP server.	no subnetting
Lease Time	The time (Lease Time) IP addresses can be assigned to a device by DHCP.	7200 seconds
Default Gateway	The IP address of the default gateway.	*'auto'* (*)
DNS Server	The IP address of the DNS server.	*'auto'* (**)

(*) Setting *'auto'* in the *'Def. Gateway'* field means, that there will be referred to the *'Routing'* page.

(**) Setting *'auto'* in the *'DNS server'* field means, that there will be referred to the *'DNS'* page.

DHCP spoofing configuration

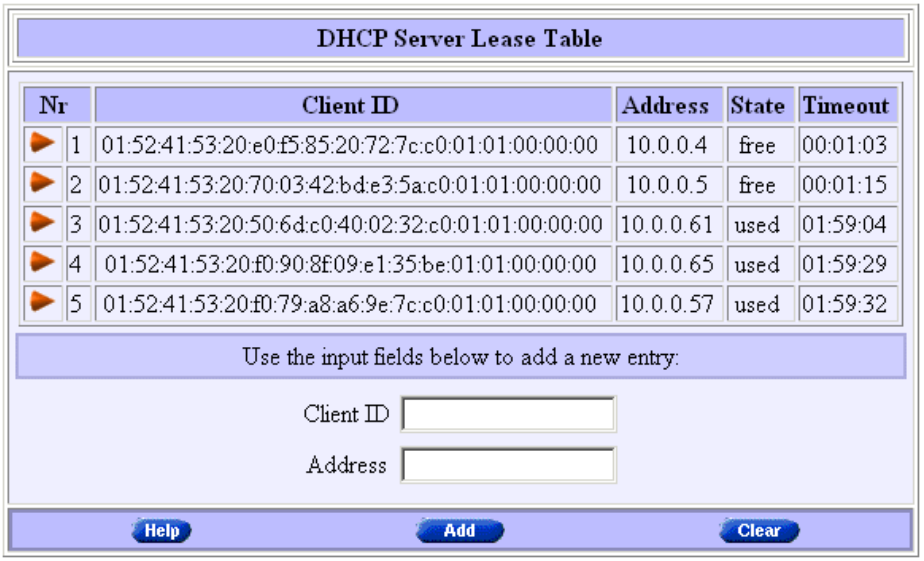
This box allows you to set the DHCP spoofing parameters for PPP-to-DHCP spoofing connections.

You can configure following parameters:

Field	This configures ...	Default
PPP link-up timeout	The number of seconds to wait for a PPP link to successfully negotiate an IP address. After timeout a private PPP connection session IP address will be issued.	4 seconds
Private lease time	The lease time on seconds of the private IP address issued when a PPP link fails.	60 seconds
Dial-on-demand lease time	The lease time in seconds of the temporary private IP address in case of a dial-on-demand PPP link.	10 seconds

DHCP lease table

This table allows you to overview all current leases of the **AST570** DHCP server (if activated) or manually add new leases:



DHCP Server Lease Table

Nr	Client ID	Address	State	Timeout
1	01:52:41:53:20:e0:f5:85:20:72:7c:c0:01:01:00:00:00	10.0.0.4	free	00:01:03
2	01:52:41:53:20:70:03:42:bd:e3:5a:c0:01:01:00:00:00	10.0.0.5	free	00:01:15
3	01:52:41:53:20:50:6d:c0:40:02:32:c0:01:01:00:00:00	10.0.0.61	used	01:59:04
4	01:52:41:53:20:f0:90:8f:09:e1:35:be:01:01:00:00:00	10.0.0.65	used	01:59:29
5	01:52:41:53:20:f0:79:a8:a6:9e:7c:c0:01:01:00:00:00	10.0.0.57	used	01:59:32

Use the input fields below to add a new entry:

Client ID

Address

Help Add Clear

Adding leases manually

You can add leases manually in case the devices need reserved IP addresses (e.g. FTP server) or in case the device is not able to send/receive DHCP requests/replies. These leases are permanent, i.e. will never be released.

Proceed as follows:

1. Click New in the *'DHCP Server Lease'* table if needed.
2. Enter the following information:
   - Enter the MAC address of the device you want to lease an IP address in the *'Client ID'* field
   - Enter an IP address in the *'IP Address'* field.
3. Click Add. As a result the new lease is applied.
4. Click Save all to store the applied lease to permanent storage.

14.4.3 The AST570 DHCP Client

In this subsection

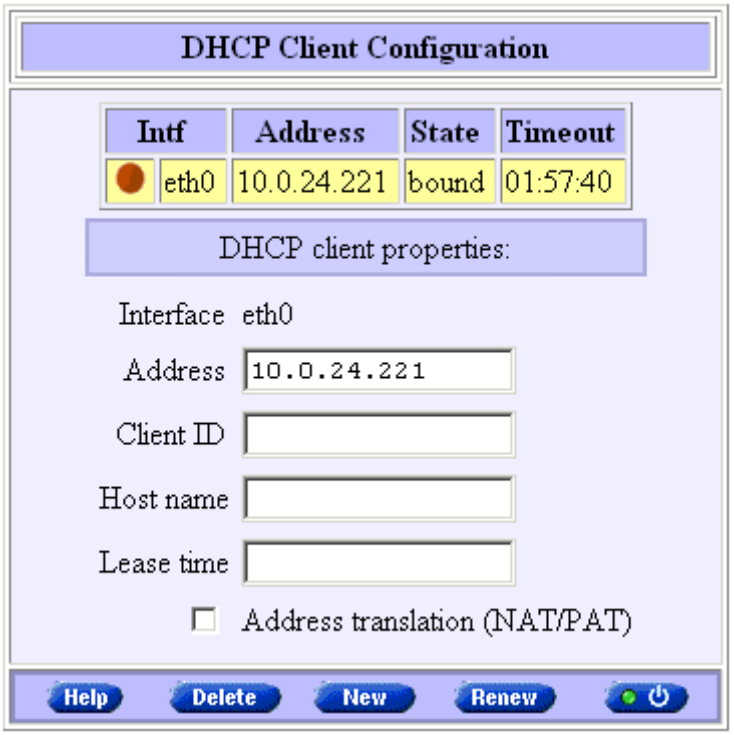
- The **AST570** DHCP Client
- *'DHCP Client Configuration'* Table
- *'DHCP Client Configuration'* Table Components
- Enabling an **AST570** DHCP Client.

The AST570 DHCP client

Apart from being DHCP server, the **AST570** can also act as DHCP client. The dynamically assigned IP addresses can be obtained from another DHCP server on the local network or a remote access DHCP server for Routed Ethernet connections.

'DHCP Client Configuration' table

On the **AST570** *'DHCP Client'* page the *'DHCP Client Configuration'* table allows configuration of the **AST570** DHCP client:



'DHCP Client Configuration' table components

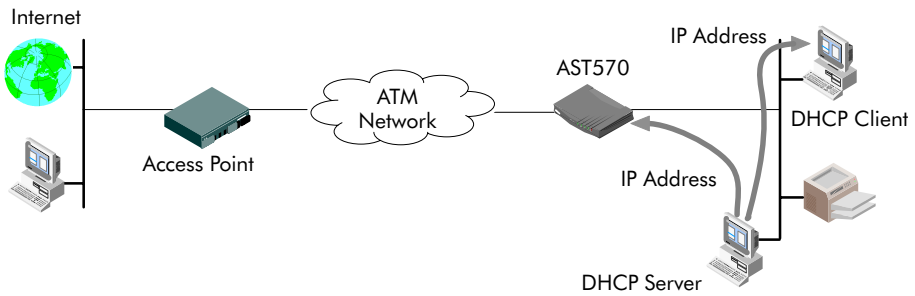
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Intf
Interface</td><td>Indicates the logical interface name on which the DHCP client settings apply.
Next to the local area eth0 interface, indicating the AST570 being DHCP client towards your (W)LAN, wide area MER interface names (being typically phonebook names) are shown, if applicable.</td></tr>
<tr><td>Address</td><td>Indicates the dynamic IP address of the interface.</td></tr>
<tr><td>State</td><td>Indicates the current state of the dynamic interface.
It can take following values:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>Init</td><td>The DHCP client has not been activated yet.</td></tr>
<tr><td>Selecting</td><td>The DHCP client is searching for a DHCP server.</td></tr>
<tr><td>Requesting</td><td>The DHCP client requests a DHCP server for an IP address.</td></tr>
<tr><td>Bound</td><td>A dynamic IP address has been assigned by the DHCP server.</td></tr>
<tr><td>Renewing</td><td>The DHCP client requests a known DHCP server to extend its lease.</td></tr>
<tr><td>Rebinding</td><td>The DHCP client searches for a DHCP server to extend its lease.</td></tr>
</table></td></tr>
<tr><td>Timeout</td><td>Indicates the remaining lease time time of the assigned dynamic IP address, if the interface is in state bound.</td></tr>
<tr><td>Client ID</td><td>Indicates the DHCP Client identity communicated to the DHCP server, if applicable.</td></tr>
<tr><td>Host name</td><td>Indicates the domain name associated with the dynamic IP address, if applicable.</td></tr>
<tr><td>Lease time</td><td>Indicates the lease time of the dynamic IP address.</td></tr>
</table>

Enabling an AST570 DHCP client

Proceed as follows:

1. If needed, click Client on the *'DHCP'* page.
2. In this table if needed, click New.
3. Select the interface you want to enable DHCP for from the *'Interface'* pop-down list:
   - Select *eth0* in case you want to enable the DHCP client for the **AST570** itself
   - Select the Routed Ethernet entry in case you want to enable the MER DHCP client.
4. Optionally enter one or more of the following fields:
   - *'IP address'*
   - *'Client ID'*
   - *'Host name'*
   - *'Lease time'*.
5. Click Add. As a result the DHCP client is enabled.
6. Click Save all to store the applied lease to permanent storage.

The AST570 as DHCP client



14.5 Speed Touch Routing

Introduction

Next to the DSL router part, the **AST570** supports also IP routing via its IP router.

This section aims to familiarize you with the **AST570** IP router abilities.

In this section

Topic	See
The **AST570** IP router	14.5.1
Configuring the **AST570** IP Routing Table	14.5.2

14.5.1 The AST570 IP Router

Introduction

Because the **AST570** can act as an IP router, it has the ability to access machines in other networks than its own. This can be achieved by adding specific routes to its IP routing table.

This subsection provides some general information on the **AST570** IP router functionality.

Features

IP routing:

- Is a standard and a well-known principle, mainly due to the widespread Internet use
- Has broad application support, as it is implemented in most, if not all Operating Systems (Windows, Unix, Mac OS, ...).

Configuring an IP routing table

The routes in an ordinary routing table or Forwarding Information Base (FIB) include, among others, destination IP addresses, subnet masks and gateways.

When an IP packet arrives at the router, the router examines the destination IP address. The router looks up the most specific match in the routing table for that destination address. Finding the most specific match equals finding the longest subnet mask for that IP address.

For example, the subnet mask 255.255.255.0 is more specific than 255.255.0.0 because the network part in the first case is longer (and thus more specific) than the network part in the second case.

Once the most specific match is found, the router forwards the IP packet to the gateway associated with that match.

Simplified example of a traditional IP routing table

The following table is an example of an IP routing table:

Route Destination	Subnet Mask	Gateway
30.0.0.2	255.255.255.255	30.0.0.10
10.0.0.0	255.255.255.0	10.0.0.138
0.0.0.0	0.0.0.0	20.0.0.10

The AST570 IP routing table

Depending on the configuration made, the **AST570** may use an extended routing table.

In addition to the data contained in an ordinary routing table, it contains information about the source IP address and the source subnet mask.

The lookup principle may also be extended: not only the combination of destination IP address and subnet mask is looked up, but also the combination of source IP address and subnet mask.

The extended IP routing table gives extra functionality to the **AST570** and is explained in subsection 14.5.2.

Example of the AST570 extended IP routing table

The following table is an example of the **AST570** extended IP routing table:

Dest. IP Address	Dest. Subnet Mask	Source IP Address	Source Subnet Mask	Gateway
30.0.0.2	255.255.255.255	10.0.0.2	255.255.255.255	30.0.0.10
10.0.0.0	255.255.255.0	10.0.0.0	255.255.255.0	10.0.0.138
0.0.0.0	0.0.0.0	10.0.0.0	255.255.255.0	20.0.0.10

CIDR prefix notation for IP addresses

The more up to date CIDR representation of masks does not refer to a subnet mask, but to a prefix length.

The prefix number equals the number of ones in the subnet mask. For example, the subnet mask 255.255.255.0 could also be written as the prefix /24.

Example

For example:

- IP address `10.0.0.138`
- netmask `255.255.255.0`

With the prefix method this will be written as :

- prefix IP address `10.0.0.138/24`

AST570 and CIDR

In the **AST570** routing table the prefix notation will be used. This notation in combination with the support for *Supernetting* and *Route Aggregation* provides the **AST570** with a mechanism to make its and other routers' IP routing tables smaller.

VLSM

Next to traditional classful netmasking, the **AST570** fully supports the use of variable length subnet masks in its IP routing tables.

14.5.2 Configuring the AST570 IP Routing Table

Introduction

The main function of the IP router in the **AST570**, is to route IP packets from the local network to the remote networks over the ATM/DSL connections and vice versa.

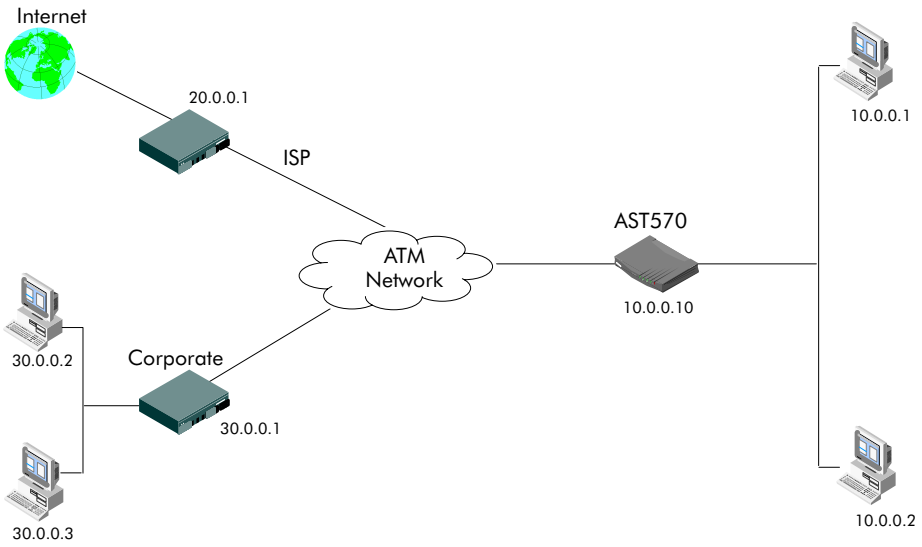
In this subsection, configuration of the **AST570** IP routing table is described.

In this subsection

- General ATM/DSL End-to-End IP Architecture
- ATM/DSL IP Routing
- **AST570** Power-on IP Routing Table Configuration
- *'IP Route'* Table
- *'IP Route'* Table Components
- Adding Routes to the *'IP Route'* Table
- Criteria for a Route to be Valid.

General ATM/DSL end-to-end IP architecture

The figure below provides an overview of the general end-to-end IP architecture:



ATM/DSL IP routing

Routing to ATM/DSL connections actually means:

- Routing between the local (W)LAN and Classical Logical IP subnets and vice/versa
- Routing between the local (W)LAN and PPPoA and/or PPPoE connections and vice/versa
- Routing between the local (W)LAN and Routed Ethernet connections and vice/versa.

Basically the IP router only cares about IP addresses, i.e. the 'Destination IP address' of any packet received on any of its interfaces (MER, PPPoE, PPPoA, CIP or Ethernet) is looked up in the IP routing table. The lookup process will determine the best route that may lead to the final destination of the packet. Consequently it will forward the packet to the interface that may reach this destination.

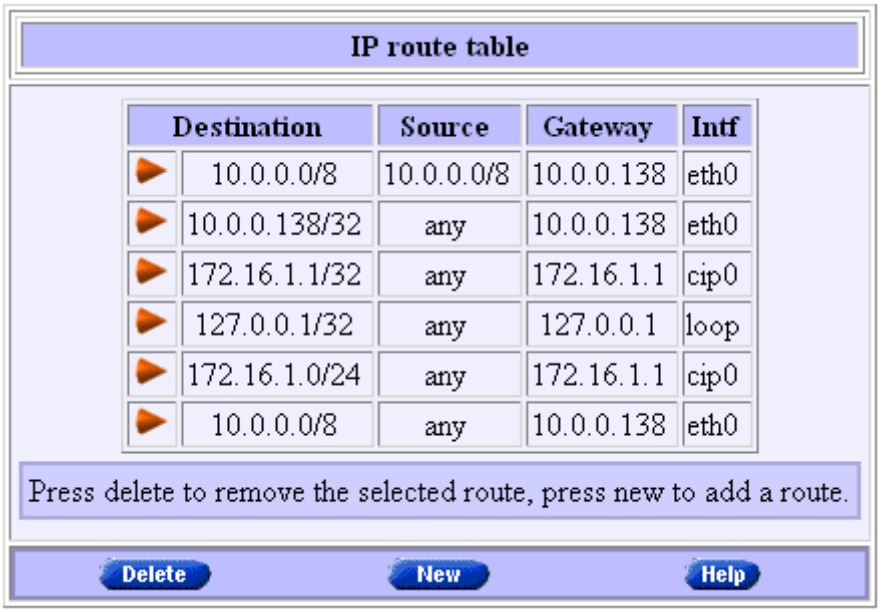
AST570 power-on IP routing table configuration

When the **AST570** is powered on, routes are automatically configured in the routing table for the following possible IP address entries in the *'IP address'* table:

- As soon as the Ethernet interface is up and running, routes are added for each of the Ethernet interface IP addresses.
- Routes are added for the IP address negotiated between the remote DHCP server of a Routed Ethernet connection configured for DHCP.
- Routes are added for the IP address negotiated between the remote peer and an **AST570** PPPoE and/or PPPoA entry (configured for Always-On).
- If a CIP member is created and explicitly configured with an IP address, routes are added for this IP address.

'IP route' table

On **AST570** *'Routing'* page the *'IP Route'* table summarizes all IP routes configured on the **AST570**:



'IP route' table components

Field	Description
Destination	Indicates the destination IP address (pool)/prefix mask or "next-hop" device IP address for the IP route.
Source	Indicates the source IP address (pool)/prefix mask of the IP route.
Gateway	Indicates the IP address of the directly connected gateway to which the routed packets for this interface are forwarded.
Intf	Indicates the interface (Intf) on which the IP route is applied. It can take several values depending on the packet services that are active. Among others the Ethernet (eth0) and the Loopback (loop) should always be present.

Adding specific routes to the 'IP route' table

Proceed as follows:

1. If needed, click New in the *'IP Route'* table.
2. Enter the following route information:
   - *'Destination'* IP address (pool) of the destination or "next-hop" device in prefix notation

     Specifying **`default`** indicates that all outgoing traffic is sent over this route.
   - *'Source'* IP address (pool) in prefix notation

     Specifying **any** indicates that all traffic coming from the Ethernet interface is sent over this route.
   - *'Gateway'* IP address of a directly connected gateway device, e.g. the **AST570** itself.
3. Click Add. As a result the route is applied.
4. Click Save all to store the routing configuration to permanent storage.

Criteria for a route to be valid

A route is only accepted by the **AST570** if it meets following conditions:

- The destination and source entries must yield correct prefixes
- The gateway must be directly connected.

15 Networking Services – DNS

Introduction

IP addresses are fundamental to the operation of the Internet. They not only uniquely identify Internet nodes but also allow IP routers to forward packets to their destinations.

IP addresses, being 32-bit numbers, are ideally suited for computers but are far from usable to humans.

Therefore, the *Domain Name System (DNS)* was designed: a distributed database, held by a hierarchical system of servers, that is used by TCP/IP applications to map between hostnames and IP addresses.

This chapter describes **AST570**' DNS abilities.

In this chapter

Topic	See
AST570 DNS Resolving	15.1
Configuring the **AST570** DNS Server	15.2

15.1 Speed Touch DNS Resolving

Introduction

The **AST570** features a DNS server for the locally attached PCs and as DNS relay for non-local DNS hostnames.

Local DNS resolving

The same mechanism for resolving computer names to IP addresses when browsing the Internet, applies to your local network.

Instead of using the IP addresses for a local IP node e.g. 10.0.0.138 for the **AST570**, you can give your nodes names and let a DNS server, e.g. the **AST570** itself, do the resolving.

Example of local DNS resolving

In the example, a (W)LAN is built around the **AST570**.

In this scenario, it is assumed that the **AST570** acts as DHCP server, and as DNS server for the local network.

During start-up, a first PC launches a DHCP request on the (W)LAN.

One of the fields in the DHCP request contains the computer name e.g. *YourPC*.

The **AST570** reacts by intercepting this request and returns a DHCP reply containing:

- The IP address for his computer, e.g. 10.0.0.1
- The local domain name, e.g. *lan* (default)
- The IP address of the local DNS server, e.g. 10.0.0.138 being the **AST570** (default).

A second PC, named *MyPC*, is powered on and is configured via a DHCP reply as below:

- The IP address for his computer, e.g. 10.0.0.2
- The local domain name, i.e. *lan*
- The IP address of the local DNS server, i.e. 10.0.0.138.

Result of local DNS resolving

In the example scenario, it is now possible to ping both PCs, *MyPC* and *YourPC*, by referring to their computer names instead of their IP addresses.

Local DNS resolving mechanism

The mechanism as follows:

Phase	Description
1	Apply a **`ping YourPC`** on *MyPC*.
2	Via this command, *MyPC* launches a DNS request, basically asking: "What is the IP address of *YourPC.lan* ?"
3	As the **AST570** is the DNS server, it will respond with the appropriate IP address, being 10.0.0.1.
4	The ping utility in *MyPC* will now submit the ping to 10.0.0.1 which may eventually reply.

Non-local DNS resolving

The **AST570** resolves names within the local domain, i.e. *lan* (default **AST570** setting) as described above.

However, all other domain names, e.g. `alcatel.com`, cannot be resolved by the **AST570** and are forwarded over the appropriate link on the DSL line.

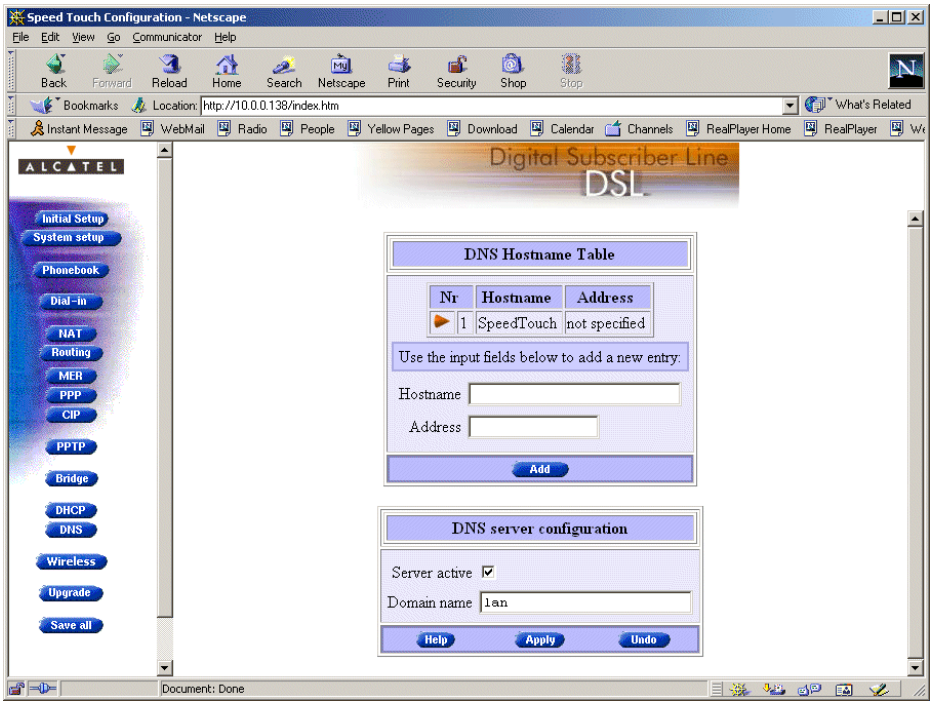
15.2 Configuring the Speed Touch DNS Server

In this subsection

The example of section 15.1, refers to a new (W)LAN, using the default **AST570** configuration, i.e. configured for DHCP server, as well as DNS server.
In case the **AST570** is added to a existing (W)LAN, configuration of the **AST570** DNS server might be necessary to meet the existing (W)LAN conditions.

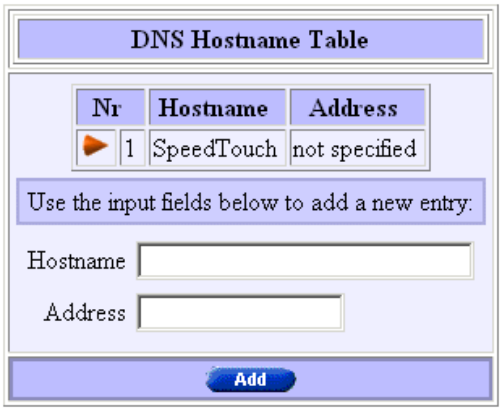
The 'DNS' page

Click DNS in the left pane of the **AST570** pages to pop up the 'DNS' page (See section 21.2 for more information):



'DNS hostname' table

This table shows the DNS hostnames of all current DNS clients and optionally allows to add DNS leases manually:

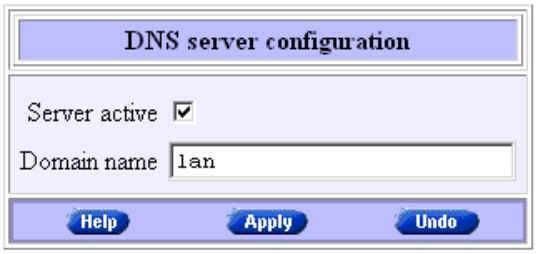


'DNS hostname' table components

Field	Description
Hostname	The DNS hostname of the device.
Address	The IP address to which the DNS hostname is assigned.

'DNS server configuration' table

This field allows configuration of the **AST570** DNS server:



'DNS server configuration' components

Field	Description	Default
Server active	Enables or disables the **AST570** DNS server.	✓, **AST570** DNS server active.
Domain Name	Specifies the domain name of your (W)LAN.	lan

Configuring the DNS server

Check the *'Server active'* checkbox to enable the **AST570** DNS server.

In the *'Domain name'* field you can enter the domain name of your (W)LAN. You may use a DNS subdomain name, e.g. *dsl.wireless.office.lan*.

This name is communicated by the DNS server to the local PCs, and is subsequently used by the PCs to complete a DNS request.

Adding DNS leases manually

The *'DNS hostname'* table allows you to configure DNS leases manually, e.g. for devices which do not support DNS.

Proceed as follows:

1. In this table if needed, click New.
2. Enter the following information in the *'DNS hostname'* table:
   - The DNS hostname for the device
   - The IP address of the device.
3. Click Add and Save all to finish the procedure.

Resetting the DNS server

To reset the **AST570** DNS server and clear all current DNS host entries, proceed as follows:

1. Browse to the *'DNS'* page.
2. If you are sure to reset the **AST570** DNS server, click Undo in the *'DNS server Configuration'* table.
3. The **AST570** will ask to confirm the reset:

4. Click OK if you are sure. Otherwise click Cancel.
5. Click Save all to make the reset permanent.
6. Press the reload button of your Web browser.

Alcatel
Speed Touch™570

Security

16 Security Services – NAT & PAT

NAPT

Network Address Translation (NAT) is a technique that allows you to shield or decouple an internal (Private) IP address from the (negotiated) external (Public) IP address.

In addition, via Port Translation (PT), this single external Public IP address is mapped onto multiple internal ports on the (W)LAN, thus allowing multiple users to share this external IP address simultaneously.

The amalgam of address & port allocation is often referred to as Network Address and Port Translation (NA(P)T).

Note: NA(P)T is described in RFC3022 which obsoletes RFC1631 "The IP Network Translator (NAT)".

In this chapter

Topic	See
AST570 and NA(P)T	16.1
Packet Services and NA(P)T	16.2
The **AST570** 'NAT' Page	16.3
NA(P)T Configuration Example	16.3

16.1 Speed Touch and NA(P)T

Use of NA(P)T

NAT is a technique used to share one IP address amongst several PCs. For most applications, enabling NA(P)T on a specific **AST570** interface, e.g. the Routed Ethernet interface is adequate. From then on, all Routed Ethernet clients behind the **AST570** NAPT router automatically share the same IP address.

To serve that purpose, on all relevant **AST570** pages a NAT checkbox can be found.

The use of these checkboxes is described in section 16.2.

However, to run one or several servers behind a NAPT router, additional configuration is needed. Therefore, the **AST570** exhibits the *'NAT'* page, allowing static IP address and UDP/TCP port mapping for inbound IP packets to be configured.

The use of the *'NAT'* page is described in section 16.3.

NA(P)T and supported protocols

All supported protocols that are insensitive for NA(P)T, pass transparently through the **AST570** NA(P)T router.

In addition, the **AST570** supports also the following protocols as NA(P)T insensitive:

- All generic TCP/User Datagram Protocol (UDP) protocols, e.g. HTTP (Hyper Text Transfer Protocol)
- Internet Control Message Protocol (ICMP)
- File Transfer Protocol (FTP)
- Internet Relay Chat (IRC)
- Real Audio
- Real Time Stream Protocol (RTSP).

To allow the multimedia protocols defined in the H.323 and H.245 ITU recommendation to be transparent for the **AST570** NA(P)T router, e.g. for using Netmeeting over the DSL line, the **AST570** exhibits specific protocol-helper applications for:

- H.323
- H.245.

16.2 Packet Services and NA(P)T

Introduction

The **AST570** supports NA(P)T to be used in combination with most of its packet services, i.e. for:

- Routed Ethernet
- Routed PPPoE
- Routed PPPoA
- CIP & IP Routing.

Routed Ethernet

You can enable/disable NA(P)T via the *'MER'* page per Routed Ethernet entry.

This allows the negotiated static IP address or dynamically assigned IP address (via the embedded Routed Ethernet DHCP client) used for the Routed Ethernet connection to be shared amongst multiple local PCs.

Routed PPPoE/PPPoA

You can enable/disable NA(P)T via the *'Detailed configuration'* table per Routed PPPoE and/or PPPoA entry. This allows the **AST570** to decouple your local IP addresses from the public IP address negotiated during a session.

CIP & IP Routing

You can enable/disable NA(P)T via the *'IP address'* table for each IP address of type CIP. This allows the **AST570** to decouple the explicit assigned or implicit assigned IP addresses from your local network configuration. That way, the **AST570** is able to act as a genuine LIS member and to route between the CIP LIS and your (W)LAN.

Consequences of NA(P)T on layers

The NA(P)T feature comes at the expense of the **AST570** transparency. This because a number of protocols that are layered on top of either TCP/IP or UDP/IP do not adhere to the ISO/OSI reference model.

Note: The ISO Open Systems Interconnection (OSI) reference model promotes the layered implementation of communications protocol stacks. Layers from protocol stacks implemented according to this model can be changed without affecting the upper or lower layers.

An important consequence is that changing IP addresses or TCP/UDP ports via NA(P)T affects the other layers as well.

Due to these changes, applications that are the ultimate consumers of the protocols cannot decode the information correctly anymore.

AST570 solutions

The **AST570** offers some solutions to cope with this situation.

Basically these solutions boil down in transporting Public IP addresses transparently through the **AST570** towards a device where a more advanced NAT and/or PAT can be performed.

Some solutions are described in the following paragraphs:

- Via the PPPoA-to-PPTP Relay
- PPP-to-DHCP Spoofing.

Via the PPP0A-to-PPTP relay

You might consider the following setup for a wired environment:

Step	Action
1	Install a second Ethernet PC-NIC next to the existing (wireless or wired) PC-NIC in your PC.
2	Install an OS on this PC that has routing capabilities, e.g. Windows NT, UNIX, etc.
3	Install on this PC a NAT/PAT package that supports all TCP/IP protocols. Now this PC can act as some *'home gateway'*.
4	Connect the Ethernet port of the **AST570** to one of the PC's two Ethernet PC-NICs (can be a wired or a wireless connection).
5	Connect your local wired LAN to the other Ethernet PC-NIC.

Result

By setting up a PPTP tunnel from the *'Home Gateway'* the Public IP address goes transparently through the **AST570** to end up in this advanced *'home gateway'*, where more complex NAT and/or PAT operations can be performed.

PPP-to-DHCP Spoofing

A second technique is to use the PPP-to-DHCP Spoofing feature of the **AST570**. The network configuration is practically identical to the one described above:

Step	Action
1	Install two Ethernet PC-NICs in a PC.
2	Install an OS on this PC that has routing capabilities, e.g. Windows NT, UNIX, etc.
3	Install on this PC a NAT/PAT package that supports all TCP/IP protocols. Now this PC can act as some *'home gateway'*.
4	Connect (one of) the Ethernet port(s) of the **AST570** to the PC's Ethernet PC-NIC port.
5	Connect your local (W)LAN to the other Ethernet PC-NIC.
6	Configure the PC (acting as *'home gateway'*) as DHCP client.
7	Configure the **AST570** as DHCP server.
8	DHCP in the **AST570** must be configured for DHCP Spoofing. See subsection 14.4.2 for more information.
9	At least one PPP connection must begin with the mnemonic "DHCP" in its phonebook name, e.g. DHCP_Spoof.

Result

As soon as a DHCP request from the home gateway hits the **AST570**, a PPP-to-DHCP Spoofing connection is triggered. The IP parameters that are negotiated with the remote peer are carried up to the home gateway via a DHCP reply message.

16.3 The Speed Touch 'NAT' Page

Introduction

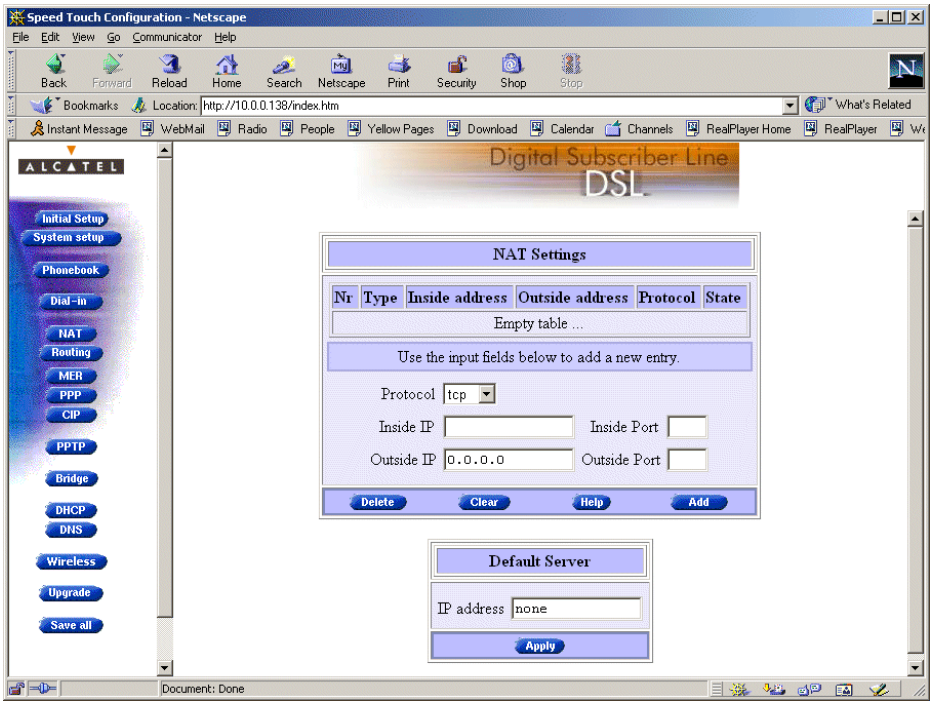
This section describes the use of the *'NAT'* page for configuring static network address and port mapping for inbound IP packets.

In this subsection

- The *'NAT'* Page
- The *'NAT Settings'* Table
- *'NAT Settings'* Table Components
- The *'Default Server'* Table
- Adding Entries
- Deleting Entries.

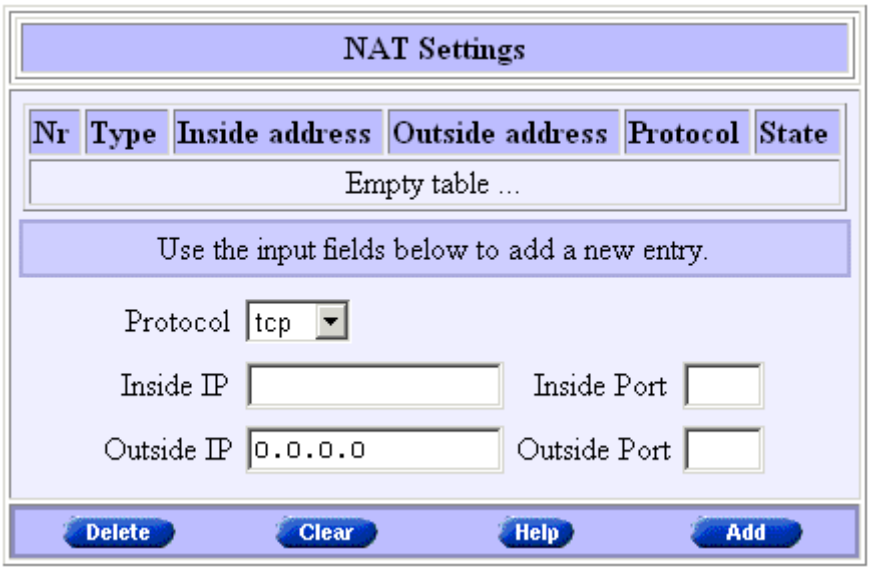
The 'NAT' page

Click NAT in the left pane of the **AST570** pages to pop up the 'NAT' page (See section 21.2 for more information):



The 'NAT Settings' table

The following figure shows the *'NAT Settings'* table:



'NAT Settings' table components

Field	Description
Nr	Indicates an index number for the static NAT entry..
Type	Indicates the template used for the NAT entry. In case dynamic addresses are used to connect to the WAN side, e.g. for PPP connections where the **AST570** receives a different IP address each time the connection is established, the **AST570** allows to save the NAT settings in a template. That way you don't have to specify which of the **AST570**' IP addresses to use.
Inside IP *Inside port* *Inside address*	Indicates the IP address and port of the local PC to which traffic is to be redirected. The *'Inside address'* field indicates both IP address and port as **IP:PORT**. **Note**: The inside port must only be specified for the TCP and UDP protocols. All other protocols do not need a port to be specified.

Field	Description
Outside IP *Outside port* *Outside address*	Indicates the IP address and port on which to perform NAT. Using *0* as IP address causes a template to be created, which will be valid for every one of **AST570**' NAT enabled IP addresses. The 'Outside address' field indicates both IP address and port as **IP:PORT**. **Note**: The outside port must only be specified for the TCP and UDP protocols. All other protocols do not need a port to be specified.
Protocol	Indicates the protocol of the traffic expected to be received on the inside IP:PORT.
State	Indicates the state of the NAT entry.

The 'Default server' table

The following figure shows the *'Default server'* table:

This field allows you to specify a default server. All incoming connections will be forwarded to the device with this IP address. In most cases this setting should be adequate for most server applications.

Adding entries

Proceed as follows:

1. Browse to the *'NAT'* page.
2. If needed, click **New** in the *'NAT settings'* table.
3. Select a protocol from the *'protocol'* pop-down list.
4. Enter the following information for the local PC to which traffic is to be forwarded:
   - Inside IP address
   - Inside port, if applicable.

   Note: You only have to enter an inside port in case the expected traffic for this entry uses the TCP or UDP protocol.
5. Enter the following information for the **AST570** IP address on which NAT is to be enabled:
   - Outside IP address

     Enter 0 in case of a dynamically assigned IP address
   - Outside port, if applicable.

   Note: You only have to enter an outside port in case the expected traffic for this entry uses the TCP or UDP protocol.
6. Click **Add** and **Save all** to finish the procedure.

CAUTION

NA(PT) and AST570 IP Addresses

The outside IP address must always be one of the **AST570**' IP addresses, i.e. it must be present in the *'IP address'* table on the *'Routing'* page.

Moreover, for this IP address *Address Translation* must be enabled, i.e. the *'Type'* field for this IP address must indicate *'pat'*.

Deleting static NAT entries

On the *'NAT'* page, click  next to the NAT entry you want to delete. As a result your selection is highlighted.

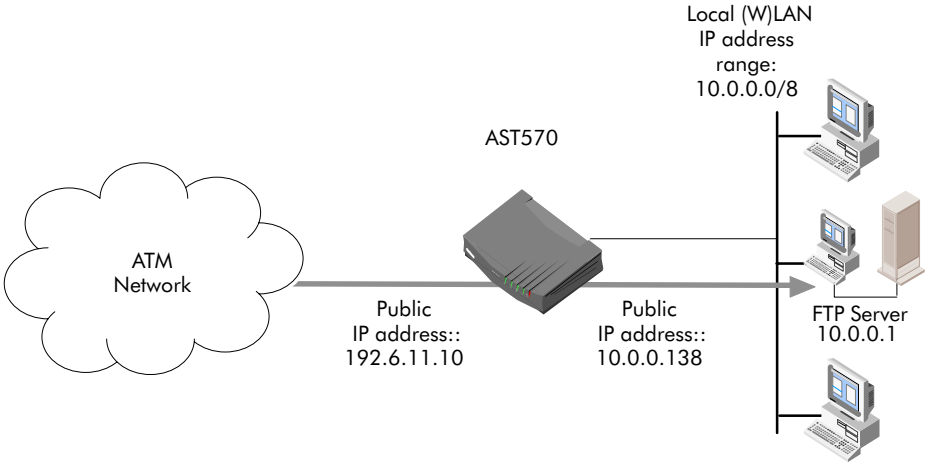
Click **Delete** and **Save all**.

16.4 NA(P)T Configuration Example

Example setup

In the following a simple example is provided to show the working and configuration of the **AST570** NA(P)T router.

It is based on a small (W)LAN, consisting of the **AST570** and a small number of PCs, all configured with static 'Net10' IP addresses and an FTP server with IP address 10.0.0.1:



The **AST570** NA(P)T router must redirect all external FTP connections to 192.6.11.10 to 10.0.0.1 (the FTP server). Without adding a static NA(P)T entry on the **AST570** *'NAT'* page, external users would make an FTP connection with the **AST570** itself instead of the FTP server.

Configuration

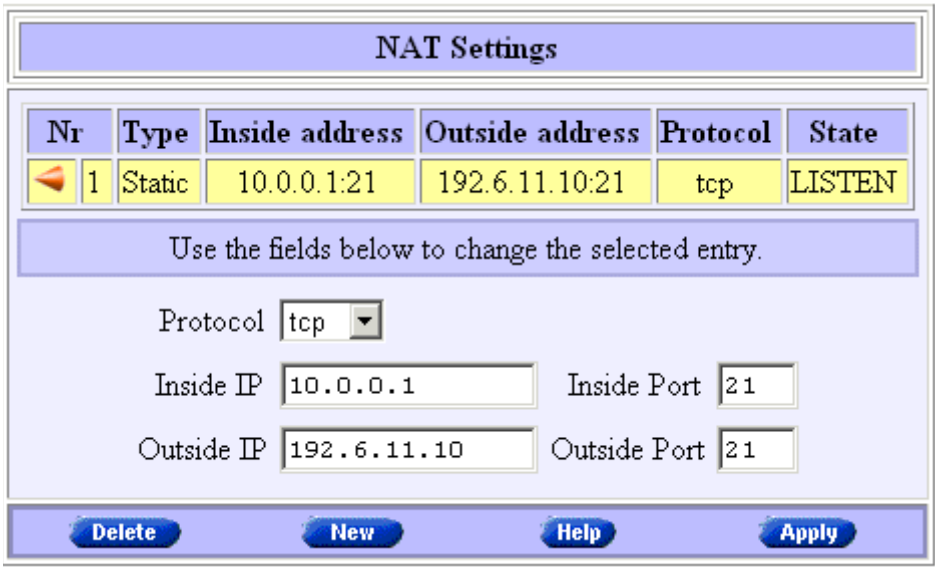
It is assumed that on the *'Routing'* page the external public IP address 192.6.11.10 is added with enabled translation (pat).

The following static NA(P)T entry must be added in the *'NAT Settings'* table:

- Inside address: 10.0.0.1
- Outside address: 192.6.11.10
- Inside/outside port: FTP = 21
- Protocol: FTP = tcp

'NAT Settings' table configuration

The following figure shows the *'NAT Settings'* table with the added static NAT entry:



17 Security Services – Firewalling

Introduction

A Firewall is a security gateway that controls access between a private (W)LAN domain, often referred to as Intranet, and the public Internet.

It secures the entry points to the network, in such a way that access is only allowed to authorized traffic. Therefore, to effectively control the flow of data, firewall protection should be placed at each point where the network connects to the WAN, or the Internet.

This chapter aims to familiarize you with the operation of the **AST570**' programmable Firewall.

In this chapter

Topic	See
Operation of the Firewall	17.1
Firewall Model	17.2
Firewall Actions	17.3
Firewall Criteria	17.4
Firewall and NAPT	17.5
Firewall Configuration	17.6
Firewall Configuration Examples	17.7

17.1 Operation of the Firewall

What is the AST570 Firewall

The **AST570** Firewall is a set of related programs that protects the resources of your local network from users from other networks.

Basically, a firewall examines each network packet to determine whether to forward it toward its destination. Firewalls work in most cases closely together with a proxy server that makes network requests on behalf of your local network users.

For the **AST570** Firewall the **AST570** acts as well as network gateway and proxy server to contact the outside world via the DSL line

The **AST570** Firewall is in fact a packet filter: inside and outside nodes are visible to each other at the IP level, but the firewall filters out, i.e. blocks the passage of certain packets, based on their header.

How the AST570 Firewall works

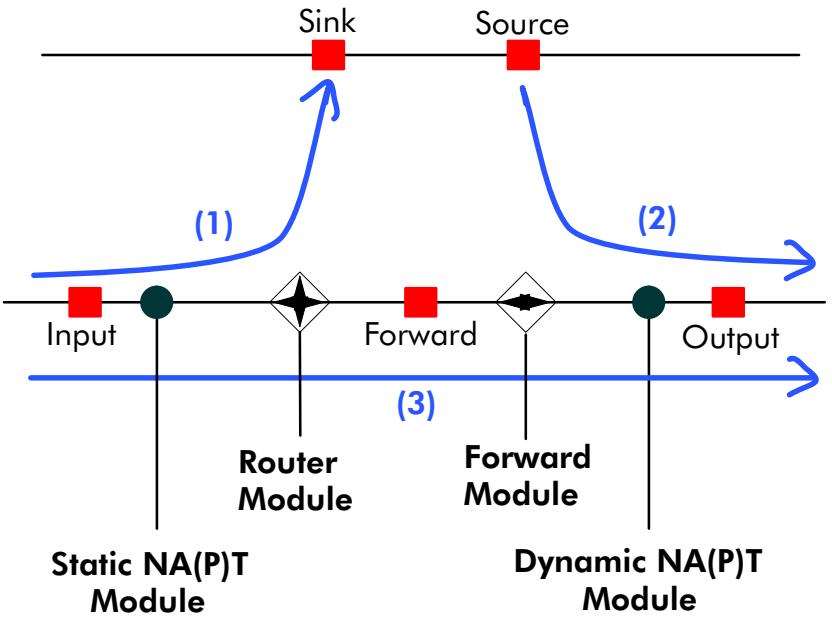
Packets are intercepted at certain Packet Interception Point (PIP), called *hooks*, in the **AST570** IP router. At this points, they are matched against a chain, which comprises rules (at least one). These rules determine the type of control implemented on the packets.

Incoming and outgoing traffic is validated by comparing certain values in the packets with configured Firewall parameters. The parameters in a rule can be divided according to the protocol to which they belong: a first group validates traffic on the interface level, a second group on IP level, a third group filters on TCP, UDP and ICMP level.

17.2 Firewall Model

AST570 Firewall Model

The following figure shows a model of the **AST570** Firewall:



AST570 Firewall modules

The following modules can be identified (See Firewall model):

- **Router Module**

  This module, which has nothing to do with the **AST570** IP router, is responsible for the traffic "within" the **AST570** Firewall, i.e. it routes the packets towards the Sink PIP or Forward PIP.

- **Forward Module**

  This module is responsible for forwarding the packets toward the output.

- **Static/Dynamic NA(P)T Modules**

  These modules are responsible for the translation of IP addresses, in case NA(PT) is used.

AST570 Firewall hooks

The following hooks, or PIPs can be determined (See Firewall model):

- **Input** : The point of all incoming traffic

  At this point it can be determined whether the packet is allowed to reach the **AST570** IP router, or the local host.

- **Sink** : The point of all traffic destined to the **AST570** IP router

  At this point it can be determined whether the packet is allowed to address the local host.

- **Forward** : The point of all traffic to be forwarded by the **AST570**

  At this point it can be determined whether the packet is allowed to be handled, i.e. routed, by the **AST570** IP router.

- **Source** : The point of all traffic sourced by the **AST570** IP router

  At this point it can be determined whether the packet is allowed to leave the local host.

- **Output** : The point of all outgoing traffic

  At this point it can be determined whether the packet is allowed to leave the **AST570** IP router or local host.

AST570 Firewall streams

The following streams (See Firewall model) can run through the PIPs:

- **(1) Input –> Sink** : The flow of packets exclusively destined to the **AST570**
- **(2) Source–> Output** : The flow of packets sourced exclusively by the **AST570** itself
- **(3) Input –> Forward –> Output** : The flow of packets sourced by the WAN, forwarded towards the local network or vice versa.

17.3 Firewall Actions

AST570 Firewall actions

Once a packet is intercepted in a hook, and a rule is found to be applicable, one of the following actions can be performed on the packet:

- **Accept**
  The packet will be submitted to the next processing stage without further action.
- **Deny**
  The packet will not be submitted to the next processing stage. A message will be sent to the sender that the packet could not be delivered, e.g. with an ICMP “host unreachable” error message.
- **Drop**
  The packet will not be submitted to the next processing stage without any further action.
- **Count**
  Each packet passing through is counted without any further action.

17.4 Firewall Criteria

AST570 Firewall criteria

At every hook (PIP) a separate access list, called *chain*, containing an ordered list of rules will operate on each processed packet, resulting in a specific treatment of this packet (See topic '**AST570** Firewall Actions').

A rule is able to operate on the following packet criteria:

- **Interface** related
- **IP** related
- **TCP** related
- **UDP** related
- **ICMP** related.

Interface related criteria

- Source interface
- Source interface group
- Destination interface
- Destination interface group.

IP related criteria

- Source IP address
- Source IP netmask
- Destination IP address
- Destination IP netmask
- Type of service
- Protocol (TCP, UDP or ICMP).

TCP related criteria

- Source Port number
- Source Port number range
- Destination Port number
- Destination Port number range
- Synchronization flag
- Urgent flag.

UDP related criteria

- Source Port number
- Source Port number range
- Destination Port number
- Destination Port number range.

ICMP related criteria

- Type
- code number
- Code number range.

17.5 Firewalling and NAPT

AST570 Firewall and NAPT

The position of the *Input, Static NA(P)T, Dynamic NA(P)T, Forward* and *Output* logical processing modules in the overall **AST570** Firewall model is relative to the traffic direction. In contrast, the **AST570**' WAN and (W)LAN interfaces are physical interfaces; their position is not relative to the traffic direction.

The Dynamic NA(P)T module is situated between the Forward and Output hook (See **AST570** Firewall model). Since the traffic direction will determine input, and output, the Dynamic NA(P)T module can always be positioned between the Forward and Output module.

If you set rules on a hook, you should know if the packets that pass through that hook contain IP addresses that are NA(P)T-translated or not.

If rules are set on the Output hook and NA(P)T is active, the IP packets that pass that hook will contain **translated** IP addresses. If you want to avoid certain traffic, by setting rules that filter on certain (ranges of) IP addresses, you should be aware of the location where the rule will be verified, since, depending on the hook, another IP address will be seen by the Firewall.

As a conclusion: if NA(P)T is activated, the IP address that identifies a local device, will be different depending on the direction of the traffic.

17.6 Firewall Configuration

Configuring the AST570 Firewall

In order to create a Firewall, suitable for your needs, you can create a chain on every hook at the **AST570**. In each chain rules can be applied with configurable parameters. Rules can also refer to a previously defined access list, thus allowing nested access lists, or chains.

You can configure the **AST570** firewall only via the CLI.

See chapter 22 for more information.

Default AST570 Firewall configuration

The **AST570** Firewall is enabled by default with following behavior:

Packets migrating

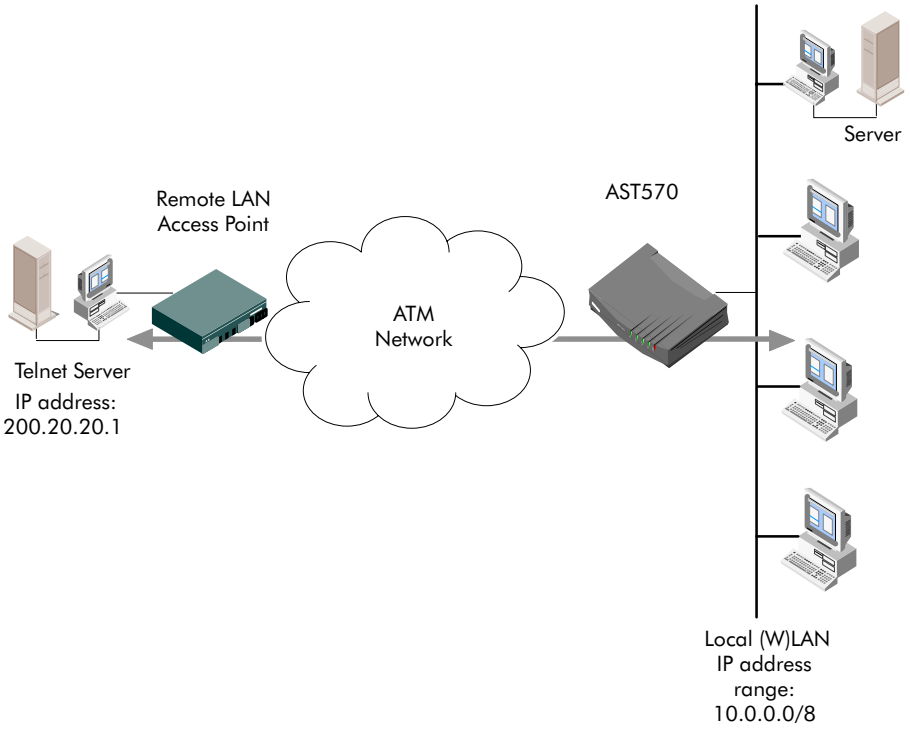
- from WAN to WAN are dropped
- from **AST570** to WAN are dropped, except Port 53 (DNS)
- from **AST570** to (W)LAN are allowed
- from (W)LAN to **AST570** are allowed
- from (W)LAN to WAN are allowed
- from WAN to (W)LAN are allowed
- from a remote LAN to local (W)LAN are allowed
- from local (W)LAN to a remote LAN are allowed.

17.7 Firewall Configuration Examples

Example setup

In the following two simple examples are provided to show the working and configuration of the **AST570** Firewall.

Both are based on a small (W)LAN, consisting of the **AST570** and a small number of PCs, all configured with dynamic "Net10" IP addresses, leased by the **AST570**' DHCP server:



In both examples the **AST570** Firewall must block all services, except an outgoing Telnet service towards one specified remote Telnet server, with IP address 200.20.20.1.

Example 1: Firewall configuration without NA(P)T

Dynamic NA(P)T is not applied on your local (W)LAN for this DSL connection. This means that the IP addresses are not hidden for the remote side of the connection.

In the following table, the rules to apply are summarized:

Flow	Source	Dest.	Prot.	Source port	Dest. port	ACK =1	Action
Out	10.0.0.0/8	200.20.20.1	TCP	1024-65535	23	–	accept
In	200.20.20.1	10.0.0.0/8	TCP	23	1024-65535	Yes	accept
Any	External	10.0.0.0/8	Any	Any	Any	–	drop

For the **AST570** Firewall, this will result in the following CLI configuration:

1. A chain must be created, e.g. 'Telnet':

   ```
   firewall chain create chain=Telnet
   ```

2. Following rules must be created for that chain:
   - For the outgoing Telnet service packets:

     ```
     firewall rule create chain=Telnet src=10.0.0.0/8
     dst=200.20.20.1 srcintfgrp=lan prot=tcp
     srcport=1024 srcportend=65535 dstport=23
     action=accept
     ```

   - For incoming Telnet service reply packets:

     ```
     firewall rule create chain=Telnet src=200.20.20.1
     dst=10.0.0.0/8 srcintfgrp=wan prot=tcp srcport=23
     dstport=1024 dstportend=65535 ack=yes
     action=accept
     ```

   - For blocking all other services:

     ```
     firewall rule create chain=Telnet action=drop
     ```

3. The chain 'Telnet' must be assigned to the *input* hook:

   ```
   firewall assign hook=input chain=Telnet
   ```

Example 2: Firewall configuration with NA(P)T

Dynamic NA(P)T is applied for this DSL connection; all outgoing "Net10" IP addressed packets are translated into the 192.6.11.10 IP address. So the complete local (W)LAN is presented towards the remote side as the single IP address 192.6.11.10.

In the following table, the rules to apply are summarized:

Flow	Source	Dest.	Prot.	Source port	Dest. port	ACK =1	Action
Out	10.0.0.0/8	200.20.20.1	TCP	1024-65535	23	–	accept
In	200.20.20.1	192.6.11.10	TCP	23	1024-65535	Yes	accept
Any	External	Internal	Any	Any	Any	–	drop

For the **AST570** Firewall, this will result in the following CLI configuration:

1. A chain must be created, e.g. 'Telnet':

   ```
   firewall chain create chain=Telnet
   ```

2. Following rules must be created for that chain:

   - For the outgoing Telnet service packets:

     ```
     firewall rule create chain=Telnet src=10.0.0.0/8
     dst=200.20.20.1 srcintfgrp=lan prot=tcp
     srcport=1024 srcportend=65535 dstport=23
     action=accept
     ```

   - For incoming Telnet service reply packets:

     ```
     firewall rule create chain=Telnet src=200.20.20.1
     dst=192.6.11.10 srcintfgrp=wan prot=tcp srcport=23
     dstport=1024 dstportend=65535 ack=yes
     action=accept
     ```

   - For blocking all other services:

     ```
     firewall rule create chain=Telnet action=drop
     ```

3. The chain 'Telnet' must be assigned to the *input* hook:

   ```
   firewall assign hook=input chain=Telnet
   ```

More information

See chapter 22 for more information on **AST570**' Firewall CLI configuration.

Alcatel
Speed Touch™570

Maintenance

18 Maintenance – Speed Touch Software

Software Upgrade

The **AST570** supports two software upgrade possibilities:

- A new version of the software can be downloaded via the DSL line to your **AST570**
- You can upload new **AST570** software yourself from a PC on your local (W)LAN.

Both features, presented in this chapter, are simultaneously supported. However the final result depends on the SP's policy.

In this chapter

Topic	See
Software Upload from the local (W)LAN	18.1
Software Download from the DSL WAN	18.2

18.1 Software Upload from the local (W)LAN

Introduction

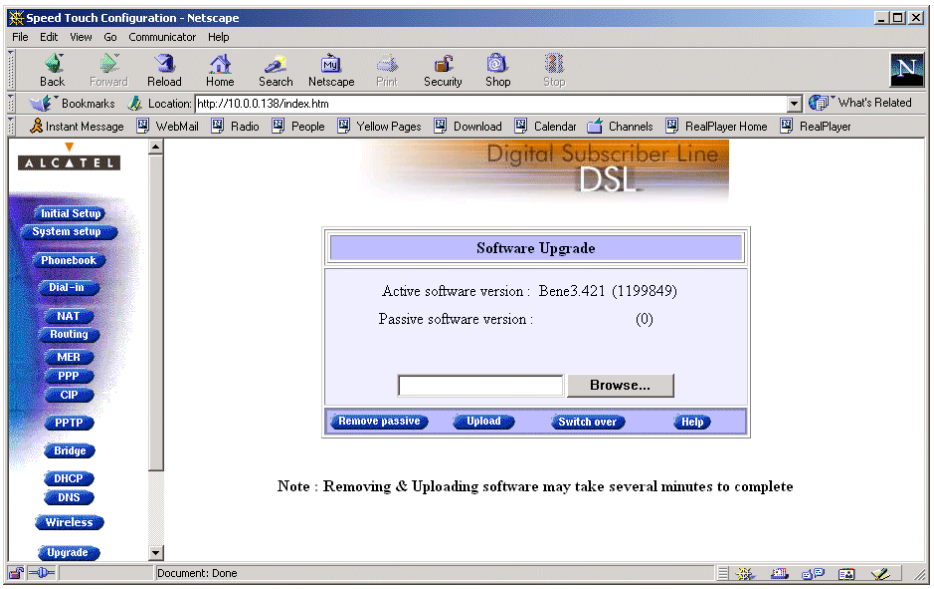
Alcatel DSL products continue to evolve. By upgrading software, the **AST570** is able to follow this evolution.

In this section

- The *'Upgrade'* Page
- *'Upgrade'* Page Components
- *'Upgrade'* Page Buttons
- Upgrade Preconditions
- Uploading Software
- Activating Software.

The 'Upgrade' page

Click Upgrade in the left pane of the **AST570** pages to pop up the *'Upgrade'* page (See section 21.2 for more information):



'Upgrade' page components

The following fields are shown:

- *'Active software version'*

  Indicates the software version the **AST570** is currently using.

- *'Passive software version'*

  Indicates the software version resident in the **AST570**, but not used. This could be a newer version which is yet to be switched to active, but also a dormant older version.

- *Software path* field

  Allows you to specify the path to the **AST570** upgrade software package to be uploaded.

  Clicking Browse... allows you to browse to the location of the upgrade software.

'Upgrade' page components

The following buttons are available:

Button	Functionality
Upload	To start the upload process. The software package indicated by the *Software path* will be transferred to the **AST570** to become the passive software version.
Remove passive	To remove the passive software version from the **AST570** memory.
Switch over	To switch active and passive software versions after a successful upload. Your **AST570** will reboot and come online again with the new version.

Upgrade preconditions

A valid **AST570** software package must reside either on a local drive, on a floppy disk or a CD-rom.

For new software upgrade packages, please contact your SP or check the Alcatel web sites at:

http://www.alcatel.com

http://www.alcateldsl.com

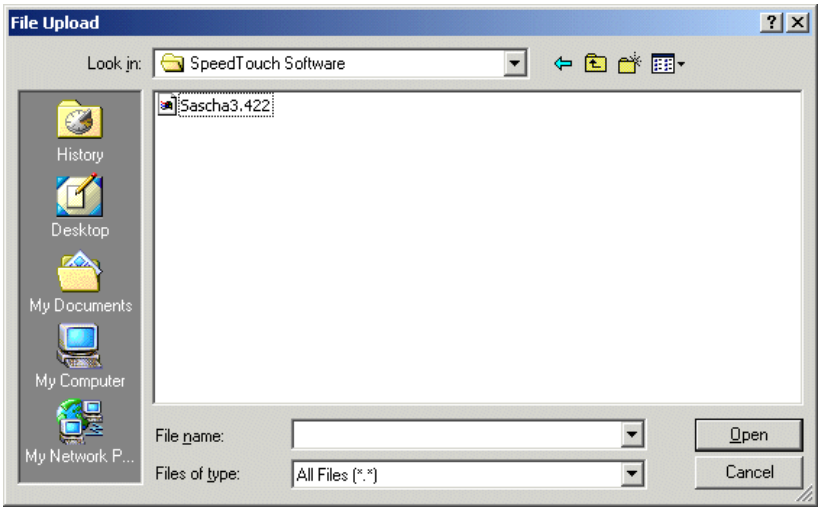
Uploading software

Proceed as follows:

1. Browse to the *'Upgrade'* page.
2. In the *'Active software version'* field the software package that is running is labeled.

   Check whether the *'Passive software version'* field is empty. If not, click **Remove passive**.
3. Click **Browse...** next to the *'Software path'* input field to locate the upgrade software package

   Note: If the path is known you can immediately enter it in the *Software path'* input field and skip step in this procedure.
4. The *'File Upload'* window pops up:

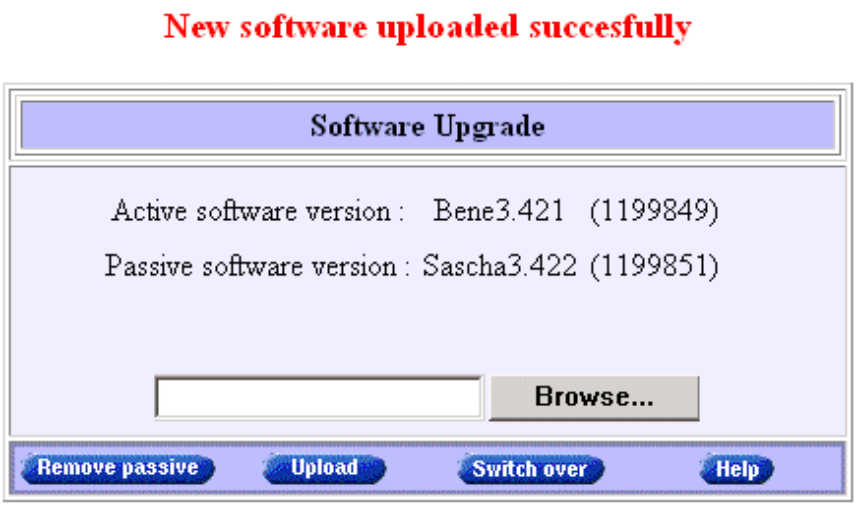


This window allows you to browse to the location of the upgrade software package on either your local drive, floppy disk or CD-rom.

5. Click on the appropriate upgrade software package name to select it and click Open.

   As a result, the upgrade software location will be inserted in the *'Software path'* input field.

6. Click Upload to start the upload. As a result the upgrade software package name will appear in the *'Passive software version'* field:



Note: In case you did not remove the passive version, prior to uploading new software, the upload will be unsuccessful and an error message will appear.

Upload Result

After a successful upload, two software versions are stored on the **AST570**: The running (active) version and a passive version.

Activating software

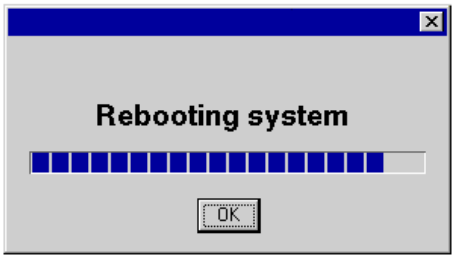
Proceed as follows to switch passive upgrade and active running software versions:

1. If needed, browse to the *'Upgrade'* page.

   Note: Make sure a passive software version is labeled in the *'Passive software version'* field. If not, firstly upload a upgrade software package as described in the previous procedure.

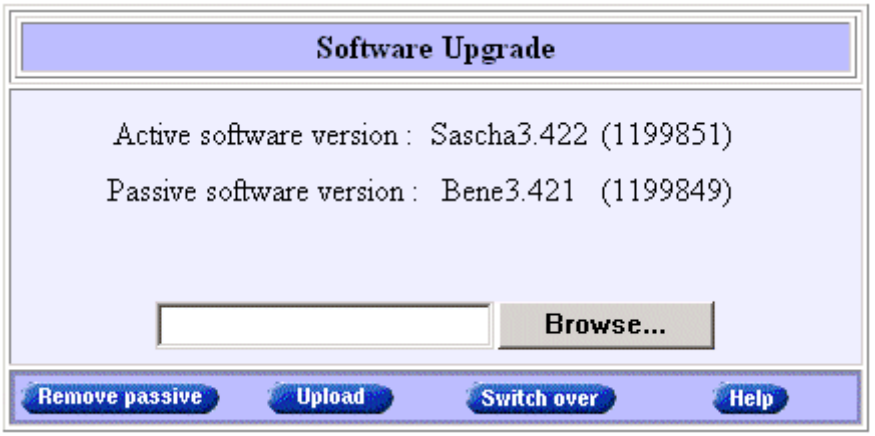
2. Click Switch over to start the switching of the two versions.

   After switching the versions, the **AST570** reboots:



Result

After reboot your **AST570** will come online with the upgrade version (active and passive software are switched):



18.2 Software Download from the DSL WAN

Introduction

The **AST570** supports a second software upgrade possibility: a new version of the software can be downloaded from the DSL network to your **AST570**.

This can be done via the **AST570** dedicated control VCs.

Software Download

This feature is controlled by the SP.

At some point in time he might decide to upgrade the software in your **AST570**.

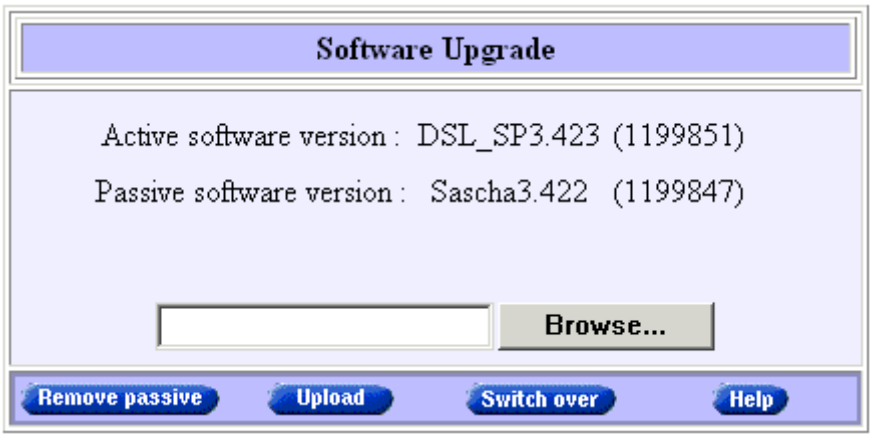
Software download will happen almost unnoticed, while you are connected to the DSL line.

The removal of a possible dormant software version, the download itself, and the switching of both versions is performed automatically.

Note: DSL service can be interrupted for a short period due to a reboot of the **AST570**.

Result

You will notice a change in the software version if you browse to the **AST570** *'Upgrade'* page:



19 Maintenance – Speed Touch Password

In this chapter

Your **AST570** is a highly advanced product, operating according the many configurations set via the **AST570** Web interface or via the CLI.

In this way, **AST570** operation is vulnerable to misconfiguration by other users.

Therefore, the **AST570** can be secured from such users by a system password to restrict access to the Web interface or the CLI.

This chapter describes how to set such a system password.

Note

Never use an obvious system password to protect the **AST570** as your name, birth date or phone number.
Moreover, you are advised to change the system password regularly.

CAUTION

Forgetting the System Password

In case you forgot the system password you are no longer able to access the web interface or the CLI and you will be no longer able to (re)configure the **AST570** settings.

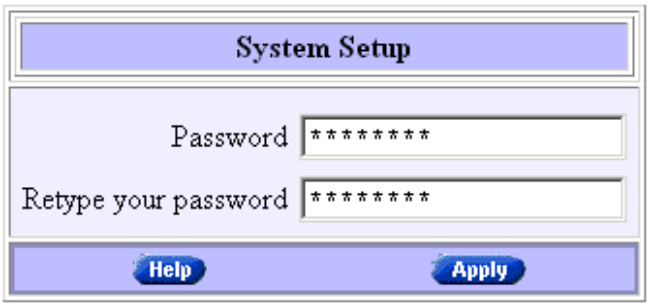
Therefore, write your system password down and keep it on a save place.

Otherwise, a *Switch-to-Defaults* must be performed restoring all original settings of the **AST570**.

Setting a system password

Proceed as follows:

1. Click System setup on the **AST570** pages (See section 21.2 for more information).
2. On the *'System setup'* page the following table is shown:



   The *'System setup'* table allows you to configure a system password.
3. In the *'Password'* field, fill in a password. Retype your password in the *'Retype your password'* field.

   Note: Asterisks will appear instead of the password. The number of asterisks is at random.
4. Click Apply.
5. To make your password permanent, click Save all.
6. Authenticate yourself, using the system password, you just configured.

Result

Every time you want to access the **AST570** pages or (Telnet) CLI you must authenticate yourself, using the system password.

Clearing a system password

To clear the **AST570** system password you must clear both the *'Password'* field and *'Retype your password'* field, i.e. delete all asterisks. Click Apply and Save all to store your changes.

No authentication is required anymore to access the **AST570** pages, or the (Telnet) CLI.

20 Maintenance – Speed Touch To-Defaults

Introduction

Non accessibility to your **AST570** may occur if wrongly configured, simply by forgetting its IP address, or forgetting the system password.

Due to the flexible nature of the **AST570**, you may end up in a situation where restoring all of the original defaults is the only solution.

The **AST570** has tools to cope with these situations.

In this chapter

Topic	See
Ping-of-Life™	20.1
AST570 Reset	20.2

20.1 Ping-of-Life

Introduction

The **AST570** offers a unique method to supply an IP address to the **AST570**' (Wireless) Ethernet interface.

This method, the *Ping-of-Life™,* allows to provide the **AST570** with an IP address without affecting other configurational settings.

General procedure

The principle is fairly simple: a special ping packet will deliver an IP address to your **AST570**.

Generally the procedure is as follows:

Step	Action
1	Pre-configure the intended IP address and a special MAC group address in the ARP cache of one of your PCs.
2	Power cycle the **AST570**, and allow the POST to end (this takes about 30 seconds).
3	Ping this same IP address within 60 seconds after the **AST570** ended its POST. If everything goes well, the **AST570** has assimilated this IP address.
4	Save the new IP setting via the **AST570** pages.

Note

Most TCP/IP packages support the *ARP* and *PING* command. The *Ping-of-Life* can be executed from any PC on your local network.

CAUTION

IP Addresses and Subnet Masks

Make sure that the intended **AST570** IP address and your PC share the same IP (sub)network.

If not, the ping will be submitted with the MAC address of the default router instead of the special MAC group address.

The Ping-of-Life™ procedure

Proceed as follows:

1. Turn off the **AST570**.
2. Open a command-line (DOS) window (Windows OS), or a terminal window (UNIX, Linux) on a PC.
3. At the command prompt execute: **`arp -a`**

   This allows you to overview the current entries in the ARP cache.
4. Add a static entry to the ARP cache, according to following syntax:

   `arp -s <ST IP address> 01-90-D0-80-01-01`

   `<ST IP address>` is a placeholder for the IP address to be assigned to the **AST570**. It can be any address within your subnet as long as it is not used by any other member of your local network.
5. To verify whether this step was successful execute **`arp -a`** a second time.

   In the entries list, your **`arp -s`** command entry should be added.
6. Initiate a continuous pinging, by executing following command:

   `ping -t <ST IP address>`
7. Turn on the **AST570**.
8. After the **AST570** finished its POST, it will configure the IP address **`<ST IP address>`** you are pinging.
9. You must clear the entry in the ARP cache by issuing the following command:

   `arp -d <ST IP address>`
10. Verify connectivity by pinging the **AST570** a second time:

    `ping <ST IP address>`

    The **AST570** should reply.
11. Browse to the **AST570** pages and click Save all to make the new IP address permanent.

Ping-of-Life™ with multiple PC-NICs

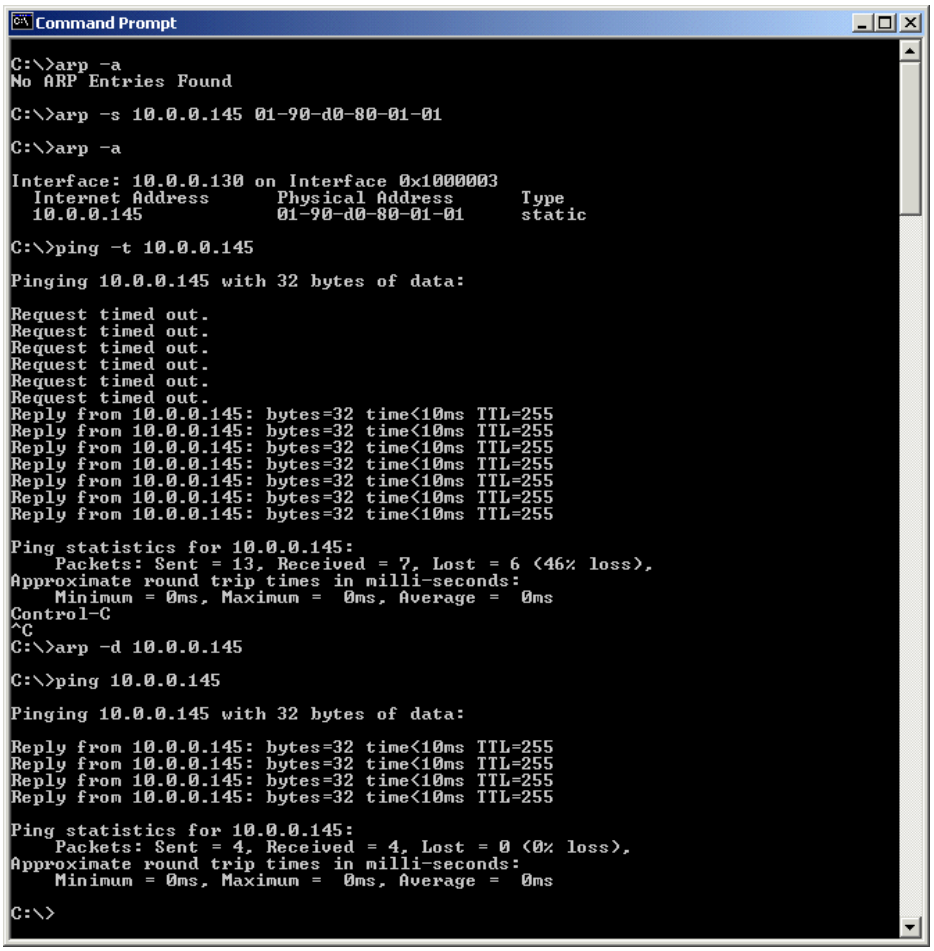
If your PC is equipped with multiple PC-NICs, make sure that the procedure is applied to the one connected to the **AST570**.

In the following syntax, **<Interface IP address>** identifies the particular PC-NIC:

```
arp –<a,s,d> <ST IP address> 01-90-D0-80-01-01 –N
<interface IP address>
```

Example DOS box

In the following figure all the steps are shown as an example of setting **AST570**' IP address to 10.0.0.145 from a PC with an MS Windows OS:



20.2 Speed Touch Reset

Overview of the To-Defaults methods

To restore **AST570**' original settings, three methods are provided:

- Two local software methods:
  - *Browse-to-Defaults*
    Which sets all parameters to original defaults, but keeps the system password, Wireless LAN settings and IP address.
  - *Ping-to-Defaults*™
    Which sets all parameters to original defaults, including the system password, Wireless LAN settings and IP address.
- One hardware method:
  - *Switch-to-Defaults*.
    Which sets all parameters to original defaults, including the system password, Wireless LAN settings and IP address.

CAUTION

Restoring Original Settings

Be careful when using To-*Defaults* procedures as these destroy all changes you previously made to the **AST570** internal settings.

A reset to defaults via a *Ping-to-Defaults*™ or via a *Switch-to-Defaults* implies the **AST570**' IP addresses are reset to the default 10.0.0.138 IP address as well as all Wireless settings. As a consequence, IP connectivity with the **AST570** could be lost. In that case you must firstly authenticate your WLAN client adapter (in case of a non-wired network) and then execute a *Ping-of-Life*™ for a suitable **AST570** IP address.

In this section

Topic	See
Browse-to-Defaults	20.2.1
Ping-to-Defaults™	20.2.2
Switch-to-Defaults	20.2.3

20.2.1 Browse-to-Defaults

Procedure

Proceed as follows:

1. Click System setup on the **AST570** pages (See section 21.2 for more information).
2. On the *'System setup'* page the following table is shown:

3. Click Defaults if you are sure to reset the **AST570** to its original defaults.
4. The **AST570** will ask to confirm the reset:

5. Click OK if you are sure. Otherwise click Cancel.
6. Click Save all to make the Browse-to-Defaults permanent.
7. Press the reload button of your Web browser.

Browse-to-Defaults result

After reset, all original configurations of the **AST570** are restored except the **AST570** Ethernet IP address(es) and Wireless settings.

20.2.2 Ping-to-Defaults

Introduction

A second software method to reset all settings to the original defaults is the *Ping-to-Defaults*™.

The technique is identical to that used for the *Ping-of-Life*™, except that another MAC address is used, i.e. **`01-90-D0-80-01-FF`**.

Procedure

Proceed as follows:

1. Turn off the **AST570**.
2. Open a command-line (DOS) window (Windows OS), or a terminal window (UNIX, Linux) on a PC.
3. Add a static entry to the ARP cache, according to following syntax:

   `arp -s <any IP address> 01-90-D0-80-01-FF`

   `<any IP address>` can be any address within your subnet as long as it is not used by any other member of your local network.
4. To verify whether this step was successful execute **`arp -a`**
5. Initiate a continuous pinging, by executing following command:

   `ping -t <any IP address>`
6. Turn on the **AST570**.
7. After the **AST570** finished its POST, it will perform a reset to default settings.
8. You must clear the entry in the ARP cache by issuing the following command:

   `arp -d <any IP address>`
9. For a non-wired network, re-authenticate your WLAN client adapter.
10. If needed, reconfigure the **AST570** IP address, e.g. via a Ping-of-Life™ and its Wireless LAN settings.

Note

The used **`<any IP address>`** to perform a *Ping-to-Defaults*™ is not assimilated by your **AST570**.

20.2.3 Switch-to-Defaults

Introduction

At the back of the **AST570** there is a small push button labeled *'Defaults'*.

Via this button a hardware reset of the **AST570**, the *Switch-to-Defaults*, is possible.

Procedure

Proceed as follows:

1. Make sure your **AST570** is turned on.
2. Use a pencil to press the push button at the back of the **AST570**. Hold on the push button for several seconds until all front LEDs go out.
3. Release the button. Via the flashing front panel LEDs, you will notice that the **AST570** will restart.
4. The **AST570** will come online with manufacturing defaults.
5. For a non-wired network, re-authenticate your WLAN client adapter.
6. If needed, reconfigure the **AST570** IP address, e.g. via a Ping-of-Life™ and its Wireless LAN settings.

21 Maintenance – Speed Touch Web Interface

Introduction

The **AST570** comes with integrated local configuration capabilities.

Two methods exist:

- Configuration via a Web browser
- Configuration through a Command Line Interface (CLI).

The AST570 web interface

The local configuration via the **AST570** web interface, is based on the HyperText Transfer Protocol (HTTP) server/Web browser concept.

It allows configuration of your **AST570** via a Web browser through HyperText Markup Language (HTML) pages from any local PC attached to the Ethernet interface(s).

In this chapter

Topic	See
Web Interface Preconditions	21.1
Browsing to the **AST570** Pages	21.2
AST570 Page Structure	21.3

21.1 Web Interface Preconditions

Preconditions

When your PC is connected to a Proxy server for accessing the Internet, you must change your Web browser preferences, because the **AST570** is a local device and its IP address cannot be resolved by the Proxy server.

Therefore, prior to access the **AST570** pages make sure that either:

- Your Web browser is not using a Proxy server
- The **AST570** IP address is not submitted to the Proxy server.

Note

The procedures described are methods for:

- Netscape Navigator, version 2.0 or above
- Microsoft Internet Explorer, version 2.2 or above.

In this section

Topic	See
Disabling Proxy Servers	21.1.1
Disabling Proxying for Local IP Addresses	21.1.2

21.1.1 Disabling Proxy Servers

Introduction

This subsection describes how to disable Proxy servers for your Web browser.

As a consequence of this action, connectivity through the Proxy server to the Internet is lost.

Therefore, after configuring your **AST570**, do not forget to reset your Web browser to its original settings !

Disabling Proxy servers for Netscape Navigator

1. Select '*Edit*' from the toolbar.
2. Select '*Preferences*'.
3. In the '*Category*' box select *Advanced, Proxies*.
4. Click the option button '*Direct Connection to the Internet*'.

Disabling Proxy servers for Internet Explorer

1. Right-click the '*Internet*' icon.
2. From the pop-up menu select '*Properties*'.
3. Clear the *'Use Proxy Server'* checkbox.

Web browser versions

Since several versions of these Web browsers exist, the proxy settings might be located in other menus than the ones described above. Consult the documentation of your Web browser for more information on proxy settings.

21.1.2 Disabling Proxying for Local IP Addresses

Introduction

This subsection describes how to avoid that IP addresses you can directly connect to (e.g. the **AST570**), are passed over to the Proxy server.

However, this option can only be used if the Proxy servers are manually configured, i.e. are not automatically configured, i.e. if the Proxy servers are known by name, and port.

Disabling Proxying for Netscape Navigator

1. Select '*Edit*' from the toolbar.
2. Select '*Preferences*'.
3. In the '*Category*' box select *Advanced, Proxies*.
4. Under *'Manual Proxies'*, click the *view* button.
5. In the *Exceptions* box, add the IP address of your **AST570**, or the IP subnetwork address pool.

Disabling Proxying for Internet Explorer

1. Select 'Tools' from the toolbar.
2. From the pop-up menu select 'Internet Options'.
3. In the *'Internet Options'* window, select the *'Connections'* tab.
4. Click the *'LAN Settings...'* button.
5. In the *'Proxy Server'* box, check the *'Bypass Proxy servers for local addresses'* box, and click '*Advanced*'.
6. In the *'Exceptions'* settings, add the **AST570** IP address, or the IP subnetwork address pool.

Web browser versions

Since several versions of these Web browsers exist, the proxy settings might be located in other menus than the ones described above. Consult the documentation of your Web browser for more information on proxy settings.

21.2 Browsing to the Speed Touch Pages

Procedure

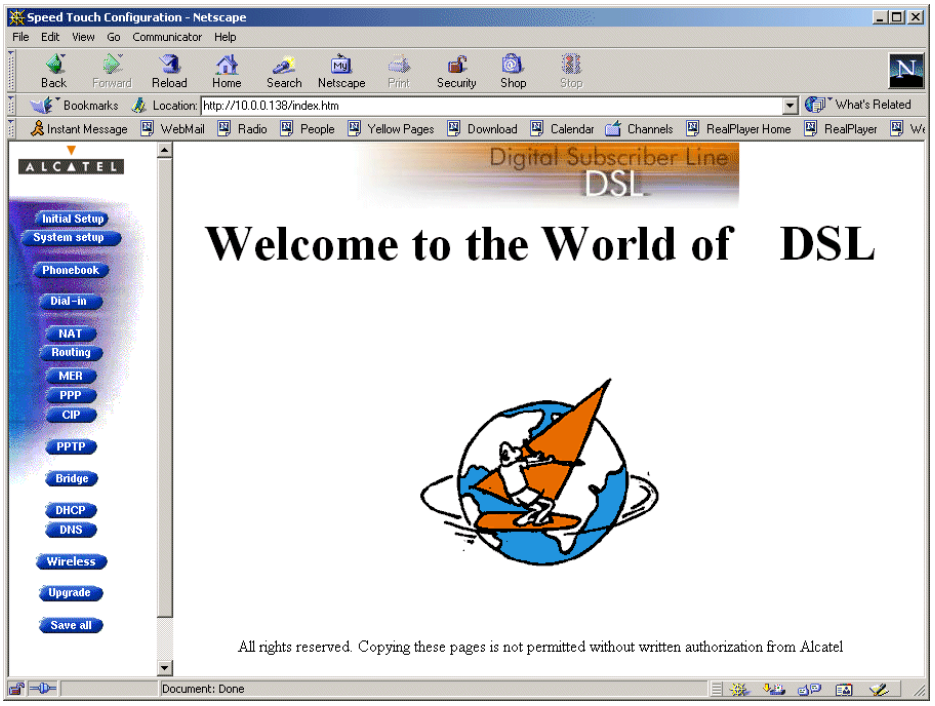
Proceed as follows:

1. Start the Web browser on your PC or workstation.
2. Contact the **AST570** by entering one of the following:
   - The **AST570** IP address (default 10.0.0.138)
   - The **AST570** DNS hostname (default SpeedTouch.lan).
3. If a system password was set (See chapter 19 for more information), an authentication window will pop up.

   Enter the system password in the *'Password'* field.

Result

As a result the *'Welcome to the World of DSL'* page pops up:

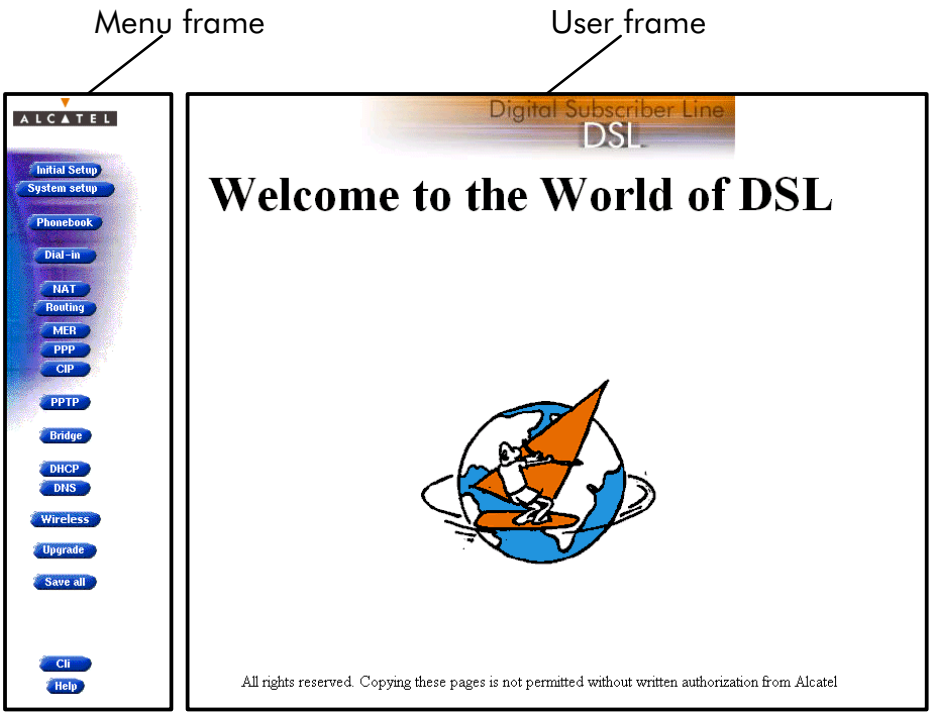


From now on the **AST570** acts as a Web server sending HTML pages/forms at your request. You can fill out these pages/forms and submit them to the **AST570**. The latter scans the pages and makes configurations accordingly.

21.3 Speed Touch Page Structure

AST570 page frames

All **AST570** pages can be divided into two frames:



Each web page contains:

- The generic *Menu frame*
- The context related *User frame*.

Menu frame components

The Menu frame is generic for all **AST570**' pages.

Each menu button represents a **AST570** configuration page, yielding all configurational possibilities related to menu subject.

The following buttons are available:

Click this button ...	To ...	See
ALCATEL	Return to the *'Welcome to the World of DSL'* page.	21.2
Initial Setup	Configure user defined **AST570** IP parameters.	14.3.2
System setup	Set a System password Perform a *Browse-to-Defaults*.	19 20.2.1
Phonebook	Overview the record of all possible, and existing ATM connections.	13.2
Dial-in	Dial-in page for Routed PPPoA and Routed PPPoE sessions.	11.2
NAT	Configure static NA(P)T entries.	16
Routing	Configure the **AST570** IP router.	14.5
MER	Configure the Routed Ethernet packet service.	7.3
PPP	Configure the Routed PPPoA and Routed PPPoE packet services.	11.3
CIP	Configure the CIP packet service.	12.4
PPTP	Overview active Relayed PPPoA connections.	10.4
Bridge	Configure the Bridging packet service. View Bridging MAC layer data.	6.3 6.4
DHCP	Configure the **AST570** DHCP server/client.	14.4
DNS	Configure the **AST570** DNS server/client.	15.2
Wireless	Configure the **AST570** WLAN parameters.	4
Upgrade	Upgrade **AST570** software.	18
Save all	Save all changes made to persistent memory.	
Cli	Open the *'CLI'* pages to allow detailed configuration of the **AST570**.	22.1
Help	Pop up the **AST570** help pages.	

22 Maintenance – Speed Touch CLI

Introduction

For advanced configurations, with full control over all the **AST570** functions, the **AST570** exhibits a low level interface, i.e. the Command Line Interface (CLI).

As the CLI has far more configurational possibilities than the regular **AST570** pages it is intended for experienced users only.

The CLI is accessible via:

- The **AST570** pages
- A Telnet session via Ethernet IP connectivity.

In this chapter

Topic	See
CLI via the **AST570** Pages	22.1
Native CLI Access	22.2

22.1 CLI via the Speed Touch Pages

In this section

- CLI Page Requirements
- The *'CLI'* Page
- CLI Commands Basics
- Example: Command Group Description
- Executing Commands
- Example: Command Execution
- Detailed CLI Commands Description.

CLI page requirements

To access the *'CLI'* page, you need one of the following:

- Microsoft's Internet Explorer 4.0, or better
- Netscape's Communicator 4.06, or better.

Both web browsers must support JavaScript.

The 'CLI' page

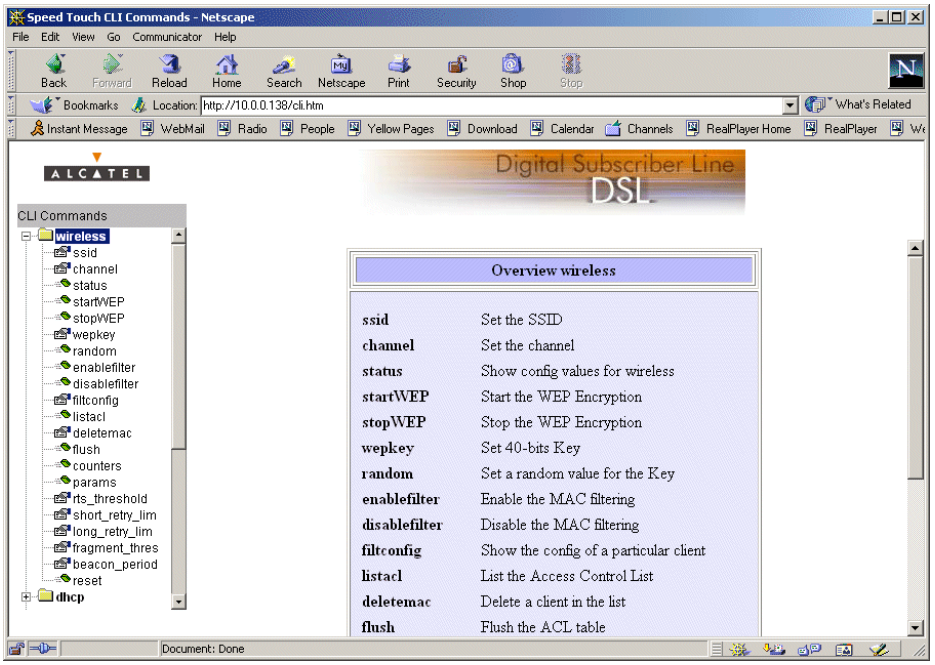
Click Cli in the left pane of the **AST570** pages to pop up the *'CLI'* page (See section 21.2 for more information):

CLI commands basics

All CLI groups and commands are placed in a menu. You can open a group by clicking the ⊞ mark next to a group name, or clicking the group name.

Example: command group description

The following example shows the output if you click ⊞ next to the *'wireless'* group name:



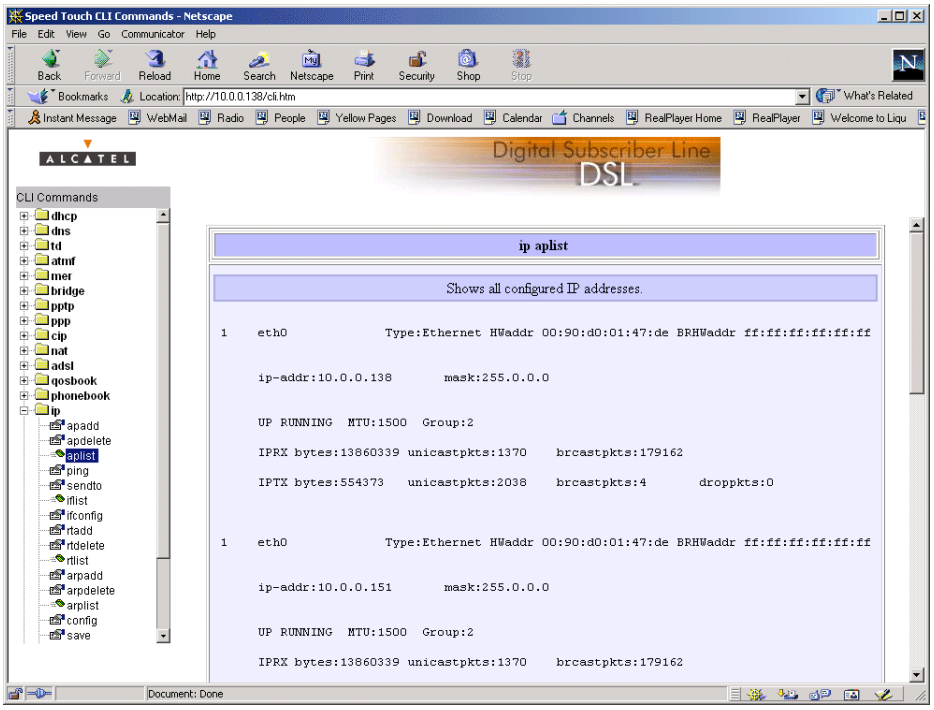
Executing commands

Clicking on a command name will execute it. Commands without parameters are indicated with and are executed immediately.

Commands which require additional parameters are indicated with . After you configured all parameters you must click Apply to execute the command.

Example: command execution

Clicking *'aplist'* in the *'ip'* command group generates the following immediate output:



CLI Reference Guide

A CLI Reference Guide with detailed CLI configuration description of all the commands can be found at:

http://www.alcatel.com

http://www.alcateldsl.com

22.2 Native CLI Access

Introduction

Next to CLI access via the **AST570** pages, you can use native access via a basic Telnet session.

This allows configuration via a character based CLI. As a consequence the use of a Web browser or even any graphical or operational environment is avoided.

In this chapter

Topic	See
CLI through a Telnet Session	22.2.1
CLI Commands Basics	22.2.2

22.2.1 CLI through a Telnet Session

Introduction

Via a PC or terminal connected via the wired or wireless Ethernet interface of the **AST570** you can execute CLI commands.

However, you must gain access to the **AST570** first by opening a TCP/IP Telnet session.

In this section

- Telnet Features
- Telnet Requirements
- Using a Telnet Session to your **AST570**.

Telnet features

Telnet is:

- A fairly general, bi-directional, eight-bit byte-oriented communication facility
- A standard method of interfacing terminal devices to each other.

Telnet requirements

Prior to using Telnet, you need:

- A connected and configured **AST570**, with known IP address or DNS hostname
- If applicable, the system password for accessing the **AST570**
- A PC or terminal connected to the (W)LAN

  Note: (W)LAN is referred to as a network containing at least one PC or terminal, and your **AST570**.
- A TCP/IP suite installed on this PC or terminal
- A Telnet session application installed on this PC or terminal.

Using a Telnet session to your AST570

After opening a Telnet session, e.g. via the command

`telnet 10.0.0.138`

you reach the CLI prompt, preceded by the opening CLI banner and optionally after supplying the system password:

```
telnet 10.0.0.138

Trying 10.0.0.138...
Connected to 10.0.0.138.
Escape character is ’^]’.
User :
SpeedTouch (00–80–9F–01–23–45)
Password :######
------------------------------------------------------------------------
*
*                             ______
*                         ___/_____/\
*                        /         /\\    ALCATEL  SPEED TOUCH 570
*                  _____/__       /  \\     Wireless ADSL Router
*                _/       /\_____/___ \         Version 1.0
*               //       /  \       /\ \
*       _______//_______/    \     / _\/______ Copyright 1999–2001.
*      /      / \       \    /    / /        /\
*   __/      /   \       \  /    / /        / _\__
*  / /      /     \_______\/    / /        / /   /\
* /_/______/___________________/ /________/ /___/  \
* \ \      \    ___________    \ \        \ \   \  /
*  \_\      \  /          /\    \ \        \ \___\/
*     \      \/          /  \    \ \        \  /
*      \_____/          /    \    \ \________\/
*           /__________/      \    \  /
*          \   _____  \      /_____\/
*            \ /    /\  \    /___\/
*             /____/  \  \  /
*             \    \  /___\/
*              \____\/
*
------------------------------------------------------------------------
=>
```

22.2.2 CLI Command Basics

Introduction

Although it is not the aim of this subsection to give a complete overview of all possible configurational **AST570** items, this subsection describes some of the generalities of the native CLI environment.

General CLI information

Once you accessed your **AST570**, you will get the CLI prompt: **=>**.

From this point you can start entering your commands.

The CLI access is structured in what is called “levels”.

The **=>** prompt indicates that you are in the “root” level of CLI.

CLI help

Typing **help** at the root prompt shows you the available command groups:

```
=>help
Following commands are available :
help              : Displays this help information
exit              : Exits group selection.
..                : Exits group selection.

Following command groups are available :
dhcp          dns          td           wireless  mer
bridge        pptp         ppp          cip       nat
adsl          qosbook      phonebook    ip        software
system        config       firewall
=>
```

Navigating through CLI levels

Entering the name of a command group, accesses you to this specific level.

For example , entering **=>config** followed by pressing ‘Enter’, brings you to the “config” level. This is indicated by its own prompt: **[config]=>**

Command group help

Typing **help** at the command group level prompt shows you the available commands.

For example, entering **help** at the "config" level generates the following output:

```
[config]=>help
Following command groups are available :
save   : Saves complete configuration.
erase  : Removes all saved data.
load   : Loads saved or factory default configuration.
flush  : Flushes complete configuration.
reset  : Flush & restore factory default configuration.
[config]=>
```

Command help

Typing **help** followed by a command generates shows you a description of the command, and a parameter syntax, if applicable:

For example , entering **help reset** in the "config" level generates the following output:

```
[config]=>help reset
   [keep_ip = <{no|yes}>]
     Reset IP settings or not.  Resetting IP can break
     current telnet/http session !
[config]=>
```

Command execution

Typing the command executes the command. In most cases you must also provide related parameters.

The consequences of a command execution have immediate effect. However, only after executing the **save** command, the new settings are stored in persistent memory.

CLI Reference Guide

A CLI Reference Guide with a detailed CLI configuration description of all the commands can be found at:

http://www.alcatel.com

http://www.alcateldsl.com

Alcatel
Speed Touch™570

Appendices

Abbreviations

ADSL	Asymmetric Digital Subscriber Line
ASAM	ATM Subscriber Access Multiplexer
ATM	Asynchronous Transfer Mode
BBRAS	BroadBand RAS
CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless Inter Domain Routing
CIP	Classical IP
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DSLAM	Digital Subscriber Line Access Multiplexer
DSSS	Direct Sequence Spread Spectrum
DTE	Data Terminal Equipment
FIB	Forwarding Information Base
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IRC	Internet Relay Chat
ISP	Internet Service Provider
ITU	International Telecommunication Union
LAN	Local Area Network
LCP	Link Control Protocol
LIS	Logical IP Subnet
MAC	Medium Access Control
MER	MAC Encapsulated Routing
NA(P)T	Network Address and Port Translation
NAT	Network Address Translation
NIC	Network Interface Card
OS	Operating System

OSI	Open Systems Interconnection
PAP	Password Authentication Protocol
PAT	Port Address Translation
PC	Personal Computer
PIP	Packet Interception Point
POST	Power On Self Test
POTS	Plain Old Telephone Service
PPC	Portable PC
PPP	Point-to-Point Protocol
PPPoA	PPP over ATM
PPPoE	PPP over Ethernet
PPTP	Point-to-Point Tunnelling Protocol
PT	Port Translation
PVC	Permanent Virtual Channel
QoS	Quality of Service
RAS	Remote Access Server
REN	Ringer Equivalence Number
RF	Radio Frequency
RIP	Routing Information Protocol
ROW	Rest Of the World
RTSP	Real Time Stream Protocol
SELV	Safety Electronic Low Voltage
SNMP	Simple Network Management Protocol
SP	Service Provider
SSID	Service Set ID
SVC	Switched Virtual Channel
TCP	Transmission Control Protocol
TNV	Telecommunication Network Voltage
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VC	Virtual Channel
VCI	Virtual Channel Identifier
VLSM	Variable Length Subnet Masking

VP	Virtual Path
VPI	Virtual Path Identifier
VPN	Virtual Private Network
WAN	Wide Area Network
WECA	Wireless Ethernet Compatibility Alliance
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless LAN

AppendixA Speed Touch Troubleshooting

Introduction

This appendix provides information on how to identify and correct some common problems you may encounter when using and configuring the **AST570**.

If the following troubleshooting tips have not resolved the problem contact the company from which you purchased the **AST570** for assistance.

Configuration problems

In case you encounter DSL connectivity problems due to misconfiguration you might consider a reset to original defaults as described in chapter 20.
However, be aware that a reset to original defaults destroys all configurational changes you made to the **AST570** internal settings.

Trouble solving table

Problem	Solution
AST570 *does not work.* *(none off the LEDs lights up)*	Make sure the **AST570** is plugged into an electrical outlet.
	Make sure the power switch on the **AST570** modem is turned on.
No wireless LAN connectivity. LAN LED does not light up.	Make sure the WLAN client adapter is correctly installed on your PC.
	Make sure the WLAN client adapter is configured for the appropriate SSID.
	Make sure the WLAN client adapter is authenticated via the physical or virtual *'Association'* button.
	Make sure the WLAN client adapter is configured for the correct 40-bits WEP key, in case of WEP encryption.
No wired LAN connectivity. *LAN LED does not light up.* *Ethernet port link integrity/Activity LED does not light up.*	Make sure the cable(s) are securely connected to the 10Base-T port.
	Make sure you are using the correct cable type for your Ethernet equipment.
Telnet session from a Windows PC is not possible.	The **AST570** system password is longer than 8 characters. Change the **AST570** system password.
Poor ***AST570*** *performance.*	Make sure the **AST570** is installed as instructed in this User's Guide and/or as instructed by the SP.
	For ADSL service, check whether a central splitter or dedicated filters are installed properly.
No Line synchronization achieved. *Line Sync LED keeps flashing*	Make sure ADSL service is enabled on the wall outlet your **AST570** is connecting to.
	Make sure the correct **AST570** variant is used for your DSL service.

AppendixB Wall Fixing Assembly

Introduction

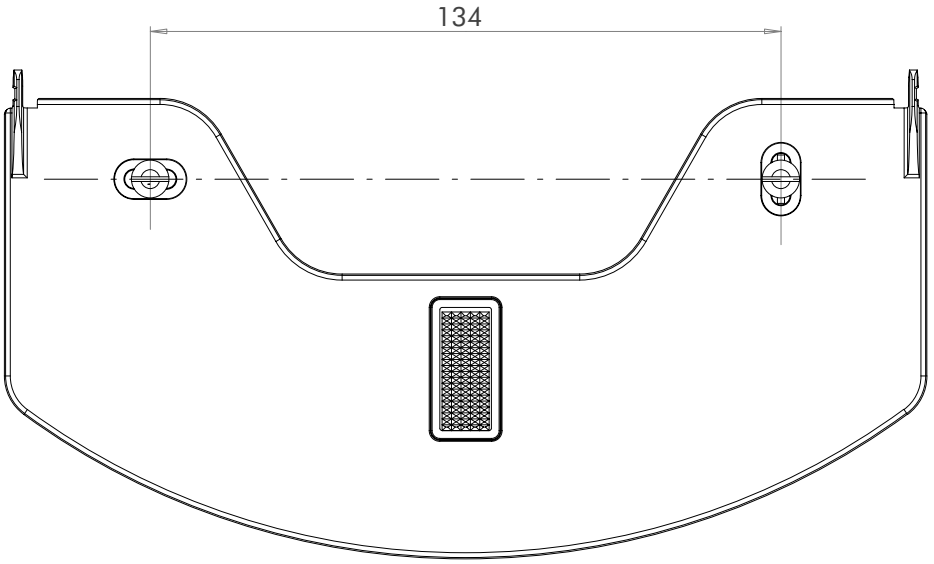
This appendix describes how to wall mount your **AST570**, with the wall fixing assembly delivered in the package.

Before you start, check for the following items:

- The wall fixing assembly
- 2 screws and 2 wall plugs
- 1 Velcro sticker.

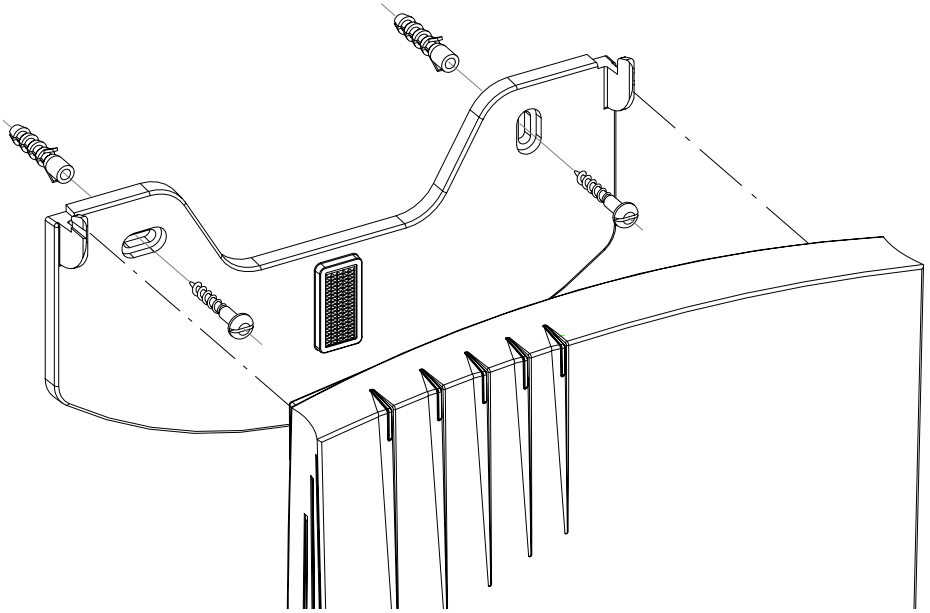
Preparing your wall fixing assembly

1. Mark two hole positions horizontal at 134 mm (5.36 inches) distance:

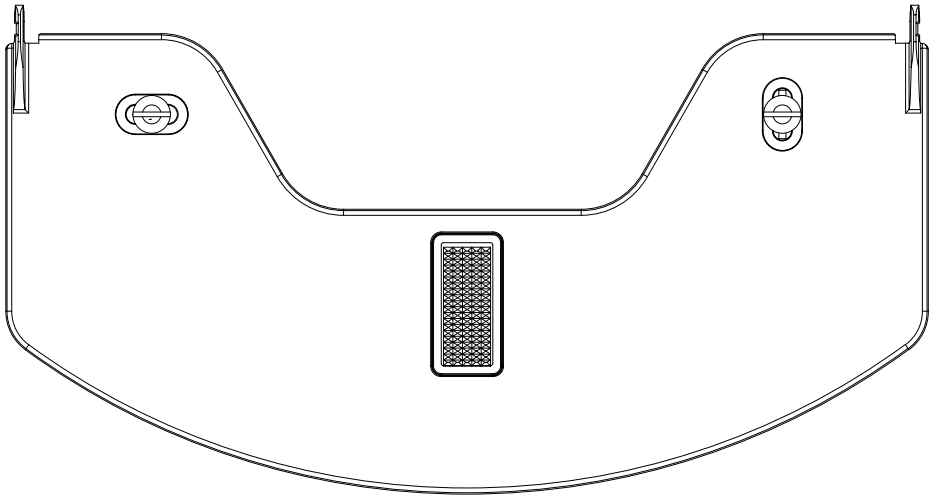


2. Drill the marked holes with a 6mm (0.24 inches) diameter drill bit to a minimum depth of 35mm (1.38 inches).

3. Insert the wall plugs in the drilled holes, position the wall fixing assembly over the holes, insert the screws in the wall plugs and tighten them firmly:



4. Place the Velcro sticker on the wall fixing assembly in the outlined area:



5. Position the **AST570** over the two hooks and pull the box down until its firmly positioned, and sticking to the Velcro.

AppendixC Speed Touch Upcoming Features

Introduction

Alcatel engineers continue to develop new features for its highly successful DSL routers. By doing so, products that server existing markets can easily withstand the demands of future markets.

The most prevalent features that will be delivered in an upcoming release are VPNs based on IPSec, Remote management and troubleshooting via SNMP and Syslog and automatic IP route distribution via RIP.

In the following a short introduction is given for each of these features and what they mean in terms of solutions.

IP VPNs based on IPSec

Ever more people and businesses rely on the Internet infrastructure for their professional and personal use. Although the Internet revolutionized communication, it exhibits an important drawback; it provides little network security.

By implementing the IP Security Protocol Suite (RFC2401, RFC2409, RFC2451 and RFC2404 to name just a few) it will be possible to create Virtual Private IP Networks on top of the public IP infrastructure. In other words, all information that is routed off your LAN will be authenticated and encrypted.

This provides a standard-based low-cost solution for home workers, tele-workers and branch offices.

Remote diagnostics and troubleshooting

An important aspect of managing a distributed network are the diagnostic capabilities of the individual network nodes.

Via the Simple Network Management Protocol (SNMP), nodes can be monitored in fine detail. In the event of failures the operator can be alerted so that the downtime is kept to a minimum.

In addition the extended logging capabilities of Syslog allow to record events which can be retrieved for later analysis and diagnosis.

This provides a standard-based low-cost solution for home workers, tele-workers and branch offices.

Automatic route processing

The existing manual and semi-automated IP route configuration methods of the **AST570** DSL router will be extended with RIPv1 and RIPv2. Routing Information Protocol (RIP) provides automatic route table construction and maintenance. In this way RIP learns the network topology to find optimal routes or select alternative routes in case of network failures.

AppendixD Speed Touch Specifications

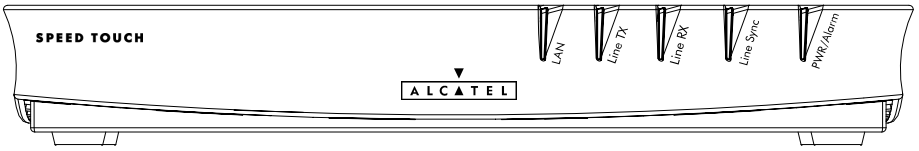
In this appendix

Topic	See
Front Panel Layout and LED Description	D.1
Power On/Off Behavior	D.2
Back Panel Layout	D.3
Connector Pin Assignments	D.4
Power Supply Adapter	D.5
LAN Cables Layout	D.6
Physical Specifications	D.7
ADSL Specifications	D.8
Wireless Specifications	D.9

D.1 Front Panel Layout and LED Description

Front panel layout

All **AST570** models have a similar front panel:



Five front panel LEDs

The **AST570** is equipped with 5 LEDs on its front panel, indicating the state of the device:

Indicator			**Description**
Name	**Color**	**State**	
LAN	Green	Flashing	Data is flowing from/to the wired and/or wireless interfaces.
		Off	No activity on the wired and wireless interfaces.
Line TX	Green	Flashing	ATM cells are being sent over the DSL line.
		Off	No transmission activity.
Line RX	Green	Flashing	ATM cells are being received via the DSL line.
		Off	No reception activity.
Line Sync	Green	Flashing	During initialization of the DSL line.
		On	DSL line synchronization achieved.
PWR/Alarm	Green	On	Power on, normal operation.
	Amber	On	Power on, start-up failed.
		Flashing	Pending WLAN client association.
	Red	Flashing	Power on, POST(*) pending.
		On	Power on, POST(*) failed.

(*) Power On Self Test (POST)

D.2 Power On/Off Behavior

Turning on/off the AST570

You can turn the **AST570** on (**I**) or off (**O**) with the power switch.

POST phases

As soon your **AST570** is turned on, you can check the "PWR/Alarm" LED (See section D.1) to see how the POST progresses.

Phase	"PWR/Alarm" LED Indication	Description
1	Flashing red	POST(*) pending
2	Solid amber	Start-up failed
	Solid red	POST(*) failed
	Solid green	Normal operation

(*) Power On Self Test (POST)

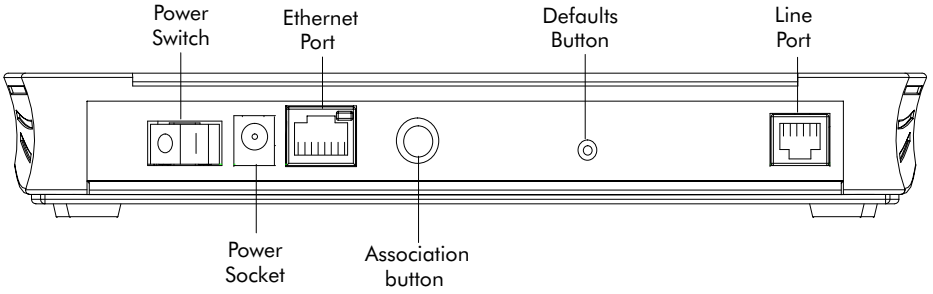
Checking link integrity of the Wired Ethernet connection

If the LAN device which is directly connected to the **AST570**' Ethernet port is powered on, the link integrity/activity LED of the port lights up green (See section D.3).

D.3 Back Panel Layout and LED description

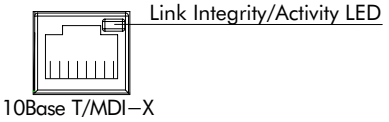
Back panel layout

The **AST570** features the following back panel:



Ethernet port LED

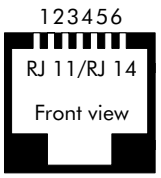
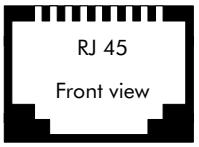
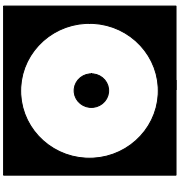
The Ethernet port on the rear panel has a LED:



Indicator			Description
Name	**Color**	**State**	
Integrity **Activity**	Green	Off	No connection on the Ethernet port.
		On	Ethernet link up. No activity on the Ethernet port.
		Flashing	Data is flowing from/to the Ethernet port.

D.4 Connector Pin Assignments

AST570 port description

Name	Port	Pin No.	Signal Name	Function	Line Port pinning
Line (DSL)		2	Wire A	Subscriber line wire A	2/5 models
		3	Wire A	Subscriber line wire A	3/4 models
		4	Wire B	Subscriber line wire B	
		5	Wire B	Subscriber line wire B	2/5 models
10Base-T MDI-X		1	R_{X+}	Receive data from DTE(*) (+)	
		2	R_{X-}	Receive data from DTE(*) (−)	
		3	T_{X+}	Transmit data to DTE(*) (+)	
		6	T_{X-}	Transmit data to DTE(*) (−)	
DC		Inner	$+9V_{DC}$	Power supply connection (+)	
		Outer	GND	Power supply connection (ground)	

(*) Data Terminal Equipment (DTE)

Free connector pins

Connector pins not mentioned are not connected.

Ports characteristics

The external ports on the back panel are classified as follows:

- **DC input port**
  SELV circuit (*)
- **10Base-T/MDI-X**
  SELV circuit
- **Line DSL port**
  TNV-3 circuit (**)

(*) Safety Electronic Low Voltage (SELV)
(**) Telecommunication Network Voltage (TNV) Category 3

D.5 Power Supply Adapter

Power adapter use

The **AST570** is equipped with one of the following pluggable power supply adapters listed in the table.

Due to the special characteristics of the output class II AC adaptor, use only the **AULT, Incorporated** types, or equivalents, listed in the table.

Power adapter models

Model Reference	**AC/DC**	**Plugtype**	**AULT, Inc. Model** (or equivalent)
US model	120V/9V	North America wall plug	P48−091000−Axxxx
UK/Sing model	230V/9V	UK wall plug	F48−091000−Axxxx
ROW(*) model	230V/9V	Euro wall plug	D48−091000−Axxxx
Australia model	240V/9V	Australia wall plug	E48−091000−Axxxx
Korea Model	220V/9V	Korea wall plug	Q48−091000−Axxxx

(*) Rest Of the World (ROW)

Output specifications

The supplied adapter has the following output specifications:

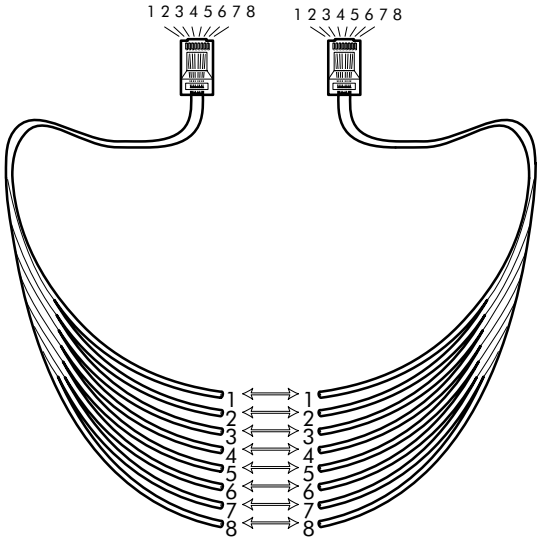
- $9V_{DC}$/1A unregulated output voltage
- Maximum 860 mV_{eff} ripple voltage
- Maximum 1A output current
- Limited power source (according to IEC/EN 60950, sub-clause 2.11 and UL1950).

Note: Do not use power adapter types with other specifications (e.g. from other Alcatel Speed Touch™ products) !

D.6 LAN Cables Layout

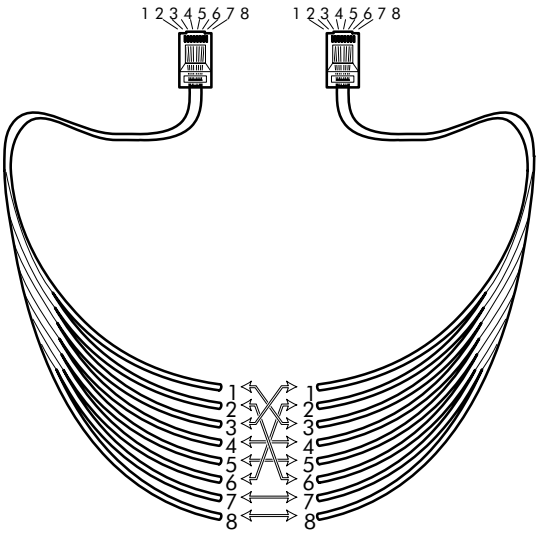
Straight-through LAN cable

Straight-through LAN cables with the following layout are applicable for interconnecting Ethernet ports:



Crossover LAN cable

Crossover LAN cables with the following layout are applicable for interconnecting Ethernet ports:



D.7 Physical Specifications

Physical dimensions

210mm W x 185mm D x 35mm H

Operating environment

Temperature: 5°C to 40°C (40F to 105F)

Humidity: 20% to 80%

Power requirements

AC voltage: 100 to 120 V_{AC}, 220 to 240 V_{AC}

DC voltage: 9V/1A

Frequency: 50/60 Hz

Power consumption: $7W_{max}$

Wireless antennas

The **AST570** is equipped with two omnidirectional Radio Frequency (RF) antennas compliant to the IEEE802.11b standard.

The long-term characteristics or the possible physiological effects of radio frequency electromagnetic fields associated with this equipment have not been evaluated.

D.8 ADSL Specifications

ADSL router specifications

- **ADSL data rates**
  - Downstream user (payload) data rates:
    Up to 8Mbit/s, depending on provisioning
  - Upstream user (payload) data rates:
    Up to 1Mbit/s, depending on provisioning
- **ADSL standards compliancy**
  - ITU(*) G.DMT (Full rate ITU G.992.1 Annex A)
  - ITU G.Lite (Lite rate ITU G.992.2)
  - Full rate ANSI T1.413 Issue 2
  - ITU G.Handshake (Automode ITU G.994.1)

(*) International Telecommunication Union (ITU)

D.9 Wireless Specifications

WLAN Access Point specifications

- Compliant to IEEE802.11b high rate wireless specification at 11Mb/s
- Two omnidirectional antennas with diversity support for maximum operating range and throughput
- Dynamic rate switching at 11, 5.5, 2 and 1 Mb/s
- DSSS channel number range:
  - 1 (2.412GHz)
  - 2 (2.417GHz)
  - 3 (2.422GHz)
  - 4 (2.427GHz)
  - 5 (2.432GHz)
  - 6 (2.437GHz)
  - 7 (2.442GHz)
  - 8 (2.447GHz)
  - 9 (2.452GHz)
  - 10 (2.457GHz)
  - **11 (2.462GHz) default**
  - 12 (2.467GHz)
  - 13 (2.472GHz)
- Typical indoor coverage : 60meter
- Supports all WECA Wi-Fi™ certified WLAN client adapters
- Ensures wireless connectivity for IEEE802.11b DSSS compliant WLAN client adapters
- WLAN client adapter MAC address based authorization filtering and association control
- 40-bits Wired Equivalent Privacy algorithm for optimal Wireless connection security and privacy

AppendixE Speed Touch Default Assignments

In this chapter

Topic	See
General Defaults	E.1
Connection Service/ATM Encapsulation Defaults	E.2

E.1 General Defaults

AST570 Wireless SSID	AlcatelXXXXXX (where XXXXXX is a placeholder for the last 6 characters of the **AST570**' WLAN access point MAC address.
AST570 DSSS channel number	11
AST570 Wireless security settings	WEP encryption = OFF Association Control = ON
AST570 IP address	10.0.0.138
AST570 DNS name	SpeedTouch
AST570 domain name	lan
AST570 DNS server	Active
AST570 DHCP server	AutoDHCP
AST570 Firewall	On (default settings)
AST570 System password	Not set

E.2 Connection Service/ATM Encapsulation Defaults

(W)LAN interfaces

VPI	VCI	Upper Layer Protocols	Service channel
0/8	35	**ETHoA** AAL5/RFC1483/Bridged RFC1483 LLC/SNAP for Bridged PDUs (FCS not preserved)	Transparent Bridging
0/8	36		Routed Ethernet
0/8	37		Bridged PPPoE
0/8	38		Routed PPPoE
0/8	48	**PPPoA** AAL5/RFC2364 RFC2364 VC-MUX for PPP PDUs	Relayed PPPoA
0/8	49		Routed PPPoA
0/8	50		
0/8	51		
0/8	64		
0/8	65		
0/8	66		
0/8	67		
0/8	80	**IPoA** AAL5/RFC1483/Routed RFC1577/RFC2225–RFC1483 LLC/SNAP for Routed non-ISO PDUs	Classical IP & IP routing
0/8	81		
0/8	82		
0/8	83		

Control channels

VPI	VCI	Upper Layer Protocols	Service channel
0	21	–	DSL/ATM Loopback channel
1	21		
15	16	AAL5/SNMP	SNMP/ASAM agent communication channel for Alcatel ASAM
15	64	AAL5/TFTP	Software TFTP download channel

AppendixF Safety and Agency Regulatory Notices

Aim of this appendix

This appendix provides basic Safety Information on Alcatel's **Speed Touch**™ product.

Prior to using the **Speed Touch**™ product, read this appendix carefully.

Reading all instructions

Follow all warnings and instructions marked on the product.

In this appendix

This chapter covers the following topics:

Topic	See
Safety Instructions	F.1
European Declaration of Conformity	F.2
Radio Frequency Interference Statement	F.3
Canadian Class B Notice	F.4

STORE THESE INSTRUCTIONS CAREFULLY

F.1 Safety Instructions

Climatic conditions

The **Speed Touch**™ product equipment is intended for:

- In-house stationary desktop use; the maximum ambient temperature may not exceed 40°C (104°F).
- It must not be mounted in a location exposed to direct or excessive solar and/or heat radiation.
- It must not be exposed to heat trap conditions and must not be subjected to water or condensation.
- It must be installed in a Pollution Degree 2 environment.

Cleaning

Unplug this product from the wall outlet before cleaning. Do not use liquid cleaners or aerosol cleaners. Use a damp cloth for cleaning.

Water and moisture

Do not use this product near water, for example, near a bathtub, wash bowl, kitchen sink, laundry tub, in a wet basement or near a swimming pool.

Power supply adapter

The **Speed Touch**™ product comes with a portable power supply adapter.

Due to the special characteristics of the output of the class II AC adaptor, only use the models or equivalent listed in the power adapter table in this User's Guide.

Power sources

The powering of this product must adhere to the power specifications indicated on the marking labels. If you are insure of the type of power supply to your home, consult your product dealer or local power company.

The mains socket outlet must be close to the equipment and easily accessible.

The **Speed Touch**™ product equipment is not intended to be connected to an IT-type power system.

Power cord protection

Do not allow anything to rest on the power cord. Do not locate this product where the cord will be subject to persons walking on it.

Overloading

Do not overload wall (mains) outlets and extension cords as this increases the risk of fire or electric shock.

Servicing

To reduce the risk of electric shock, do not disassemble this product. None of its internal parts are user-replaceable; therefore, there is no reason to access the interior. Opening or removing covers may expose you to dangerous voltages. Incorrect reassembly could cause electric shock if the appliance is subsequently used.

If service or repair work is required, take it to a qualified service dealer.

Wireless RF antennas

The long-term characteristics or the possible physiological effects of radio frequency electromagnetic fields associated with this equipment have not been evaluated.

Damage requiring service

Unplug this product from the wall outlet and refer servicing to qualified service personnel under the following conditions:

- When the power supply cord or plug is damaged or frayed.
- If liquid has been spilled into the product.
- If the product has been exposed to rain or water.
- If the product does not operate normally.
- If the product has been dropped or damaged in any way.
- If the product exhibits a distinct change in performance.

Modem/Telephone use

Avoid using a modem/telephone (other than a cordless type) during an electric storm. There is a slight risk of electric shock caused by lightning.

Do not use the telephone to report a gas leak in the vicinity of the leak.

If telephone service is required on the same line, a central splitter, or distributed filter(s) must be installed for optimal DSL performance.

Depending on your DSL configuration and type of splitter/filters, installation must be carried out by qualified service personnel.

Consult your telephone service company or DSL service provider for instructions.

Modifications

Changes or modifications not expressly approved by Alcatel could invalidate the users authority to operate this equipment.

STORE THESE INSTRUCTIONS CAREFULLY

F.2 European Community Declaration of Conformity

CE

Products with the CE marking comply with both EMC and Low Voltage Directives issued by the Commission of the European Community.

EC Declaration of Conformity

A copy of the European Community Declaration of Conformity is provided in your **Speed Touch**™ product shipping box.

F.3 Radio Frequency Interference Statement

This device has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against such interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy. If not installed and used in accordance with the instructions, it may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment ON and OFF, the user is encouraged to try correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/television technician for help.

This equipment complies with Part 68 of the FCC Rules. On the back of this equipment is a label that contains, among other information, the FCC certification number (FCC ID) and Ringer Equivalence Number (REN) for this equipment. If requested, this information must be provided to the telephone company.

An FCC compliant telephone cord and modular plug is provided with this equipment. This equipment is designed to be connected to the telephone network or premises wiring using a compatible modular jack that is Part 68 compliant.

The Ringer Equivalence Number (REN) is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in the devices not ringing in response to an incoming call. Typically, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line (as determined by the total RENs) contact the local telephone company.

If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the telephone company will notify the customer as soon as possible. Also you will be advised of your right to file a compliant with the FCC if you believe it is necessary.

The telephone company may make changes to its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens the telephone company will provide advance notice so you can make the necessary modifications to maintain uninterrupted service.

If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved. Connection to party lines is subject to state tariffs (contact the state public utility commission, public service commission or corporation commission for information).

No repairs can be performed by the customer, if you experience trouble with this equipment for repair or warranty information, please contact: (919) 850−1231 for locations in North America.

F.4 Canadian DOC Class B Notice

Notification of Canadian RF Interference Statements

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus as set out in the radio interference regulations of the Canadian Department of Communication.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicable aux appareils numérique de classe B prescrites dans le règlement sur le brouillage radioélectrique édicté par le Ministère des Communications du Canada.