

SPEED TOUCH

WIRELESS

User Manual



Status Released

Change Note BD F aa –PreRL

Short Title CD–UG STWire R1.0

All rights reserved. Passing on and copying of this document, use and communication of its contents not permitted without written authorization from Alcatel.

Contents

1	Speed Touch Wireless Quick Guide	13
1.1	Get Acquainted with your Speed Touch Wireless	14
1.2	Speed Touch Wireless Installation	16
1.2.1	What you Need	17
1.2.2	STWireless Connections	18
1.2.3	Check your Service Provider's Offering	21
1.2.4	Select an STWireless Packet Service	22
1.2.5	Configure your STWireless (If Necessary)	23
1.2.6	Surf the Internet	24
1.2.7	Detailed STWireless Information	25
2	Wiring Guide – ADSL, Power and Console	29
2.1	Locating Ports	30
2.2	Connecting the ADSL Port	31
2.3	Connecting the Power Adapter	32
2.4	Connecting the Serial Port (Optional)	33
3	Wiring Guide – Network Connections	35
3.1	Connecting Wireless LAN	36
3.2	LAN Cables	39
3.3	Connecting Wired Ethernet (Optionally)	40
3.3.1	The Ethernet Port on your STWireless	41
3.3.2	Wired Single PC Connection	42
3.3.3	Wired Ethernet LAN	43
3.4	Wired Ethernet vs. WLAN Connectivity	44
4	Data Services – Packet Services	47
4.1	Supported Packet Services	48
4.2	Packet Services at a Glance	49
4.3	Internet & Corporate Intranet Access vs. LAN-to-LAN Interconnection ..	52
4.4	Direct Networking vs. Dial-up Networking	53
4.5	ADSL Modem vs. ADSL Gateway	55
4.5.1	ADSL Modem Model	56
4.5.2	ADSL Gateway Model	57
5	Data Services – Transparent Bridging	59
5.1	Preparatory Steps	60
5.2	Using Bridging	62
5.3	Bridging Configuration	63
5.3.1	Bridging Phonebook Entries	64

5.3.2	Bridging Entries	65
5.4	Advanced Bridging Concepts	69
5.4.1	STWireless Bridge Operation	70
5.4.2	STWireless 'Bridge Data' Web Page	73
6	Data Services – MAC Encapsulated Routing	75
6.1	Preparatory Steps	76
6.2	Using MER	77
6.3	MER Configuration	78
6.3.1	MER Phonebook Entries	79
6.3.2	MER Entries	80
6.4	Advanced MER Concepts	86
7	Data Services – PPPoA-to-PPTP Relaying	89
7.1	Preparatory Steps	90
7.2	Configuring and Using a PPTP Connection	92
7.2.1	Preparing your PC for PPPoA/PPTP	93
7.2.2	Using PPTP towards your STWireless	94
7.3	Example : MS Windows 98 Dial-Up Networking	95
7.3.1	Create a New Dial-Up Networking Icon	96
7.3.2	Create a Shortcut on your Desktop (Optional)	99
7.3.3	Open a PPPoA/PPTP Dial-Up Session	100
7.3.4	Close a PPPoA/PPTP Dial-Up Session in Use	102
7.4	PPPoA/PPTP Configuration	103
7.4.1	PPPoA/PPTP Phonebook Entries	104
7.4.2	PPPoA/PPTP Active Connections	105
7.5	Customizing PPPoA/PPTP Connections	108
7.5.1	PPPoA/PPTP Phonebook Entries	109
7.5.2	Single Destination	110
7.5.3	Multiple Destinations	111
7.5.4	Restrictions on Using Specific Virtual Channels	115
7.5.5	PPTP Profiles	116
7.6	Advanced PPPoA/PPTP Concepts	117
7.6.1	Point-to-Point Tunneling	118
7.6.2	Local Tunneling	119
7.6.3	PPPoA-to-PPTP Relaying (PPPoA/PPTP)	120
7.6.4	Simultaneous PPPoA/PPTP Sessions	121
8	Data Services – PPP & IP Routing	123
8.1	Preparatory Steps	124
8.2	Using PPP & IP Routing	125
8.3	PPP Configuration	127
8.3.1	PPP Phonebook Entries	128
8.3.2	PPP Entries	129

8.4	PPP Entry Configuration	133
8.4.1	The PPP Configuration Web Page	134
8.4.2	Link Related Configuration	135
8.4.3	Security Related Configurations	136
8.4.4	IP Routing Related Configurations	137
8.4.5	Connection Related Configuration	141
8.4.6	NAPT and PPP & IP Routing	144
8.4.7	NAPT and STWireless Transparency	145
9	Data Services – Classical IP & IP Routing	149
9.1	Preparatory Steps	150
9.2	CIP Configuration for a LIS	151
9.2.1	General CIP Configuration Procedure	152
9.2.2	Retrieving LIS Parameters	153
9.2.3	Implicit Assignment Mechanism	154
9.2.4	Explicit Assignment Mechanism	155
9.2.5	Configuring the STWireless for CIP	156
9.2.6	Adding Appropriate Routes to the Routing Tables	157
9.2.7	Example Configuration	159
9.3	Using CIP & IP Routing	161
9.4	CIP Configuration	162
9.4.1	CIP Phonebook Entries	163
9.4.2	CIP Entries	164
9.5	Advanced CIP Configurations	170
9.5.1	Configuring Multiple CIP PVCs	171
9.5.2	Creating Multiple CIP Members.	173
10	Networking Services – ATM	177
10.1	The ATM Packet Switching Technology	178
10.1.1	ATM Parameters	179
10.1.2	ATM and the STWireless	180
10.1.3	ATM and Interfaces	181
10.2	The Speed Touch Wireless Phonebook	182
10.2.1	The STWireless 'Phonebook' Web Page	183
10.2.2	Using the Phonebook	187
10.2.3	AutoPVC and the Phonebook	190
11	Networking Services – IP	193
11.1	General IP Information	194
11.1.1	IP Addresses and Subnet Masks	195
11.1.2	Private vs. Public Addresses	197
11.1.3	Choosing an IP Address	199
11.1.4	Dynamic IP Address Configuration: DHCP	201
11.2	Packet Services and IP Addressing	202
11.2.1	Transparent Bridging and IP Addresses	203

11.2.2	MER and IP Addresses	205
11.2.3	PPPoA-to-PPTP Relaying and IP Addresses	206
11.2.4	PPP & IP Routing and IP Addresses	207
11.3	Speed Touch Wireless and IP Addressing	208
11.3.1	STWireless IP Address Types	209
11.3.2	Static IP Address Configuration	211
11.3.3	Dynamic IP Address Configuration: DHCP	214
11.3.4	Configuring the STWireless DHCP Server	218
11.4	IP Routing	222
11.4.1	The STWireless IP Router	223
11.4.2	Configuring the STWireless IP Routing Table	225
12	Networking Services – DNS	229
12.1	Speed Touch Wireless DNS Resolving	230
12.2	Configuring the Speed Touch Wireless DNS Server	233
13	Networking Services – Firewalling	235
13.1	Operation of the Firewall	236
13.2	Firewall Model	237
13.3	Firewall Actions	239
13.4	Firewall Criteria	240
13.5	Firewalling and NAT	242
13.6	Firewall Configuration	243
13.7	Firewall Configuration Examples	244
14	Wireless LAN Services – WLAN Configuration	249
15	Maintenance – Software Upgrade	255
15.1	Upload Software from a PC	256
15.2	Software Download	261
16	Maintenance – Speed Touch Wireless Security	263
17	Maintenance – Lost Speed Touch Wireless	267
17.1	Ping-of-Life	268
17.2	Speed Touch Wireless Reset	271
17.2.1	Browse-to-Defaults	272
17.2.2	Ping-to-Defaults	273
17.2.3	Switch-to-Defaults	274
18	Maintenance – Speed Touch Wireless Web Interface	275
18.1	Web Interface Preconditions	276
18.1.1	Disabling Proxy Servers	277
18.1.2	Disabling Proxying for Local IP Addresses	278
18.2	Browsing to the Web Pages	279

18.3	Web Page Structure	281
19	Maintenance – Speed Touch Wireless Command Line Interface	285
19.1	CLI via the Web Pages	286
19.2	Native CLI Access	289
19.2.1	CLI through a Telnet Session	290
19.2.2	CLI via Serial Access	294
19.2.3	CLI Command Basics	295
	Abbreviations	299
AppendixA	Troubleshooting	301
AppendixB	ADSL Connectivity	303
AppendixC	Microsoft Dial-Up Networking	311
AppendixD	STWireless Layout and Behaviour	331
AppendixE	STWireless Original Settings	335
AppendixF	Hardware Reference	345
AppendixG	Wall Fixing Assembly	353
AppendixH	Safety and Agency Regulatory Notices	355

Welcome to the Speed Touch Wireless



Welcome to the Alcatel **Speed Touch™ Wireless** Asymmetric Digital Subscriber Line (ADSL) router.

With the Alcatel **Speed Touch™ Wireless** ADSL router, surfing the Internet, downloading files and interconnecting computer networks become a whole new experience.

With download speeds up to 8 Mega bits per seconds (Mbps) the **Speed Touch™ Wireless** is around 200 times faster than present day modems. This superior Alcatel ADSL technology outperforms all similar products on the market.

Your **Speed Touch™ Wireless** provides the brand-new Wireless LAN (WLAN) technology. With **Speed Touch™ Wireless's** WLAN solution, users can access other members of your (W)LAN, and surf the Internet, without using any wire to connect.

Users are not bound to a fixed location in the building anymore, and enlarging the network can happen without the need of expensive wiring installation.

Next to the ADSL router part, for the management of your wired and/or Wireless Ethernet environment, your **Speed Touch™ Wireless** features also a complete toolbox for excellent Local Area Network (LAN) performance. Among others the most important are a DNS server, a DHCP server, IP Routing. 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.

Safety instructions Prior to connecting the **Speed Touch™ Wireless**, read the Safety Instructions in appendix H.



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.
-

Terminology For readability, the **Speed Touch™ Wireless** will be referred to as **STWireless** further in this User Manual.

Service Provider For readability, Service Provider (SP) will refer to all instances, responsible for your ADSL connections, i.e. ADSL Service Provider (ASP), Internet Service Provider (ISP), Corporate, etc.

**PC, workstation,
terminal, ...**

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

LAN, network, WLAN

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

Disclaimer

All examples throughout this document refer to :

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

However, your SP might prefer other values.

User Manual updates

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

For more information on the newest technological breakdowns and documents, please consult our Alcatel web site at:

<http://www.alcatel.com>

<http://www.alcateldsl.com>

1 Speed Touch Wireless Quick Guide

Aim of this Quick Guide Use this chapter to quickly connect your **STWireless** to the Internet.

In this chapter

Topic	See
Get Acquainted with your STWireless	1.1
STWireless Installation	1.2

1.1 Get Acquainted with your Speed Touch Wireless

- Delivery check** Check your **STWireless** package for the following items:
- ▶ The **Speed Touch™ Wireless**
 - ▶ 1 Power supply adapter with 2m (6.56ft.) connecting cable
 - ▶ 2m Ethernet/ATMF straight-through cable (RJ45/RJ45)
 - ▶ 2m ADSL cable (RJ11/RJ11, RJ14/RJ14)
 - ▶ 1 Wall mounting assembly
 - ▶ 1 Velcro sticker for the wall mounting assembly
 - ▶ 2 Screws and 2 wall plug for the wall mounting assembly
 - ▶ This User Manual, either in hard copy format, or on CD-rom.
-

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

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

Your STWireless Your **STWireless** ADSL router is presented in a slim line box:



For a detailed information and a LED description, refer to Appendix D.

POTS vs. ISDN Ensure you have the correct **STWireless**:

- ▶ A POTS **STWireless**, connecting to an analog POTS line
- ▶ An ISDN **STWireless**, connecting to a digital ISDN line.

See the marking label to identify your **STWireless**.

To avoid damage to your equipment, use only the appropriate **STWireless**.

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

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

1.2 Speed Touch Wireless Installation

Aim of this section Execute the steps in this section and in no-time you are on the Internet.

In this section

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

1.2.1 What you Need

ADSL and telephone service ADSL service must be enabled on your telephone line. You need a central splitter, or distributed filters for decoupling ADSL, and telephone signals. For more information, refer to Appendix B.

Wireless LAN For wireless LAN connectivity:

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

Each WLAN client adapter must be:

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

Ethernet port To use the 10Base-T 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 (if needed), and the necessary connection cables.

Accessing the STWireless For local configuration via HTTP/HTML, you need:

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

For native Command Line Interface (CLI) you need:

- ▶ A serial cable
- ▶ An ASCII terminal (VT100), or a PC with ASCII terminal emulation.

1.2.2 STWireless Connections

- You must connect**
- ▶ The ADSL Port (Line)
 - ▶ The Power Port (DC).

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

- ▶ Your WLAN clients
- ▶ Optionally the Ethernet Port (10Base-T)

ADSL port (Line) Use the included ADSL cable to wire the **STWireless**'s Line port to your ADSL wall outlet.

Refer to section 2.2 for more information.

Power port (DC) Only use the included power adapter to source your **STWireless**. The **STWireless** should be operated only from the type of power source, indicated on its marking label.

Refer to section 2.3 for more information.

If you are not sure of the regional power conditions, check the adapter's specifications in section F.3, and your local power company.

Turn on your STWireless Use the power switch on the **STWireless** back panel to turn on your **STWireless**.

Refer to section D.3 for more information.

Connecting WLAN clients**► Preconditions:**

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

The (portable) PCs, intended to be connected to the **STWireless**, must have a WLAN adapter readily installed, and must be configured as DHCP client.

► Joining the STWireless WLAN network

As soon as the WLAN adapter detected the presence of the **STWireless** WLAN network, you must push the 'WLAN' button on the **STWireless**'s back panel to allow the WLAN adapter to join the **STWireless** WLAN network.

Repeat this procedure for each (portable) PC you want to join the **STWireless** WLAN network.

Refer to section 3.1 for more information.

Optionally Ethernet port (10Base-T)

Next to the WLAN clients, a 10Base-T Ethernet port on the back panel of the **STWireless** allows wired Ethernet connectivity.

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

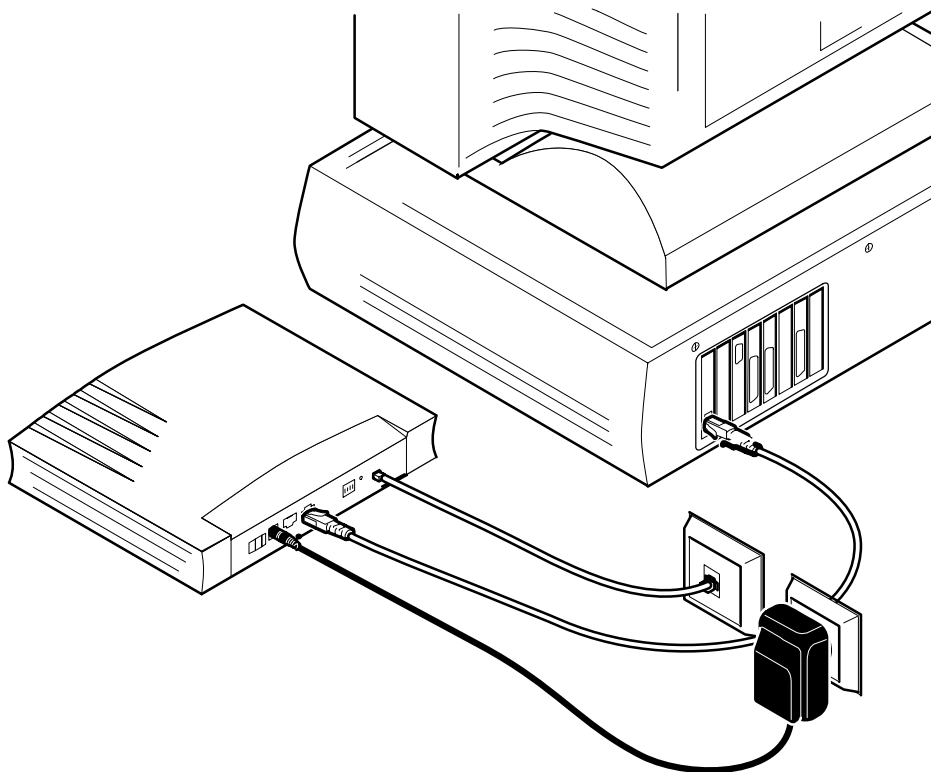
Refer to section 3.3 for more information.

Note There is no difference between wired Ethernet and WLAN connections for the **STWireless**, i.e. all network configurations are equally valid for both.

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

Refer to section 3.3 for more information.

Check your wiring After you finished wiring the **STWireless**, the result should resemble the following figure:



Note: WLAN client PCs are not shown in the above figure.

1.2.3 Check your Service Provider's Offering

- Service offering** The SP provides at least the following information:
- ▶ The *Virtual Channel Identifier*, that is, the **VPI/VCI** value of the VC to use on the ADSL line
 - ▶ The **Connection Service** supported on this VC

Example: VPI/VCI = 0/35; Connection Service = PPPoE

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

- Default STWireless 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 **STWireless** defaults, you can change VC settings via the **STWireless** web pages.
- See section 10.2 for more information.
-

1.2.4 Select an STWireless 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	Packet Service
ETHoA (RFC1483 Bridging)	IEEE 802.1D Transparent Bridging
	MAC Encapsulated Routing
PPPoE (implies RFC1483 Bridging)	IEEE 802.1D Transparent Bridging (*)
PPPoA (RFC2364 PPPoA)	PPPoA-to-PPTP Relaying
	PPP & IP Routing
	PPP-to-DHCP Spoofing
CIP (RFC1483 Routing/RFC1577)	CIP & IP Routing

(*) A PPPoE Client application must also be installed on your PC.

Selection criteria Criteria to prefer one Packet Service over the other for a given Connection Service are enumerated below.

▶ **ETHERnet over ATM (ETHoA)**

If your application relies on protocols other than TCP/IP, e.g. IPX/SPX, or PPPoE to name a few, select the **bridge**.

Select **MER** if multiple users want to share the Internet connection.

▶ **PPP over ATM (PPPoA)**

If your application relies on protocols other than TCP/IP, e.g. IPX/SPX, or NETBEUI, or if you want to avoid NAPT, select the **PPPoA-to-PPTP Relay**.

If PPTP Tunneling is not supported by your PC's OS, and if you want to avoid NAPT, select **PPP-to-DHCP Spoofing**.

For all other cases use **PPP & IP Routing**. This allows you to share the IP address obtained via PPP by the users on your (W)LAN.

▶ **Classical IP (CIP)**

In some special circumstances, advanced user can use the **CIP & IP routing** Packet Service.

1.2.5 Configure your STWireless (If Necessary)

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

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

- ▶ Its web pages (See chapter 18)
- ▶ A Telnet CLI session (See subsection 19.2.1)
- ▶ A Serial CLI session (See section 19.2.2).

STWireless Configuration Configure the **STWireless** via its web pages.

All packet services, the **STWireless** 's local networking tools, i.e. DHCP server, DNS server and IP router, and system setup tools, have their own web page.

Context related Help web pages provide detailed information.

For profound configurations the Command Line Interface (CLI) is provided.

1.2.6 Surf the Internet

Finishing setup After wiring (and optionally configuring) your **STWireless**, you are ready to surf the Internet.

Access Types Depending on the used packet service(s), you can have:

- ▶ Always-On Access
 - ▶ Dial-Up Access.
-

Always-on access With Bridging, MER and CIP, no connection procedure is needed. Make sure your **STWireless** is turned on, open your PC's web browser and you are online, i.e. you are Always-on connected.

Note: Although no connection procedure is needed, in some cases the SP expects authentication before granting complete access to the remote side's resources.

Dial-up access The **STWireless** features also the traditional Dial-in connectivity. Now you can manually make a connection to the remote side, either via the **STWireless**'s web pages, in the case of PPP & IP Routing, or via Operating System (OS) dependent Dial-in applications, e.g. Microsoft's Dial-Up Networking, or a PPPoE session client application.

Note: During the connectioning procedure you will have to authenticate yourself, via a User Name and Password.

1.2.7 Detailed STWireless Information

The STWireless is more than “just” an ADSL router

Use the following parts (marked grey) of this manual to explore STWireless’s advanced features:

Speed Touch™Wireless Quick Guide	1
Speed Touch™Wireless Wiring Guide	
ADSL, Power and Console	2
Network Connections	3
Speed Touch™Wireless Data Services	
Packet Services	4
Transparent Bridging	5
MAC Encapsulated Routing	6
PPP-to-PPTP Relaying	7
PPP & IP Routing	8
Classical IP & IP Routing	9
Speed Touch™Wireless Networking Services	
ATM	10
IP	11
DNS	12
Firewalling	13
Speed Touch™Wireless Wireless LAN Services	
WLAN Configuration	14
Speed Touch™Wireless Maintenance	
Software Upgrade	15
Speed Touch™Wireless Security	16
Lost Speed Touch™Wireless	17
Speed Touch™Wireless Web Interface	18
Speed Touch™Wireless CLI	19
Speed Touch™Wireless Appendices	

Speed Touch™ Wireless

Wiring Guide

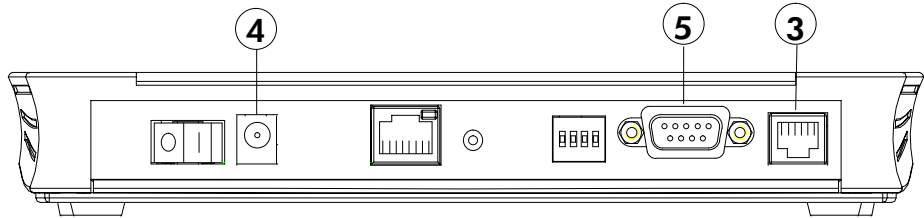
2 Wiring Guide – ADSL, Power and Console

In this chapter

Topic	See
Locating Ports	2.1
Connecting the ADSL Port	2.2
Connecting the Power Adapter	2.3
Connecting the Serial Port (Optional)	2.4

2.1 Locating Ports

Port description



Following ports are used:

- ▶ ③: ADSL line port, marked "LINE"
- ▶ ④: Power socket, market "DC"
- ▶ ⑤: Serial port, marked "Console".

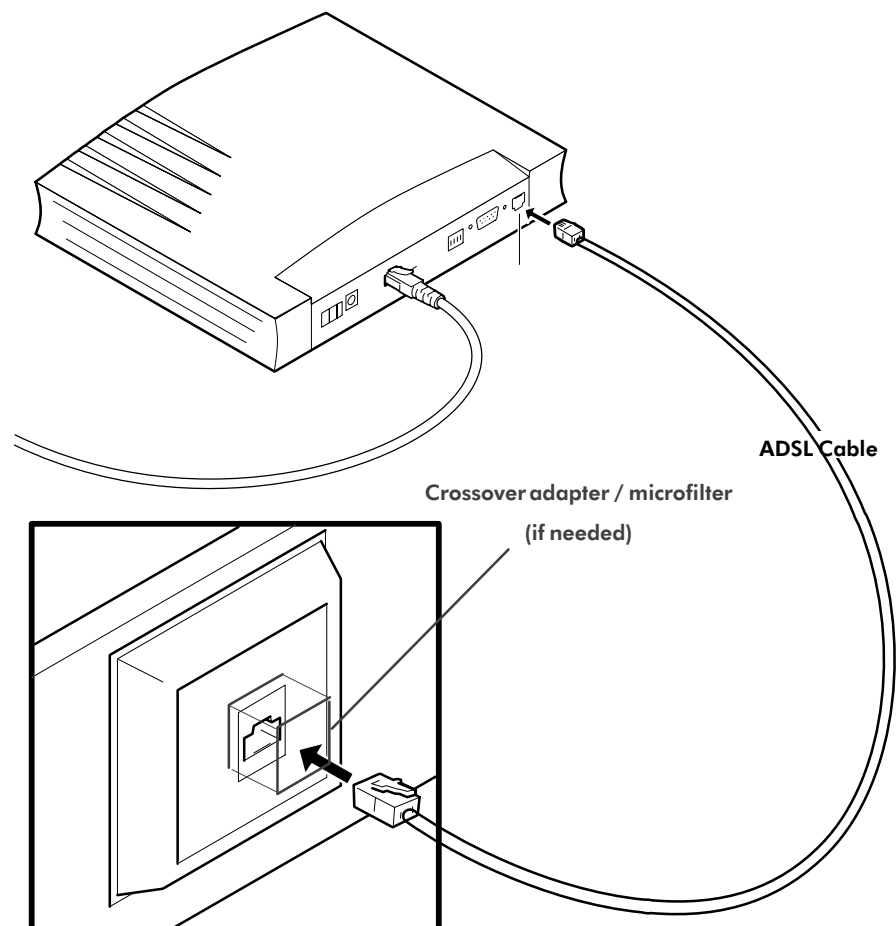
2.2 Connecting the ADSL Port

Important information Read appendix B before you connect the **STWireless**.

Preconditions prior to connecting A **central splitter**, or **distributed filters** for decoupling ADSL and POTS, or ISDN signals must be installed. Crossover adapters might be required.

See appendix B for more information.

Procedure Proceed as indicated in the following figure to connect the **STWireless** to the ADSL line, using the included black ADSL cable:

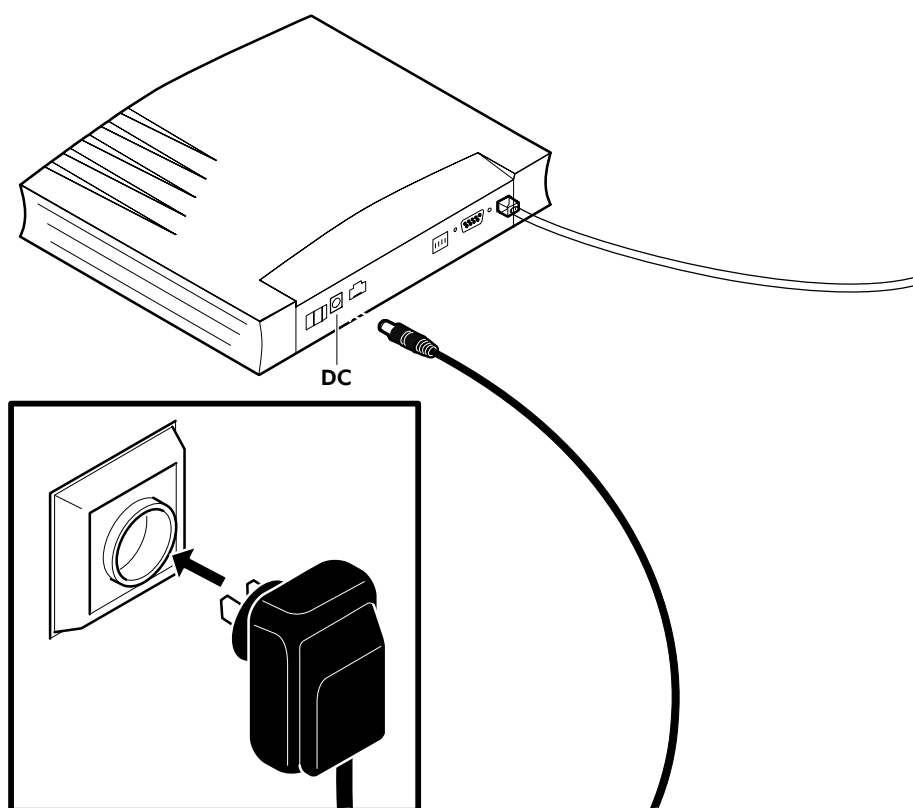


2.3 Connecting the Power Adapter

Introduction The **STWireless** 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 **STWireless** package is compatible with your local electrical power specifications. See section F.3 for connector layout and output specifications. If you are unsure 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 :



2.4 Connecting the Serial Port (Optional)

Serial access Like most routers, the **STWireless** carries a serial port on its rear panel, featuring access from a remote host via a modem connection, or local access from a terminal.

Requirements for using the serial access

For access via the serial port, you must have the following:

- ▶ A serial cable
- ▶ An ASCII terminal (VT100), or a workstation/PC with ASCII terminal emulation, or emulation application, for local configuration via the CLI,

or

- ▶ A (voiceband) modem, for allowing remote configuration of the **STWireless** via the CLI.

Procedure Proceed as follows to connect the **STWireless** serial port:

Step	Action
1	Determine the serial port on the rear panel of your STWireless .
2	Connect the serial cable to the STWireless serial port.
3	Connect the other end of the serial cable to the serial interface of the (emulated) ASCII terminal, or modem.

3 Wiring Guide – Network Connections

In this chapter

Topic	See
Connecting Wireless LAN	3.1
LAN Cables	3.2
Connecting Wired Ethernet (Optional)	3.3
Wired Ethernet vs. WLAN Connectivity	3.4

3.1 Connecting Wireless LAN

Introduction Next to the single Ethernet port, enabling wired LAN connectivity, the **STWireless** contains a Wireless LAN (WLAN) hub.

This WLAN hub allows wireless connection of several devices 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 LAN environment.

- In this section**
- ▶ Wireless LAN Basics
 - ▶ Wireless LAN Requirements
 - ▶ Connecting WLAN Clients
 - ▶ Configuration of your WLAN Environment.
-

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

In most cases, the WLAN client will automatically recognize the presence of WLAN networks, and their SSID. It is up to the WLAN hub's policy whether the client is accepted to join the WLAN network, or not. This is particularly interesting in case several independent WLAN hubs (e.g. two **STWireless**s of different "workgroups") are co-located.

The IEEE802.11b standard for WLANs allows for several WLAN systems to be co-located, without sharing the bandwidth. Several channels are available for use which are associated to a slightly different frequency in the allowed range. The **STWireless** supports operation on all allowed channels.

WLAN client requirements

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

It is advisable that the WLAN client adapter is WECA Wi-Fi™ certified to ensure smooth interoperability.

Connecting WLAN clients

Before you start connecting the WLAN clients, make sure your **STWireless** is powered on and finished its POST.

Proceed as follows:

Step	Action
1	Install the WLAN Client adapter (WLAN-NIC, or WLAN PCMCIA card) in your (portable) PC, according the WLAN client adapter's user manual.
3	For initial connectivity it is recommended to configure your (portable) PC as DHCP client.
2	In most cases the WLAN client adapter cards automatically detect the presence of WLAN networks (that is why the STWireless must be powered up first). The STWireless WLAN's initial SSID is configured as 'Alcatel_STW'. In case your WLAN adapter does not find this network, you may configure it manually, or perform a rescan of the radio environment.
3	Let your WLAN adapter try to join the STWireless's WLAN.
4	Use a pencil to push the <i>Wireless LAN Authentication button</i> , marked "WLAN" on the rear panel of your STWireless . This allows the STWireless to authenticate the WLAN client. Note: In fact this step allows your WLAN to be secure: without the physical authentication, i.e. pushing the WLAN Authentication button, while your WLAN client tries to join your WLAN, no connectivity will be enabled between the WLAN client and the STWireless WLAN.

Result After performing the last step of the procedure, you should be able to contact the **STWireless**, e.g. pinging 10.0.0.138, or open the **STWireless** web pages. See chapter 18 for more information.

Configuration of your WLAN environment

As soon you have connectivity with the **STWireless** you are able to configure the **STWireless** WLAN parameters via the web pages.

You can configure the following parameters:

▶ **SSID**

You can change the default SSID 'Alcatel_STW' into another value. This can be useful in case another **STWireless** is located nearby. It will avoid a WLAN client from his wireless network to connect by accident to yours.

▶ **Channel**

You can change the default channel number to another value. If you know another wireless equipment runs nearby yours, e.g. another **STWireless** WLAN environment, you can avoid sharing the channel bandwidth by changing the channel in use.

Note: After the SSID, and/or channel number has been changed inside the **STWireless**, the contact may be lost and the WLAN clients might be reconfigured, and re-authenticated to use the same SSID, and/or channel number.

See chapter 14 for more information on **STWireless's** Wireless configuration.



3.2 LAN Cables

Included LAN cable In your **STWireless** 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, etc. However, make sure that these have the correct layout.

See section F.4 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:

Port Type Interconnection	Type of LAN cable	Symbol
MDI-X to MDI	Straight-through	
MDI-X to MDI-X MDI to MDI	Crossover	

Devices and their ports The **STWireless**'s Ethernet port is of type MDI-X.
A PC's Ethernet port is always of type MDI.
An Ethernet hub's port is always of type MDI-X.

3.3 Connecting Wired Ethernet (Optionally)

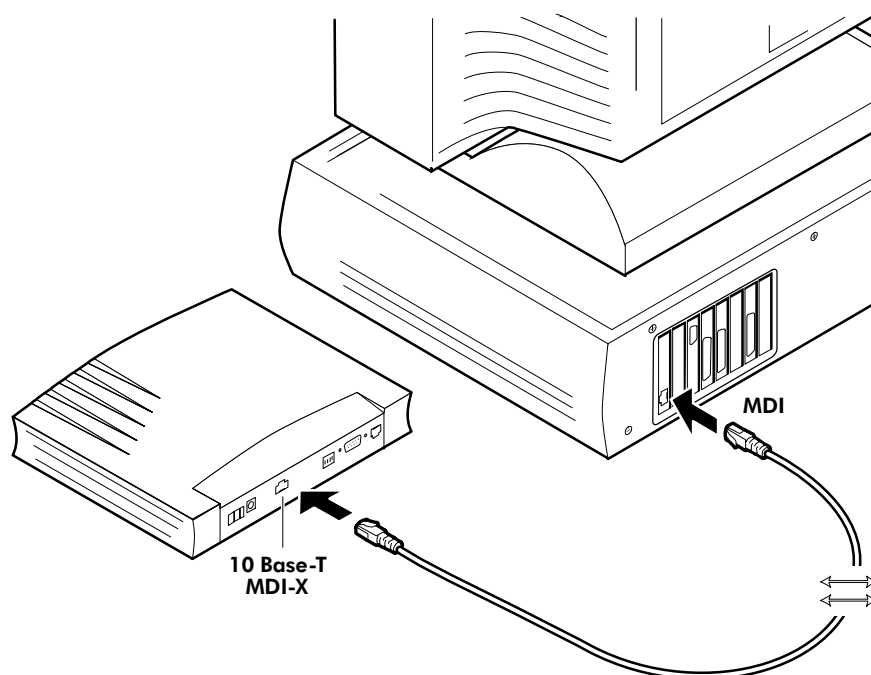
In this section

Topic	See
The Ethernet Port on your STWireless	3.3.1
Wired Single PC Connection	3.3.2
Wired Ethernet LAN	3.3.2

3.3.2 Wired Single PC Connection

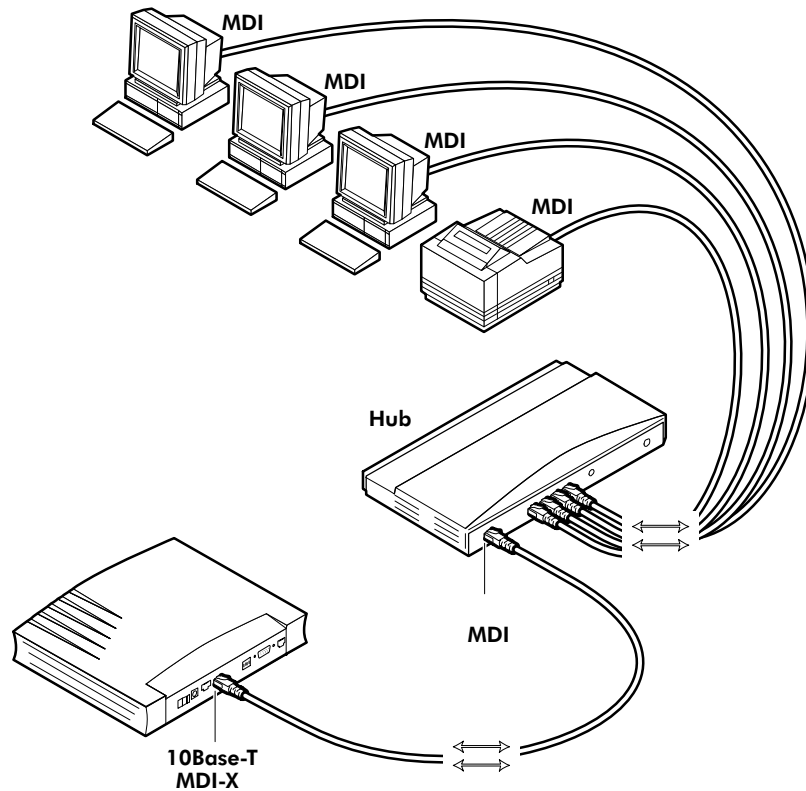
Single PC configuration In this configuration the **STWireless** is connected to a single PC.

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



3.3.3 Wired Ethernet LAN

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



Cascading Repeating Hubs

Because of the limitations of Repeating Ethernet V2.0/IEEE802.3 hubs, the maximum number of *repeating* hubs cascaded in your LAN is four. This restriction does not apply to switching hubs.

MDI vs. MDI-X hub ports and the STWireless

In the above figure example the MDI “uplink”, also referred to as “cascade”, port on the hub connects the **STWireless**. Therefore, the included straight-through LAN cable can be used.

Note: This port can also be a switchable MDI/MDI-X port.

You can also use one of the MDI-X ports of your hub. Then a crossover LAN cable must be used.

3.4 Wired Ethernet vs. WLAN Connectivity

Wireless vs. Wired LANs

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

STWireless network configurations

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

- ▶ An IP router (See section 11.4)
- ▶ A DHCP server (See subsection 11.1.4)
- ▶ NAPT abilities (See subsection 8.4.6)
- ▶ A DNS server for local name resolving and DNS proxying (See chapter 12)
- ▶ A Firewall (See chapter 13)

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

STWireless ADSL configurations

All **STWireless** configurations for ADSL connectivity, are equally valid for both wired Ethernet clients, as for WLAN clients, upon configuration.

STWireless configuration examples

This User Manual 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.

Speed Touch™ Wireless

Data Services

4 Data Services – Packet Services

Introduction This chapter is about selecting the appropriate packet service for your application.

In this chapter

Topic	See
Supported Packet Services	4.1
Packet Services at a Glance	4.2
Internet & Corporate Access vs. LAN-to-LAN Interconnection	4.3
Direct Networking vs. Dial-Up Networking	4.4
ADSL Modem vs. ADSL Gateway	4.5

4.1 Supported Packet Services

What is a packet service ?

A *packet service* can be defined as:

“The actions that need to be performed on every data packet in order to filter or forward packets to the next device in the communication chain.”

The STWireless offers five types of packet services

- ▶ IEEE 802.1D Transparent Bridging
 - ▶ MAC Encapsulated Routing
 - ▶ PPPoA-to-PPTP Relaying
 - ▶ PPP & IP Routing
 - ▶ Classical IP & IP Routing.
-

Networking protocols

All examples in this manual, use the Transmission Control Protocol (TCP)/Internet Protocol (IP) suite because it is widely available (See chapter 11 for more information).

However, the **STWireless** ADSL router is a true multiprotocol device, as it is able to manage most other forms of protocols.

Examples in this manual

Only typical solutions are presented in this manual.

However, this does not prevent you from experimenting with various configurations and settings.

An optimal solution may be discovered through experimentation. You can also try a combination of the presented solutions.

4.2 Packet Services at a Glance

- In this section**
- ▶ IEEE 802.1D Transparent Bridging
 - ▶ MAC Encapsulated Routing
 - ▶ PPPoA-to-PPTP Relaying
 - ▶ PPP & IP Routing
 - ▶ CIP & IP Routing
 - ▶ Selection Criteria
 - ▶ Simultaneous Use of Packet Services
 - ▶ Résumé.

IEEE 802.1D Transparent Bridging The **STWireless** *IEEE802.1D Transparent Bridging* packet service offers complete protocol transparency and has inherent configuration simplicity. Yet it provides excellent forwarding performance.

MAC Encapsulated Routing Next to the Bridge, the **STWireless** contains an IP router. The **STWireless** *RFC1483 MAC Encapsulated Routing (MER)* packet service relies on standard IP Routing for its packet forwarding on the (W)LAN side. However, to the remote access router on the WAN side, the **STWireless** presents itself as a IEEE802.1D Bridge.

That way the remote side can be fooled, i.e. via Network Address & Port Translation (NAPT), the single public IP address, assigned to the MAC entity, i.e. the “Bridge”, can be shared by multiple users on the local (W)LAN.

PPPoA-to-PPTP Relaying In contrast to Transparent Bridging, and MAC Encapsulated Routing, which both provide an “Always-On” type of connection, *PPPoA-to-PPTP Relaying (PPPoA/PPTP)*, supports a session concept. An important advantage of *PPPoA-to-PPTP Relaying* is that it avoids the complexity of a network router, yet to a certain extent, provides identical features.

PPP & IP Routing *Point-to-Point Protocol (PPP)* combined with *IP routing* is the technology of choice to create a small IP based home-(W)LAN. Similar to PPPoA/PPTP, it provides a session concept. Additionally, IP routing combined with NAPT allows to multiplex users into a single VC.

CIP & IP Routing The **STWireless** 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.

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 session aspect: an “Always-on” connection or a connection that is established when needed, i.e. “Dial-up”
- ▶ Connectivity to a single, or simultaneously to multiple remote network(s)
- ▶ Security features such as identification, authentication and encryption
- ▶ ADSL modem vs. ADSL gateway router model.

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

Note: For Transparent Bridging, the maximum number of configured Bridging ports is four.

Resumé All **STWireless**'s packet services can be summarized in the following table:

Port	Packet Service	Protocol	Chapter
10Base-T Ethernet	IEEE 802.1D Bridging	Multiprotocol	5
	MAC Encapsulated Routing	TCP/IP	6
	PPPoA-to-PPTP Relaying	TCP/IP, IPX/SPX, NETBEUI	7
	PPP & IP Routing	TCP/IP	8
	CIP & IP Routing	TCP/IP	9

4.3 Internet & Corporate Intranet Access vs. LAN-to-LAN Interconnection

Exemplary applications using ADSL

This manual highlights the two most prominent ADSL applications:

- ▶ *High speed Internet access, or corporate Intranet access*
 - ▶ *Private Wide Area Network (WAN) / Local Area Network (LAN) interconnection*
-

Internet & corporate access

Although the objective (Internet vs. Intranet access) is different, the networking model/configuration is almost identical.

Traditionally, the user must open a session by dialing into a remote access server. Prior to accessing the resources, this remote server will ask for the user's credentials.

The most appropriate **STWireless** configurations are:

- ▶ PPPoA-to-PPTP Relaying (See chapter 7)
 - ▶ PPP & IP Routing (See chapter 8).
-

LAN-to-LAN interconnection

Multiple PCs on a (W)LAN are interconnected via public, or private wide area ADSL/ATM networks to devices on remote LANs.

In the LAN-to-LAN scenario, users are less concerned about a session concept. Their networking experience should be as if they are part of a large and widely dispersed LAN.

The most appropriate **STWireless** configurations are:

- ▶ IEEE 802.1D Transparent Bridging (See chapter 5)
 - ▶ MAC Encapsulated Routing (See chapter 6)
 - ▶ Classical IP & IP Routing (See chapter 9).
-

Selecting the packet service

In the case of Internet, or corporate access, your SP will usually determine which networking model to use. In the LAN-to-LAN scenario you determine the end-to-end set-up yourself.

Independent of your application, the protocols supported at both ends of the connection must be mirror images of each other for successful communication.

4.4 Direct Networking vs. Dial-up Networking

- In this section**
- ▶ What is Direct Networking
 - ▶ Comparison with LAN Networking
 - ▶ What is Dial-Up Networking
 - ▶ **STWireless** & Networking
 - ▶ Ethernet Port(s) & Networking.

What is direct networking ? Direct networking refers to how the network connection is experienced by the user. The connection is continuously active, thus no actions need be performed.

Powering on the local PCs and the **STWireless** is enough to enable the user to interact with the network, once the initial configuration is done.

Comparison with LAN networking Direct networking is what is typically experienced on a LAN. Initial configuration of all networking nodes in the end-to-end network is still required, but this is performed only once, i.e. when the service is enabled.

What is dial-up networking ? In this mode, there is no initial connectivity. You must explicitly request a connection by dialing up to the remote access server.

The remote side will require you to identify and authenticate yourself.

STWireless vs. networking The **STWireless** supports both direct networking, and dial-up networking solutions, independently whether you are using the Ethernet port.

Ethernet port(s) & networking

Following scenarios are available:

- ▶ Direct and continuous connectivity is accomplished via the IEEE 802.1D transparent databridge, in the **STWireless**. See chapter 5 for more information.

 - ▶ MER provides continuous connectivity See chapter 6 for more information.

 - ▶ PPPoA-to-PPTP Relaying dial-up networking relies on the standard PPP protocol family and local tunneling, using the industry PPTP protocol. See chapter 7 for more information.

 - ▶ PPP & IP Routing provides dial-up networking. See chapter 8 for more information.

 - ▶ CIP & IP Routing provides continuous connectivity. See chapter 9 for more information.
-

4.5 ADSL Modem vs. ADSL Gateway

Introduction In the configuration where multiple PCs reside on a common LAN, they must share a gateway for specific services. The most important service is ADSL for accessing the outside world.

The **STWireless** can be used as a fast ADSL modem, leaving the gateway tasks to another (W)LAN member.

However, the **STWireless** is able to act as an ADSL gateway router itself. The latter is often called *home* or *residential* gateway.

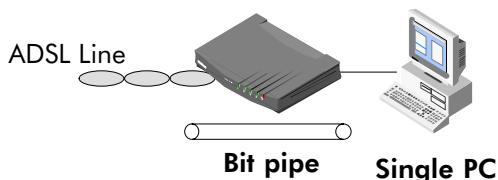
Note The boundaries between the ADSL modem model and the ADSL gateway function are not as clearly defined as explained in this section. They are portrayed that way to focus the attention on both models.

In this section

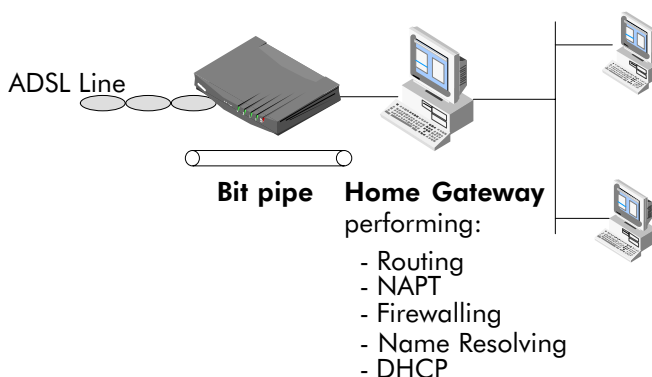
Topic	See
ADSL Modem Model	4.5.1
ADSL Gateway Model	4.5.2

4.5.1 ADSL Modem Model

ADSL modem model The **STWireless** in this role, provides connectivity to either a single PC: or to a dedicated home gateway:



Or to a dedicated home gateway:



Role of the STWireless The desired functionality of the **STWireless** ADSL router in this model, is maximum transparency. Packets arriving on inbound ports must be forwarded transparently to outbound ports. All intelligent decisions will be made in either the single PC, or the home gateway.

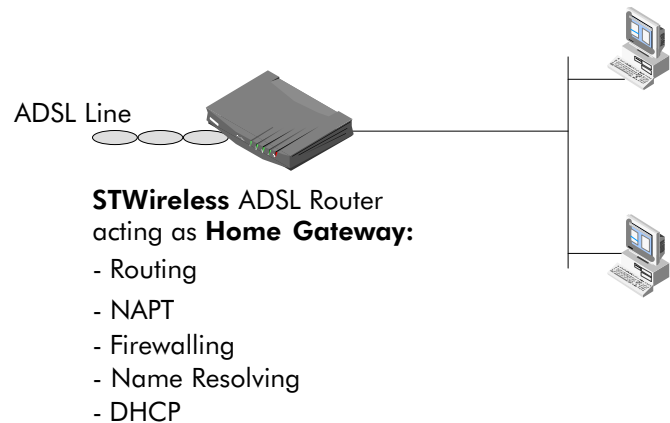
In fact, this functionality has been offered by voiceband modems for a long time, but then with an important speed limit.

Packet services and STWireless ADSL modem model The IEEE 802.1D transparent databridge, the PPPoA-to-PPTP relay and the PPP-to-DHCP Proxy – all bound to the Ethernet port and the ATM switching capabilities of the ATMF25.6 port –, adhere best to this model.

4.5.2 ADSL Gateway Model

ADSL gateway model The gateway to access the outside world can be a dedicated PC as shown in subsection 4.5.1.

However, the **STWireless** itself is designed to act as a cost effective ADSL gateway.



Role of the STWireless To perform the gateway tasks itself, the **STWireless** has, in addition to the ADSL modem part:

- ▶ An IP router (See section 11.4)
- ▶ A DHCP server (See subsection 11.1.4)
- ▶ NAPT abilities (See subsection 8.4.6)
- ▶ A DNS server for local name resolving and DNS proxying (See chapter 12)
- ▶ A Firewall (See chapter 13)

Packet services and STWireless ADSL gateway model MER, PPP & IP Routing and CIP & IP Routing are ideally suited for the ADSL gateway model.

5 Data Services – Transparent Bridging

Introduction The **STWireless IEEE802.1D Transparent Bridging** packet service offers complete protocol transparency and has inherent configuration simplicity. Yet it provides excellent forwarding performance.

In this chapter

Topic	See
Preparatory Steps	5.1
Using Bridging	5.2
Bridging Configuration	5.3
Advanced Bridging Concepts	5.4

5.1 Preparatory Steps

- Features** IEEE 802.1D Transparent Bridging:
- ▶ Is platform and OS independent
 - ▶ Is simple to configure and easy to use
 - ▶ Is a true multiprotocol device
 - ▶ In the Alcatel implementation, has no performance limitations
 - ▶ Has no theoretical constraints on the number of attached users
(There is a practical limit to achieve a reasonable performance, e.g. 16 PCs)
 - ▶ Features concurrent access to multiple remote destinations
 - ▶ Supports up to four concurrent Bridge ports.
-

- What you should know in advance**
- ▶ The **VPI/VCI** value of the VC(s) to use on the ADSL line
 - ▶ **ETHoA connection service** must be supported on this VC
 - ▶ Whether IP configuration is static, or dynamic (**DHCP**)
-

- STWireless** The **STWireless** comes with four preconfigured Bridging/MER phonebook entries, i.e. *Br1 ... Br4*.
- If the SP(s) impose settings which differ from the **STWireless** defaults, perform the necessary adjustments via the **STWireless** web pages.
- See section 5.3 for more information.
-

- PC(s)** The **STWireless**'s Transparent Bridging packet service does not impose specific requirements to your PC's networking protocol layers. However, ensure that the applied protocols are properly installed and configured on your PC.
-

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



Transparent Bridging and DHCP

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

This is to avoid conflicts between two DHCP servers, i.e. the **STWireless** DHCP server and a remote DHCP server, being active at the same time.

See subsection 11.3.3 for more information.

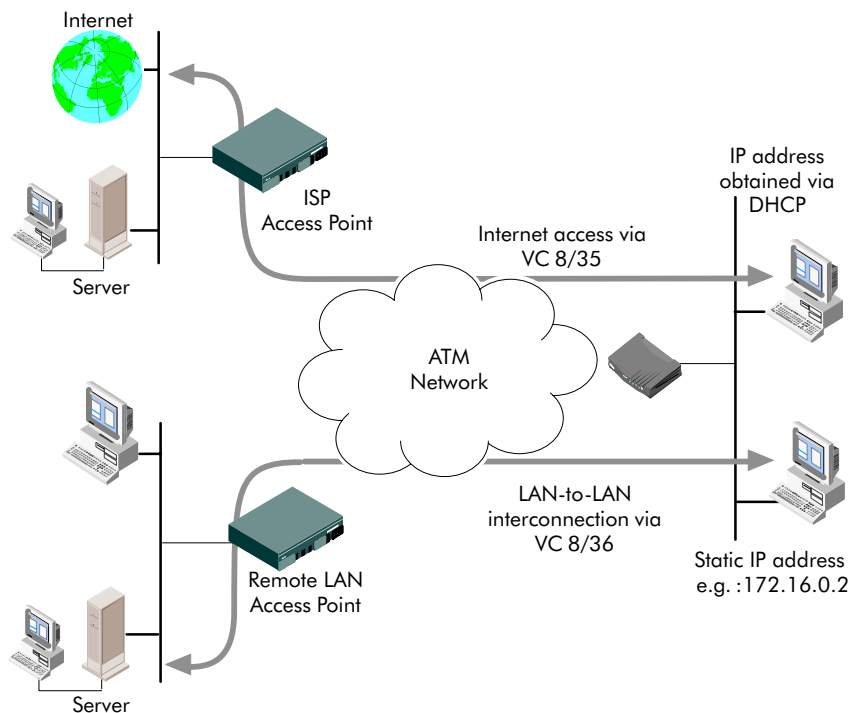
5.2 Using Bridging

Using Bridging From this point on, using Transparent Bridging is rather straight-forward. Turn on both your **STWireless** and PC, start your Web browser and you are on the Internet.

Always-on and credentials This form of remote network access is sometimes referred to as “Always-on”. No connection procedure must be performed prior to connectivity. However, the remote organization might present you with a welcome screen asking for a user name and password prior to granting access to secured servers or the Internet.

Configuration example In the following figure an example configuration is given:

- ▶ One PC is connected to an ISP
- ▶ Another PC is connected to a remote LAN.



5.3 Bridging Configuration

Introduction The **STWireless** allows local configurations via the **STWireless** web pages.

This section describes the configuration of Bridging entries, and the use of the 'Bridging' web page.

In this section

Topic	See
Bridging Phonebook Entries	5.3.1
Bridging Entries	5.3.2

5.3.1 Bridging Phonebook Entries

Bridging phonebook entries

Central to the **STWireless** VC pool management, is the 'Phonebook' web page.

The **STWireless** in its default state features the following Bridging/MER related phonebook entries:

Name	Address	Type	AutoPVC	Avail	Action
Br1	8.35	bridge	No	yes	Delete
Br2	8.36	bridge	No	yes	Delete
Br3	8.37	bridge	No	yes	Delete
Br4	8.38	bridge	No	yes	Delete
Use input fields below to add a new entry					
<input type="text"/>	<input type="text"/>	any	-	-	Add

Note: Both Bridging and MER share the same type of phonebook entries, i.e. **bridge**.

Adding/deleting phonebook entries

See section 10.2 for more information.

5.3.2 Bridging Entries

- In this subsection**
- ▶ The **STWireless** 'Bridging' Web Page
 - ▶ The 'Bridging Ports' Table
 - ▶ 'Bridging Ports' Table Components
 - ▶ The 'Aging' Box
 - ▶ Adding Bridging Entries
 - ▶ Deleting Bridging Entries.

The STWireless 'Bridging' web page

Clicking **Bridge** in the left pane of the **STWireless** web pages, pops up the 'Bridging' web page (See section 18.2 for more information):

The screenshot shows the 'Bridging Ports' configuration page. A warning message states 'WARNING : Modem is down'. The main content area displays a table of bridging ports:

Intf	Address	State	Port	Encap	FCS	Action
Br1	Br1	connected	wan0	LLC/SNAP	NO	Delete

Below the table, there is a form to add a new entry with the following fields:

Use input fields below to add a new entry

The 'Aging' section includes a text input field with the value '300' and a label 'Seconds'.

The 'Bridging Ports' table







The following figure shows the 'Bridging Ports' table in its default state:

Intf	Address	State	Port	Encap	FCS	Action
Use input fields below to add a new entry						
<input type="text"/>	<input type="text"/>	Br1	<input type="text"/>	LLC/SNAP	-	<input type="button" value="Add"/>

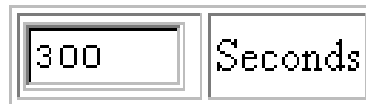
'Bridging Ports' table components

The following fields are shown:

Field	Description						
<i>Intf</i>	Allows you to choose an interface name for the Bridge interface. Note: In most cases, the interface name will be the same as the phonebook entry name.						
<i>Destination</i>	Indicates available Phonebook entries for Bridging. Note: Specific free MER/Bridging phonebook Entries are shown, as well as free 'any type' phonebook entries						
<i>State</i>	Indicates the state of the individual (W)LAN port. It can take following values: <table border="1" data-bbox="754 1173 1374 1541"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>connected</td> <td>The Bridge interface is attached to the Bridge port. In most cases this also implies that the Bridge port is connected and forwarding.</td> </tr> <tr> <td>idle</td> <td>The Bridge port only submits information to the filtering database. It does not participate in the relaying of frames.</td> </tr> </tbody> </table>	Value	Description	connected	The Bridge interface is attached to the Bridge port. In most cases this also implies that the Bridge port is connected and forwarding.	idle	The Bridge port only submits information to the filtering database. It does not participate in the relaying of frames.
Value	Description						
connected	The Bridge interface is attached to the Bridge port. In most cases this also implies that the Bridge port is connected and forwarding.						
idle	The Bridge port only submits information to the filtering database. It does not participate in the relaying of frames.						
<i>Port</i>	Indicates the name of the Bridge port on the WAN side: wan0, wan1, wan2, etc. by default.						

Field	Description						
Encap	Refers to the encapsulation, and decapsulation of Ethernet, or IEEE 802.3 frames in/from AAL5/ATM. The STWireless is compliant with RFC 1483 "Multiprotocol Encapsulation over ATM Adaptation Layer 5" and supports both the LLC/SNAP method and the VC-MUX method for Bridged Ethernet V2.0/IEEE 802.3 PDUs. By default the encapsulation method is set to LLC/SNAP.						
FCS	Is part of the RFC 1483 encapsulation method and indicates whether the last four bytes of the Medium Access Control (MAC) frames (mostly referred to as Ethernet or IEEE 802.3 frames) will be preserved or not. For all Bridge ports, the FCS is set to NO by default. However, via the CLI, you can set the FCS to YES . See chapter 19 for more information.						
Action	Contains one of the two following action buttons: <table border="1" data-bbox="751 819 1390 978"> <thead> <tr> <th>Button</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td></td> <td>Add an entry to the list.</td> </tr> <tr> <td></td> <td>Delete an existing entry from the list.</td> </tr> </tbody> </table>	Button	Action		Add an entry to the list.		Delete an existing entry from the list.
Button	Action						
	Add an entry to the list.						
	Delete an existing entry from the list.						

The 'Aging' box The following figure shows the 'Aging' box of the 'Bridging' web page:

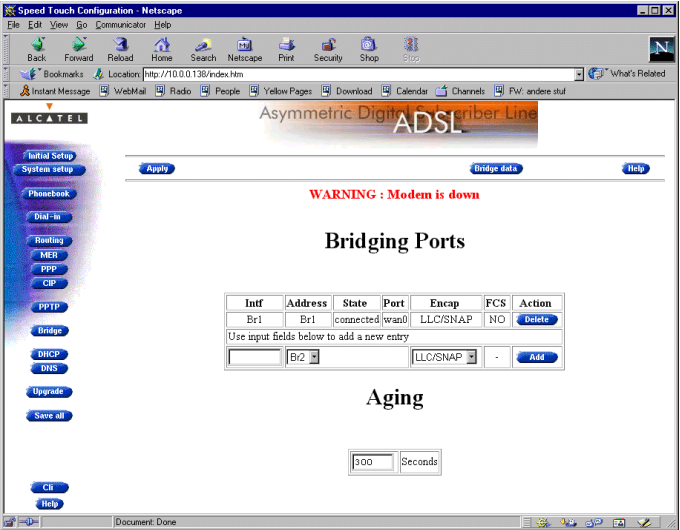


This box contains the aging timer of the bridge internal database. If the aging time of a MAC entry has expired, this entry will be removed from the database.

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 (IEEE 802.1D Bridging standard).

Adding Bridging entries

Proceed as follows:

Step	Action and Description
1	<p>Browse to the 'Bridging' web page.</p>  <p>The bottom row of the table allows addition of a new entry.</p>
2	<p>In the 'Destination' column of the bottom row, click <input type="text"/> and select the Bridging entry you want to add to the table.</p>
3	<p>In the 'Encap' column, click <input type="text"/> and select the encapsulation method for the connection, i.e. LLC/SNAP, or VC-MUX.</p>
4	<p>Click Add and Save all to finish the procedure.</p>

Note The maximum number of remote Bridging ports supported is 4. However, if no multiple connectivity is required, leave the configuration as is, to conserve ADSL upstream bandwidth.

Deleting Bridging entries

Proceed as follows:

Step	Action and Description
1	<p>Browse to the 'Bridging' web page.</p>
2	<p>Select the Bridging entry you want to delete, and click Delete and Save all to finish the procedure.</p>

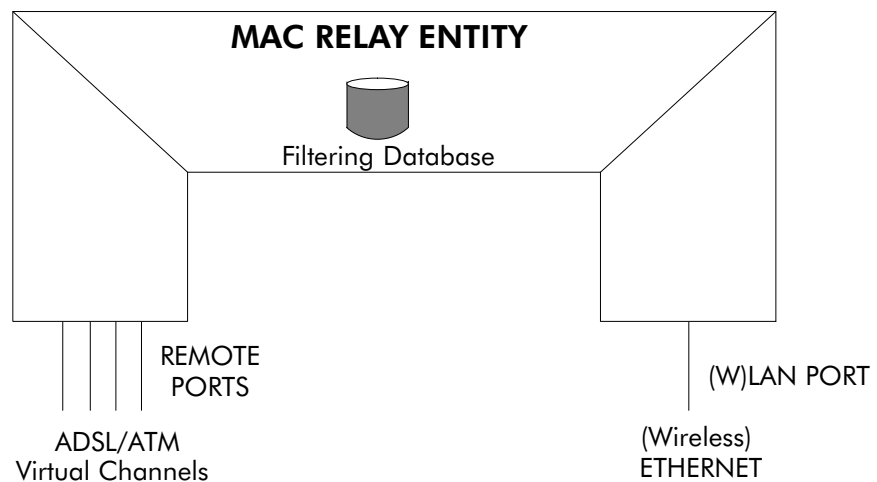
5.4 Advanced Bridging Concepts

Bridging Bridging is a LAN technology that transparently relays Ethernet frames between Bridging ports.

Depending on the destination MAC addresses of Ethernet frames, the bridge makes decisions whether to forward or discard frames.

Central to the operation of a databridge is its filtering database. All forwarding and filtering actions are based on information in this database.

Simplified bridge architecture



In this section

Topic	See
STWireless Bridge Operation	5.4.1
STWireless 'Bridge Data' Web Page	5.4.2

5.4.1 STWireless Bridge Operation

Introduction to bridge operation

This section describes how the **STWireless** bridge operates. All of these operations have an impact on the entries in the filtering database of the bridge.

One of the characteristics of a databridge is the number of supported Bridge ports. A Bridge port is the logical equivalent of an interface. By default the **STWireless** supports one local port, i.e. the Ethernet port, and four remote ports. The remote ports are mapped to virtual ATM channels on the ADSL line.

In this subsection

- ▶ Learning
 - ▶ Aging
 - ▶ Learning and Aging
 - ▶ Flooding
 - ▶ Forwarding
 - ▶ Filtering
 - ▶ Isolation
 - ▶ Multiprotocol Bridging
 - ▶ Number of Supported Devices.
-

Learning If the bridge is turned on, the filtering database is empty. Over time it is filled with entries via the learning mechanism.

Ethernet frames arriving on any port are inspected for their source MAC address and put into the filtering database together with the port ID the frames arrived on.

Through this knowledge, it is able to keep traffic submitted to your local printer from crossing the bridge. Yet it allows frames belonging to sessions with remote machines to pass over the ADSL line.

Aging Entries are aged, i.e. removed from the filtering database, after a certain time has elapsed (Aging time).

Learning and Aging The learning and aging process make the bridge Plug & Play. Both keep the filtering database up-to-date with the current network configuration.

Example: Suppose a PC-NIC is replaced, the old MAC address is aged (and will be consequently discarded), while a new MAC address will be learned.

Flooding If an Ethernet frame arrives, the destination MAC address is searched for in the filtering database. If the destination MAC address is not found (implying it is not yet learned), it is forwarded to all ports in the forwarding state, except the one the frame arrived on.

Note: Broadcast and multicast MAC addresses are always flooded.

Forwarding If an Ethernet frame arrives with a destination MAC address that is found in the filtering database (implying it is already learned), it is forwarded to the port that is associated with that entry.
In contrast to flooding, forwarding is more selective.

Filtering If the destination MAC address is found on the same port as the frame arrived on, it is filtered, i.e. silently discarded.
Indeed, it makes little sense to forward the frame on this port as the destination is directly connected to the source.

Isolation The *Alcatel Multiport* bridge in the **STWireless** provides isolation between remote ports.
i.e. Frames (including broadcasts) arriving via ADSL/ATM ports will never be forwarded/flooded to another ADSL/ATM port.

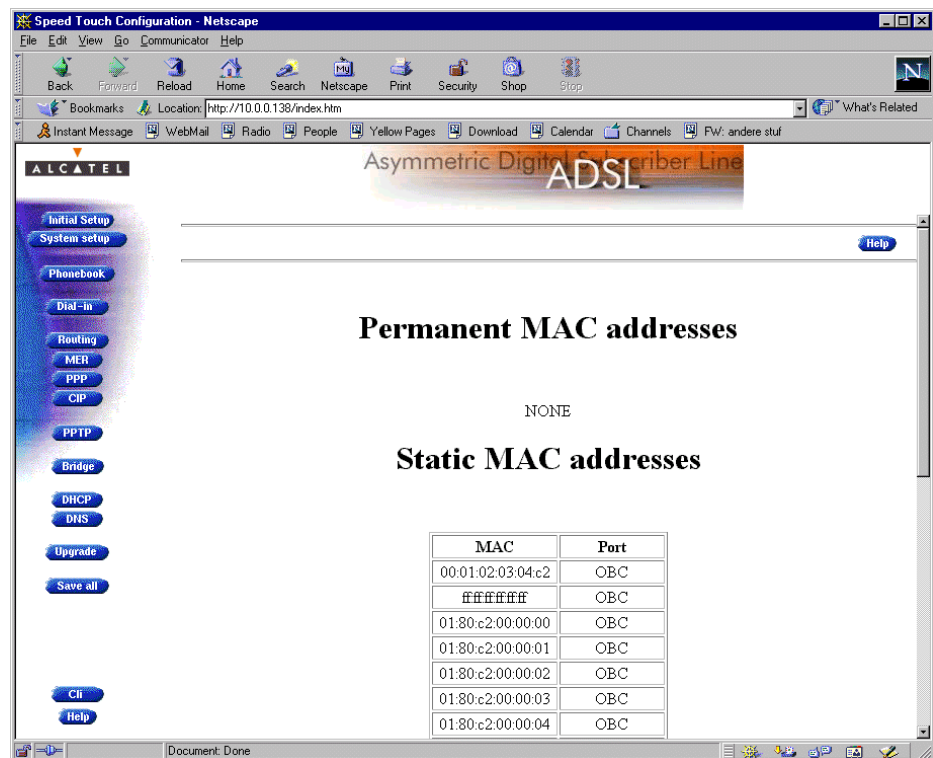
Multi Protocol Bridging Bridging actions are performed on MAC frames. The contents of the MAC frame is not of importance to the bridge.
Consequently it makes no difference whether your PCs or workstations use TCP/IP, Appletalk, IPX/SPX or any other protocol suite.
However, some operators might embed restrictions into the bridge. In this way only traffic that passes through the bridge filter will be allowed on the ADSL line.

Number of supported devices Via the dynamic learning and aging mechanism of the bridge, the number of PCs that can be connected to either the local, or virtual ports is theoretically unlimited.
Practically, the filtering database can hold as many as 256 entries simultaneously.

5.4.2 STWireless 'Bridge Data' Web Page

Introduction Transparent Bridging relies completely on its filtering database for managing the traffic, passing through the bridge. This filtering database is accessible via the **STWireless 'Bridging'** web page, and allows you to overview all MAC-layer entries.

The 'Bridge Data' web page Clicking **Bridge data** on the 'Bridging' web page pops up the 'Bridge Data' web page:



Available 'Bridge Data' tables The filtering database's MAC addresses are spread over 3 tables:

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

Permanent MAC addresses

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

- ▶ The **STWireless**'s own 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

Static MAC addresses

This table list the MAC addresses you have added to the filtering database via the CLI. These MAC addresses, dedicated to a particular port, will never be aged by the bridge.

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

Dynamic MAC addresses

This table lists all the MAC addresses that are currently learned by the **STWireless** bridge.

While the learning process adds MAC addresses received on any of its ports, the aging process will swap them out of the table when their aging timer expired.

6 Data Services – MAC Encapsulated Routing

Introduction Via the **STWireless** *MAC Encapsulated Routing* packet service you can connect to an ADSL line supporting the Ethernet over ATM (ETHoA) connection service. In contrast to bridging though, packet filtering and forwarding is performed by the IP router of the **STWireless** and consequently inherits all the features that come with IP.

In the following, MAC Encapsulated Routing will be referred to as MER.

Note: MAC is the standardized term for Ethernet.

In this chapter

Topic	See
Preparatory Steps	6.1
Using MER	6.2
MER Configuration	6.3
Advanced MER Concepts	6.4

6.1 Preparatory Steps

- Features** MAC Encapsulated Routing:
- ▶ Is instantly replaceable with an IEEE Transparent Bridge
 - ▶ Provides Always-on type of connections and is auto-configurable if DHCP is enabled
 - ▶ If used in combination with NAPT, allows multiple users to share a single IP address
 - ▶ When Firewalling is turned on, your local network is shielded for threats from the Internet.
 - ▶ Supports up to 12 concurrent virtual channels assigned to MER.
-

- What you should know in advance**
- ▶ The **VPI/VCI** value of the VC(s) to use on the ADSL line
 - ▶ **ETHoA connection service** must be supported on this VC
 - ▶ Whether IP configuration is static, or dynamic (**DHCP**)
-

STWireless The **STWireless** comes with four preconfigured MER/Bridging phonebook entries, i.e. *Br1 ... Br4*.

If the SP(s) impose settings which differ from the **STWireless** defaults, perform the necessary adjustments via the **STWireless** web pages.

See section 6.3 for more information.

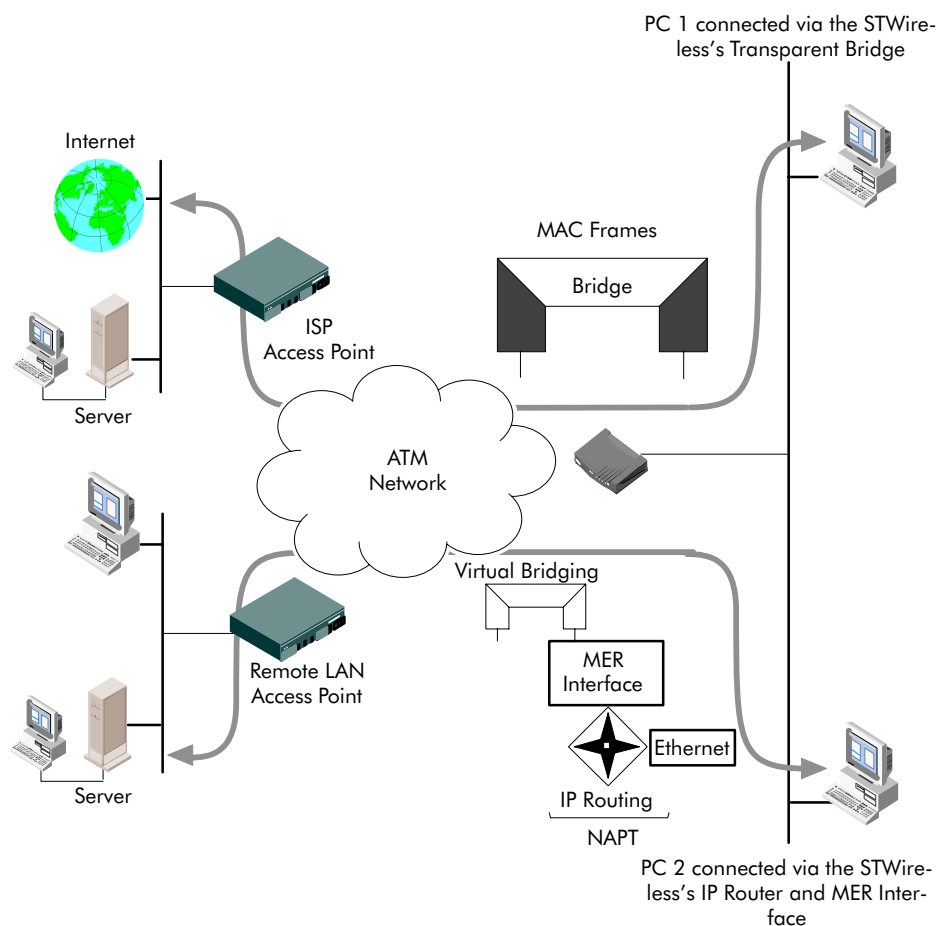
- PC(s)** For MER it is assumed that communication between the **STWireless** and your PC(s) is performed via the Internet protocol.
- You can:
- ▶ Enable the **STWireless**'s DHCP server to enable dynamic IP configuration of your (W)LAN
 - ▶ Configure all (W)LAN's IP settings statically.
-

6.2 Using MER

Using Bridging From this point on, using MER is rather straight-forward. Turn on both your **STWireless** and PCs, and your connected to the remote access router.

Always-on and credentials As MER presents itself as a Bridge, the connection behaves as for the Transparent Bridging packet service. No connection procedure must be performed prior to connectivity.

MER end-to-end architecture In the following figure an example configuration of a Transparent Bridging connection, and a MER connection is given:



6.3 MER Configuration

Introduction The **STWireless** allows local configurations via the **STWireless** web pages.

This section describes the configuration of MER entries, and the use of the 'MER' web page.

In this section

Topic	See
MER Phonebook Entries	6.3.1
MER Entries	6.3.2

6.3.1 MER Phonebook Entries

MER phonebook entries

Central to the **STWireless** VC pool management, is the 'Phonebook' web page.

The **STWireless** in its default state features the following MER related phonebook entries:

Name	Address	Type	AutoPVC	Avail	Action
Br1	8.35	bridge	No	yes	Delete
Br2	8.36	bridge	No	yes	Delete
Br3	8.37	bridge	No	yes	Delete
Br4	8.38	bridge	No	yes	Delete
Use input fields below to add a new entry					
<input type="text"/>	<input type="text"/>	any	-	-	Add

Note: Both MER and Bridging share the same type of phonebook entries, i.e. **bridge**.

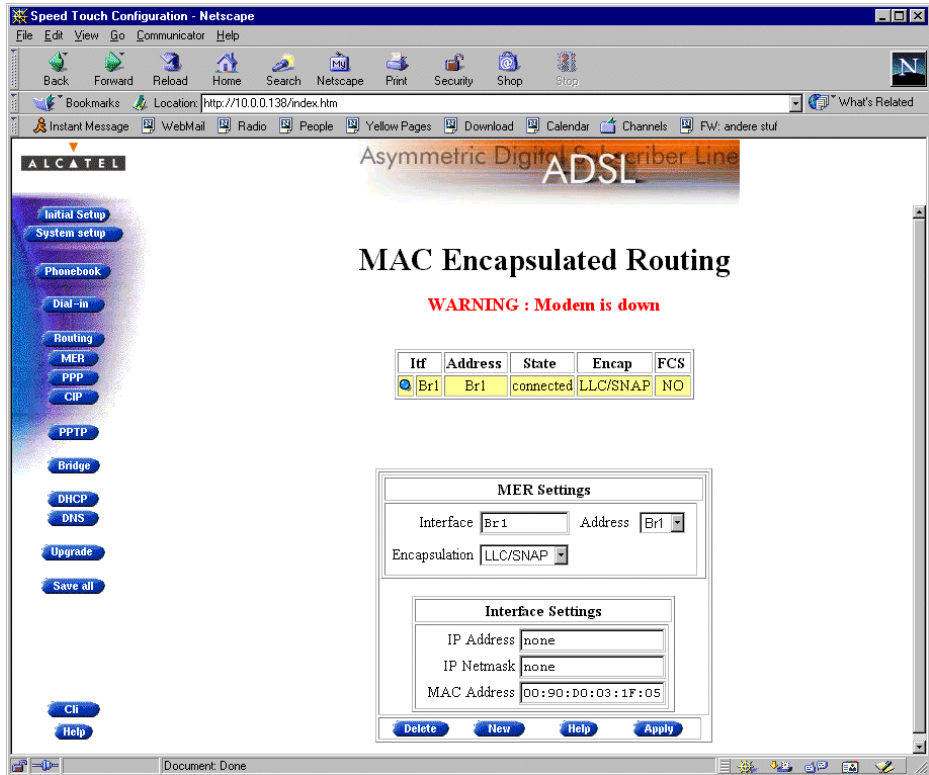
Adding/deleting phonebook entries

See section 10.2 for more information.

6.3.2 MER Entries

The STWireless 'MER' web page

Clicking **MER** in the left pane of the **STWireless** web pages, pops up the 'MER' web page (See section 18.2 for more information):




The 'MER Connections' table

The following figure shows the 'MER Connections' table:

Itf	Address	State	Encap	FCS
Br1	Br1	connected	LLC/SNAP	NO

**'MER Connections'
table components**

The following fields are shown:

Field	Description								
	Click the button next to the MER connection you want to configure. Selected MER connections are indicated by a yellow bar, and a button which is lit.								
<i>lrf</i>	Indicates the interface name. Note: In most cases, the interface name will be the same as the phonebook entry name.								
<i>Address</i>	Indicates the name you have chosen for the MER phonebook entry. Note: Specific free MER phonebook entries are shown, as well as free 'any type' phonebook entries								
<i>State</i>	Indicates the state of the MER connection. It can take following values: <table border="1" data-bbox="762 922 1382 1211"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Idle</td> <td>The MER interface has no WAN connection at this time.</td> </tr> <tr> <td>Retry</td> <td>The MER interface tries to setup a WAN connection.</td> </tr> <tr> <td>Connected</td> <td>WAN connectivity is achieved on this MER interface.</td> </tr> </tbody> </table>	Value	Description	Idle	The MER interface has no WAN connection at this time.	Retry	The MER interface tries to setup a WAN connection.	Connected	WAN connectivity is achieved on this MER interface.
Value	Description								
Idle	The MER interface has no WAN connection at this time.								
Retry	The MER interface tries to setup a WAN connection.								
Connected	WAN connectivity is achieved on this MER interface.								
<i>Encap</i>	Refers to the encapsulation, and decapsulation of Ethernet, or IEEE 802.3 frames in/from AAL5/ATM. The STWireless is compliant with RFC 1483 "Multiprotocol Encapsulation over ATM Adaptation Layer 5" and supports both the LLC/SNAP method and the VC-MUX method for Bridged Ethernet V2.0/IEEE 802.3 PDUs. By default the encapsulation method is set to LLC/SNAP.								
<i>FCS</i>	Is part of the RFC 1483 encapsulation method and indicates whether the last four bytes of the MAC frames (mostly referred to as Ethernet or IEEE 802.3 frames) will be preserved or not. For all MER connections, the FCS is set to NO by default. However, via the CLI, you can set the FCS to YES . See chapter 19 for more information.								

The 'MER Settings' table

The following figure shows the 'MER Settings' table:

MER Settings	
Interface	Br1
Address	Br1
Encapsulation	LLC/SNAP

'MER Settings' table components

The following fields are shown:

Field	Description
<i>Interface</i>	Allows to enter an interface name for the MER connection. Note: You don't have to fill in a name for the MER interface. The name applied will be the same as the phonebook entry name.
<i>Address</i>	Indicates free MER phonebook entries, as well as free 'any type' phonebook entries.
<i>Encapsulation</i>	Allows to select the encapsulation method, i.e. LLC/SNAP (default), or VC-MUX.

The 'MER Interface Settings' table

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

Interface Settings	
IP Address	none
IP Netmask	none
MAC Address	00:90:D0:03:1F:05






'MER Interface Settings' table components

The following fields are shown:

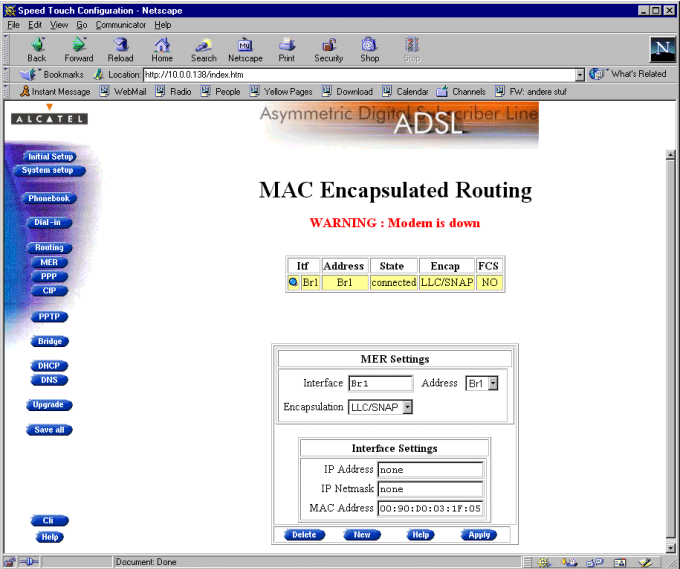
Field	Description
<i>IP Address</i>	Allows to enter a static IP address for the MER connection. Note: In case no IP address is entered, the MER connection will receive an IP address from the remote access server.
<i>IP Netmask</i>	Allows to enter an associated IP netmask for the static IP address. Note: In case no IP address is entered in the IP address field, or no IP netmask is entered, the default associated netmask will be used.
<i>MAC Address</i>	Allows to enter a MAC address for the MER connection. This MAC address, visible for the remote access server, overrules the STWireless MAC address. Note: In case no MAC address is entered, the source MAC address of the bridged frames is the STWireless MAC address.

'MER Configuration' Buttons

The following buttons are available:

Field	Description
	Deletes the selected MER connection.
	If you create a new MER connection, this button allows to clear all configurational fields for the connection, i.e. returns them to their default settings.
	Creates a new MER connection, in addition to (an) existing MER connection(s).
	Adds the configured MER connection to the 'MAC Encapsulated Routing' table, i.e. "activates" the MER connection.
	Applies changes you made to an existing MER connection.

Adding MER entries Proceed as follows:

Step	Action and Description
1	<p>Browse to the 'MER' web page.</p> 
2	<p>If the 'MAC Encapsulated Routing' table is empty, i.e. you are creating the first MER connection, proceed with step 3.</p> <p>If you want to add a MER connection in addition to existing MER connections (see 'MAC Encapsulated Routing' table), click New</p>
3	<p>In the 'Address' field, click <input type="text"/> and select the (free) phonebook entry for your MER connection.</p>
4	<p>In the 'Encap' column, click <input type="text"/> and select the encapsulation method for the connection, i.e. LLC/SNAP, or VC-MUX.</p>
5	<p>Optionally, enter the appropriate configuration in one, or more of the following fields:</p> <ul style="list-style-type: none"> • the 'Interface' field • the 'IP Address' field • the 'IP Netmask' field • the 'MAC Address' field. <p>Note: See topics 'MER Settings table' and MER Interface Settings table' in this subsection for more information.</p>
6	<p>Click Apply and Save all to finish the procedure.</p>

Maximum number of MER connections

The **STWireless** can manage up to 12 MER connections simultaneously. This can be achieved by deleting all other packet service entries.

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

Reconfiguring an existing MER connection

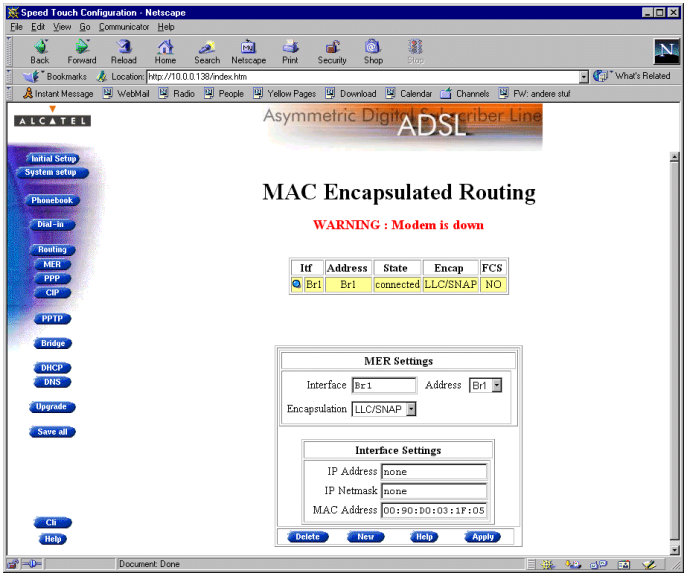
Click the selection button of a MER interface.

The settings shown in the 'MER Settings' and 'MER Interface Settings' table apply to the MER connection which is marked with a yellow bar and a selection button which is lit (●).

Make the changes to the fields, and click **Apply**. Click **Save all** to make the changes persistent.

Deleting Bridging entries

Proceed as follows:

Step	Action and Description
1	<p>Browse to the 'Bridging' web page.</p> 
2	<p>Click the selection button of the MER connection you want to delete, and click Delete.</p> <p>Click Save all to finish the procedure.</p>

6.4 Advanced MER Concepts

- In this subsection**
- ▶ MAC Encapsulated Routing
 - ▶ MER operation: From (W)LAN to **STWireless**'s IP router
 - ▶ MER operation: From IP Router to MER
 - ▶ MER operation: From MER to WAN
 - ▶ Configuration and Operation Example.

MAC Encapsulated Routing

MAC Encapsulated Routing allows IP packets to be carried as bridged frames. The RFC1483 link protocol with MER is a multiprotocol encapsulation method over ATM. While the true IEEE802.1D Transparent Bridge is a hardware component of the **STWireless**, for MER, the encapsulation method is implemented by software.

MER Operation: from (W)LAN to STWireless's IP router

In the PCs, IP packets are encapsulated in MAC frames, according their destination:

- ▶ For local networking, the destination MAC address is the one of the destination device, e.g. another PC
- ▶ For non-local traffic, the destination MAC address is that of the **STWireless**
- ▶ In both cases, the source MAC address, is the MAC address of the source device, e.g. your PC.

All MAC frames arrive via the Ethernet segment in the **STWireless**. It decapsulates the MAC frames and routes the IP packets, according their destination.

MER Operation: from STWireless's IP router to MER

IP packets destined for MER, can be subjected to NAPT, prior to end up in the appropriate MER interface

NAPT allows local (W)LAN PCs to share the single static, or dynamically obtained public IP address for the MER connection.

MER Operation: from MER to WAN

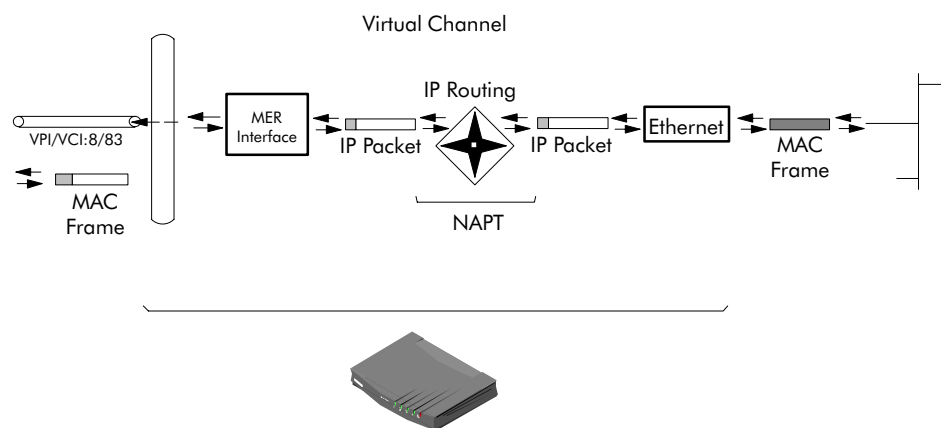
The IP packets, ending up in the MER interface are encapsulated in MAC frames:

- ▶ The source MAC address is now the **STWireless** MAC address, or the MAC address, configured on the 'MER' web page
- ▶ The destination MAC address is obtained via ARP.

Finally these MAC frames are processed to the WAN, over the ADSL line by the **STWireless**, as if it were an IEEE802.1D compliant bridge, sending MAC, i.e. bridged frames.

Configuration and operation example

The figure below provides an overview of the **STWireless** rear-to-front end MER operation:



7 Data Services – PPPoA-to-PPTP Relaying

Introduction The **STWireless PPPoA-to-PPTP Relaying** packet service relays PPP frames, arriving via local IP tunnels to a previously selected VC, and vice versa.

The PPP protocol that originates, or terminates in the locally attached PCs, offers a session concept, and provides security via identification, authentication and encryption.

A major advantage of *PPPoA-to-PPTP Relaying* is that it avoids the complexity of an IP router, yet to a certain extent, provides identical features.

Topics

Topic	See
Preparatory Steps	7.1
Configuring and Using a PPTP Connection	7.2
Example : MS Windows 98 Dial-Up Networking	7.3
PPPoA/PPTP Configuration	7.4
Customizing PPPoA/PPTP Connections	7.5
Advanced PPPoA/PPTP Concepts	7.6

7.1 Preparatory Steps

- Features** PPPoA-to-PPTP Relaying:
- ▶ Provides standard “Dial-up” 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 NATP is required
 - ▶ Supports concurrent access to multiple remote destinations (depending on provisioning).
 - ▶ Supports up to 12 concurrent virtual channels assigned to PPPoA/PPTP.
-

- What you should know in advance**
- ▶ The **VPI/VCI** value of the VC(s) to use on the ADSL line
 - ▶ **PPPoA connection service** must be supported on this VC
 - ▶ User name and password for your **user account**.
- Note:** If connectivity to multiple remote organizations is required, you need additional sets of these parameters.
-

STWireless The **STWireless** comes with five preconfigured free PPP phonebook entries, i.e. *Relay_PPP1 ... Relay_PPP4*, and *PPP3*.
If the SP(s) impose PPPoA/PPTP settings which differ from the **STWireless** defaults, perform the necessary adjustments via the **STWireless** web pages.
See section 7.4 for more information.

PC(s) Your PC must support PPP and Point-to-Point Tunnelling Protocol (PPTP).
e.g. All Microsoft Windows platforms support PPP and PPTP.

TCP/IP Before you can establish PPTP tunnels, you must configure:

- ▶ An IP address in each PC which initiates a PPTP tunnel
- ▶ An IP address in your **STWireless** which terminates the PPTP tunnel(s)

To configure an IP address, or enable DHCP in your PC(s), see Appendix NO TAG.

To configure an IP address, or enable DHCP in your **STWireless**, see section 11.3.

7.2 Configuring and Using a PPTP Connection

Introduction Before you can open a PPTP tunnel towards the **STWireless**, 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 PPPoA/PPTP connection to the remote side of the ADSL 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 7.3 an example is provided how to create and use a PPTP Dial-Up icon in MS Windows 98.

Refer to appendix C for more information on other OSs.

In this section

Topic	See
Preparing your PC for PPPoA/PPTP	7.2.1
Using PPTP towards your STWireless	7.2.2

7.2.1 Preparing your PC for PPPoA/PPTP

Creating a PPTP connection icon

Most, if not all OSs provide a 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.

PPPoA/PPTP 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 **STWireless**'s IP address, or DNS hostname

Optionally, you can complete this entry with

- ▶ The VC's phonebook name to use for this connection
- ▶ A PPTP profile name

7.2.2 Using PPTP towards your STWireless

Opening a session Depending on your OS, you can open a session by either double-clicking the PPTP connection 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 username
- ▶ An associated password

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





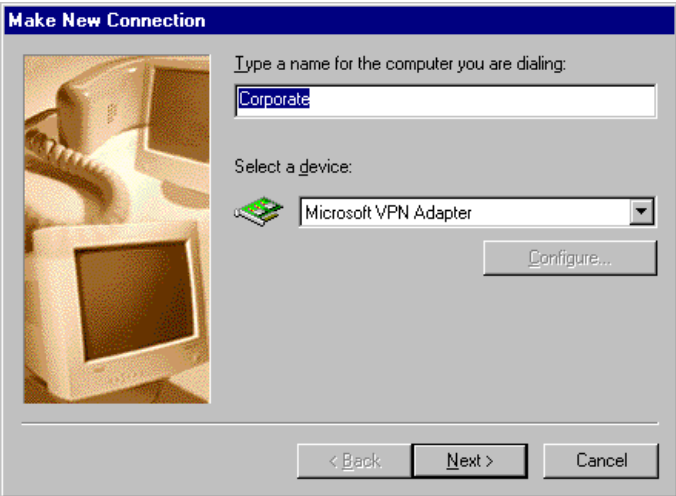
7.3 Example : MS Windows 98 Dial-Up Networking


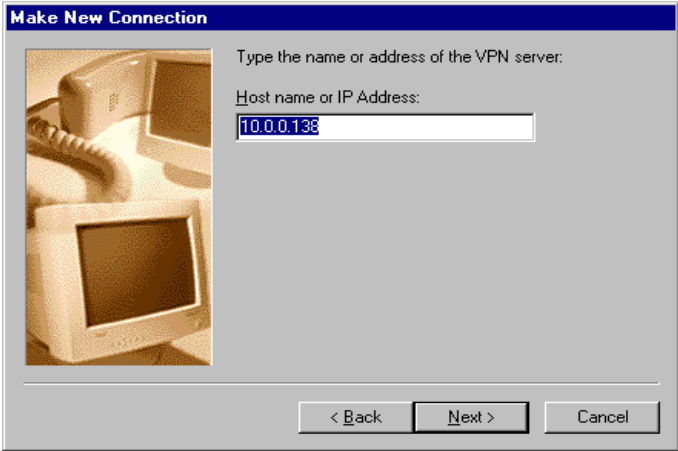

In this section The following overview summarizes the necessary steps to setup a Microsoft Windows 98 PC for the use of PPPoA-to-PPTP Relaying:

Step	Action	See
1	Configure a <i>Private</i> IP address on your PC	
2	Create a new Dial-Up Networking icon	7.3.1
3	Adapt Dial-Up Networking Properties	C.1
4	Create a shortcut on your desktop (optional)	7.3.2
5	Open a PPPoA/PPTP Dial-Up Session	7.3.3
6	Surf the Internet.	
7	Close a PPPoA/PPTP Dial-Up Session in Use	7.3.4

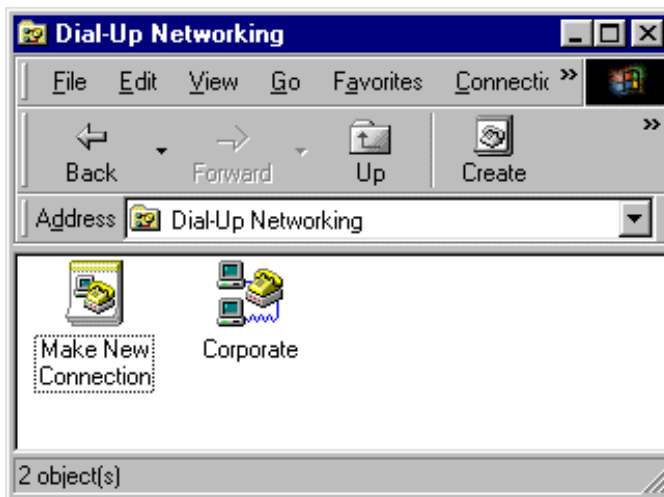
7.3.1 Create a New Dial-Up Networking Icon

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  The 'Make New Connection' window pops up: 

Step	Action and Description
5	<p>In the first input field of the 'Make New Connection' window, type a name, or alias of the organization you are connecting to.</p> <p>Note: This name will appear below the Dial-Up icon at the end of this procedure.</p>
6	<p>In the 'Select a device' listbox of the Make New Connection' window, you must select the 'Microsoft VPN Adapter' for PPTP tunneling.</p>
7	<p>Click  to pop up the VPN server window:</p> 
8	<p>Enter the DNS hostname or IP address of the Virtual Private Network (VPN) server.</p> <p>Note: "VPN server" is another word for PPTP server, which is in this case your STWireless.</p> <p>The default IP address for the STWireless is 10.0.0.138. Its default hostname is "SpeedTouch".</p> <p>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. See section 7.5 for more information.</p>
9	<p>A window pops up confirming that you have successfully installed a new Dial-Up connection.</p> <p>Click  to finish the procedure.</p>

Result A new icon with the name of the connection that 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 3 of the previous procedure.



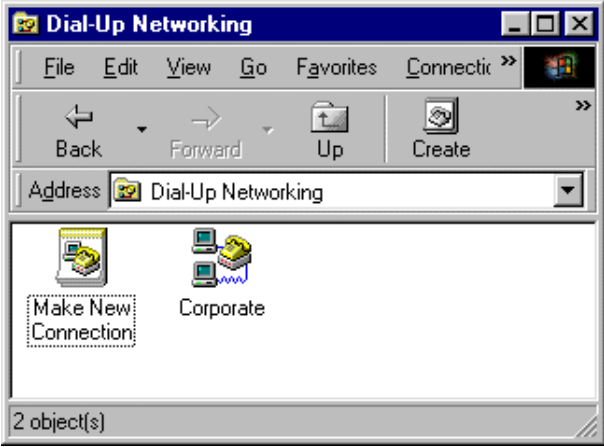

Specific VC and PPTP Profiles

Using a specific PPP phonebook entry and/or PPTP profile is described in section 7.5.

7.3.2 Create a Shortcut on your Desktop (Optional)


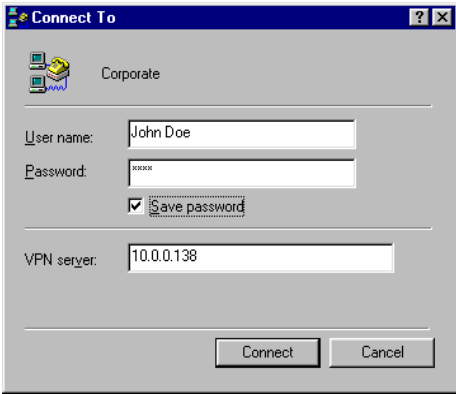


Introduction To work comfortably with the Dial-Up connection(s) you created, Windows 98 offers you the possibility to place a shortcut of the connection icon on your desktop.

Shortcut 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 The 'Dial-Up Networking' window pops up. 
3	Select the appropriate Dial-Up connection icon (in the example 'Corporate') and drag it to your desktop to create a copy of the icon.  Corporate

7.3.3 Open a PPPoA/PPTP Dial-Up Session

Procedure Proceed as follows:

Step	Action and Description
1	<p>Double-click the appropriate PPPoA/PPTP Dial-Up icon in the 'Dial-Up Networking' folder, or double-click its shortcut on your desktop.</p>  <p>Corporate</p> <p>The 'Connect To' window pops up</p> 
2	<p>Fill in your <i>user name</i> and <i>password</i>, according your user account at the ISP, or corporate.</p> <p>Note: If you want the current Dial-Up connection application to remember your credentials for future use, tick the 'Save Password' box (✓). Make sure though, that you have logged into Windows 98 when you boot your PC.</p>
3	<p>Click </p> <p>The 'Connecting To Corporate' window appears shortly before being minimized in the system tray.</p> 
4	Start your application now, e.g. a Web browser.

While you are connected


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



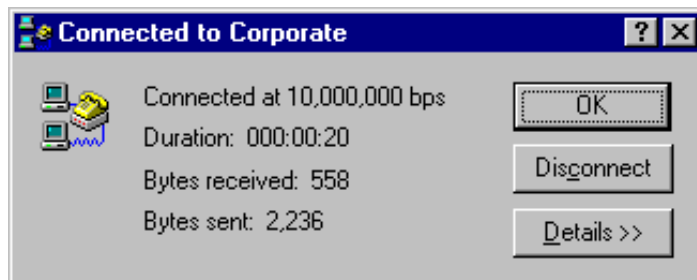
The MSDUN icon symbolizes activity on the PPPoA/PPTP connection by flashing PC(s):

- ▶ A flashing “Front” PC symbolizes upstream (Tx) link activity (from your local PC towards the remote device).
- ▶ A flashing “Behind” PC symbolizes downstream (Rx) link activity (from the remote device towards your PC).

The ‘Connected To’ window



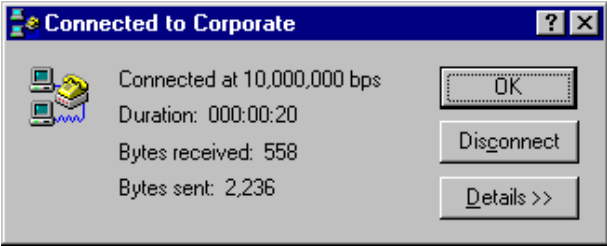

You can check the status of the connection by double-clicking the MSDUN icon  in the system tray.

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



7.3.4 Close a PPPoA/PPTP Dial-Up Session in Use

Procedure Proceed as follows:

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

Result The PPPoA/PPTP Dial-Up connection will no longer exist. The PPPoA/PPTP connection is idle, e.g. for other hosts.

7.4 PPPoA/PPTP Configuration

Introduction The **STWireless** allows local configuration via the **STWireless** web pages.

This section describes the configuration of PPPoA/PPTP entries, and how to use the '*PPTP*' web page.

In this section

Topic	See
PPPoA/PPTP Phonebook Entries	7.4.1
PPPoA/PPTP Active Connections	7.4.2

7.4.1 PPPoA/PPTP Phonebook Entries

PPTP phonebook entries

Basic to the **STWireless** VC pool management, is the 'Phonebook' web page.

The **STWireless** in its default state features the following PPP related phonebook entries:

Name	Address	Type	AutoPVC	Avail	Action
RELAY_PPP1	8.48	ppp	No	yes	Delete
RELAY_PPP2	8.49	ppp	No	yes	Delete
RELAY_PPP3	8.50	ppp	No	yes	Delete
RELAY_PPP4	8.51	ppp	No	yes	Delete
PPP1	8.64	ppp	No	no	Delete
PPP2	8.65	ppp	No	no	Delete
PPP3	8.66	ppp	No	yes	Delete
DHCP_SPOOF	8.67	ppp	No	no	Delete
Use input fields below to add a new entry					
<input type="text"/>	<input type="text"/>	any	-	-	Add

Note: Both PPPoA/PPTP and PPP & IP Routing share the same type of phonebook entries, i.e. **ppp**.

PPTP and PPP phonebook entries

As you notice, four phonebook entries exist, named *Relay_PPP*, which are free, and specifically suitable for PPPoA/PPTP, and four other phonebook entries, named *PPP*, and *DHCP_SPOOF*. Only use the latter in exceptional cases for PPPoA/PPTP service.

Adding/deleting phonebook entries

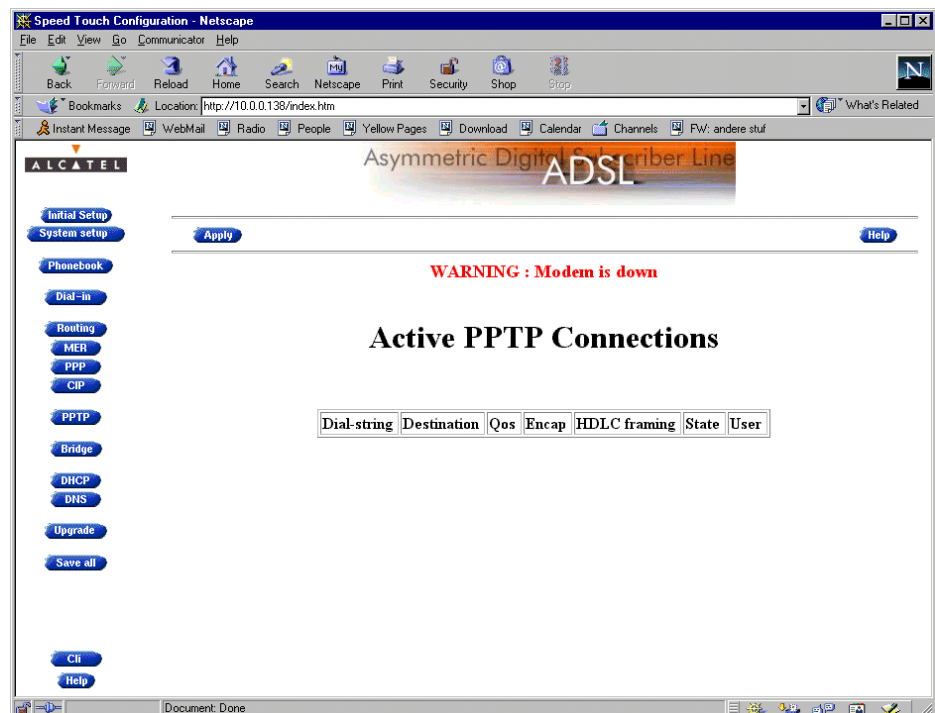
See section 10.2 for more information.

7.4.2 PPPoA/PPTP Active Connections

- In this subsection**
- ▶ The **STWireless** 'PPTP' Web Page
 - ▶ The 'Active PPTP Connections' Table
 - ▶ 'Active PPTP Connections' Table Components
 - ▶ Configuring PPTP Profiles

The STWireless 'PPTP' web page

Clicking **PPTP** in the left pane of the **STWireless** web pages, pops up the 'PPTP' web page (See section 18.2 for more information):



The 'Active PPTP Connections' table

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

Dial-string	Destination	Qos	Encap	HDLC framing	State	User
-------------	-------------	-----	-------	--------------	-------	------

'Active PPTP Connections' table components

The following fields are shown:

Field	Description
Dial-string	Indicates the name you have chosen for the PPTP connection. Note: In your Dial-Up application you are able to specify which PPTP connection is to be used by adding the appropriate Dial-string, indicated here.
Destination	Indicates the PPTP phonebook entry name, active for this connection.
Qos	Indicates the Quality of Service (QoS) applicable for the PPPoA/PPTP connection. In most cases the QoS column will indicate <code>default</code> . Via CLI a specific QoS can be configured.
Encap	Refers to the encapsulation, and decapsulation of PPP frames in/from AAL5/ATM. The STWireless is compliant with RFC 2364 "PPP over AAL5" and supports both the LLC/NLPID method and the VC-MUX method. By default the encapsulation method for PPP frames is VC-MUX. The encapsulation method for a PPPoA/PPTP connection can be configured via the CLI, see section 7.5 for more information.
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)": <div style="text-align: center;"> </div> Whereas the PPP format within a tunnel follows "Point-to-Point Tunneling Protocol (PPTP)": <div style="text-align: center;"> </div> 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".

Field	Description								
HDLC Framing (continued)	<p>In order to cope with these PPP frame differences, the STWireless adapts to the different formats on a 'per connection' base.</p> <p>Additionally, the STWireless offers the following PPP/AAL5 format configuration options via the CLI if interoperability problems should arise (See section 7.5 for more information):</p> <table border="1"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Never</td> <td>The STWireless 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 STWireless 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 STWireless will not change the PPP frame arriving via a tunnel.</td> </tr> </tbody> </table> <p>Note: This configuration possibility applies only to the upstream direction ! In the downstream direction, the STWireless will always make sure that FF-03 is in front of the frame prior to put it in a PPTP tunnel.</p>	Value	Description	Never	The STWireless 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.	Always	The STWireless 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.	Keep	The STWireless will not change the PPP frame arriving via a tunnel.
Value	Description								
Never	The STWireless 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.								
Always	The STWireless 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.								
Keep	The STWireless will not change the PPP frame arriving via a tunnel.								
State	<p>Indicates the connection state of the active PPTP connection. It can take following values:</p> <table border="1"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Resolving</td> <td>The PPTP entry is setting up the connection.</td> </tr> <tr> <td>Retry</td> <td>The PPTP entry did not succeed in connecting to the remote side, and is retrying.</td> </tr> <tr> <td>In Use</td> <td>A user opened a session on this PPTP entry.</td> </tr> </tbody> </table>	Value	Description	Resolving	The PPTP entry is setting up the connection.	Retry	The PPTP entry did not succeed in connecting to the remote side, and is retrying.	In Use	A user opened a session on this PPTP entry.
Value	Description								
Resolving	The PPTP entry is setting up the connection.								
Retry	The PPTP entry did not succeed in connecting to the remote side, and is retrying.								
In Use	A user opened a session on this PPTP entry.								
User	Indicates the IP address of the host, i.e. PC, using this PPTP connection								

Configuring PPTP profiles

PPTP profiles can be configured via the CLI.
See section 7.5 for more information.

7.5 Customizing PPPoA/PPTP Connections

Introduction In this section the advanced configuration and use of PPPoA/PPTP connections is described.
Firstly, this section deals with some concepts on the customization of PPPoA/PPTP connections.

In this section

Topic	See
PPTP Phonebook Entries	7.5.1
Single Destination	7.5.2
Multiple Destinations	7.5.3
Restrictions of Using Specific Virtual Channels	7.5.4
PPTP Profiles	7.5.4

7.5.1 PPPoA/PPTP Phonebook Entries

Introduction To establish a PPPoA/PPTP session, all you need to do is opening a PPTP tunnel.
However, this does only apply in the case only a single destination is reachable via one, or more VCs.
With the **STWireless**, it is possible to open multiple simultaneous sessions, or even simultaneously open sessions to multiple destinations.

Customizing PPPoA/PPTP entries Via the **STWireless** 'Phonebook' web page, you are able to add PPP phonebook entries in addition to the defaults.
You can give them names of your choice (in the name field). See section 7.4 for more information.

Using added phonebook entries The name you gave the PPTP phonebook entries in the **STWireless**'s phonebook can be used to specify which PPPoA/PPTP VC is to be issued by a particular PPTP connection icon.

PPPoA/PPTP session scenarios The PPPoA/PPTP entries can be used in several ways:

- ▶ (All) directed to a single destination
- ▶ Directed to specific destinations.

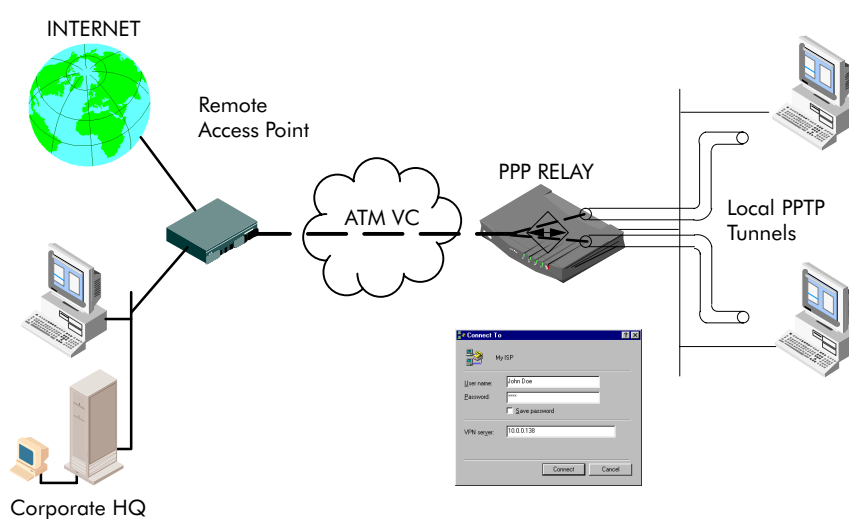
7.5.2 Single Destination

Single destination PPPoA/PPTP sessions

If the 'VPN Server' field of the PPTP Dial-Up application is left unchanged, i.e. only the IP address of the **STWireless** (or its host name) is visible, the **STWireless** automatically chooses a free PPP phonebook entry from the Phonebook.

This is the most easy scenario and works best if all (one, or more) PPPoA/PPTP related PPP VCs are attached to the same remote destination.

Single destination architecture



Two scenarios Two scenarios are possible:

▶ **Single PPP VC to a single destination**

In this scenario, the SP supplied one PPP VC for connectivity. It is most applicable when a single PC is connected to the **STWireless**.

▶ **Multiple PPP VCs to single destination**

In this scenario, the SP supplied multiple PPP VCs, all direct to the same destination. This implies that several PCs can connect to this destination at the same time (as long there is an idle channel left). Therefore, this is most applicable with a **STWireless** connected to a (W)LAN.

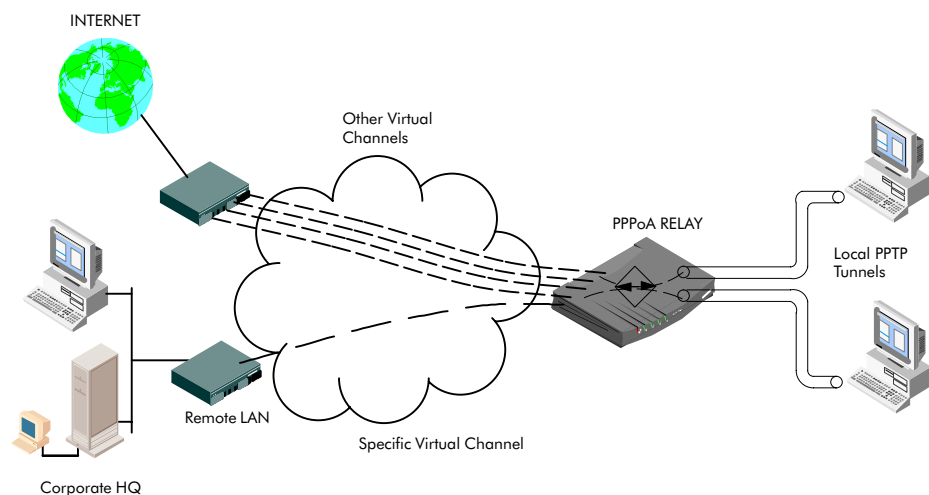
7.5.3 Multiple Destinations

Multiple destination PPPoA/PPTP sessions

Multiple SPs might be connected to your **STWireless**, e.g., your private ISP and your corporate.

In this case, the **STWireless**'s PPP VCs can be split over both locations. For example, 6 PPP VCs could be provisioned to your ISP, while 6 other PPP VCs are used for connecting to your corporate.

Multiple destination architecture



Procedure to specify a VC for a PPTP connection icon

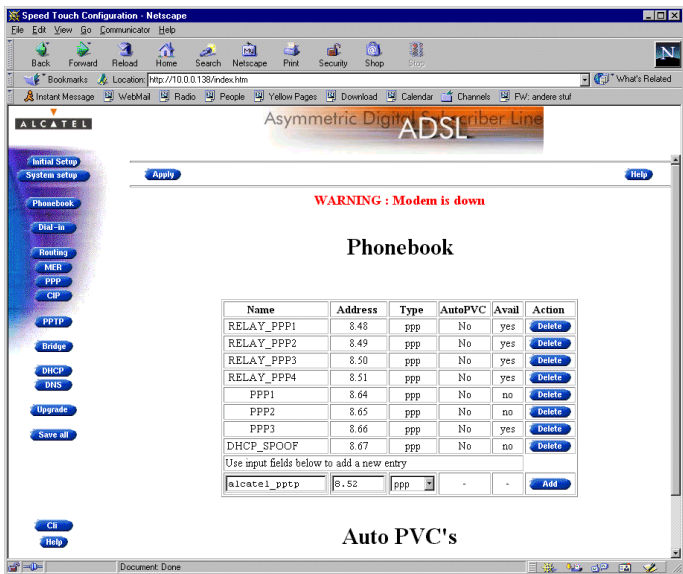
Proceed as follows to specify which VC (i.e. Phonebook entry) is to be used by a Dial-Up connection:

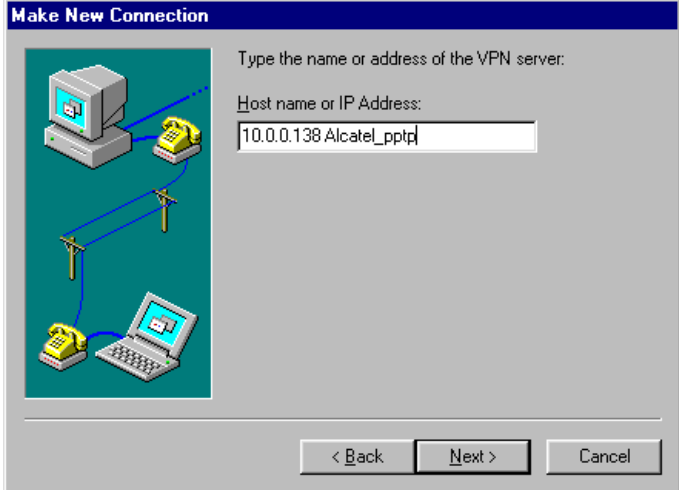
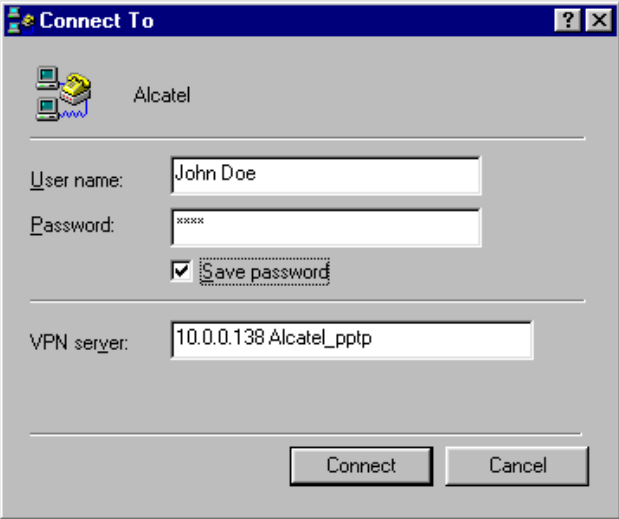
Step	Action
1	Add, if needed, a PPP phonebook entry to the STWireless 's phonebook with the appropriate VPI/VCI values for the specific destination.
2	When creating a new PPTP tunnel configuration, add this PPP VC phonebook name next to the IP address, or DNS name of the VPN server (i.e. the STWireless).

Result If you open this PPPoA/PPTP session, it will use the PPP Phonebook entry, specified in the VPN server field.

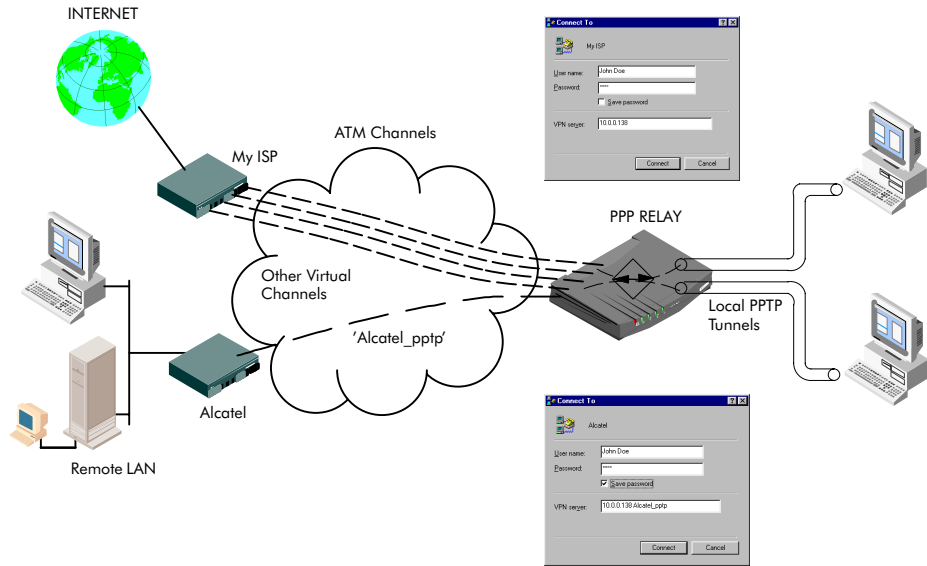
Note You must check with your ISP and your corporate LAN administrator to verify which cross-connections exist between the PPP VCs and the locations.

Example for Windows 9x Proceed as follows to create an MS Windows 9x Dial-Up Networking icon to the corporate 'Alcatel', which has to use the VC, named 'Alcatel_pptp':

Step	Action and Description																																																												
1	<p>Configure a PPP phonebook entry, named 'Alcatel_pptp', in the Phonebook as described in subsection 7.4.1.</p>  <p>The screenshot shows the 'Speed Touch Configuration - Netscape' window. The 'Phonebook' section is active, displaying a table of entries:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Address</th> <th>Type</th> <th>AutoPVC</th> <th>Avail</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>RELAY_PPP1</td> <td>8.48</td> <td>ppp</td> <td>No</td> <td>yes</td> <td>Delete</td> </tr> <tr> <td>RELAY_PPP2</td> <td>8.49</td> <td>ppp</td> <td>No</td> <td>yes</td> <td>Delete</td> </tr> <tr> <td>RELAY_PPP3</td> <td>8.50</td> <td>ppp</td> <td>No</td> <td>yes</td> <td>Delete</td> </tr> <tr> <td>RELAY_PPP4</td> <td>8.51</td> <td>ppp</td> <td>No</td> <td>yes</td> <td>Delete</td> </tr> <tr> <td>PPP1</td> <td>8.64</td> <td>ppp</td> <td>No</td> <td>no</td> <td>Delete</td> </tr> <tr> <td>PPP2</td> <td>8.65</td> <td>ppp</td> <td>No</td> <td>no</td> <td>Delete</td> </tr> <tr> <td>PPP3</td> <td>8.66</td> <td>ppp</td> <td>No</td> <td>yes</td> <td>Delete</td> </tr> <tr> <td>DHCP_SPOOF</td> <td>8.67</td> <td>ppp</td> <td>No</td> <td>no</td> <td>Delete</td> </tr> </tbody> </table> <p>Below the table, the 'Auto PVC's' section shows a form for adding a new entry:</p> <p>Use input fields below to add a new entry</p> <table border="1"> <tr> <td>alcatel_pptp</td> <td>8.52</td> <td>ppp</td> <td>-</td> <td>-</td> <td>Add</td> </tr> </table>	Name	Address	Type	AutoPVC	Avail	Action	RELAY_PPP1	8.48	ppp	No	yes	Delete	RELAY_PPP2	8.49	ppp	No	yes	Delete	RELAY_PPP3	8.50	ppp	No	yes	Delete	RELAY_PPP4	8.51	ppp	No	yes	Delete	PPP1	8.64	ppp	No	no	Delete	PPP2	8.65	ppp	No	no	Delete	PPP3	8.66	ppp	No	yes	Delete	DHCP_SPOOF	8.67	ppp	No	no	Delete	alcatel_pptp	8.52	ppp	-	-	Add
Name	Address	Type	AutoPVC	Avail	Action																																																								
RELAY_PPP1	8.48	ppp	No	yes	Delete																																																								
RELAY_PPP2	8.49	ppp	No	yes	Delete																																																								
RELAY_PPP3	8.50	ppp	No	yes	Delete																																																								
RELAY_PPP4	8.51	ppp	No	yes	Delete																																																								
PPP1	8.64	ppp	No	no	Delete																																																								
PPP2	8.65	ppp	No	no	Delete																																																								
PPP3	8.66	ppp	No	yes	Delete																																																								
DHCP_SPOOF	8.67	ppp	No	no	Delete																																																								
alcatel_pptp	8.52	ppp	-	-	Add																																																								

Step	Action and Description
2	<p>Create a Dial-Up Networking icon, named 'Alcatel', according to section 7.3.1.</p> <p>In step 9 of the procedure (See section 7.3.1), you not only specify the VPN server, i.e. the STWireless, but also the VC 'Alcatel_pptp':</p> 
3	<p>Double-click the 'Alcatel' icon to open the PPPoA/PPTP session. The following Dial-Up window pops up:</p>  <p>As you can see in the 'VPN Server' field, the VC, i.e. alcatel_pptp, to be used is specified by its name. Consequently, this PPPoA/PPTP session will always use this VC for establishing a connection to the corporate 'Alcatel'.</p>

Example Result The following figure shows an example of both single and multiple PPPoA/PPTP connections established simultaneously.



7.5.4 Restrictions on Using Specific Virtual Channels

Similar phonebook names The **STWireless** will look for a match between the string, specified next to the VPN server's DNS hostname or IP address (in the previous example the string 'Alcatel_pptp').

If however, several PPPoA/PPTP entries exist, with names starting with the same string, e.g. Alcatel_pptp1, Alcatel_pptp2, etc., it can not be determined which of these will be used to establish the connection.

Positive use of similar names This can be used in a positive way however: if a selection of PPPoA/PPTP VCs may be used by a particular PPPoA/PPTP session, you just have to give them names with a stringmatch in the beginning, e.g. 'Alcatel_pptpX' ,where X is a number.

Case of no entry matches In case no match is found in the **STWireless** phonebook, or if the specified VC is already used, the Dial-Up application will use the first available idle PPPoA/PPTP VC found in the '*PPTP connections*' table.

Consequently, again it can not be determined which PPPoA/PPTP VC will be used to establish the connection.

7.5.5 PPTP Profiles

Introduction In most cases, the **STWireless**'s PPP phonebook entries are ideally suited to make PPPoA/PPTP connections over the ADSL line.

However, in case the remote access server demands specific configurations for PPPoA/PPTP, you can easily configure a PPTP profile via the CLI.

PPTP profile selections By default a 'default' profile exists, applicable for all PPP phonebook entries. This default profile inhibits the following settings:

- ▶ Encapsulation method : VC-MUX
- ▶ HDLC framing : never
- ▶ QoS : default.

Creating a PPTP Profile A PPTP Profile can only be created and configured via the CLI. See chapter 19 for more information on the CLI.

7.6 Advanced PPPoA/PPTP Concepts

Introduction This section describes some advanced concepts of the **STWireless**'s PPPoA-to-PPTP Relaying packet service.

Topics

Topic	See
Point-to-Point Tunneling	7.6.1
Local Tunneling	7.6.2
PPPoA-to-PPTP Relaying (PPPoA/PPTP)	7.6.3
Simultaneous PPPoA/PPTP Sessions	7.6.4

7.6.1 Point-to-Point Tunneling

What is Tunneling Tunneling is a technique that allows to transport certain protocols over a network, which is not designed for that purpose.

Example: IPX Packets can be wrapped in IP, ready to be routed over an IP network.

At the destination, the IPX packets are decapsulated and made available in their original format again.

Tunneling applied to the STWireless Tunneling applied to the **STWireless** implies that:

- ▶ Tunnels have a local scope.
Indeed, tunnels are established between two peers on the local IP network: local PCs initiate tunnels, the **STWireless** terminates these tunnels.
 - ▶ IP tunnels are established and released for the duration of a session.
 - ▶ The protocol carried inside the tunnels is PPP. However, various protocols can be carried inside the PPP frames.
-

Result of PPTP tunneling The net result of PPTP tunneling is that PPP frames can cross the local Ethernet segment between the **STWireless** and the client computer and vice versa.

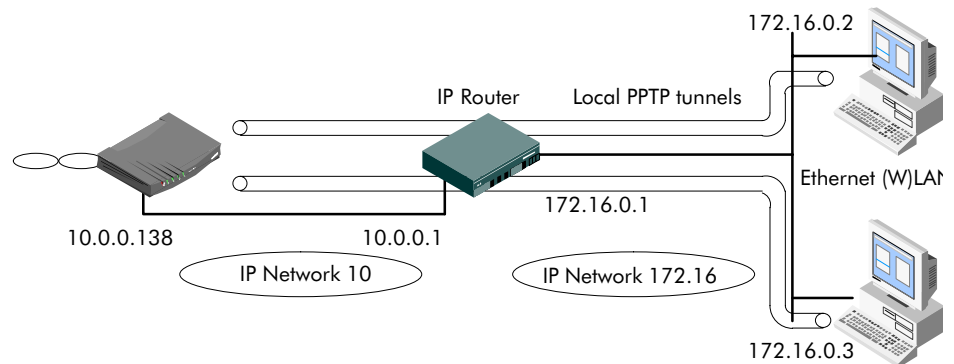
This would otherwise not be possible as PPP is designed to run on point-to-point connections, e.g. Dial-Up connections, whereas Ethernet is a shared medium.

Supported (W)LAN Protocols Within PPP, all kinds of protocols can be transported. The PPP/PPTP client, however, is the limiting factor. Some OSs only allow specific protocols to be transported within PPP tunnels (e.g. TCP/IP, IPX/SPX, or NETBEUI in case of Window 9x).

7.6.2 Local Tunneling

Tunneling from behind an IP router

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




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

STWireless You must add a default route for the **STWireless** via the 'Routing' web page (See subsection 11.4.2 for more information).

In the example of the above figure, 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 **STWireless**. Proceed as follows for a Windows OS:

Step	Action and Description
1	Click  , select 'Programs', and 'MS-DOS' prompt.
2	At the DOS prompt, enter: <code>route add <Destination IPaddress> <Gateway IPaddress></code> In the example of the previous figure, the command would be: <code>route add 10.0.0.138 172.16.0.1</code>
3	To verify IP connectivity, you can ping the STWireless . If it responds, setting up PPTP tunnels is possible.

7.6.3 PPPoA-to-PPTP Relaying (PPPoA/PPTP)

What is PPPoA-to-PPTP Relaying

By opening a PPPoA/PPTP session, PPTP tunnels are established between the **STWireless** and the PCs on your (W)LAN.

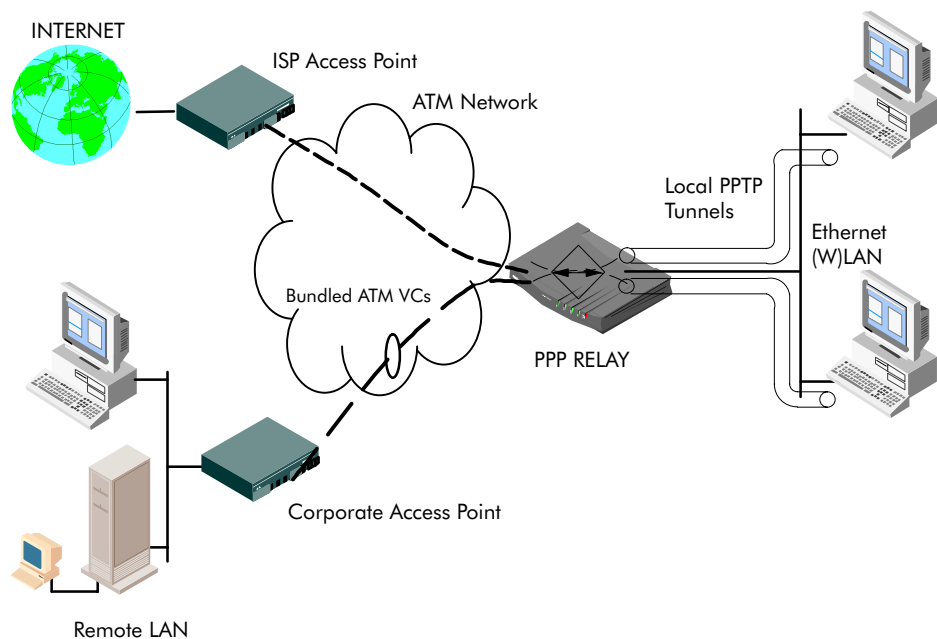
These PPTP tunnels trigger the Relaying utility of the **STWireless**: it chooses a free VC from the pool of available free PPP phonebook entries and relays all PPP frames, sourced by the PPTP tunnel from the tunnel to the VC, and vice versa.

At the remote end of the VC, i.e. ADSL line, the remote access server extracts the PPP frames, reconstructs the encapsulated IP packets and forwards them to their destination, e.g. the Internet.

At the end of a PPPoA/PPTP session, the PPTP tunnel is destroyed. This triggers the **STWireless's** Relay utility to release the VC.

PPPoA/PPTP overview architecture

The figure below provides an overview of the end-to-end architecture.



7.6.4 Simultaneous PPPoA/PPTP Sessions

Upper limit of simultaneous PPPoA/PPTP sessions

PPTP tunneling does not influence your local communication; you can add as many hosts as your local network supports.

However, there is an upper limit to the number of simultaneous outbound connections. Unlike Bridging, or MER, a PPPoA/PPTP related VC cannot be shared by multiple users. A user establishing a tunnel requires at least one PPPoA/PPTP related VC.

Therefore, any user on the local network can only initiate tunnels as long as there are idle PPPoA/PPTP VCs, i.e. idle PPTP phonebook entries.

STWireless and simultaneous connections

By disabling all other packet service entries in the **STWireless** Phonebook, the **STWireless** is capable of managing up to 12 simultaneous PPPoA/PPTP VCs.

If all PPPoA/PPTP VCs are in use, and a user tries to set-up a new tunnel, the **STWireless** will refuse the request and an error message will appear on the screen.

8 Data Services – PPP & IP Routing

Introduction The **STWireless** features the PPP & IP Routing packet service. Via the PPP protocol an authenticated session is established with your SP. IP packets, arriving over the PPP connection, are forwarded by the IP router to PCs on your (W)LAN. Optionally, Network Address & Port Translation (NAPT) can be enabled to isolate your local network from the Internet, or to share a single IP address.

In this chapter

Topic	See
Preparatory Steps	8.1
Using PPP & IP Routing	8.2
PPP Configuration	8.3
PPP Entry Configuration	8.4

8.1 Preparatory Steps

- Features** PPP & IP Routing:
- ▶ Has an authenticated session concept: it supports identification, authentication and autoconfiguration.
 - ▶ Requires no session client on the PC(s), avoiding special installation procedures
 - ▶ Combined with NAPT, allows multiple users to share a single IP address simultaneously on a single VC
 - ▶ Supports up to 12 concurrent virtual channels for PPP.
-

- What you should know in advance**
- ▶ The **VPI/VCI** value of the VC(s) to use on the ADSL line
 - ▶ **PPPoA connection service** must be supported on this VC
 - ▶ User name and password for your **user account**.
- Note:** If connectivity to multiple remote organizations is required, you need additional sets of these parameters.
-

- STWireless** The **STWireless** comes with eight phonebook entries available for PPP & IP Routing, of which three are preconfigured for immediate use.
- If the SP(s) impose settings which differ from the **STWireless** defaults, perform the necessary adjustments via the **STWireless** web pages.
- See sections 8.3 and 8.4 for more information.
-

- PC(s)** In order to use the PPP & IP Routing mode of the **STWireless**, the OS on your PC(s) must support the TCP/IP suite.
- See chapter 11 for more information on IP.
-

8.2 Using PPP & IP Routing

Always-on, Dial-in and Dial-on-Demand PPP sessions

Three methods exist to open a PPP:

▶ **Dial-in**

The PPP session is opened manually

▶ **Always-on**

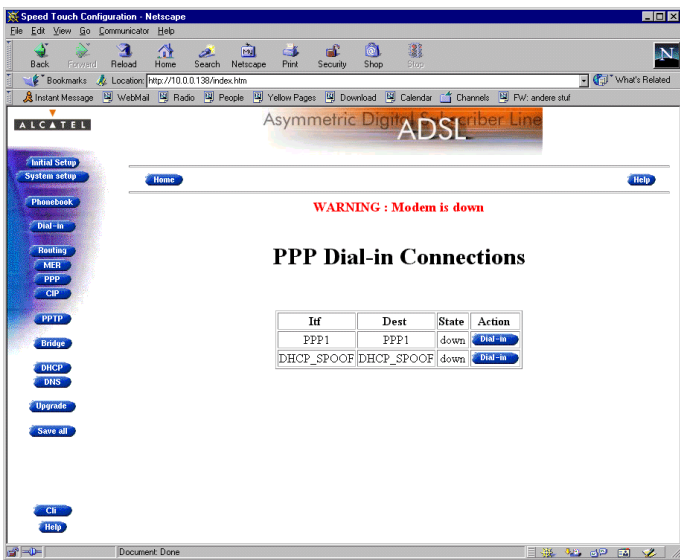
After the **STWireless** is powered and finished its POST successfully, the **STWireless** automatically tries to open the PPP session

▶ **Dial-on-demand**

The PPP session is opened automatically, triggered by the arrival of packets at a/the **STWireless** Ethernet port, destined for a PPP connection.

Opening dial-in PPP sessions

Proceed as follows (See section 18.2 for more information):

Step	Action and Description
1	Browse to the 'Dial-in' web page: 
2	Click Dial-in next to a PPP entry in the list.

Step	Action and Description
3	<p>If applicable the 'Authentication' web page pops up: Enter user name and password in the appropriate fields.</p> <div style="border: 1px solid black; padding: 10px; width: fit-content; margin: 10px auto;"> <p style="text-align: center;">Authentication</p> <p>User : <input type="text" value="John Doe"/></p> <p>Password : <input type="password" value="*****"/></p> <p>Save password : <input type="checkbox"/></p> </div>
4	Click Apply .
5	<p>After identification and authentication, the 'PPP connections' web page reappears.</p> <p>While the STWireless 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.</p> <p>Note: "Always-on" PPP connections will not appear in this table.</p>

Closing dial-in PPP sessions

Proceed as follows:

Step	Action and Description
1	Browse to the 'Dial-in' web page.
2	<p>Active PPP sessions are indicated via up in the 'State' field.</p> <p>Click Hang-Up next to the PPP entry you want to close the session for.</p> <p>The session state of the PPP entry will change to down, i.e. it becomes idle.</p>

Saving credentials

If you want the **STWireless** to remember your credentials, check 'Save password' (✓) in the 'Authentication' web page.

See subsection 8.4.4 for more information.

8.3 PPP Configuration

Introduction The **STWireless** allows local configurations via its web pages. This section describes the enabling of PPP entries, and the use of the 'PPP' web page.

Prior to be able to use the PPP entry, you must configure the PPP entry. This is described in section 8.4.

In this section

Topic	See
PPP Phonebook Entries	8.3.1
PPP Entries	8.3.2

8.3.1 PPP Phonebook Entries

PPP phonebook entries Central to the **STWireless** VC pool management, is the 'Phonebook' web page.

The **STWireless** in its default configuration features the following PPP related phonebook entries:

Name	Address	Type	AutoPVC	Avail	Action
RELAY_PPP1	8.48	ppp	No	yes	Delete
RELAY_PPP2	8.49	ppp	No	yes	Delete
RELAY_PPP3	8.50	ppp	No	yes	Delete
RELAY_PPP4	8.51	ppp	No	yes	Delete
PPP1	8.64	ppp	No	no	Delete
PPP2	8.65	ppp	No	no	Delete
PPP3	8.66	ppp	No	yes	Delete
DHCP_SPOOF	8.67	ppp	No	no	Delete
Use input fields below to add a new entry					
<input type="text"/>	<input type="text"/>	any	-	-	Add

Note: Both PPP & IP Routing and PPPoA/PPTP share the same type of phonebook entries, i.e. **ppp**.

Adding/deleting phonebook entries

See section 10.2 for more information.

8.3.2 PPP Entries

- In this subsection**
- ▶ The 'PPP' Web Page
 - ▶ The 'PPP Configuration' Table
 - ▶ 'PPP Configuration' Table Components
 - ▶ Adding PPP Entries
 - ▶ Deleting PPP Entries.

The 'PPP' web page Clicking **PPP** in the left pane of the **STWireless** web pages, pops up the 'PPP' web page (See section 18.2 for more information):

The screenshot shows a Netscape browser window titled "Speed Touch Configuration - Netscape". The address bar shows "http://10.0.0.138/index.htm". The main content area displays the "ALCATEL" logo and "Asymmetric Digital Subscriber Line ADSL". A navigation menu on the left includes options like "Initial Setup", "System setup", "Phonebook", "Dial-in", "Routing", "MER", "PPP", "CIP", "PPTP", "Bridge", "DHCP", "DNS", "Upgrade", "Save all", "Cli", and "Help". The "PPP" option is highlighted. The main content area shows a "WARNING : Modem is down" message and the "PPP Configuration" section. Below this is a table with columns: If, Dest, Mode, Link, State, and Action. The table contains three entries: PPP1, PPP2, and DHCP_SPOOF. Below the table is a form to add a new entry with a dropdown menu set to "RELAY_PPP1" and an "Add" button.


If	Dest	Mode	Link	State	Action
PPP1	PPP1	dial-in	idle	down	Config Delete
PPP2	PPP2	always-on	connected	down	Config Delete
DHCP_SPOOF	DHCP_SPOOF	dial-in	idle	down	Config Delete

Use input fields below to add a new entry

RELAY_PPP1

The 'PPP configuration' table

The following figure shows the 'PPP Configuration' table of the 'PPP' web page:

Itf	Dest	Mode	Link	State	Action
PPP1	PPP1	dial-in	idle	down	Config Delete
PPP2	PPP2	always-on	connected	down	 Config Delete
DHCP_SPOOF	DHCP_SPOOF	dial-in	idle	down	Config Delete






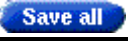










Use input fields below to add a new entry

<input type="text"/>	<input type="text" value="PPP3"/>	-	Add
----------------------	-----------------------------------	---	---------------------

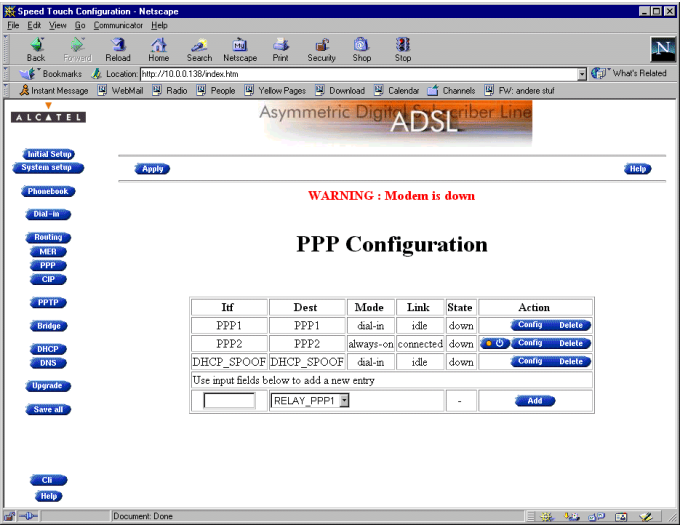



'PPP Configuration' table components

The following fields are shown:

Field	Description						
<i>Itf</i>	Allows you to choose an interface name for the PPP interface. Note: In most cases, the interface name will be the same as the phonebook entry name.						
<i>Dest</i>	Indicates available phonebook entries for PPP. Note: Specific free PPPoA/PPTP phonebook entries are shown, as well as free 'any type' phonebook entries						
<i>Mode</i>	Indicates whether the PPP connection is: <ul style="list-style-type: none"> • An "Always-on" connection • A "Dial-in" connection • A "Dial-on-Demand" connection. See section 8.4.5 for more information.						
<i>Link</i>	Indicates the link state of the PPP entry. It can take following values: <table border="1" data-bbox="754 1487 1375 1700"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <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> </tbody> </table>	Value	Description	idle	The PPP entry is not activated, i.e. it does not setup a PPP connection.	Connected	The PPP entry is active, i.e. it tries to setup a PPP connection, or PPP connectivity is achieved.
Value	Description						
idle	The PPP entry is not activated, i.e. it does not setup a PPP connection.						
Connected	The PPP entry is active, i.e. it tries to setup a PPP connection, or PPP connectivity is achieved.						

Field	Description														
State	<p>Indicates the active state of the PPP session.</p> <p>It can take following values:</p> <table border="1"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <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> </tbody> </table>	Value	Description	Up	The PPP session is opened and active.	Down	The PPP session is closed, the PPP connection is idle.	Trying	The PPP session is trying to reach the active state.						
Value	Description														
Up	The PPP session is opened and active.														
Down	The PPP session is closed, the PPP connection is idle.														
Trying	The PPP session is trying to reach the active state.														
Action	<p>This field contains the three following action buttons:</p> <table border="1"> <thead> <tr> <th>Button</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td></td> <td>Add a PPP entry to the list.</td> </tr> <tr> <td></td> <td>Delete an existing entry from the list.</td> </tr> <tr> <td></td> <td>Configure the PPP entry. See subsection 8.4 for more.</td> </tr> </tbody> </table> <p>For always-on PPP entries, also an on/off button is included:</p> <table border="1"> <thead> <tr> <th>Button</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td></td> <td>The always-on PPP connection is enabled, i.e. activated.</td> </tr> <tr> <td></td> <td>The always-on PPP connection is disabled, i.e. not active.</td> </tr> </tbody> </table> <p>Clicking the button activates/deactivates the always-on PPP connection.</p> <p>Click  to make the on/off change permanent</p>	Button	Action		Add a PPP entry to the list.		Delete an existing entry from the list.		Configure the PPP entry. See subsection 8.4 for more.	Button	Action		The always-on PPP connection is enabled, i.e. activated.		The always-on PPP connection is disabled, i.e. not active.
Button	Action														
	Add a PPP entry to the list.														
	Delete an existing entry from the list.														
	Configure the PPP entry. See subsection 8.4 for more.														
Button	Action														
	The always-on PPP connection is enabled, i.e. activated.														
	The always-on PPP connection is disabled, i.e. not active.														



Adding PPP entries Proceed as follows:

Step	Action and Description
1	Browse to the 'PPP' web page:  The bottom row of the table allows addition of a new entry.
2	In the 'Destination' column of the bottom row, click  and select the PPP entry you want to add to the table.
3	Optionally, enter a name for the PPP interface in the 'If' column.
4	Click  and  to finish the procedure.

Result The PPP entry is added to the 'PPP Configuration' table. Prior to be able to open a PPP session on this PPP entry, you **MUST** configure the PPP entry.

See section 8.4 for more information.

Deleting PPP entries Proceed as follows:

Step	Action and Description
1	Browse to the 'PPP' web page.
2	Select the PPP connection you want to delete, click  and  to finish the procedure.

8.4 PPP Entry Configuration

Introduction After enabling the PPP entry in the 'PPP Configurations' table, you must configure the PPP connection.

Configuration of PPP entries must be done per PPP entry.

This section describes the various PPP entry configurations the *Pro* offers for assuring end-to-end connectivity.

In this section

Topic	Section
The PPP Configuration Web Page	8.4.1
Link Related Configuration	8.4.1
Security Related Configuration	8.4.3
IP Routing Related Configuration	8.4.4
Connection Related Configuration	8.4.5
NAPT and PPP & IP Routing	8.4.6
NAPT and STWireless Transparency	8.4.7

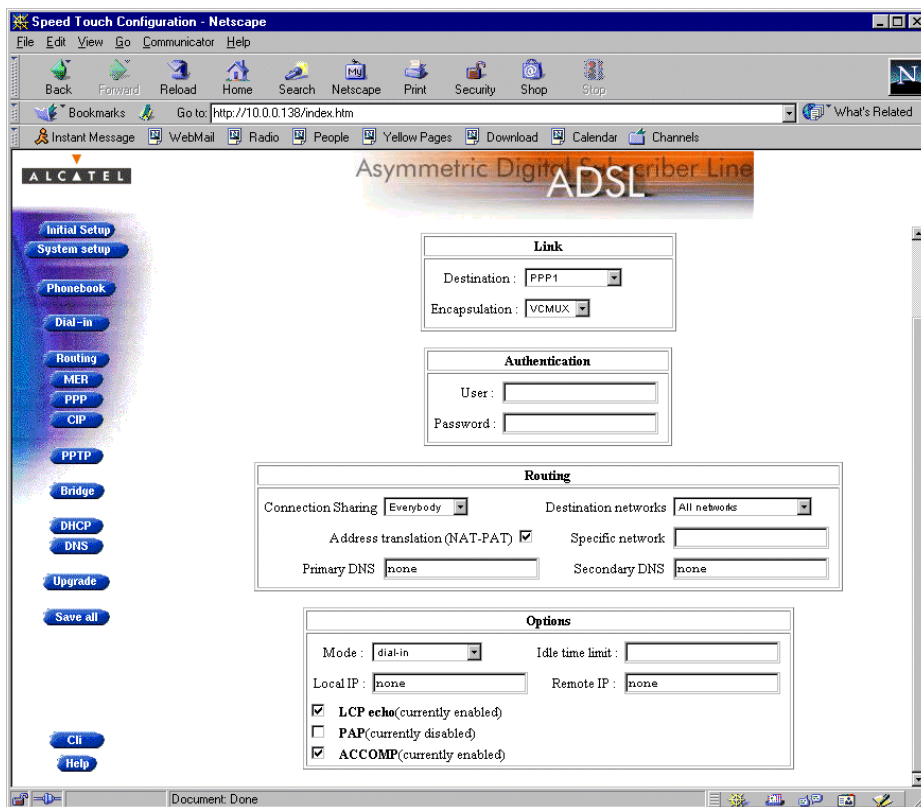
Interaction with the STWireless IP router Most of the configurations described in this section, influence the IP router in the **STWireless**.

See section 11.4, and subsection 11.2.4 for more information on IP routing aspects.

8.4.1 The PPP Configuration Web Page

PPP configuration web page

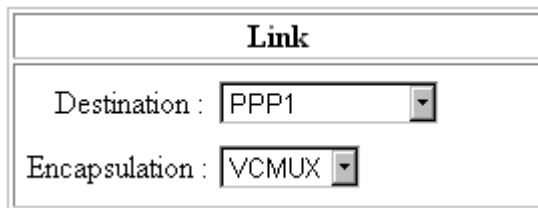
Clicking **Config** next to a PPP connection you want to configure, pops up the particular 'PPP Configuration' web page:



8.4.2 Link Related Configuration

Introduction The following options allow to configure the link related aspects of your PPP connection.

'Link' box Following figure shows the '*Link*' box:



The image shows a configuration window titled "Link". Inside the window, there are two dropdown menus. The first is labeled "Destination:" and has "PPP1" selected. The second is labeled "Encapsulation:" and has "VCMUX" selected.

Destination networks The '*Link*' box contains the following fields:

- ▶ **Destination**
Displays the PPP phonebook entry for the PPP connection.
Click to select another free PPP phonebook entry for the PPP connection.
- ▶ **Encapsulation**
Allows you to select the encapsulation method for the PPP connection, i.e. VC-MUX (default), or LLC/NLPID.

8.4.3 Security Related Configurations

Introduction In most cases you will have a user account, with user name and password, at the SP.
Via the 'Authentication' box in the 'PPP Configuration' web page, you can fill out your credentials for permanent storage.

'Authentication' box Following figure shows the 'Authentication' box:



The image shows a screenshot of a web form titled "Authentication". It contains two input fields. The first field is labeled "User:" and contains the text "guest". The second field is labeled "Password:" and contains seven asterisks "*****".

"Guest" credentials As default, the user account "guest" is assumed (Both user name and password are 'guest').
If your SP has a guest account, you are able to open a session without having an actual subscription.

Memorizing Credentials The **STWireless** is able to memorize user name, and password per PPP connection; just fill out both, and click **Save all**.
The next time you establish this PPP connection, the information is retrieved from permanent storage.

Note: Leaving the entries free, forces you to identify and authenticate yourself each time the session is opened.

8.4.4 IP Routing Related 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 **STWireless**'s routing table. The settings in the PPP '*IP Routing*' box, are reflected in the routing table.

Advanced routing For advanced users, the **STWireless** allows manual configuration of permanent routes to dedicated destinations. See section 11.4 for more information on the **STWireless**'s 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 19 for more information on the CLI.

- In this subsection**
- ▶ '*Routing*' box
 - ▶ Connection Sharing
 - ▶ Connection Sharing Subnet Values
 - ▶ 'My net only' Configuration
 - ▶ Destination Networks
 - ▶ Destination Networks Subnet Values
 - ▶ Primary and Secondary DNS Server.

'Routing' box The following figure shows the '*Routing*' input box:

Routing			
Connection Sharing	Everybody <input type="button" value="v"/>	Destination networks	All networks <input type="button" value="v"/>
Address translation (NAT-PAT) <input checked="" type="checkbox"/>		Specific network	<input type="text"/>
Primary DNS	none <input type="text"/>	Secondary DNS	none <input type="text"/>

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 connection.

Three options are available:

▶ **Only Me**

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

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 connection to your corporate as their gateway to the Internet.

▶ **Everybody**

All PC(s) on the local (W)LAN can forward frames over this PPP connection. 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 connection. In this way they are not required to open a session themselves.

▶ **My net only**

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

Connection sharing subnet values

The following table lists the used 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	255.255.255.0 (default) This value depends on the subnet mask in use.	/*

'My net Only' configuration

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

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

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

Destination networks

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

Four options are available:

▶ **All networks**

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

▶ **Remote net only**

A PPP connection 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 **STWireless** routing table are forwarded over this PPP connection. 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 connection. Only if the destination IP address of a packet matches with this entry, the packet is forwarded over this PPP connection.

**Destination networks
subnet values**

The following table lists the used 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.	/*

**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 **STWireless** will negotiate these addresses with the remote side of the PPP connection. If these fields are left blank, the remote side will supply the IP addresses of the primary and secondary DNS servers.

See chapter 12 for more information on DNS.

8.4.5 Connection Related Configuration

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

- In this subsection**
- ▶ 'Options' box
 - ▶ Mode: Triggering of a PPP Session
 - ▶ Idle Time Limit
 - ▶ Local and/or Remote IP: **STWireless** PPP Client/Server Behavior
 - ▶ LCP Echo (✓) Requests
 - ▶ PAP (✓): Authentication Protocols
 - ▶ ACCOMP (✓): PPP Framing

'Options' box Following figure shows the 'Options' input box:


Options	
Mode : <input type="text" value="dial-in"/>	Idle time limit : <input type="text"/>
Local IP : <input type="text" value="none"/>	Remote IP : <input type="text" value="none"/>
<input checked="" type="checkbox"/> LCP echo (currently enabled) <input type="checkbox"/> PAP (currently disabled) <input checked="" type="checkbox"/> ACCOMP (currently enabled)	

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  next to the PPP connection in the 'Dial-in' web page.

▶ **Always-on**

After the **STWireless** is powered and finished its POST successfully, the **STWireless** automatically tries to open a PPP session for the PPP connection.

▶ **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 **STWireless** Ethernet port, to be sent over the PPP connection.

Note: By default one PPP connection is configured as 'Dial-in' (i.e. PPP1), and 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: STWireless PPP server/client behavior

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

Typically at the client side, the *Local IP*, and *Remote IP* boxes are left empty. This forces the client to ask the remote server for addresses.

In case you want to set up the **STWireless** 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 **STWireless** 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.

LCP echo (✓) requests

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

This checkbox allows to turn on/off LCP echo request/replies by respectively setting (✓), or clearing the flag.

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 default PPP authentication protocol is Challenge Handshake Authentication Protocol (CHAP).

Setting the PAP flag (✓) will use Password Authentication Protocol (PAP) instead.

ACCOMP (✓): used PPP framing

Address and Control field COMPression (ACCOMP), sometimes abbreviated as ACCM, is by default enabled, i.e. flagged (✓).

This option flag should not be cleared, except in special circumstances, i.e. where the remote PPP server expects to see HDLC like framing (FF03 imposed to the PPP packet).

8.4.6 NAPT and PPP & IP Routing

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 NAPT.

NAPT and supported protocols

All supported protocols that are NAPT insensitive, pass transparently through NAPT.

In addition, the **STWireless** supports also the following protocols as NAPT insensitive:

- ▶ All generic TCP/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).
-

Configuration of NAPT

You can enable/disable NAPT via the 'PPP Configuration' web page per PPP entry.

In the 'Routing' box (See subsection 8.4.4) it is possible to set/unset the NAT flag (✓).

Advanced NAPT can be configured via the CLI. See chapter 19 for more information.

NAT/PAT and STWireless transparency

The NAPT feature comes at the expense of the **STWireless** transparency. For consequences and solutions, see subsection 8.4.7.

8.4.7 NAPT and STWireless Transparency

NAPT and STWireless transparency

As described in subsection 8.4.6, the **STWireless** can perform NAPT to decouple your local IP addresses from the public IP address negotiated during a PPP session.

However, this feature comes at the expense of the **STWireless** 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.

In this subsection

- ▶ Consequences of NAPT on Layers
- ▶ **STWireless** Solutions
- ▶ ATMF-25
- ▶ Via the PPPoA-to-PPTP Relay
- ▶ PPP-to-DHCP Spoofing.

Consequences of NAPT on layers

An important consequence is that changing IP addresses, or TCP/UDP ports via NAPT 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.

STWireless solutions The **STWireless** offers some solutions to cope with this situation. Basically these solutions boil down in transporting Public IP addresses transparently through the **STWireless** towards a device where a more advanced NAT, and/or PAT can be performed.

Some solutions are described in the following paragraphs:

- ▶ Via the PPP-to-PPTP Relay
- ▶ PPP-to-DHCP Spoofing.

Via the PPP-to-PPTP Relay You might consider the following setup below (which can be used only for wired LANs):

Step	Action
1	Install a second Ethernet PC-NIC, next to the existing Ethernet PC-NIC, in a PC.
2	Install an OS on this PC that has routing capabilities, e.g. Windows NT, UNIX, Linux, 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 an Ethernet port of the STWireless to one of two PC's Ethernet PC-NIC.
5	Connect your local LAN to the second Ethernet PC-NIC.

Result By setting up a PPTP tunnel from the 'home gateway', the Public IP address is transported transparently through the **STWireless** to end up in the '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 **STWireless**. The network configuration is practically identical to the one described above, for wired LANs applicable only:

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, Linux, 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 interface(s) of the STWireless to the PC's Ethernet PC-NIC port.
5	Connect your local LAN to the other Ethernet PC-NIC.
6	Configure the PC (acting as 'home gateway') as DHCP client.
7	Configure the STWireless as DHCP server.
8	DHCP in the STWireless must be configured for DHCP Spoofing. See subsection 11.3.4 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 **STWireless**, 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.

9 Data Services – Classical IP & IP Routing

Introduction Classical IP is a popular term for RFC1577: Classical IP and ARP over ATM . This RFC describes how a classical IP network can be created with ATM technology.

“Classical” refers to the way IP operates in legacy (W)LANs. i.e. IP communication between nodes within the same IP subnet is made possible by the shared nature of popular (W)LAN media (e.g. Ethernet) and their inherent broadcast capabilities.

For communication between IP subnets, routers do intervene. In the following, Classical IP will be referred to as CIP.

In this chapter

Topic	Section
Preparatory Steps	9.1
CIP Configuration for a LIS	9.2
Using CIP & IP Routing	9.3
CIP Configuration	9.4
Advanced CIP Configurations	9.5

9.1 Preparatory Steps

Features Classical IP:

- ▶ Next to PPPoA, is a second standardized method 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
 - ▶ Supports up to 12 concurrent virtual channels assigned to CIP.
-

What you should know in advance

- ▶ The **VPI/VCI** value of the VC(s) to use on the ADSL line
- ▶ **CIP connection service** must be supported on this VC
- ▶ The remote access device must issue and respond to **InATMARP** messages.

Note: If connectivity to multiple remote organizations is required, you need additional sets of these parameters.

STWireless The **STWireless** comes with four preconfigured CIP entries. If the SP(s) impose CIP settings which differ from the **STWireless** defaults, perform the necessary adjustments via the **STWireless** web pages.

See section 9.4 for more information.

PC(s) In CIP mode, the **STWireless** exchanges IP packets with computers on your local network. As a consequence all that is required on your local PC(s) is “standard” TCP/IP.

Prior to configuring CIP, you must establish IP connectivity with the **STWireless**. The easiest method is to configure your PCs as DHCP clients. By default the **STWireless** acts as DHCP server and leases IP addresses to local PCs during startup.

See subsection 11.1.4 for more information.

9.2 CIP Configuration for a LIS

Introduction In this section the basic procedure to enable connectivity in a Logical IP Subnet (LIS) via the ADSL line is described.

In this section

Topic	See
General CIP Configuration Procedure	9.2.1
Retrieving LIS Parameters	9.2.2
Implicit Assignment Mechanism	9.2.3
Explicit Assignment Mechanism	9.2.4
Configuring the STWireless for CIP	9.2.5
Adding Appropriate Routes to the Routing Tables.	9.2.6
Example of a CIP LIS Configuration	9.2.7

9.2.1 General CIP Configuration Procedure

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

Step	Decision and/or Action	See									
1	Are you configuring the STWireless for an existing LIS ?	9.2.2									
	<table border="1"> <thead> <tr> <th>Answer</th> <th>Action and Description</th> </tr> </thead> <tbody> <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 <i>Existing LIS</i>' of subsection 9.2.2.</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 9.2.2. In case you create a new LIS, you must create the LIS at both end of the ADSL connection, i.e. at the local, and on the remote side.</td> </tr> </tbody> </table>	Answer	Action and Description	Yes	You must retrieve the LIS IP parameters to which your local configuration must adhere to. See topic 'Configuration for an <i>Existing LIS</i> ' of subsection 9.2.2.	No	You can create the LIS with IP parameters of your choice. See topic 'Creating a New LIS' of subsection 9.2.2. In case you create a new LIS, you must create the LIS at both end of the ADSL connection, i.e. at the local, and on the remote side.				
Answer	Action and Description										
Yes	You must retrieve the LIS IP parameters to which your local configuration must adhere to. See topic 'Configuration for an <i>Existing LIS</i> ' of subsection 9.2.2.										
No	You can create the LIS with IP parameters of your choice. See topic 'Creating a New LIS' of subsection 9.2.2. In case you create a new LIS, you must create the LIS at both end of the ADSL connection, i.e. at the local, and on the remote side.										
2	Retrieve the appropriate LIS parameters, and check on which VCs (identifiable by their VPI/VCI values) your service provider enabled the CIP packet service.	9.2.2									
3	If needed, create a CIP phonebook entry, i.e. a CIP PVC, in the 'Phonebook' web page.	9.4									
4	Is the remote access router a RFC1577 compliant device, e.g. another STWireless ?										
	<table border="1"> <thead> <tr> <th>Answer</th> <th>Action and Description</th> <th>See</th> </tr> </thead> <tbody> <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>9.2.3</td> </tr> <tr> <td>No</td> <td>The remote access router will not respond to 'InATMARP' requests submitted by the STWireless, thus the CIP PVC must be explicitly assigned to the CIP member.</td> <td>9.2.4</td> </tr> </tbody> </table>	Answer	Action and Description	See	Yes	The remote access router will respond to 'InATMARP' requests, thus the CIP PVC can be implicitly assigned to the CIP member.	9.2.3	No	The remote access router will not respond to 'InATMARP' requests submitted by the STWireless , thus the CIP PVC must be explicitly assigned to the CIP member.	9.2.4	
Answer	Action and Description	See									
Yes	The remote access router will respond to 'InATMARP' requests, thus the CIP PVC can be implicitly assigned to the CIP member.	9.2.3									
No	The remote access router will not respond to 'InATMARP' requests submitted by the STWireless , thus the CIP PVC must be explicitly assigned to the CIP member.	9.2.4									
5	If needed, create a CIP member in the 'CIP Interfaces' table of the 'CIP' web page.	9.4									
6	Add appropriate IP routes to the STWireless via the 'IP route' table on the 'Routing' web page.	9.2.6									
7	Add appropriate IP routes in you PC(s).	9.2.6									

9.2.2 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 (W)LAN/WAN environment, which is interconnected via the ADSL/ATM network.

LIS parameters In order to be able to properly configure your **STWireless** 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 compliancy state
- ▶ The remote access router IP address, in the case it is not RFC1577 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 **STWireless** 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 **STWireless**, 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 **STWireless**. In case the remote access router is also a **STWireless**, best results are assured.

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

9.2.3 Implicit Assignment Mechanism

Implicit assignment If the remote side is RFC1577 compliant, e.g. another **STWireless**, your local **STWireless** 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:

Phase	Decision and Description	
1	Suppose you added a CIPPVC without supplying an IP address (e.g. CIPPVC2).	
2	The STWireless will automatically issue an InATMARP request on this PVC.	
3	Is the remote side is RFC1577 compliant ?	
	Yes	No
4	It responds with an InATMARP reply, containing its IP address. The CIP's remote IP address in the 'CIP Connections' table is completed.	"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.
5	Does the remote address share a LIS with a local CIP member ?	
	Yes	
6	the CIPPVC is assigned to this member. Connectivity is assured.	"Unresolved" will show up. No connectivity exists.

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

9.2.4 Explicit Assignment Mechanism

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

As a consequence, the **STWireless** 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 **STWireless** 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:

Name	Local IP-Address	Mask
cip0	172.16.1.1	255.255.255.0

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

Dest	Remote IP-Address
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.

9.2.5 Configuring the STWireless for CIP

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

This section describes in short the global procedure for configuring your **STWireless** 'Phonebook', and 'CIP' web page.

Configuration of the STWireless 'Phonebook' web page

By default the **STWireless** is configured for a CIP VC as used in the example of section 9.2.7. If this VC is appropriate to your, and/or the ADSL provider's needs, nothing has to be configured in the **STWireless** 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 CIP phonebook entries is described in subsection 9.4.1.

Configuration of the STWireless 'CIP' web page

The default CIP phonebook entry mentioned above is by default configured for a LIS according to the example of section 9.2.7. If this LIS configuration meets your requirements, nothing needs to be configured, and your **STWireless** 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 compliancy of the remote access router.

Configuration of the **STWireless** 'CIP' web page is fully described in subsection 9.4.2.

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

Configuring the **STWireless** for LIS connectivity, basic

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

If the remote access router is RFC1577 compliant, no routes for LIS connectivity need to be configured by yourself for the **STWireless**'s 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 **STWireless**'s CIP interface address as destination

and

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

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

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

Configuring the STWireless 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 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 **STWireless** Ethernet interface IP address as gateway.

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

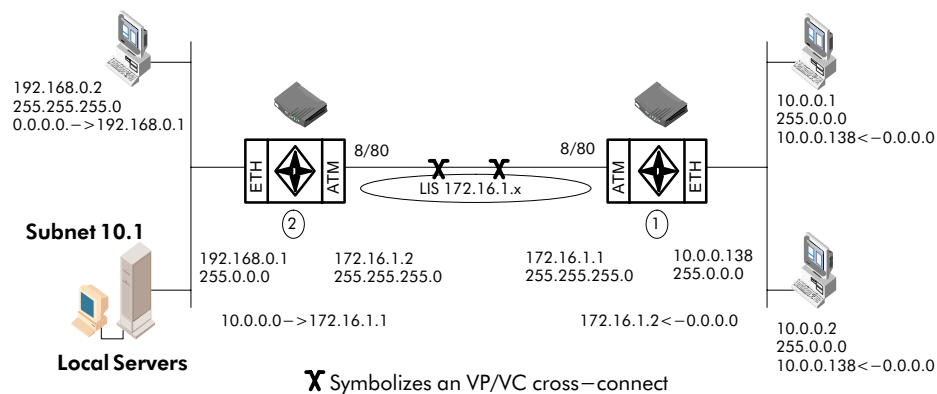
However, you can specify a destination IP address pool; e.g. if the remote LAN's IP subnetwork is 192.6.11.x, you can add routes in your PC's routing table with destination 192.6.11.0/32, and the **STWireless** as gateway.

Routing table configuration

Configuring routes for the **STWireless** is described in subsection 11.4.2.

9.2.7 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 **STWireless (1)** and the remote 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 ADSL side of the **STWireless (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 **STWireless (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 ADSL side, the CIP LIS is terminated by the remote 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 **STWireless (1)** is RFC1577 compliant).

Routing configuration

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

For the given example, the configuration is as follows:

- ▶ **STWireless (1)** has its default route pointing to the remote access router (2)

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

- ▶ The remote access router (2) has a route for “Net10” (10.0.0.0) pointing to **STWireless (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 NAT (configurable via the CLI) can be used.

9.3 Using CIP & IP Routing

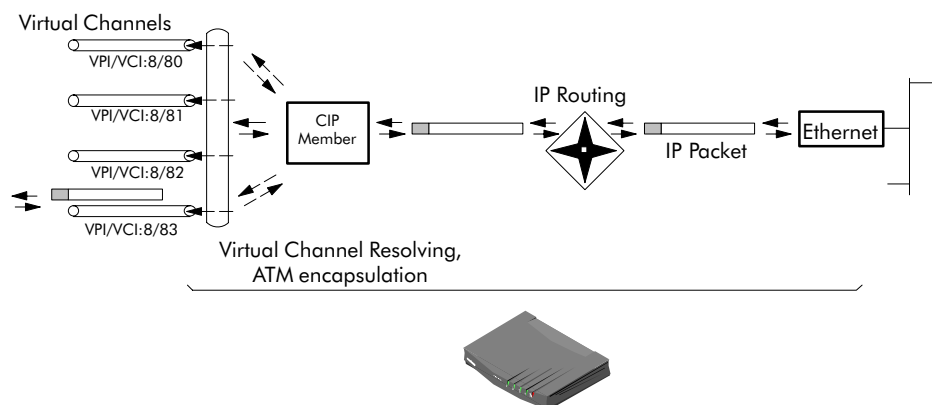
CIP operation Similar to classical LAN networking, IP Routing and CIP adhere to the “always-on” concept. That is, no special actions (e.g. dialing) must be undertaken prior to IP connectivity.

IP packets sourced by local PCs, arrive via the Ethernet segment in the **STWireless**. 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. Therefore, ping the IP address at the far end of the virtual connection; e.g. for the example of subsection 9.2.7, this would be 172.16.1.2, or thus `ping 172.16.1.2`.

Classical IP and STWireless The IP router in the **STWireless** forwards packets between the Ethernet port and the Classical IP entity sitting on top of the ADSL/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 **STWireless** rear-to-front end Classical IP operation:



9.4 CIP Configuration

Introduction The **STWireless** allows local configuration via the **STWireless** web pages.

This section describes the configuration of CIP entries, and how to use the 'CIP' web page.

In this section

Topic	See
CIP Phonebook Entries	9.4.1
CIP Entries	9.4.2

9.4.1 CIP Phonebook Entries

- In this subsection**
- ▶ CIP Phonebook Entries
 - ▶ Adding CIP Phonebook Entries
 - ▶ Deleting CIP Phonebook Entries.

See subsection 10.2.2 for more information.

CIP phonebook entries Basic to the **STWireless** VC pool management, is the 'Phonebook' web page.

The **STWireless** in its default state features the following CIP related phonebook entries:

Name	Address	Type	AutoPVC	Avail	Action
CIPPVC1	8.80	cip	No	no	Delete
CIPPVC2	8.81	cip	No	yes	Delete
CIPPVC3	8.82	cip	No	yes	Delete
CIPPVC4	8.83	cip	No	yes	Delete
Use input fields below to add a new entry					
<input type="text"/>	<input type="text"/>	cip	-	-	Add

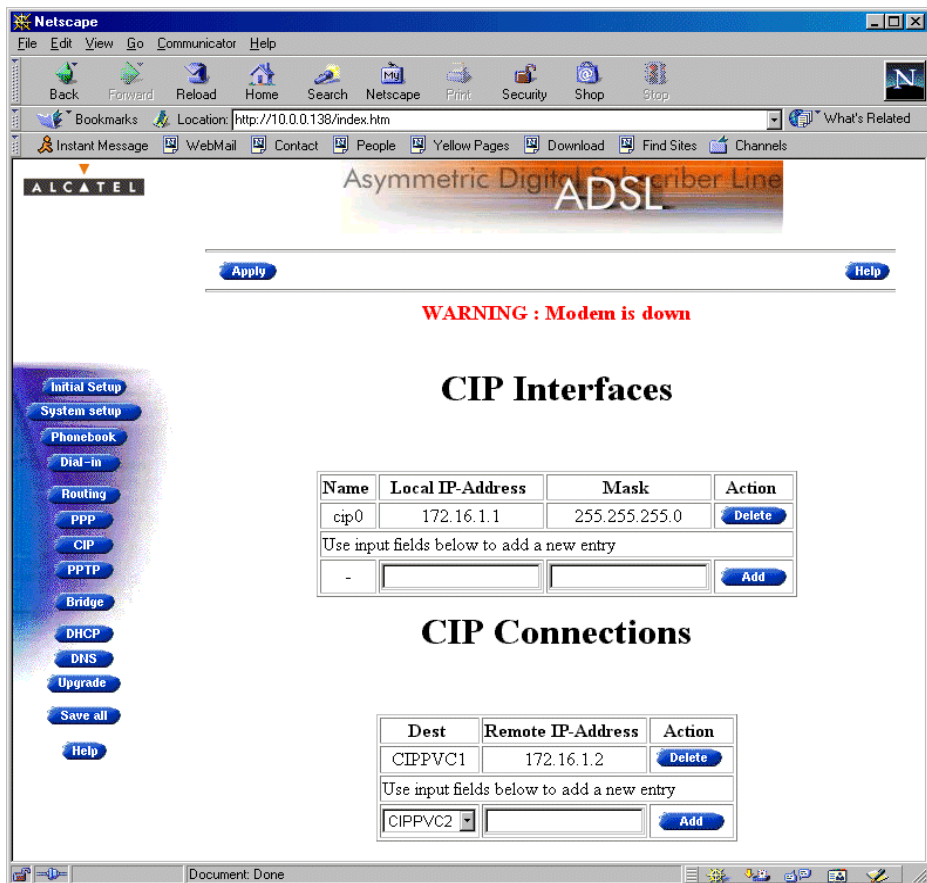
Adding/deleting phonebook entries See section 10.2 for more information.

9.4.2 CIP Entries

- In this subsection**
- ▶ The **STWireless** 'CIP' Web 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 STWireless 'CIP' web page

Clicking **CIP** in the left pane of the **STWireless** web pages, pops up the 'CIP' web page:









The 'CIP Interfaces' table

The following figure shows the 'CIP Interfaces' table:

Name	Local IP-Address	Mask	Action
cip1	172.16.1.1	255.255.255.0	
Use input fields below to add a new entry			
-	<input type="text"/>	<input type="text"/>	




'CIP Interfaces' table components

The following fields are shown:

Field	Description						
Name	Indicates the CIP member name. All CIP members are named as <i>cipX</i> , where X is a number.						
Local IP Address	Indicates the IP address of the local ADSL side of the LIS, i.e. the IP address of your CIP interface.						
Mask	Indicates the netmask/subnetmask of the local IP address.						
Action	This field contains one of the two following action buttons: <table border="1" data-bbox="751 1093 1390 1272"> <thead> <tr> <th>Button</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td></td> <td>Add a CIP member to the list.</td> </tr> <tr> <td></td> <td>Delete an existing member from the list.</td> </tr> </tbody> </table>	Button	Action		Add a CIP member to the list.		Delete an existing member from the list.
Button	Action						
	Add a CIP member to the list.						
	Delete an existing member from the list.						







The 'CIP Connections' table

The following figure shows the 'CIP Connections' table:

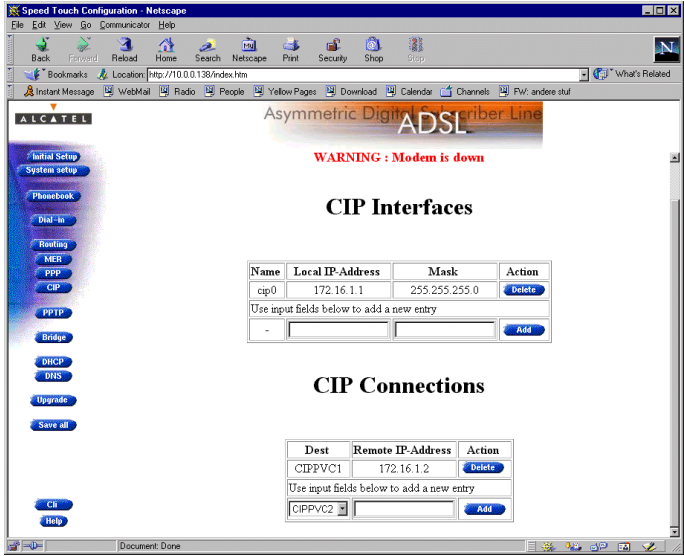
Dest	Remote IP-Address	Action
CIPPVC1	172.16.1.2	
Use input fields below to add a new entry		
CIPPVC2 	<input type="text"/>	

'CIP Connections' table components

The following fields are shown:

Field	Description						
<i>Dest</i>	Indicates the CIP VC phonebook name.						
<i>Remote IP Address</i>	Indicates the remote IP address of the remote ADSL 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".						
<i>Action</i>	This field contains one of the two following action buttons: <table border="1" data-bbox="743 1079 1378 1258"> <thead> <tr> <th>Button</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td></td> <td>Add a CIP connection to the list.</td> </tr> <tr> <td></td> <td>Delete an existing connection from the list.</td> </tr> </tbody> </table>	Button	Action		Add a CIP connection to the list.		Delete an existing connection from the list.
Button	Action						
	Add a CIP connection to the list.						
	Delete an existing connection from the list.						

Adding CIP members Proceed as follows:

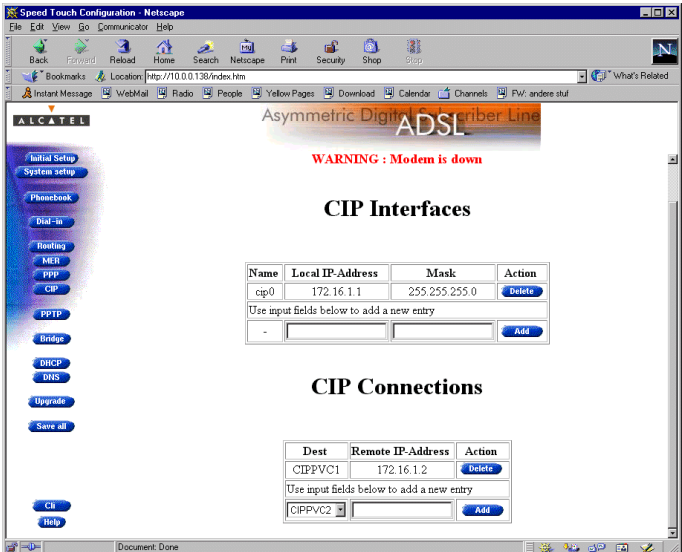
Step	Action and Description						
1	<p>Browse to the 'CIP' web page:</p>  <p>The bottom row of the 'CIP Interfaces' table allows addition of a new CIP member.</p>						
2	<p>Fill in the following CIP member parameters:</p> <table border="1" data-bbox="715 1140 1337 1339"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Local IP Address</td> <td>The IP address at the CIP member at your local side of the LIS.</td> </tr> <tr> <td>Mask</td> <td>The associated netmask/subnetmask for that local IP address.</td> </tr> </tbody> </table>	Value	Description	Local IP Address	The IP address at the CIP member at your local side of the LIS.	Mask	The associated netmask/subnetmask for that local IP address.
Value	Description						
Local IP Address	The IP address at the CIP member at your local side of the LIS.						
Mask	The associated netmask/subnetmask for that local IP address.						
3	<p>Click Add and Save all to finish the procedure.</p>						

Result A CIP member of the LIS is created at your **STWireless's** 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 **STWireless** as gateway, but the first with the CIP member itself as destination, and the second with the LIS subnetwork IP address pool as destination.

Assigning CIP PVCs to CIP members

Proceed as follows:

Step	Action and Description						
1	<p>Browse to the 'CIP' web page:</p>  <p>The bottom row of the 'CIP Connections' table allows addition of a new CIP connection.</p>						
2	<p>In the 'Dest' column of the bottom row, click <input type="button" value="v"/> and select the CIP PVC you want to assign.</p>						
3	<p>Depending the RFC1577 compliancy of the remote access router, the following must be filled in, in the 'Remote IP address' column:</p> <table border="1" data-bbox="707 1256 1329 1518"> <thead> <tr> <th>Compliancy</th> <th>Remote IP Address</th> </tr> </thead> <tbody> <tr> <td>YES</td> <td>You don't have to fill in anything; the InATMARP reply will implicitly assign the PVC to the CIP member.</td> </tr> <tr> <td>NO</td> <td>You must fill in the exact IP address of the remote access router; the PVC is explicitly assigned to the CIP member.</td> </tr> </tbody> </table>	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.
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.						
3	<p>Click <input type="button" value="Add"/> and <input type="button" value="Save all"/> to finish the procedure.</p>						

Result A CIP PVC is assigned, and added in the 'CIP Connections' table.

Deleting CIP entries Proceed as follows:

Step	Action and Description
1	Browse to the 'CIP' web page.
2	Select the CIP connection, and/or CIP member you want to delete, and click Delete
3	Click Save all to store the changes in permanent memory.

9.5 Advanced CIP Configurations

Introduction The example of subsection 9.2.7 showed a configuration with a single VC, used for ADSL connectivity within one LIS.

In this section the use of multiple VCs to connect to a LIS, and the connectivity to multiple LISs is described.

In this section

Topic	See
Configuring multiple CIP PVCs	9.5.1
Creating multiple CIP members	9.5.2

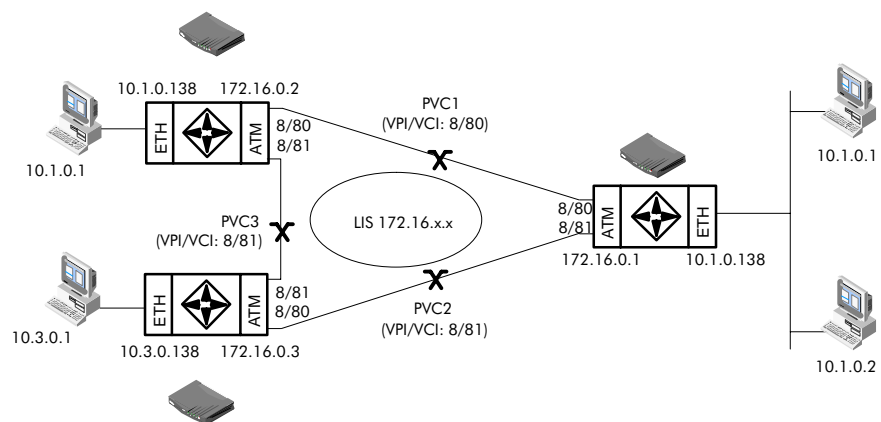
9.5.1 Configuring Multiple CIP PVCs

Multiple VCs for one LIS

Multiple VCs can be assigned, either explicit or implicit, to CIP members in the 'CIP Connections' table.



By doing so, local PCs can simultaneously access multiple ADSL nodes of one LIS.

Example The following figure shows an example of such a configuration:



Procedure Proceed as follows to assign multiple CIP PVCs to one CIP member:

Step	Action and Description
1	Browse to the 'CIP' web page. The bottom row of the 'CIP Connections' table allows addition of a new CIP connection.
2	In the 'Dest' column of the bottom row, click <input type="button" value="v"/> and select the CIP PVC you want to assign. E.g., you can select the preconfigured CIPPVC2, 3, or 4 if these are supported for the CIP packet service by the ADSL provider.

Step	Action and Description						
3	Depending the RFC1577 compliancy of the remote access router, the following must be filled in, in the 'Remote IP address' column of the CIP PVC: <table border="1" data-bbox="708 387 1329 696"> <thead> <tr> <th>Compliancy</th> <th>Remote IP Address</th> </tr> </thead> <tbody> <tr> <td>YES</td> <td>You don't have to fill in anything; the InATMARP reply will implicitly assign the PVC to the CIP member.</td> </tr> <tr> <td>NO</td> <td>You must fill in the exact IP address of the remote access router; the PVC is explicitly assigned to the CIP member</td> </tr> </tbody> </table>	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
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						
4	Click 						
5	Repeat steps 2, 3 and 4 until all provided cross-connects are added to the 'CIP Connections' table.						
6	Click  to store the changes in permanent memory.						

Result The CIP PVCs you have added, appear in the 'CIP Connections' table.

However, check whether the remote IP addresses get resolved on these new CIPPVCs.

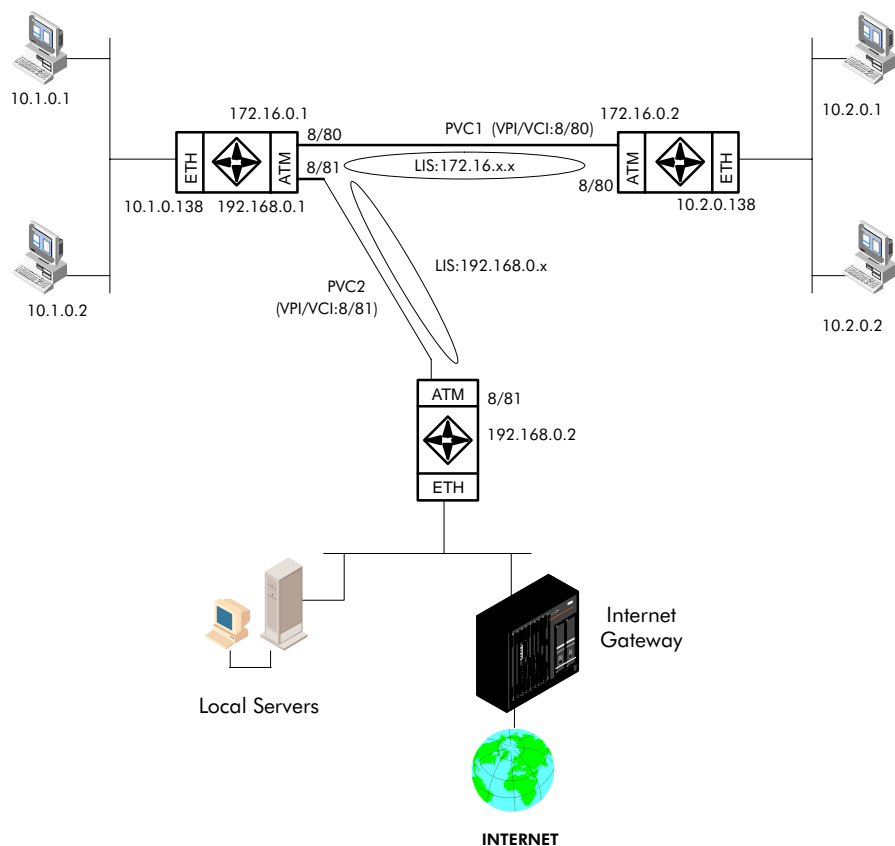
If yes, check IP connectivity with the remote device via a ping utility on one of the local PCs.

Note As your SP is responsible for the cross-connects, check whether he supports this advanced configuration.



9.5.2 Creating Multiple CIP Members.

Multiple VCs for multiple LISs You can create multiple CIP members, and consequently the **STWireless** can be part of multiple LISs. By doing so, your PC(s) can connect to multiple LISs.

Example The following figure shows an example of such a configuration:



Adding CIP members Proceed as follows to add multiple CIP members to the 'CIP Interfaces' table:

Step	Action and Description						
1	Browse to the 'CIP' web page. The bottom row of the 'CIP Interfaces' table allows addition of a new CIP member.						
2	Fill in the following CIP interface parameters: <table border="1" data-bbox="708 618 1329 817"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Local IP Address</td> <td>The IP address at the additional CIP member.</td> </tr> <tr> <td>Mask</td> <td>The associated netmask/subnetmask for that local IP address.</td> </tr> </tbody> </table>	Value	Description	Local IP Address	The IP address at the additional CIP member.	Mask	The associated netmask/subnetmask for that local IP address.
Value	Description						
Local IP Address	The IP address at the additional CIP member.						
Mask	The associated netmask/subnetmask for that local IP address.						
3	Click 						
4	Repeat steps 2 and 3 for each LIS you want to connect to.						
5	For each additional CIP member, at least one CIP PVC must be assigned. This can be done implicit, or explicit (according each remote side's RFC1577 compliancy). See the procedure in subsection 9.5.1 for adding CIP PVCs to the 'CIP Connections' table.						
6	Click  to store the changes in permanent memory.						

Result The CIP members you created, appear in the 'CIP Interfaces' table.

The CIP PVCs, you have added appear in the 'CIP Connections' table.

However, check whether the remote IP addresses get resolved on these new CIP members and their associated CIP PVCs.

If yes, check IP connectivity with the LISs via a ping utility on one of the local PCs.

Note As your SP is responsible for the cross-connects, check whether he supports this advanced configuration.

Speed Touch™ Wireless

Networking Services

10 Networking Services – ATM

Introduction All data arriving at and departing from your **STWireless** via the ADSL line is carried in ATM cells.

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

In this chapter

Topic	See
The ATM Packet Switching Technology	10.1
The STWireless Phonebook	10.2

10.1 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	10.1.1
ATM and the STWireless	10.1.2
ATM and Interfaces	10.1.3

10.1.1 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. 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 VC (SVC) is created dynamically for each session and released when the information exchange is complete.

VCs and the STWireless Currently all **STWireless** ATM connections are static, i.e. of type PVC.

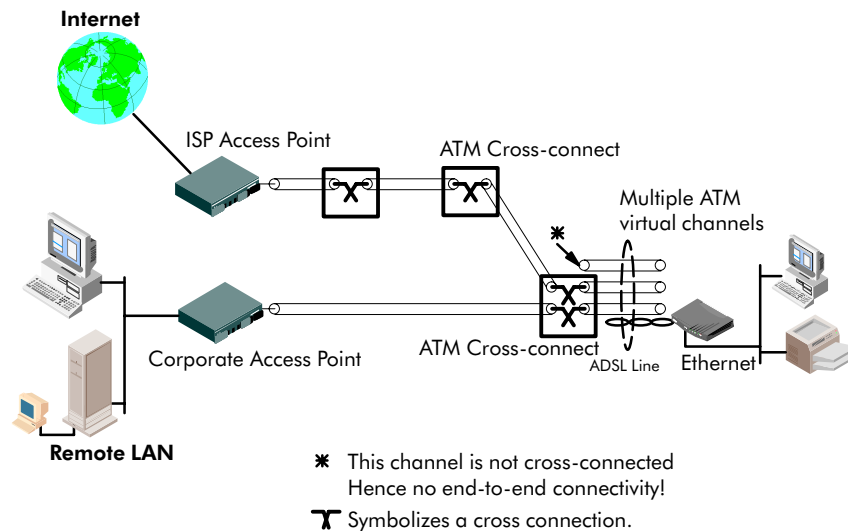
Channel identifiers Each ATM cell carries two labels called VPI and VCI as part of its header.

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

10.1.2 ATM and the STWireless

End-to-end ATM connectivity

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



STWireless vs. remote destination

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

By default, a number of channels are terminated in the **STWireless**.

ATM provision

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

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

STWireless default PVCs

See Appendix E for the specific default VPI/VCI values.

10.1.3 ATM and Interfaces

ATM traffic handling ATM traffic, arriving at the **STWireless**, is switched to the Ethernet port, and WLAN hub.

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.

Ethernet port This port terminates a number of ATM connections and extracts frames from arriving cells and encapsulates frames in departing cells.

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

Currently the supported encapsulations are:

- ▶ For **Bridged** connections:
RFC 1483, Ethernet V2.0/IEEE 802.3 bridged PDUs for both the LLC/SNAP method and VC-MUX method
- ▶ For **MER** connections:
RFC 1483, Ethernet V2.0/IEEE 802.3 bridged PDUs for both the LLC/SNAP method and VC-MUX method
- ▶ For **PPPoA/PPTP** connections:
RFC 2364, PPP PDUs for both the LLC/NLPID method and VC-MUX method
- ▶ For **Routed PPP** connections:
RFC 2364, PPP PDUs for both the LLC/NLPID method and VC-MUX method
- ▶ For **Routed CIP** connections:
RFC 1483 LLC/SNAP method for Routed PDUs.

10.2 The Speed Touch Wireless Phonebook

Introduction The **STWireless** 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 **STWireless** ADSL router operation are ATM VCs. The **STWireless** phonebook is the management tool for all possible ATM VC connections.

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

In this section

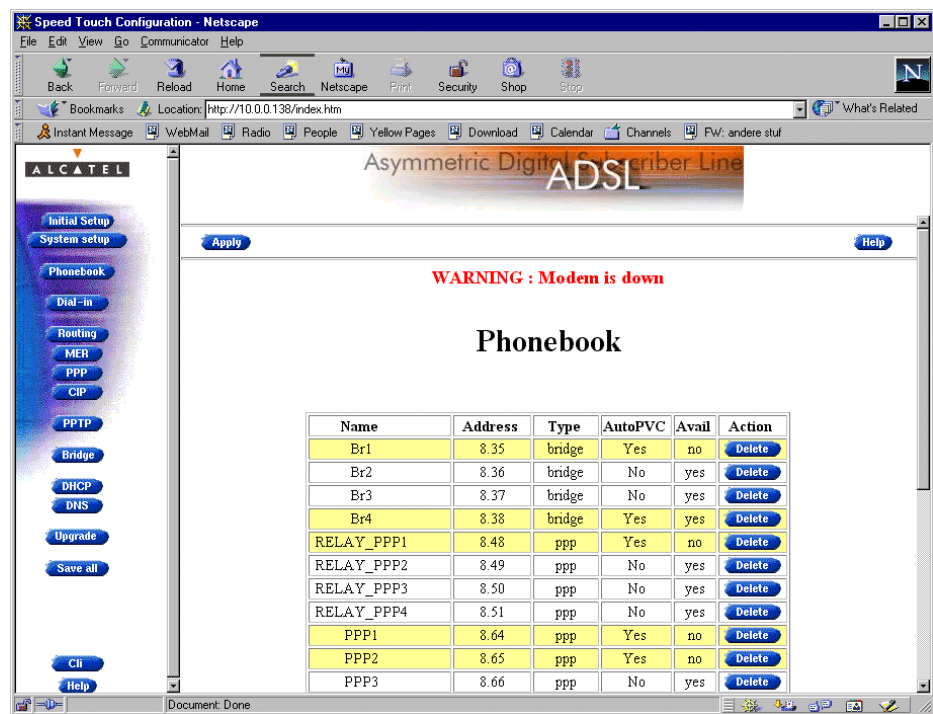
Topic	See
The 'Phonebook' Web Page	10.2.1
Using the Phonebook	10.2.2
AutoPVC and the Phonebook	10.2.3

10.2.1 The STWireless 'Phonebook' Web Page

- In this subsection**
- ▶ The **STWireless** 'Phonebook' Web Page
 - ▶ The 'Phonebook' Table
 - ▶ 'Phonebook' Table Components
 - ▶ Phonebook Defaults
 - ▶ The 'AutoPVC' Table.

The STWireless 'Phonebook' web page

Clicking **Phonebook** in the left pane of the **STWireless** web pages, pops up the 'Phonebook' web page (See section 18.2 for more information):



The screenshot shows the 'Phonebook' web page with a warning message and a table of entries. The table is as follows:

Name	Address	Type	AutoPVC	Avail	Action
Br1	8.35	bridge	Yes	no	Delete
Br2	8.36	bridge	No	yes	Delete
Br3	8.37	bridge	No	yes	Delete
Br4	8.38	bridge	Yes	yes	Delete
RELAY_PPP1	8.48	ppp	Yes	no	Delete
RELAY_PPP2	8.49	ppp	No	yes	Delete
RELAY_PPP3	8.50	ppp	No	yes	Delete
RELAY_PPP4	8.51	ppp	No	yes	Delete
PPP1	8.64	ppp	Yes	no	Delete
PPP2	8.65	ppp	Yes	no	Delete
PPP3	8.66	ppp	No	yes	Delete

The 'Phonebook' table

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

Name	Address	Type	AutoPVC	Avail	Action
Br1	8.35	bridge	Yes	no	Delete
Br2	8.36	bridge	No	yes	Delete
Br3	8.37	bridge	No	yes	Delete
Br4	8.38	bridge	Yes	yes	Delete
RELAY_PPP1	8.48	ppp	Yes	no	Delete
RELAY_PPP2	8.49	ppp	No	yes	Delete
RELAY_PPP3	8.50	ppp	No	yes	Delete
RELAY_PPP4	8.51	ppp	No	yes	Delete
PPP1	8.64	ppp	Yes	no	Delete
PPP2	8.65	ppp	Yes	no	Delete
PPP3	8.66	ppp	No	yes	Delete
DHCP_SPOOF	8.67	ppp	Yes	no	Delete
CIPPVC1	8.80	cip	Yes	no	Delete
CIPPVC2	8.81	cip	No	yes	Delete
CIPPVC3	8.82	cip	No	yes	Delete
CIPPVC4	8.83	cip	No	yes	Delete







Use input fields below to add a new entry

<input type="text"/>	<input type="text"/>	any	-	-	Add
----------------------	----------------------	-----	---	---	-----

'Phonebook' table components

The following fields are shown:

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

Field	Description												
Type	<p>Represents the sort of packet services that are supported on the ATM VC. It can take the following values:</p> <table border="1"> <thead> <tr> <th>Value</th> <th>Packet Service</th> </tr> </thead> <tbody> <tr> <td rowspan="2">bridge</td> <td>IEEE802.1D Transparent Bridging See chapter 5 for more information.</td> </tr> <tr> <td>MAC encapsulated Routing See chapter 6 for more information.</td> </tr> <tr> <td rowspan="2">ppp</td> <td>PPPoA-to-PPTP Relaying See chapter 7 for more information.</td> </tr> <tr> <td>IP Routing & PPP. See chapter 8 for more information.</td> </tr> <tr> <td>cip</td> <td>IP Routing & CIP. See chapter 9 for more information.</td> </tr> <tr> <td>any</td> <td>Any kind of packet service is allowed.</td> </tr> </tbody> </table>	Value	Packet Service	bridge	IEEE802.1D Transparent Bridging See chapter 5 for more information.	MAC encapsulated Routing See chapter 6 for more information.	ppp	PPPoA-to-PPTP Relaying See chapter 7 for more information.	IP Routing & PPP. See chapter 8 for more information.	cip	IP Routing & CIP. See chapter 9 for more information.	any	Any kind of packet service is allowed.
Value	Packet Service												
bridge	IEEE802.1D Transparent Bridging See chapter 5 for more information.												
	MAC encapsulated Routing See chapter 6 for more information.												
ppp	PPPoA-to-PPTP Relaying See chapter 7 for more information.												
	IP Routing & PPP. See chapter 8 for more information.												
cip	IP Routing & CIP. See chapter 9 for more information.												
any	Any kind of packet service is allowed.												
Avail	Indicates the availability of the VC phonebook entry. An entry is available if it is not configured in any packet service web page, or not in temporary use by a packet service.												
Auto PVC	<p>Indicates whether the entry is listed in the 'AutoPVC' list (yes), or not (no).</p> <p>If the ATM VC related to the phonebook entry is listed in the 'AutoPVC' list, the phonebook entry row is highlighted by a yellow bar.</p> <p>See subsection 10.2.3 for more information.</p>												
Action	<p>Contains one of the two following action buttons:</p> <table border="1"> <thead> <tr> <th>Button</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td></td> <td>Add a phonebook entry to the list.</td> </tr> <tr> <td></td> <td>Delete a phonebook entry from the list.</td> </tr> </tbody> </table>	Button	Action		Add a phonebook entry to the list.		Delete a phonebook entry from the list.						
Button	Action												
	Add a phonebook entry to the list.												
	Delete a phonebook entry from the list.												

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:

Type	VPI	VCI
bridge	8	35
bridge	8	38
ppp	8	48
ppp	8	61
ppp	8	65
ppp	8	67
cip	8	80

Any PVC, identified by its VPI/VCI, communicated via AutoPVC, is added to the 'AutoPVC' table. If AutoPVC is not supported at the remote side, the 'AutoPVC' table stays empty.

See subsection 10.2.3 for more information.

10.2.2 Using the Phonebook

Introduction The main function of the **STWireless** 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 **STWireless** VC connection possibilities.

- In this subsection**
- ▶ Restrictions for Adding Phonebook Entries
 - ▶ Adding Phonebook Entries
 - ▶ Deleting Phonebook Entries.
-

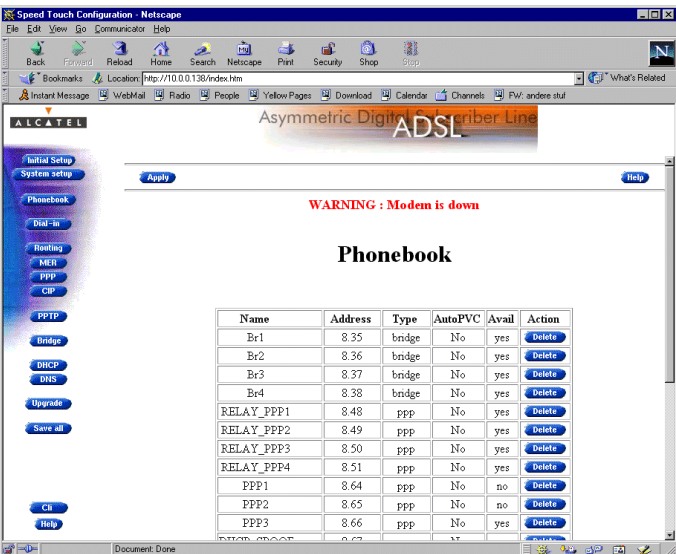
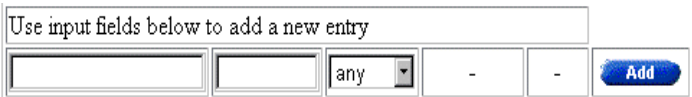


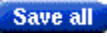
Restrictions for adding phonebook entries Although you are free to give any name to a phonebook entry, a few restrictions apply:

- ▶ 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 PPPoA-to-PPTP Relaying packet service may not start with a capital 'P', or a capital 'T'.
- ▶ In case you want to use the **STWireless** 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 **STWireless** 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:

Step	Action and Description
1	<p>Browse to the 'Phonebook' web page:</p> 
2	<p>Scroll to the bottom row of the 'Phonebook' table:</p>  <p>The bottom row of the table allows addition of a new entry.</p>
3	In the 'Name' column of the bottom row, enter a name of your choice for identifying the phonebook entry.
4	In the 'Address' column, enter the VC's VPI.VCI values. In most cases these values are provided by your SP.
5	In the 'Type' column of the bottom row, click  and select the packet service of your choice, or choose any.
6	Click  and  to finish the procedure.

Deleting phonebook entries

Proceed as follows:

Step	Action and Description						
1	Browse to the 'Phonebook' web page.						
2	Select the phonebook entry you want to delete, and click 						
3	If the phonebook is currently in use, i.e. is connected, or configured, you are asked to confirm the deletion of the entry: <p style="text-align: center;">Entry 'PPP1' is in use. Delete anyway ?</p> <p style="text-align: center;"> <u>Cancel</u></p>						
4	Make the following selection: <table border="1" style="margin-left: 20px;"> <thead> <tr> <th>If ...</th> <th>Then click ...</th> </tr> </thead> <tbody> <tr> <td>You are sure that the phonebook entry may be deleted ...</td> <td></td> </tr> <tr> <td>The phonebook entry, which is in use, may not be deleted ...</td> <td><u>Cancel</u></td> </tr> </tbody> </table>	If ...	Then click ...	You are sure that the phonebook entry may be deleted ...		The phonebook entry, which is in use, may not be deleted ...	<u>Cancel</u>
If ...	Then click ...						
You are sure that the phonebook entry may be deleted ...							
The phonebook entry, which is in use, may not be deleted ...	<u>Cancel</u>						
4	Click  to store the changes in permanent memory.						

10.2.3 AutoPVC and the Phonebook

AutoPVC The default VCs, can be remotely modified via the *AutoPVC* feature of the **STWireless**.

AutoPVC operates only in conjunction with the Alcatel DSLAM and **STWireless**, and offers the functionality that user VCs that are to be terminated on the Ethernet port, can be notified by the **STWireless**.

Operation of AutoPVC Basically the following steps are executed:

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

Criterion 1 Any PVC, or VPI/VCI communicated via AutoPVC is added to the AutoPVC list on the 'Phonebook' web page.

If AutoPVC is not supported, this list is empty.

Criterion 2 An AutoPVC VPI value in the range from 0 up to 15 will be notified in the AutoPVC list.

If the VPI/VCI value is used in the Phonebook, this phonebook entry will be highlighted by a yellow bar.

Example 1 If the ADSL provider configures Virtual **Path** (VP) 5 on the DSLAM, then the **STWireless** cross-connects VPI 5 on the ADSL line to VPI 5 on the Ethernet port, and WLAN hub

Example 2 Suppose the ADSL provider configures one of the **STWireless**'s default **terminated VCs**, e.g. 8/35, on the DSLAM. VPI/VCI 8/35 will end up in the 'AutoPVC' list:

Type	VPI	VCI
bridge	8	35

As this VC matches with the Bridging entry *Br1*, this phonebook entry will be highlighted in the 'Phonebook' table:

Phonebook

Name	Address	Type	AutoPVC	Avail	Action
Br1	8.35	bridge	Yes	no	Delete
Br2	8.36	bridge	No	yes	Delete

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

11 Networking Services – IP

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

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 ADSL/ATM network
- ▶ Local IP connectivity towards other PCs on your (W)LAN.

In this chapter

Topic	See
General IP Information	11.1
Packet Services and IP Addresses	11.2
STWireless and IP Addressing	11.3
IP Routing	11.4

11.1 General IP Information

In this section

Topic	See
IP Addresses and Subnet Masks	11.1.1
Private vs. Public IP Addresses	11.1.2
Choosing an IP Address	11.1.3
Dynamic IP Address Configuration: DHCP	11.1.4

IP address network classes

By splitting up the IP address in a network part and a subnetwork part, it is possible to divide IP addresses in four classes (In fact five).

These classes are differentiated by the initial bits of an IP address:

Class	Range from ... up to ...	Network Part Bits
A	0.0.0.0 ... 127.255.255.255	8
B	128.0.0.0 ... 191.255.255.255	16
C	192.0.0.0 ... 223.255.255.255	24
D	224.0.0.0 ... 239.255.255.255	32

Prefix notation for IP addresses

A more up to date representation of subnet 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: prefix notation

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

IP address notation and the STWireless

In the routing table of the **STWireless** this notation will be used.

11.1.2 Private vs. Public Addresses

Introduction Private PC(s) do not require access to PC(s) in other enterprises, or to the Internet. Therefore it is sufficient for the PC to have an IP address that is unique within the enterprise but may be ambiguous between enterprises and on the Internet.

On the other hand there is also a need for “Internet-wide” unique IP addresses to allow web servers to be constantly online.

The first set of addresses are called *Private IP addresses*; the second set *Public IP addresses*.

Private IP addresses In the examples throughout this document Private IP addresses are used for local IP configurations.

Private IP addresses are defined in RFC1918 “Address Allocation for Private Internets”. This RFC is categorized as “Best Current Practice”.

Using private addresses In principle if an IP address is assigned to a PC and the connectivity is limited to intra-enterprise communication only, the IP address can be assumed to be privately held.

The limitation however is that communication between enterprises and connection to the Internet itself via those private IP addressed PCs is not possible, and even not allowed.

Private PC(s) accessing public services Via mediating gateways (e.g. the **STWireless**) private PC(s) can still have access to external services, e.g. the Internet.

Private IP address classes

IANA (the Internet Assigned Number Authority), defined blocks of IP addresses for private purposes:

Class Type	From	To	Number of Network Numbers
A	10.0.0.0	10.255.255.255	1
B	172.16.0.0	172.16.255.255	16 (Contiguous)
C	192.168.0.0	192.168.255.255	256 (Contiguous)

Public IP addresses

A Public IP address is an officially assigned IP address by an Internet Registry and is guaranteed to be **worldwide unique**.

As a consequence the PC to which the address is assigned, has worldwide Internet connectivity.

Using Public IP addresses

Public IP addresses are used by PC(s) that need global connectivity, outside the enterprise, and/or with the Internet; therefore these PC(s) require public IP addresses to be globally unique.

You may not assign Public IP addresses yourself. If you need a Public IP address or block of IP addresses, contact your Internet Service Provider (ISP).

The ISP must in turn contact its upstream registry, or his appropriate regional registry, e.g.: the American Registry for Internet Numbers (ARIN) (<http://www.arin.net>).

11.1.3 Choosing an IP Address

Introduction Regardless of your application, IP addresses must always be configured at both ends of the connection.

Prior to configuring an IP address, you must choose a suitable one. In this subsection a few criteria are listed that may influence your choice.

Use of public IP addresses Public IP addresses are required when accessing the Internet. Each PC on the Internet must have a unique IP address. If not, IP packets cannot be routed.

For end-to-end IP communication your ISP or LAN administrator will supply you with a Public IP address.

Use of private IP addresses Private IP addresses are to be used for local IP communication. E.g. configuring the **STWireless**, or dumping files to your local printer.

For this purpose it is best to choose addresses from the private ranges.

Further, all examples will be given with 10.x.x.x private addresses, sometimes referred to as “**Net10**” IP addresses.

Simultaneous use of public & private IP addresses In most networking scenario's, *Private* and *Public* IP addresses will be in use simultaneously, e.g.:

- ▶ PPPoA-to-PPTP Relaying

In this configuration, one IP layer is carried into another. Otherwise stated: on your local (home) (W)LAN the *Public* IP layer is carried inside a *Private* IP layer (a so called IP Tunnel).
- ▶ PPP & IP Routing

In this scenario the *Public* IP layer will be terminated in the **STWireless** and translated into a *Private* IP layer via the NAPT translation feature of the **STWireless**.

Local vs. end-to-end

In the various configurations, multiple IP addresses are in use at the same time, however their scope will differ. The Public IP addresses will run end-to-end, Private IP addresses will remain local.

Dynamic vs. static IP configuration

Both Public and Private IP addresses can either be *statically* configured, or can be distributed *dynamically* via DHCP.

See section 11.1.4 for more information.

Again, for end-to-end IP communication, your ISP or (W)LAN administrator will decide on the method. For local configuration you can choose the method yourself.

11.1.4 Dynamic IP Address Configuration: DHCP

DHCP DHCP is short for *Dynamic Host Configuration Protocol* and is part of the TCP/IP protocol suite. It provides a framework for passing configuration information to PC(s) on a TCP/IP network.

The intention is for individual PC(s) to extract their IP parameters from a central server, rather than configuring them manually.

Use of DHCP A PC supporting DHCP, will receive the following IP parameters via DHCP:

- ▶ Its own IP address and subnet mask
 - ▶ The IP address of the default gateway
 - ▶ The IP addresses of the primary and secondary DNS servers.
-

Operation of DHCP DHCP operates in client/server mode: a PC in its booting stage acts as a DHCP client and emits broadcast DHCP requests. These are intercepted by a DHCP server (on the same network) which responds with DHCP replies.

These DHCP replies contains, among other information, the IP address for the DHCP client.

Mostly this IP address is given for a limited period of time. This allows automatic reuse of an address that is no longer needed by the PC to which it was assigned.

DHCP and STWireless The task of being DHCP server can also be performed by the **STWireless**.

STWireless DHCP server configuration is possible via the 'DHCP' web page. See section 11.3.3 for more information.

11.2 Packet Services and IP Addressing

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

Apart from Bridging, all packet services require the TCP/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 and IP Addresses	11.2.1
MER and IP Addresses	11.2.2
PPPoA-to-PPTP Relaying and IP Addresses	11.2.3
PPP & IP Routing and IP Addresses	11.2.4

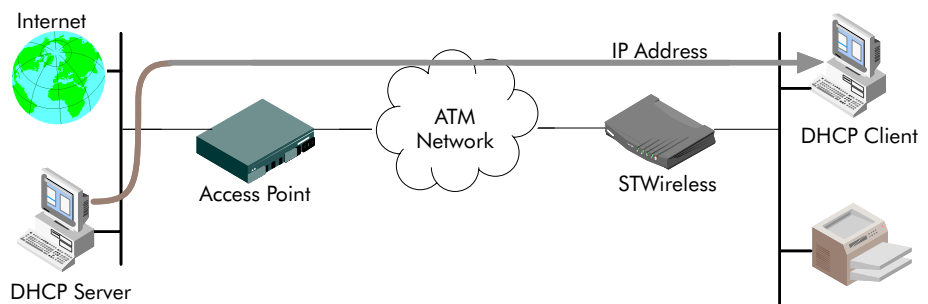
11.2.1 Transparent Bridging and IP Addresses

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

However, in case of Internet access or private IP networking, 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 ADSL connection. Therefore, also your **STWireless**'s DHCP server must be disabled.

As you can see in the following figure, this typical configuration setup, illustrates the transparency of the Bridging packet service:



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.



Bridging & DHCP Service

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

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

Setting the DHCP modes of your **STWireless** is described in section 11.3.3.

11.2.2 MER and IP Addresses

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

STWireless IP addresses As the **STWireless** 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 **STWireless** DHCP server.

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

See sections 11.3 and 17.1 for more information.

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

See subsection 11.3.3 for more information.

Default gateway for the PCs In addition, configure the **STWireless**'s IP address as default gateway in your PCs.

MER & IP routing At the ADSL side of the **STWireless** IP router, MER will receive an IP address from the remote access server. However, you can also configure an IP address for the MER connection on the 'MER' web page. In this case, the **STWireless** negotiates the acceptance of the IP address with the remote side.

Via NAT, both Private and Public IP addresses can coexist in the router.

11.2.3 PPPoA-to-PPTP Relaying and IP Addresses

IP vs. PPPoA/PPTP 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 Consequently 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 **STWireless** 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.

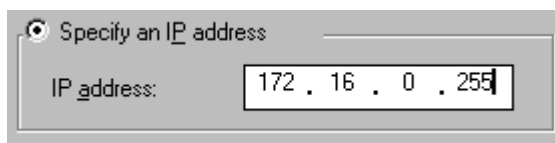
Note: IP addresses can be configured automatically via **STWireless**’s DHCP server. See section 11.3.3, for more information.

Public IP addresses For PPPoA/PPTP, 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 PPTP 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 PPPoA/PPTP, you can supply a static IP address:



The image shows a screenshot of a network configuration window. At the top, there is a radio button labeled "Specify an IP address" which is selected. Below this, there is a text input field labeled "IP address:" containing the value "172.16.0.255".

11.2.4 PPP & IP Routing and IP Addresses

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

STWireless IP addresses As the **STWireless** 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 **STWireless** DHCP server.

In case another IP address is required, you can set **STWireless**’s IP address via the **STWireless** web pages, or via a *Ping-of-Life*[™].

See sections 11.3 and 17.1 for more information.

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

Default gateway for the PCs In addition, configure the **STWireless**’s IP address as default gateway in your PCs.

PPP & IP routing At the ADSL side of the **STWireless** IP router, PPP automatically negotiates an IP address with its remote PPP peer. Via NAT, both Private and Public IP addresses can coexist in the router.

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

See subsection 8.4.5 for more information.

NAPT NAT is enabled by default on PPP connections. In case your (W)LAN uses Public IP addresses, NAT is not required.

See subsection 8.4.6 for more information.

11.3 Speed Touch Wireless and IP Addressing

Introduction Like any other member of a (W)LAN, the **STWireless** 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 **STWireless** for local communication only.

In this section

Topic	See
STWireless IP Address Types	11.3.1
Static IP Address Configuration	11.3.2
Dynamic IP Address Configuration	11.2.4
Configuring the STWireless DHCP Server	11.2.4

11.3.1 STWireless IP Address Types

Assigning IP addresses to the STWireless

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

- ▶ The default IP address: 10.0.0.138
- ▶ IP addresses assigned via the 'Initial Setup' web page
- ▶ IP addresses assigned via a 'Ping-of-Life™
- ▶ IP addresses assigned via the 'Routing' web page.

Moreover, IP addresses can be configured, and/or negotiated during connection sessions (e.g. MER, and PPP & IP Routing).

STWireless and multiple IP addresses

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

'IP address' table

If you browse to the 'Routing' web page (See section 18.2 for more information), you can find the 'IP address' table. This table summarizes all IP addresses configured on any of the **STWireless** interfaces:







Intf	Address	Netmask	Type	Transl	Action
eth0	10.0.0.138	255.0.0.0	Extra	none	Delete
cip0	172.16.1.1	255.255.255.0	CIP	none	-
loop	127.0.0.1	255.0.0.0	Auto	none	-

Use input fields below to add a new entry

eth0	<input type="text"/>	<input type="text"/>	Extra	none	Add
------	----------------------	----------------------	-------	------	---------------------

'IP address' table components

The following fields are shown:

Field	Description										
<i>Intf</i>	<p>Indicates the interface (Intf) to which the IP parameter set was assigned to.</p> <p>It can take several values depending on the packet services that are active. The Ethernet (eth0) and the Loopback (loop) are always present.</p>										
<i>Address</i>	Shows the IP address of the interface.										
<i>Netmask</i>	If available, it shows the Netmask of the interface.										
<i>Type</i>	<p>Indicates the origin of the IP parameters.</p> <p>It can take following values:</p> <table border="1"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <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' web page.</td> </tr> <tr> <td>Extra</td> <td>Implies that an additional IP parameter set was added through the 'Routing' web 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 <i>Ping-of-Life™</i>.</td> </tr> </tbody> </table>	Value	Description	Auto	Implies that the parameters were acquired automatically through DHCP, or are typical standard IP addresses (e.g. 'loop').	User	Implies that an additional IP parameter set was added through the 'Initial Setup' web page.	Extra	Implies that an additional IP parameter set was added through the 'Routing' web page. The default IP address 10.0.0.138 is also of this type.	Temp	Implies that this (additional) IP parameter set was added via a <i>Ping-of-Life™</i> .
Value	Description										
Auto	Implies that the parameters were acquired automatically through DHCP, or are typical standard IP addresses (e.g. 'loop').										
User	Implies that an additional IP parameter set was added through the 'Initial Setup' web page.										
Extra	Implies that an additional IP parameter set was added through the 'Routing' web page. The default IP address 10.0.0.138 is also of this type.										
Temp	Implies that this (additional) IP parameter set was added via a <i>Ping-of-Life™</i> .										
<i>Transl</i>	<p>This field indicates the translation performed.</p> <p>It can take following values:</p> <table border="1"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>None</td> <td>No address translation is performed on this address.</td> </tr> <tr> <td>NAT</td> <td>NAPT is performed on this address.</td> </tr> </tbody> </table>	Value	Description	None	No address translation is performed on this address.	NAT	NAPT is performed on this address.				
Value	Description										
None	No address translation is performed on this address.										
NAT	NAPT is performed on this address.										
<i>Action</i>	<p>Contains one of the two following action buttons:</p> <table border="1"> <thead> <tr> <th>Button</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td></td> <td>Add an IP address to the list.</td> </tr> <tr> <td></td> <td>Delete an IP address from the list.</td> </tr> </tbody> </table>	Button	Action		Add an IP address to the list.		Delete an IP address from the list.				
Button	Action										
	Add an IP address to the list.										
	Delete an IP address from the list.										

11.3.2 Static IP Address Configuration

Default STWireless IP address

The **STWireless** comes with a preconfigured “Net10” IP address, i.e. 10.0.0.138.

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

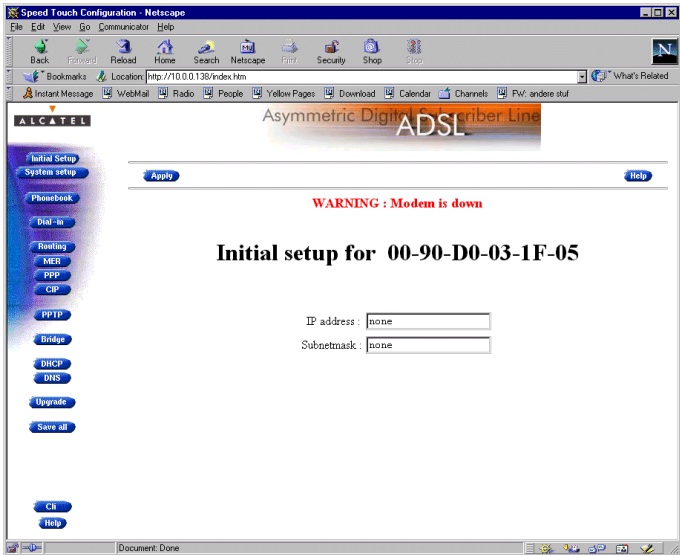
In this subsection



- ▶ Setting an IP Address via the ‘Initial Setup’ Web Page
- ▶ Setting an IP Address via the ‘Routing’ Web Page
- ▶ **STWireless** Associated Netmasks
- ▶ Sample Configuration: Single PC
- ▶ Sample Configuration: Small Workgroup.

See section 18.2 for more information.

Setting an IP address via the ‘Initial Setup’ web page



Proceed as follows:

Step	Action and Description
1	<p>Browse to the ‘Initial Setup’ web page:</p> 

Step	Action and Description
2	In the 'IP Address' field you can configure a user defined IP address for the STWireless . This IP address will show up as " User " in the STWireless 'IP address' table (See section 11.3.1).
3	In the 'Subnetmask' field you must configure an appropriate netmask for applying subnetting in your (W)LAN.
4	Click  . As a result, the new IP settings are applied.
5	To verify connectivity, point your Web browser to the new IP address. Make sure though that your PC shares the same subnetwork.
6	Click  to store the IP settings to permanent storage.

Setting an IP address via the 'Routing' web page

Proceed as follows to configure an "Extra" IP address:

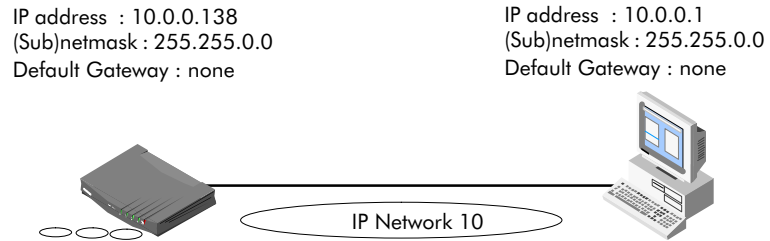
Step	Action and Description
1	Browse to the 'Routing' web page.
2	In the 'IP address' table, you can configure an extra IP address, using the table's bottom row. Fill in the bottom row as follows: <ul style="list-style-type: none"> • Intf: "Eth0" • IP address: the IP address for the STWireless. • Netmask: the appropriate netmask.
3	Click  . As a result, the new IP settings are applied.
4	To verify connectivity, point your browser to the new address. Make sure though that your PC shares the same subnetwork. Click  to store the IP settings to permanent storage.

STWireless associated netmasks

(Private) IP Address Class	Associated Netmask	Example IP Address
A (1.x.x.x to 126.x.x.x)	255.0.0.0	10.x.x.x
B (128.0.x.x to 191.255.x.x)	255.255.0.0	172.16.x.x
C (192.0.0.x to 223.255.255.x)	255.255.255.0	192.168.x.x

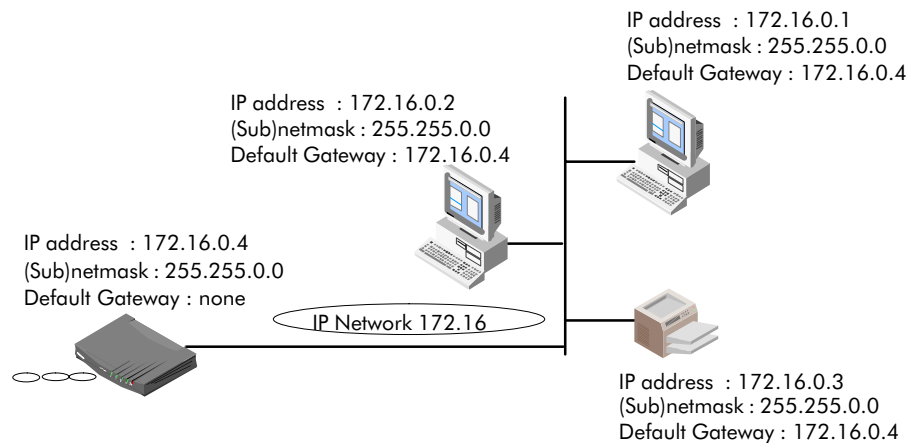
**Sample configuration:
single PC**

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



**Sample configuration:
small workgroup**

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



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

11.3.3 Dynamic IP Address Configuration: DHCP

STWireless DHCP client/server setting

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 STWireless .
Medium sized	Server	For small home (W)LANs it might be worthwhile to configure all of your (W)LAN devices as DHCP clients, and the STWireless as the DHCP server. In this configuration each time a computer starts, it will obtain its IP configuration from the STWireless .
Advanced	Client	For advanced networks, the role of DHCP server might be performed by an IP node other than the STWireless 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 STWireless .

Default STWireless DHCP configuration

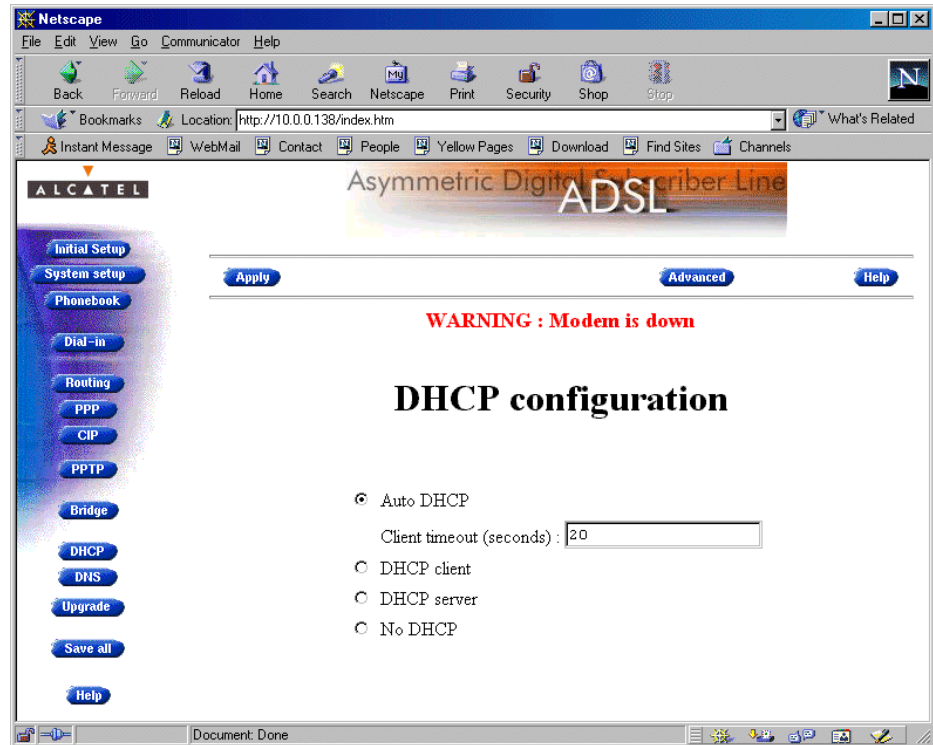
For the **STWireless**, the DHCP server is by default enabled, i.e. set for 'Auto DHCP'.

In this subsection

- ▶ The **STWireless** 'DHCP' Web Page
- ▶ Configuring the **STWireless** for (W)LANs without DHCP Server
- ▶ Configuring the **STWireless** as DHCP Server
- ▶ Configuring the **STWireless** as DHCP Client
- ▶ Configuring the **STWireless** Auto DHCP
- ▶ Dynamic IP Addressing.

The STWireless 'DHCP' web page

Clicking **DHCP** in the left pane of the **STWireless** web pages, pops up the 'DHCP' web page:



Configuring the STWireless for a (W)LAN without DHCP

To setup the **STWireless** without DHCP, tick No DHCP on the 'DHCP' web page.

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

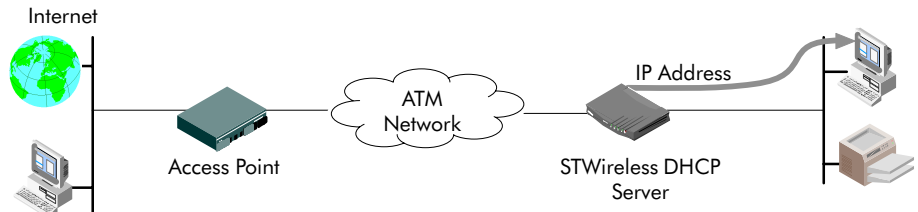
See subsection 11.3.2 for static IP addressing of the **STWireless**.

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

Configuring the STWireless as DHCP server

To setup the **STWireless** as DHCP server, tick DHCP server on the 'DHCP' web page.

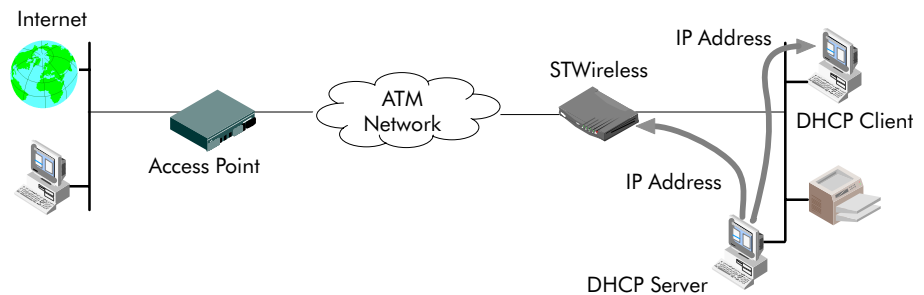
Via the 'DHCP Server Configuration' web page, you can configure the **STWireless** DHCP server settings. See subsection 11.3.4 for more information.



Note: This setting might cause side effects with Bridging. See section 11.2.1 for more information.

Configuring the STWireless as DHCP client

To setup the **STWireless** as DHCP client, tick DHCP client on the 'DHCP' web page.



Configuring the STWireless for Auto DHCP

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

At boot time the **STWireless** 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 **STWireless** becomes a DHCP server.

To allow the **STWireless** to act as Auto DHCP client/server, tick

Auto DHCP

Client timeout (seconds): on the *'DHCP'* web page.

Additionally, you can configure the *'Client timeout'* in seconds.

Via the *'DHCP server configuration'* web page, you can configure the **STWireless** DHCP server settings. See subsection 11.3.4 for more information.

Automatic IP addressing

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

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

Indeed, when the **STWireless** 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 too 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.

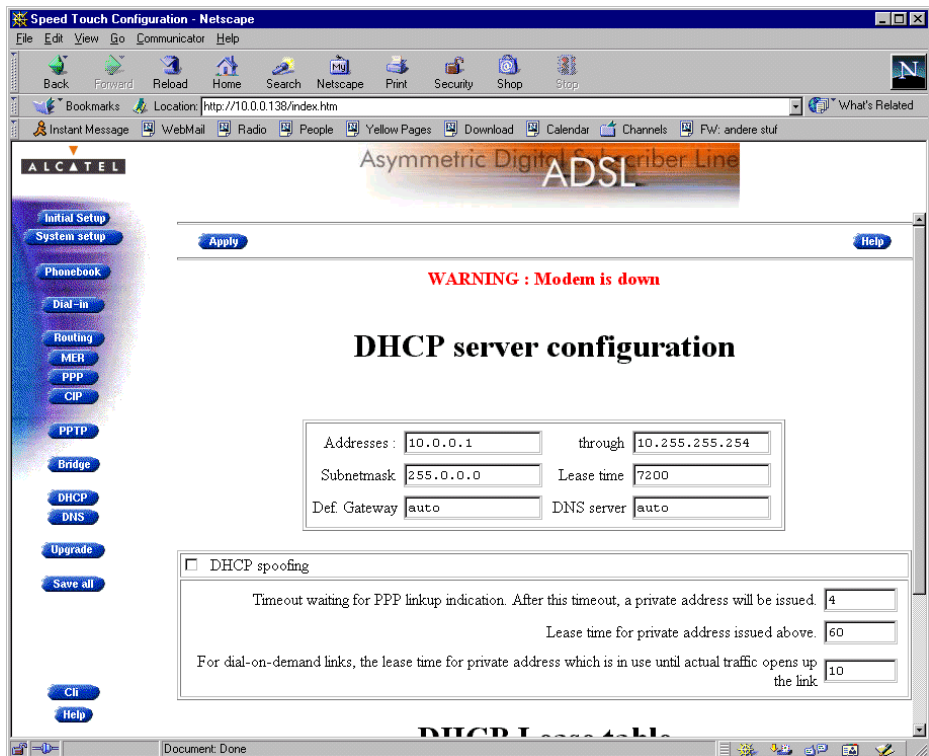
If the DHCP server is back online, the client will now lease an IP address from the server, after discarding its temporary automatic IP address.

11.3.4 Configuring the STWireless DHCP Server

Introduction If the **STWireless** is configured for 'Auto DHCP' or 'DHCP server', additional configuration must be done.

- In this subsection**
- ▶ The 'DHCP server configuration' Web Page
 - ▶ DHCP Server IP Addressing Box
 - ▶ DHCP Spoofing Box
 - ▶ DHCP Lease Table.

The 'DHCP server configuration' web page Clicking **Advanced** on the 'DHCP' web page, pops up the 'DHCP server configuration' web page:



DHCP server IP addressing box

This box allows to specify the **STWireless** DHCP server features:

Addresses :	<input type="text" value="10.0.0.1"/>	through	<input type="text" value="10.255.255.254"/>
Subnetmask	<input type="text" value="255.0.0.0"/>	Lease time	<input type="text" value="7200"/>
Def. Gateway	<input type="text" value="auto"/>	DNS server	<input type="text" value="auto"/>

DHCP server IP addressing box options

You can configure following parameters:

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

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

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

DHCP spoofing box

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

See section 8.4.7 for more information on PPP-to-DHCP spoofing.

<input type="checkbox"/> DHCP spoofing	
Timeout waiting for PPP linkup indication. After this timeout, a private address will be issued.	<input type="text" value="4"/>
Lease time for private address issued above.	<input type="text" value="60"/>
For dial-on-demand links, the lease time for private address which is in use until actual traffic opens up the link	<input type="text" value="10"/>

DHCP spoofing box options

You can configure following parameters:

Field	This configures ...	Default
<i>Timeout</i>	The time limit the STWireless is waiting for a negotiated PPP connection session IP address. After timeout a Private PPP connection session IP address will be issued.	4 seconds
<i>Lease Time</i>	The time (Lease Time) the Private PPP connection session IP address, issued after timeout, can be assigned to the STWireless .	60 seconds
<i>Dial-on-Demand Lease Time</i>	The lease time for the Private PPP dial-on-demand IP address which is in use until actual traffic opens up the link.	10 seconds

DHCP lease table This table allows you to manually assign IP addresses to devices, identified by their MAC address, with the possibility to let this lease expire after some specified time.

Client id	address	Expires	State	Action
Use input fields below to add a new entry				
<input type="text"/>	<input type="text"/>	-	-	<input type="button" value="Add"/>

DHCP lease table options You can configure following parameters:

Field	Description								
<i>Client ID</i>	Configures the MAC address of the device the STWireless leases to.								
<i>Address</i>	Configures the lease IP address for the device.								
<i>State</i>	Indicates if the lease is: <table border="1"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>on</td> <td>Device is up, running and using the lease.</td> </tr> <tr> <td>off</td> <td>Device is unreachable.</td> </tr> <tr> <td>expired</td> <td>Timeout time limit has expired for the lease.</td> </tr> </tbody> </table>	Value	Description	on	Device is up, running and using the lease.	off	Device is unreachable.	expired	Timeout time limit has expired for the lease.
Value	Description								
on	Device is up, running and using the lease.								
off	Device is unreachable.								
expired	Timeout time limit has expired for the lease.								
<i>Action</i>	Contains one of the two following action buttons: <table border="1"> <thead> <tr> <th>Button</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td><input type="button" value="Add"/></td> <td>Manually add a lease to the list.</td> </tr> <tr> <td><input type="button" value="Delete"/></td> <td>Delete an existing lease.</td> </tr> </tbody> </table>	Button	Action	<input type="button" value="Add"/>	Manually add a lease to the list.	<input type="button" value="Delete"/>	Delete an existing lease.		
Button	Action								
<input type="button" value="Add"/>	Manually add a lease to the list.								
<input type="button" value="Delete"/>	Delete an existing lease.								

11.4 IP Routing

Introduction Next to the ADSL router part, the **STWireless** supports also standard IP routing via its IP router.
This section aims to familiarize you with the **STWireless** IP router abilities.

In this section

Topic	See
The STWireless IP router	11.4.1
Configuring the STWireless IP Routing Table	11.4.2

11.4.1 The STWireless IP Router

Introduction Because the **STWireless** 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 **STWirelessIP** 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 STWireless IP routing table

Depending on the configuration made, the **STWireless** 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 **STWireless** and is explained in subsection 11.4.2.

Example of the STWireless extended IP routing table

The following table is an example of the **STWireless** 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

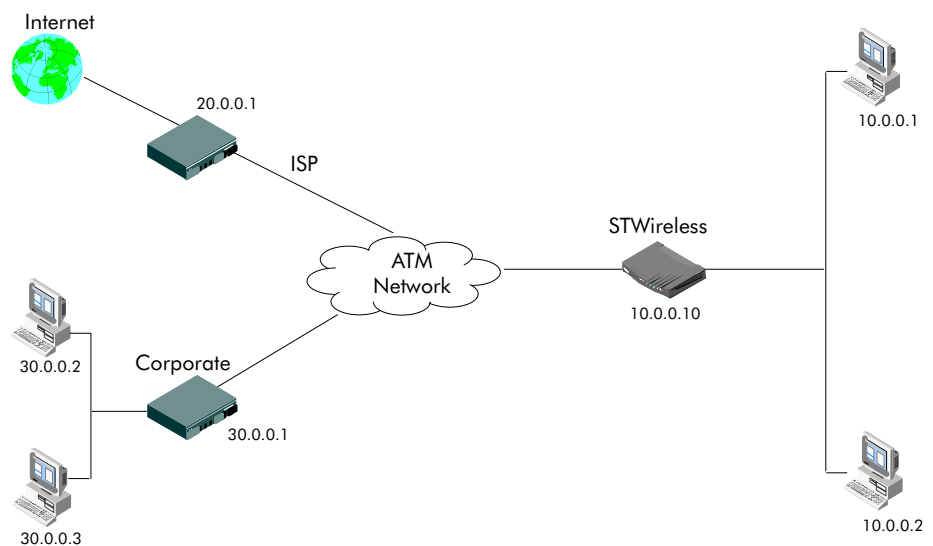
11.4.2 Configuring the STWireless IP Routing Table

Introduction The main function of the IP router in the **STWireless**, is to route IP packets from the local network to the remote networks over the ATM/ADSL connections and vice versa.

In this subsection, configuration of the STWireless IP routing table is described.

- In this subsection**
- ▶ General ATM/ADSL End-to-End IP Architecture
 - ▶ ATM/ADSL IP Routing
 - ▶ **STWireless** Power-on IP Routing Table Configuration
 - ▶ IP Route Table
 - ▶ Adding Specific Routes to the 'IP Route' Table
 - ▶ Criteria for a Valid IP Route.

General ATM/ADSL end-to-end IP architecture The figure below provides an overview of the general end-to-end IP architecture:



ATM/ADSL IP routing

Routing to ATM/ADSL connections actually means:

- ▶ Routing between the local (W)LAN and Classical Logical IP subnets and vice/versa
- ▶ Routing between the local (W)LAN and PPP 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 (PPP, 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.

**STWireless power-on
IP routing table
configuration**

When the **STWireless** is powered, routes are automatically configured in the routing table, e.g.:

- ▶ As soon as the Ethernet interface is up and running, a route (being the IP address of the Ethernet interface) is added
 - ▶ If a CIP member is created and configured with an IP address, this IP address will show up in the table
 - ▶ The IP address negotiated between the remote peer and a PPP connection (configured for Always-On) will also be automatically added to the routing table.
-

'IP route' table If you browse to the 'Routing' web page (See section 18.2 for more information), you can find the 'IP route' table:

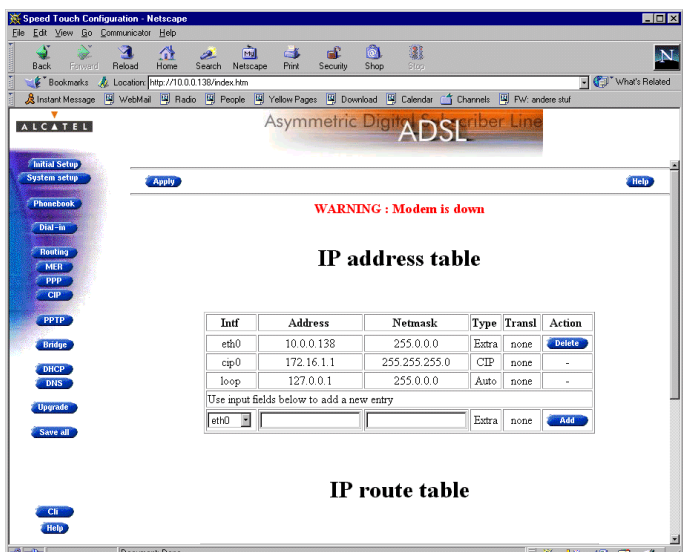
Destination	Source	Gateway	Intf	Action
10.0.0.0/8	10.0.0.0/8	10.0.0.138	eth0	Delete
255.255.255.255/32	any	10.0.0.138	eth0	Delete
10.0.0.138/32	any	10.0.0.138	eth0	Delete
172.16.1.1/32	any	172.16.1.1	cip0	Delete
127.0.0.1/32	any	127.0.0.1	loop	Delete
172.16.1.0/24	any	172.16.1.1	cip0	Delete
10.0.0.0/8	any	10.0.0.138	eth0	Delete



Use input fields below to add a new entry

<input type="text"/>	<input type="text"/>	<input type="text"/>	-	Add
----------------------	----------------------	----------------------	---	-----

Adding specific routes to the 'IP route' table

Proceed as follows:

Step	Action and Description
1	<p>Browse to the 'Routing' web page:</p>  <p>The screenshot shows the 'Speed Touch Configuration' web page in a Netscape browser. The 'Routing' menu item is selected in the left sidebar. The main content area displays a 'WARNING: Modem is down' message and two tables: 'IP address table' and 'IP route table'. The 'IP address table' has columns for Intf, Address, Netmask, Type, Transl, and Action. The 'IP route table' has input fields for Intf, Address, Netmask, and Type, with an 'Add' button.</p>

Step	Action and Description								
2	<p>In the 'IP route' table, you can configure an IP route, using the table's bottom row.</p> <p>Fill in the following IP route parameters:</p> <table border="1"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Destination</td> <td>The IP prefix of the destination, or "next-hop" device.</td> </tr> <tr> <td>Source</td> <td>The IP prefix of the source device (pool). Specifying any, indicates that all traffic, coming from the Ethernet interface, is sent over this route</td> </tr> <tr> <td>Gateway</td> <td>The IP address of the gateway.</td> </tr> </tbody> </table> <p>Note: See section 11.1.1 for more information on the prefix notation.</p>	Value	Description	Destination	The IP prefix of the destination, or "next-hop" device.	Source	The IP prefix of the source device (pool). Specifying any , indicates that all traffic, coming from the Ethernet interface, is sent over this route	Gateway	The IP address of the gateway.
Value	Description								
Destination	The IP prefix of the destination, or "next-hop" device.								
Source	The IP prefix of the source device (pool). Specifying any , indicates that all traffic, coming from the Ethernet interface, is sent over this route								
Gateway	The IP address of the gateway.								
3	Click 								
4	Click  to store the changes in permanent memory.								

Criteria for a valid IP route

The criteria for an IP route to be valid are that:

- ▶ The destination and source entries must yield correct prefixes
- ▶ The gateway must be directly connected.

12 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 datagrams 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*, or *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 **STWireless**'s DNS abilities.

In this chapter

Topic	See
STWireless DNS Resolving	12.1
Configuring your STWireless DNS Server	12.2

12.1 Speed Touch Wireless DNS Resolving

Introduction The **STWireless** 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 **STWireless**, you can give your nodes names and let a local DNS server, e.g. the **STWireless** itself, do the resolving.

Example of local DNS resolving

In the following example, a (W)LAN is built around the **STWireless**.

In this scenario, it is assumed that the **STWireless** 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 **STWireless** 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 **STWireless** (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 <code>ping YourPC</code> on <i>MyPC</i> .
2	Via this command, <i>MyPC</i> launches a DNS request, basically asking: “What is the IP address of <i>YourPC.lan</i> ?”
3	As the STWireless is the DNS server, it will respond with the appropriate IP address, being 10.0.0.1.
4	The ping utility in <i>MyPC</i> will now submit the ping to 10.0.0.1 which may eventually reply.

Non-local DNS resolving

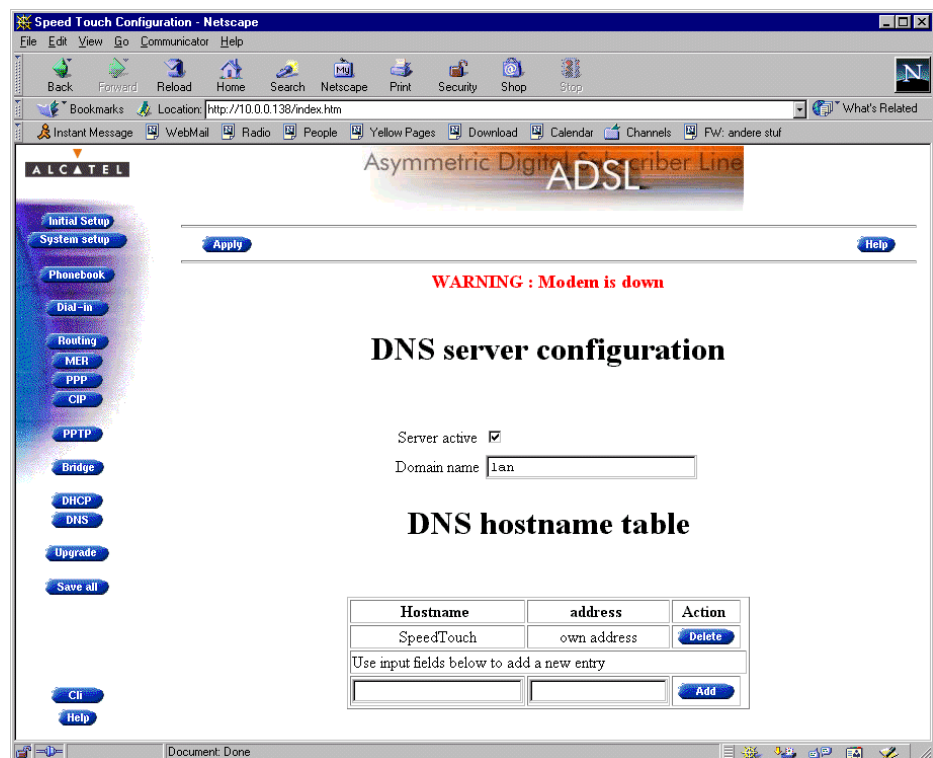
The **STWireless** resolves names within the local domain, i.e. *lan* (default **STWireless** setting) as described above.

However, all other domain names, e.g. `Alcatel.com`, cannot be resolved by the **STWireless**, and are forwarded over the appropriate link on the ADSL line.

12.2 Configuring the Speed Touch Wireless DNS Server

In this subsection The example of section 12.1, refers to a new (W)LAN, using the default **STWireless** configuration, thus as well as Auto DHCP server, as DNS server.
In case the **STWireless** is added to a existing (W)LAN, configuration of the **STWireless** DNS server might be necessary to meet the existing (W)LAN conditions.

The STWireless 'DNS' web page Clicking **DNS** in the left pane of the **STWireless** web pages, pops up the 'DNS' web page:



DNS server field This field allows configuration of the **STWireless** DNS server:

Server active

Domain name

DNS server field components You can configure the following parameters:

Field	Description	Default
Server active	This check box enables (✓), or disables the STWireless DNS server.	✓, STWireless DNS server active.
Domain Name	Specifies the domain name of your (W)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.	lan

DNS hostname table This table allows you to manually configure DNS hostnames to hosts, identified by their IP address:

Hostname	address	Action
SpeedTouch	own address	Delete
Use input fields below to add a new entry		
<input type="text"/>	<input type="text"/>	Add

DNS hostname table components You can configure the following parameters:

Field	Description
Hostname	A DNS hostname of your choice for the PC.
Address	The IP address of the PC to which you assign the DNS hostname.

13 Networking 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 **STWireless**'s programmable Firewall.

In this chapter

Topic	See
Operation of the Firewall	13.1
Firewall Model	13.2
Firewall Actions	13.3
Firewall Criteria	13.4
Firewall and NAPT	13.5
Firewall Configuration	13.6
Firewall Configuration Examples	13.7

13.1 Operation of the Firewall

What is the STWireless Firewall

The **STWireless** 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 **STWireless** Firewall the **STWireless** acts as well as network gateway and proxy server to contact the outside world via the ADSL line

The **STWireless** 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 STWireless Firewall works

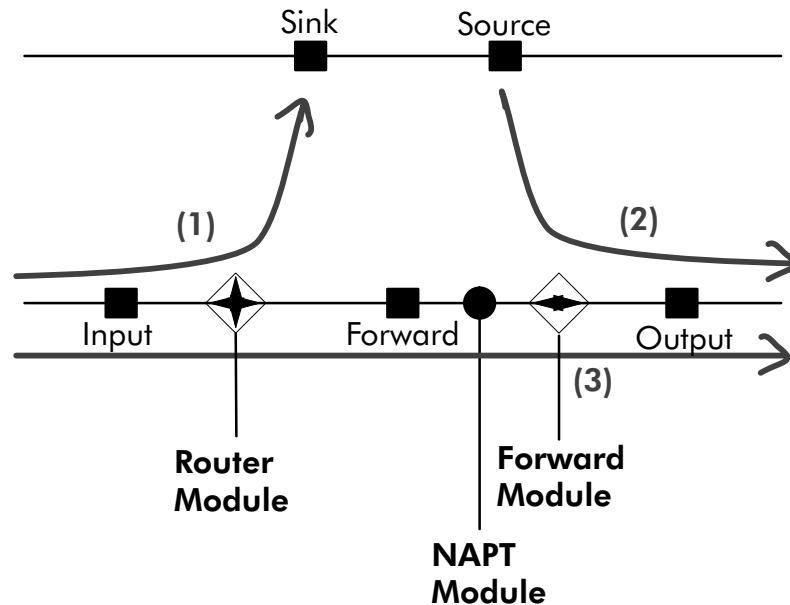
Packets are intercepted at certain Packet Interception Point (PIP), called *hooks*, in the **STWireless** IP router. At this points, they are matched against a chain, which comprises rules (at least one). These rules determine the type of control implemented on the packets.

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.

13.2 Firewall Model

STWireless Firewall Model

The following figure shows a model of the **STWireless** Firewall:



STWireless Firewall modules

The following modules can be identified (See Firewall model):

- ▶ **Router Module** : This module, which has nothing to do with the **STWireless** IP router, is responsible for the traffic “within” the **STWireless** 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.
- ▶ **NAPT Module** : This module is responsible for the translation of IP addresses, in case firewalling is used with NAPT.

STWireless 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 **STWireless** IP router, or the local host.
 - ▶ **Sink** : The point of all traffic destined to the **STWireless** 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 **STWireless**
At this point it can be determined whether the packet is allowed to be handled, i.e. routed, by the **STWireless** IP router.
 - ▶ **Source** : The point of all traffic sourced by the **STWireless** 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 **STWireless** IP router, or local host.
-

STWireless Firewall streams

The following streams (See Firewall model) can run through the PIPs:

- ▶ **(1) Input –> Sink** : The flow of packets exclusively destined to the **STWireless**.
 - ▶ **(2) Source –> Output** : The flow of packets sourced exclusively by the **STWireless** itself
 - ▶ **(3) Input –> Forward –> Output** : The flow of packets sourced by the WAN, forwarded towards the local network, or vice versa.
-

13.3 Firewall Actions

STWireless 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.
-

13.4 Firewall Criteria

STWireless 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 '**STWireless** 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.
-

13.5 Firewalling and NAPT

What is NAPT NAT (Network Address Translation), is the translation of an IP address used within one network to another IP address, known within another network.

NAPT (Network Address and Port Translation) uses a combination of IP addressing and port number mapping to create unique combinations. That way, the **STWireless** can determine which packet, sourced by the WAN, is destined to which device on your local (W)LAN, and vice versa, without revealing the internal device information towards the remote side.

STWireless Firewall and NAPT

The position of the *Input*, *NAPT*, *Forward* and *Output* logical processing modules in the overall **STWireless** Firewall model is relative to the traffic direction. In contrast, the **STWireless**'s WAN and (W)LAN interfaces are "physical" interfaces; their position is not relative to the traffic direction.

The NAPT module is situated between the Forward and Output hook (See **STWireless** Firewall model). Since the traffic direction will determine input, and output, the NAPT 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 NAPT-translated or not.

If rules are set on the Output hook and NAPT 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 NAPT is activated, the IP address that identifies a local device, will be different depending on the direction of the traffic.

13.6 Firewall Configuration

Configuring the STWireless Firewall

In order to create a Firewall, suitable for your needs, you can create a chain on every hook at the **STWireless**. 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 **STWireless** firewall only via the CLI.

See chapter 19 for more information.

Default STWireless Firewall configuration

The **STWireless** Firewall is enabled by default with following behavior:

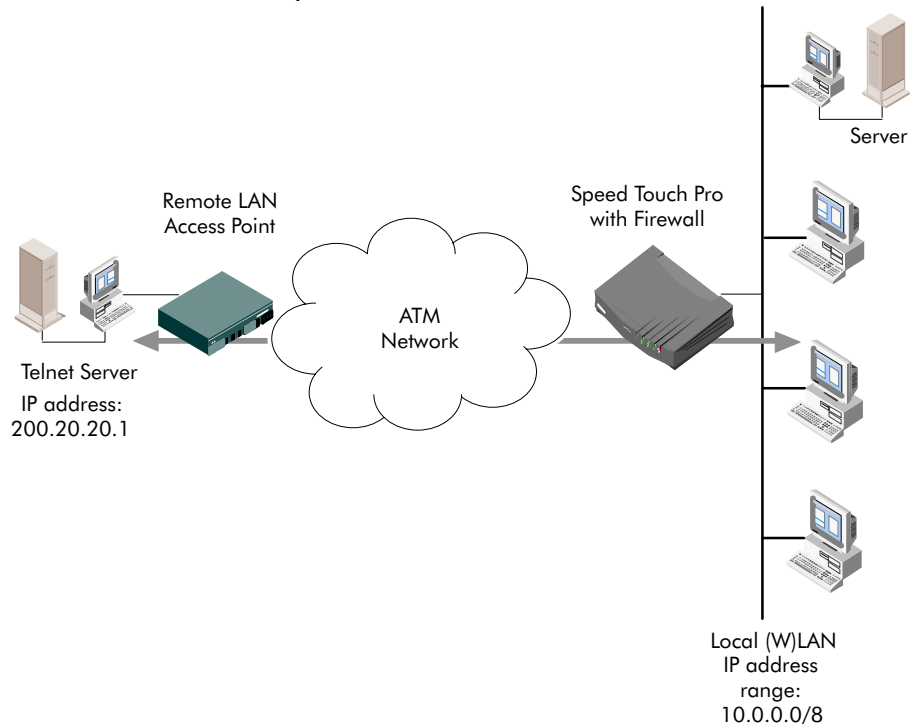
Packets migrating

- ▶ from WAN to WAN are dropped
 - ▶ from **STWireless** to WAN are dropped, except Port 53 (DNS)
 - ▶ from **STWireless** to (W)LAN are allowed
 - ▶ from (W)LAN to **STWireless** 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.
-

13.7 Firewall Configuration Examples

Example setup In the following two simple examples are provided to show the working and configuration of the **STWireless** Firewall.

Both are based on a small (W)LAN, consisting of the **STWireless** and a small number of PCs, all configured with dynamic 'Net10' IP addresses, leased by the **STWireless**'s DHCP server:



In both examples the **STWireless** 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 NAPT

NAPT is not applied on your local (W)LAN for this ADSL 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 **STWireless** 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 NAT

NAPT is applied for this ADSL connection; all outgoing 'Net10' IP addressed packets are translated into the 192.6.11.10 IP address. So the complete local 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 **STWireless** 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 19 for more information on **STWireless's** Firewall CLI configuration.

Speed Touch™ Wireless

Wireless LAN Services

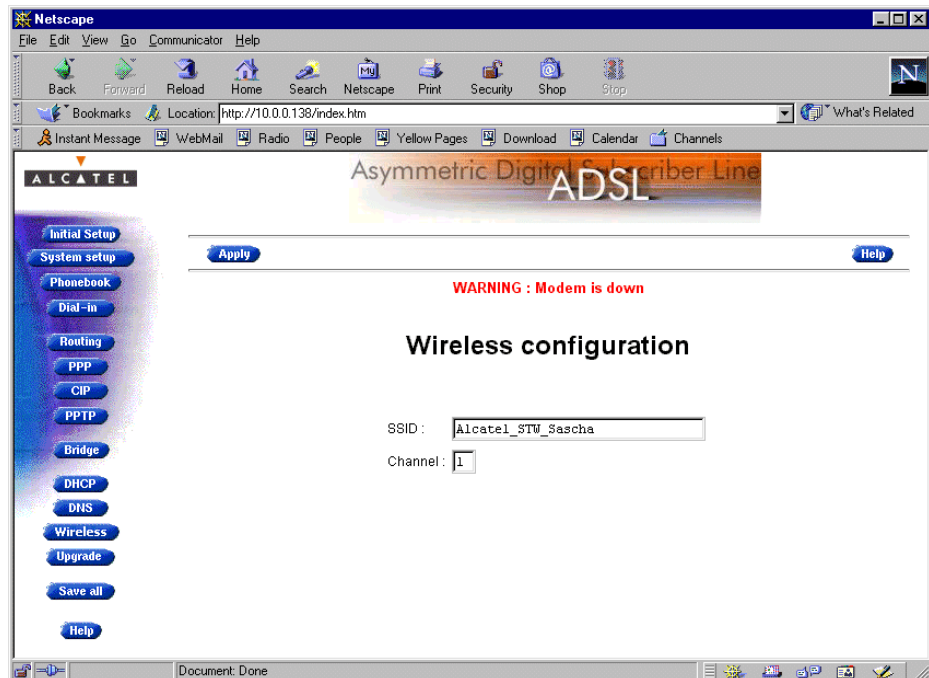
14 Wireless LAN Services – WLAN Configuration

Introduction After having initial WLAN connectivity, you can configure your **STWireless** WLAN parameters. Additional configuration of your WLAN environment settings might be required in case, e.g. another **STWireless**, with identical WLAN configuration, is located nearby.

- In this chapter**
- ▶ The **STWireless** 'Wireless' Web Page
 - ▶ The 'SSID' Field
 - ▶ 'Channel' Field
 - ▶ Connectivity after Configuration
-

The STWireless 'Wireless' web page

Clicking **Wireless** in the left pane of the **STWireless** web pages, pops up the 'Wireless' web page (See chapter 18 for more information):



The 'SSID' field

The following figure shows the 'SSID' field:

SSID:

The Service Set ID (SSID) allows you to uniquely identify your **STWireless** WLAN in the radio environment. This can be useful in case multiple WLAN environments are present nearby your location.

Changing the default SSID 'Alcatel_STW' into another value can be useful in case another **STWireless** is located nearby. It will avoid a WLAN client from his wireless network to connect by accident to yours.

The 'Channel' field The following figure shows the 'Channel' field:

Channel :

The channel number identifies the frequency on which your WLAN connectivity is enabled in the WLAN environment.

Changing the default channel number to another value can be useful in case you know another wireless equipment runs nearby yours, e.g. another **STWireless** WLAN environment. This way you can avoid sharing the channel bandwidth with other WLANs by selecting different channel numbers for concurrent WLANs.

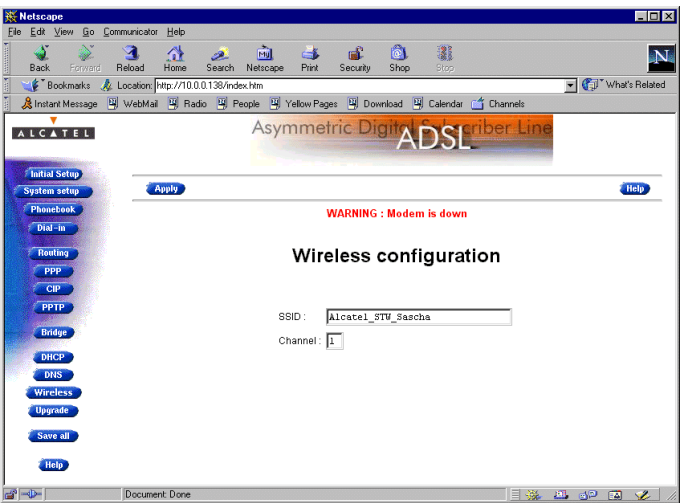
You may not freely choose any channel number. The channel number range is from 1 up to 14 (included).

Moreover, restrictions apply depending on the country where the **STWireless** is used:

- ▶ US: 1, 6, or 11
 - ▶ Europe (except France): 1, 7, or 13
 - ▶ France: 14.
-

Configuring Wireless parameters

Proceed as follows:

Step	Action and Description
1	<p>Browse to the 'Wireless Configuration' web page.</p> 
2	<p>Enter the appropriate configuration in the following fields:</p> <ul style="list-style-type: none"> • the 'SSID' name of your WLAN • the 'channel' number for your WLAN connectivity <p>Note: See the corresponding topics in this chapter for more information.</p>
3	<p>Click Apply and Save all to finish the procedure.</p>

WLAN connectivity after configuration

After the SSID, and/or channel number has been changed inside the **STWireless**, the contact is lost.

All your WLAN clients must be reconfigured, and/or re-authenticated to use the same new SSID, and/or new channel number as the **STWireless**.

See section 3.1 for more information.

Speed Touch™ Wireless

Maintenance

15 Maintenance – Software Upgrade

Software Upgrade The **STWireless** supports two software upgrade possibilities:

- ▶ A new version of the software can be downloaded via the ADSL line to your **STWireless**.
- ▶ You can upload new **STWireless** software yourself from a PC on your local LAN.

Both features, presented in this chapter, are simultaneously supported. However the final result depends on the ADSL provider's policy.

In this chapter

Topic	See
Upload Software from a PC	15.1
Software Download	15.2

15.1 Upload Software from a PC

Introduction Alcatel ADSL products continue to evolve. By upgrading software, the **STWireless** is able to follow this evolution.

- In this section**
- ▶ The 'Software Upgrade' Web Page
 - ▶ 'Upgrade' Web Page Components
 - ▶ 'Upgrade' Web Page Buttons
 - ▶ Upgrade Preconditions
 - ▶ Uploading Upgrade Software
 - ▶ Activating Upgrade Software.

The 'Software Upgrade' web page

Click **Upgrade** to pop up the 'Upgrade' web page:



'Upgrade' web page components

The following fields are shown:

▶ *'Active software version'*


Indicates the software version that the **STWireless** is currently using.

▶ *'Passive software version'*

Indicates the software version resident in the **STWireless**, 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 **STWireless** upgrade software package to be uploaded.

Clicking  allows you to browse to the location of the upgrade software.

'Upgrade' web page components

The following buttons are available:

Button	Functionality
	To start the upload process. The software package indicated by the <i>Software path</i> will be transferred to the STWireless to become the passive software version.
	To remove the passive software version from the STWireless memory.
	To switch active and passive software versions after a successful upload. Your STWireless will reboot and come online again with the new version.

Upgrade Preconditions

A valid **STWireless** software package must reside either on your harddisk, on a floppy disk, or CD-rom.

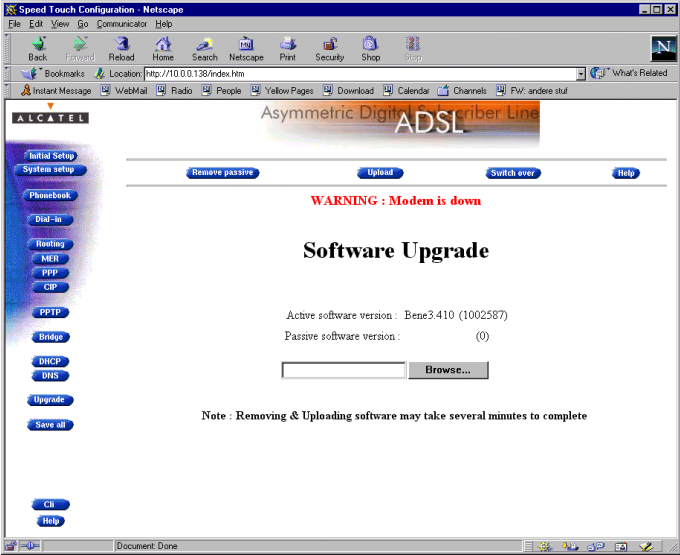
For new software upgrade packages, please contact your SP, or check the Alcatel web sites at:

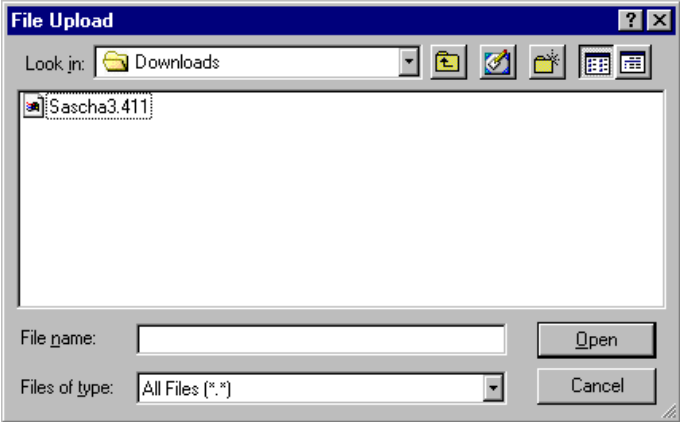


http://www.alcatel.com

http://www.alcateldsl.com

Uploading software

Proceed as follows:

Step	Action and Description
1	<p>Browse to the 'Software Upgrade' web page</p>  <p>In the 'Active software version' field the software package that is running is labeled.</p>
2	<p>Check whether the 'Passive software version' field is empty. If not, click Remove passive</p>
3	<p>Click Browse... next to the <i>Software path</i> input field to locate the upgrade software package</p> <p>Note: If the path is known, you can immediately enter it in the <i>Software path input field</i> and skip step 4 in this procedure.</p>

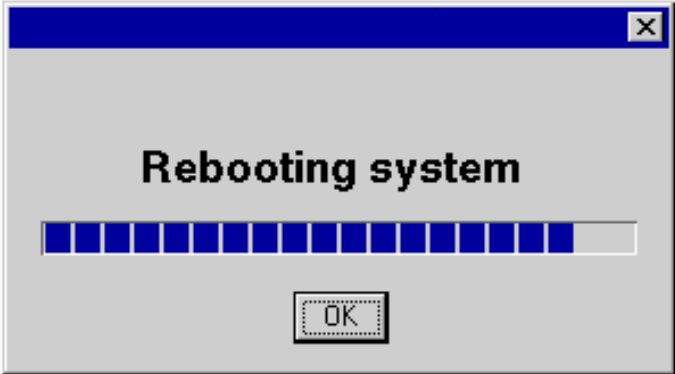
Step	Action and Description
4	<p>The 'File Upload' window pops up:</p>  <p>This window allows you to browse to the location of the upgrade software package on either your harddisk, floppy, or CD-rom.</p>
5	<p>Click on the appropriate upgrade software package name to select it, and click </p> <p>As a result, the upgrade software location will be inserted in the <i>Software path</i> field.</p>
6	<p>Click  to start the upload.</p> <p>As a result the upgrade software package name will appear in the '<i>Passive software version</i>' field.</p> <p>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.</p>

Upload Result After a successful upload, two software versions are stored on the **STWireless**:

- ▶ The running, active version
- ▶ The dormant, passive version.

Activating upgrade software

Proceed as follows to switch passive upgrade and active running software versions:

Step	Action and Description
1	<p>If needed, browse to the 'Upgrade' web page.</p> <p>Note: Make sure a passive software version is labeled in the 'Passive software version' field.</p> <p>If not, firstly upload a upgrade software package as described in the previous procedure.</p>
2	<p>Click Switch over to start the switching of the two versions.</p> <p>After switching the versions, the STWireless reboots:</p> 

Result After reboot your **STWireless** will come online with the new version.

In the 'Upgrade' web page you will notice that active and passive versions (prior to the upgrade) have trade places.

15.2 Software Download

Introduction The **STWireless** supports a second software upgrade possibility: a new version of the software can be downloaded from the ADSL network to your **STWireless**.
This can be done via the **STWireless** 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 **STWireless**.
Software download will happen almost unnoticed, while you are connected to the ADSL line.
The removal of a possible dormant software version, the download itself, and the switching of both versions is performed automatically.
ADSL service can be interrupted for a short period due to a reboot of the **STWireless**.

Result You will notice a change in the software version if you browse to the **STWireless** 'Software Upgrade' web page.

16 Maintenance – Speed Touch Wireless Security

In this chapter Your **STWireless** is a highly advanced product, operating according to the many configurations set via the **STWireless** Web interface, or via the CLI.

In this way, **STWireless** operation is vulnerable to misconfiguration by other users.

Therefore, the **STWireless** 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 **STWireless**, as your name, birth date, or phone number.



Forgetting the System Password

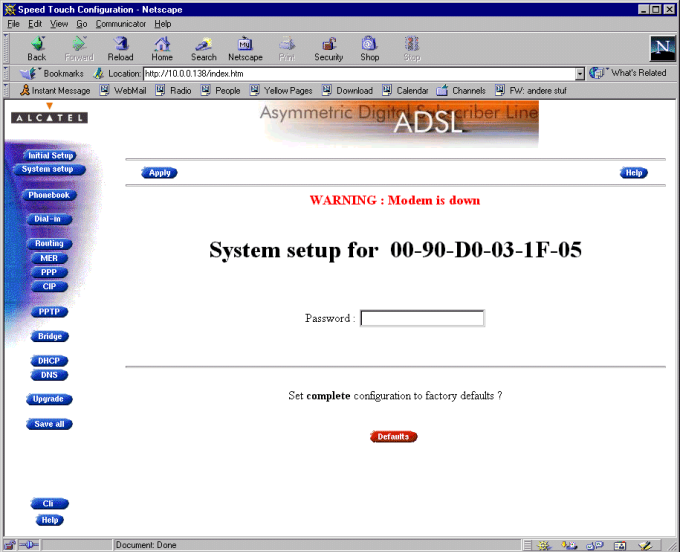
In case you forgot the system password, you are no longer able to access the web interface, or the CLI, and you will be no longer able to (re)configure the **STWireless** settings.

Therefore, write your system password down and keep it on a safe place.

Otherwise, a *Switch-to-Defaults*, must be performed, restoring all original settings of the **STWireless**.

Setting a system password

Proceed as follows:

Step	Action and Description
1	<p>Browse to the 'System' web page.</p> 
2	<p>In the 'Password' field, fill in a password.</p> <p>Note: Asterisks will appear instead of the password. The number of asterisks is at random:</p> <p style="text-align: center;">System setup for 00-80-9F-24-AB-CF</p> <p style="text-align: center;">Password: <input type="password" value="*****"/></p>
3	<p>Click Apply in the header frame.</p>
4	<p>To make your password permanent, click Save all in the menu frame.</p>
5	<p>Authenticate yourself, using the system password, you just configured.</p>

Result Every time you want to access the **STWireless** web pages, or (Telnet) CLI, you must authenticate yourself, using the system password you configured.

Clearing a system password

Proceed as follows to set a system password for your **STWireless**:

Step	Action and Description
1	Browse to the 'System' web page.
2	In the 'Password' field, delete the asterisks <div style="text-align: center;"> System setup for 00-80-9F-24-AB-CF Password : <input type="text"/> </div>
3	Click Apply in the header frame.
4	To make the deletion permanent, click Save all in the menu frame.

Result No authentication is required anymore to access the **STWireless** web pages, or the (Telnet) CLI.

17 Maintenance – Lost Speed Touch Wireless

Introduction Non accessibility to your **STWireless** may occur if wrongly configured, simply by forgetting its IP address, or forgetting the system password.

Due to the flexible nature of the **STWireless**, you may end up in a situation where restoring all of the original defaults is the only solution.

The **STWireless** has tools to cope with these situations.

In this chapter

Topic	See
Ping-of-Life™	17.1
STWireless Reset	17.2

17.1 Ping-of-Life

Introduction The **STWireless** offers a unique method to supply an IP address to the **STWireless**.

This method, the *Ping-of-Life™*, allows to provide the **STWireless** 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 **STWireless**.

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 STWireless , and allow the POST to end (this takes about 30 seconds).
3	Ping this same IP address within 60 seconds after the STWireless ended its POST. If everything goes well, the STWireless has assimilated this IP address.
4	Save the new IP setting via the STWireless web 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.

The Ping-of-Life™ procedure

Proceed as follows:

Step	Action and Description
1	Turn off the STWireless .
2	Open an DOS window (Windows OS), or a terminal window (UNIX, Linux) on a PC.
3	In the DOS window, or terminal window, execute: arp -a This command allows you to overview the current entries in the ARP cache.

Step	Action and Description
4	Add a static entry to the ARP cache, according to following syntax: <pre>arp -s <STWireless IP address> 01-90-D0-80-01-01</pre> or <pre>arp -s <STWireless IP address> 01:90:D0:80:01:01</pre> <STWireless IP address> is a placeholder for the IP address to be assigned to the STWireless .
5	Verify if this step was successful. Execute: <code>arp -a</code> a second time. In the entries list, your <code>arp -s</code> command entry should be added.
6	Turn on the STWireless and allow the POST to end.
7	Ping the IP address you just entered in the ARP cache within 60 seconds: <pre>ping <STWireless IP address></pre>
8	If successful, the STWireless has configured this IP address and will reply to the ping.
8	You may clear the entry in the ARP cache by issuing the following command: <pre>arp -d <STWireless IP address></pre> Note: Leaving the entry in the ARP cache does not harm the general operation.
10	Browse to the STWireless web pages, and  to make the new IP address permanent.

Ping-of-Life™ with multiple PC-NICs

If your PC is equipped with multiple PC-NICs, or WLAN adapters, make sure that the procedure is applied to the one which joined the **STWireless** WLAN environment.

In the following syntax, <Interface IP address> identifies the particular PC-NIC:

```
arp -<a,s,d> <STWireless IP address> -N <interface IP address>
```



IP Addresses and Subnet Masks

Make sure that the intended **STWireless** 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.

Example DOS box In the following figure all the steps are shown as an example of setting **STWireless**'s IP address to 10.0.0.145 from a PC with an MS Windows OS:

```

MS-DOS Prompt
Auto
C:\>arp -a
No ARP Entries Found
C:\>arp -s 10.0.0.145 01-90-d0-80-01-01
C:\>arp -a
Interface: 10.0.0.1 on Interface 0x3000004
Internet Address      Physical Address      Type
10.0.0.145           01-90-d0-80-01-01   static
C:\>ping 10.0.0.145
Pinging 10.0.0.145 with 32 bytes of data:
Reply from 10.0.0.145: bytes=32 time=3ms TTL=255
Reply from 10.0.0.145: bytes=32 time=1ms TTL=255
Reply from 10.0.0.145: bytes=32 time=1ms TTL=255
Reply from 10.0.0.145: bytes=32 time=3ms TTL=255
Ping statistics for 10.0.0.145:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 2ms
C:\>
    
```

The 'Ping -t' command You can avoid waiting 30 and then 60 seconds by proceeding as follows:

Step	Action and Description
1 .. 5	Follow the <i>Ping-of-Life™</i> procedure as described, from step 1 up to step 5.
6	Initiate a continuous ping, by executing ping -t <STWireless IP address>
7	Turn on the STWireless .
8	After the POST, the STWireless will reply to the ping.
9	Terminate the continuous ping by pressing CTRL-C.
10	Save the IP address via the STWireless web pages.

17.2 Speed Touch Wireless Reset

Overview of the To-Defaults methods

To restore **STWireless**'s 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 and IP address.
 - *Ping-to-Defaults*[™]
Which sets all parameters to original defaults, including the system password and IP address.
- ▶ One hardware method:
 - *Switch-to-Defaults*.
Which sets all parameters to original defaults, including the system password and IP address.



CAUTION

Restoring Original Settings

Be careful when using *To-Defaults* procedures as these destroy changes you previously made to the **STWireless** internal settings.

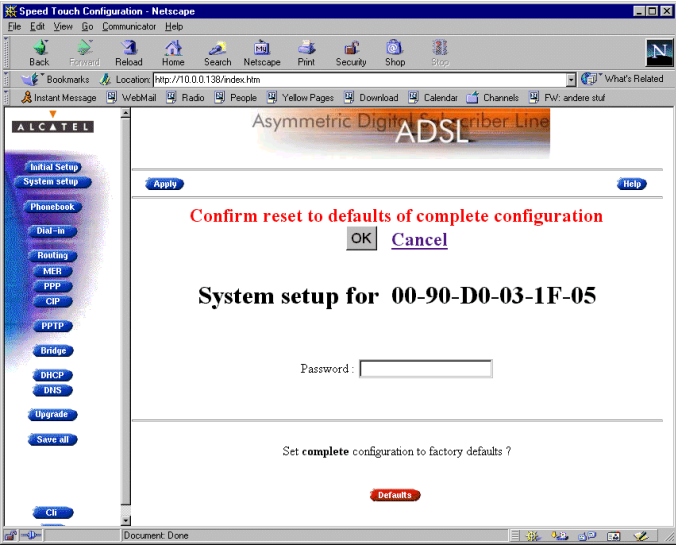
A reset to defaults via a *Ping-to-Defaults*[™], or via a *Switch-to-Defaults*, also implies the **STWireless**'s IP address is reset to 10.0.0.138. As a consequence, IP connectivity with the **STWireless** could be lost. In that case you must execute a *Ping-of-Life*[™].

In this section

Topic	See
Browse-to-Defaults	17.2.1
Ping-to-Defaults [™]	17.2.2
Switch-to-Defaults	17.2.3

17.2.1 Browse-to-Defaults

Procedure

Step	Action and Description						
1	<p>Browse to the 'System' web page.</p> 						
2	<p>If you are sure to reset the STWireless to its original defaults, click Defaults</p>						
3	<p>The STWireless will ask to confirm the reset:</p> <p>Confirm reset to defaults of complete configuration</p> <p>OK <u>Cancel</u></p>						
4	<p>Make the following selection:</p> <table border="1" data-bbox="667 1335 1369 1532"> <thead> <tr> <th>If ...</th> <th>Then click ...</th> </tr> </thead> <tbody> <tr> <td>You are sure that you want to reset the STWireless completely ...</td> <td>OK</td> </tr> <tr> <td>You do not want to continue with the reset to original defaults ...</td> <td><u>Cancel</u></td> </tr> </tbody> </table>	If ...	Then click ...	You are sure that you want to reset the STWireless completely ...	OK	You do not want to continue with the reset to original defaults ...	<u>Cancel</u>
If ...	Then click ...						
You are sure that you want to reset the STWireless completely ...	OK						
You do not want to continue with the reset to original defaults ...	<u>Cancel</u>						
4	<p>To make the reset permanent, click Save all in the menu frame.</p>						
5	<p>Press the reload button of your Web browser.</p>						

Browse-to-Defaults result

After reset, all original configurations of the **STWireless** are restored, except the **STWireless** system password, and Ethernet IP address(es).

17.2.2 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:

Step	Action and Description
1	Turn off the STWireless .
2	Open an MSDOS command prompt window (Windows OS), or a terminal window (UNIX, Linux).
3	Add a static entry to the ARP cache, according to following syntax: arp -s <IP address> 01-90-D0-80-01-FF This <IP address> can be any address <u>within your subnet</u> as long as it is not used by any other member of your local network.
4	Verify if this step was successful. Execute arp -a In the entries list, your arp -s command entry should be added.
5	Turn on the STWireless and allow the POST to end.
6	Ping the IP address <IP address> you just entered in the ARP cache: ping <IP address>
7	You must clear the entry in the ARP cache by issuing the following command: arp -d <IP address>
8	If needed, reconfigure the STWireless 's IP address.

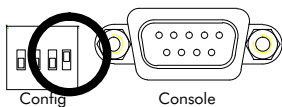
Note The IP address **<IP address>** used to perform a *Ping-to-Defaults*[™] is not assimilated by your **STWireless**. The **STWireless** will restart with the original defaults, including the default IP address 10.0.0.38.

17.2.3 Switch-to-Defaults

Introduction At the back of the **STWireless** there is a set of DIP switches labeled "Config".

Via these switches a hardware reset of the **STWireless**, the *Switch-to-Defaults*, is possible.

Procedure Proceed as follows:

Step	Action and Description
1	Make sure your STWireless is turned on.
2	Put DIP switch number 4 in the UP position:  You will notice that the PWR/Alarm LED flashes amber.
3	Power cycle the STWireless and wait to allow the POST to end. The STWireless will come online with manufacturing defaults.
4	Reset the DIP switch in its original position. If not, the 'PWR/Alarm' LED will flash amber as a warning.
5	After a reset to original defaults a reconfiguration of STWireless's IP address might be necessary. This because the reset to defaults also resets your STWireless's IP address to its default value 10.0.0.138.



DIP Switch Position

Leaving the DIP switch in the UP position, will cause unintended reset to manufacturing defaults !

18 Maintenance – Speed Touch Wireless Web Interface

Introduction The **STWireless** comes with integrated local configuration capabilities.

Two methods exist:

- ▶ Configuration via a Web Browser
- ▶ Configuration through a Command Line Interface (CLI).

The STWireless web interface The local configuration via the **STWireless** web interface, is based on the HyperText Transfer Protocol (HTTP) server/Web browser concept.

It allows configuration of your **STWireless** via a Web browser through HyperText Markup Language (HTML) web pages from any local PC attached to the Ethernet interface(s).

In this chapter

Topic	See
Web Interface Preconditions	18.1
Browsing to the Web Pages	18.2
Web Page Structure	18.3

18.1 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 **STWireless** is a local device and its IP address cannot be resolved by the Proxy server.

Therefore, prior to access the **STWireless** web pages, make sure that, either:

- ▶ Your Web browser is not using a Proxy server
 - ▶ The **STWireless** 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 This section covers the following topics:

Topic	See
Disabling Proxy Servers	18.1.1
Disabling Proxying for Local IP Addresses	18.1.2

18.1.1 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 **STWireless**, 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' check box.
-

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.

18.1.2 Disabling Proxying for Local IP Addresses

Introduction This subsection describes how to avoid that IP addresses, you can connect to directly, as for the **STWireless**, 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, or 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 **STWireless**, or the IP subnetwork address pool.
-

Disabling Proxying for Internet Explorer

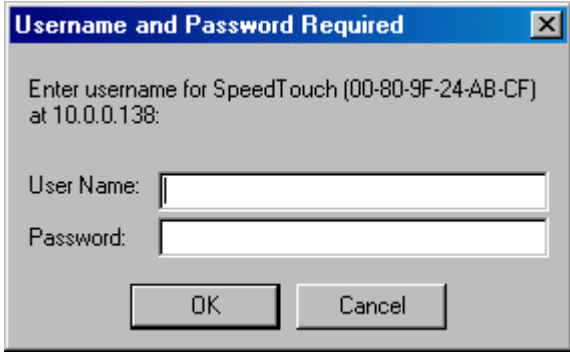
1. Select 'Tools' from the toolbar
 2. From the pop-up menu select 'Internet Options'
 3. In the 'Internet Options' window, select the 'Connections' tab
 4. Click the 'LAN Settings...' button
 5. In the 'Proxy Server' box, check the 'Bypass Proxy servers for local addresses' box, and click 'Advanced'
 6. In the 'Exceptions' settings, add the **STWireless** IP address.
-

Web browser versions

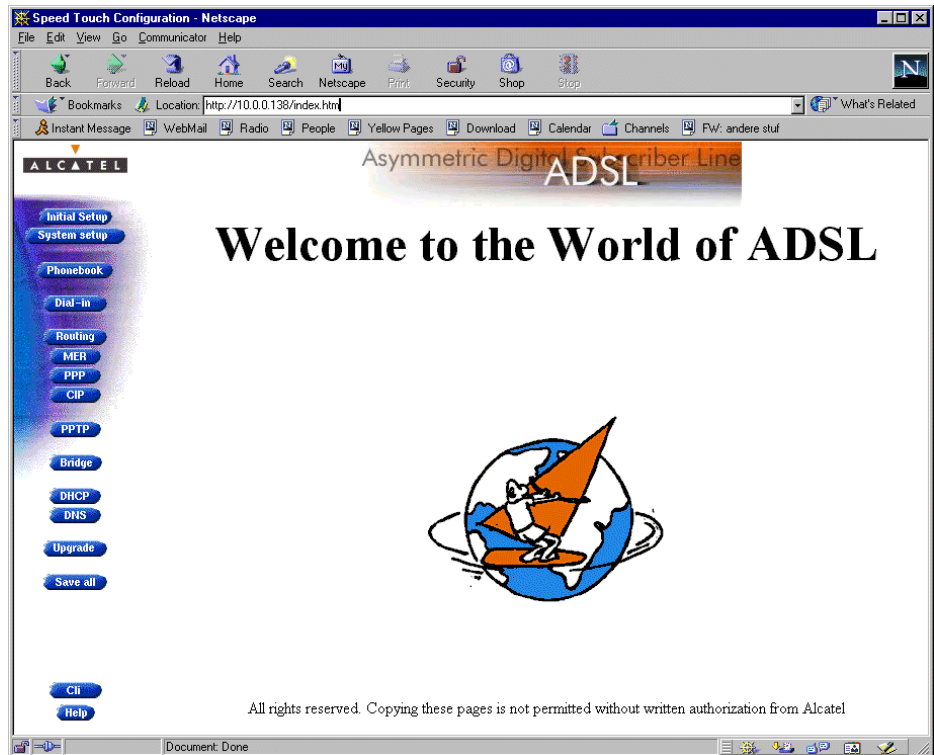
Since several versions of these Web browsers exist, the proxy settings might be located in other menus than the ones described above. Consult the documentation of your Web browser for more information on proxy settings.

18.2 Browsing to the Web Pages

Procedure Proceed as follows:

Step	Action and Description
1	Start the Web browser on your PC or workstation.
2	<p>Contact the STWireless by entering either:</p> <ul style="list-style-type: none"> ▶ The STWireless IP address or ▶ The STWireless DNS hostname. <p>Note: The default IP address is 10.0.0.138 The default DNS hostname is SpeedTouch.</p>
3	<p>If a system password was set (See chapter 16 for more information), an authentication window will pop up:</p> <div style="text-align: center;">  </div> <p>Enter the system password in the 'Password' field and press Enter.</p>

Result As a result the 'Welcome to the World of ADSL' web page pops up:



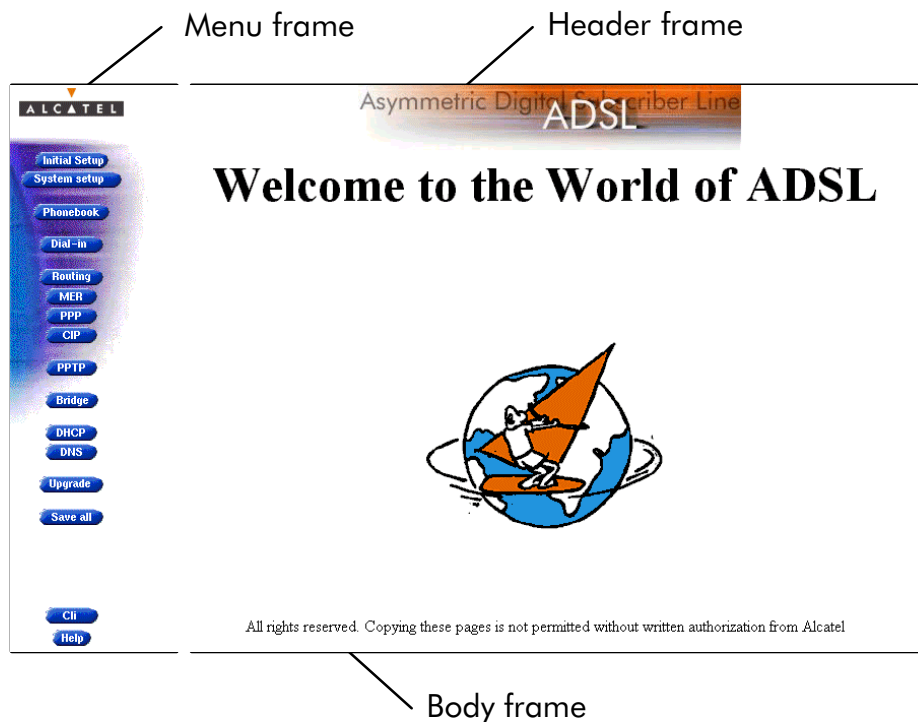
From now on the **STWireless** acts as a Web server sending HTML pages/forms at your request. You can fill out these pages/forms and submit them to the **STWireless**. The latter scans the pages and makes configurations accordingly.

18.3 Web Page Structure

- In this section**
- ▶ **STWireless** Web Page Frames
 - ▶ Header Frame Components
 - ▶ Menu Frame Components
 - ▶ Body Frame Components.

STWireless web page frames

All web pages can be divided into three sections:






Each web page contains:

- ▶ A horizontal bar, referred to as *Menu frame* hereafter
- ▶ A vertical pane, referred to as *Header frame* hereafter
- ▶ The user field, referred to as *Body frame* hereafter.

Header frame components The header frame is present in all of the **STWireless** web pages. Under the generic ADSL banner it contains on most pages also subject related command buttons.










Two command buttons are always available:










Button	Functionality
	To let the changes you made, take effect. However, you must still click  to store the changes to permanent memory.
	To pop up the STWireless online help pages.

Subject related command buttons are only visible in the appropriate web page you have selected.

Menu frame components The Menu frame is generic for all **STWireless**'s web pages. Each menu button represents a **STWireless** configuration web page, yielding all configurational possibilities related to menu subject.

The following buttons are available:

Click this button ...	To ...	See
	Return to the 'Welcome to the World of ADSL' web page.	18.2
	Configure user defined STWireless IP parameters.	11.3.2
	Set a System password Perform a <i>Browse-to-Defaults</i> .	16 17.2.1
	Overview the record of all possible, and existing ATM connection information.	10.2
	Dial-in to WAN via the PPP packet service.	8.2
	Configure the STWireless IP router.	11.4.1
	Configure the MER packet service.	6.3
	Configure the PPP packet service.	8.3
	Configure the CIP packet service.	9.4

Click this button ...	To ...	See
	Overview active PPTP connections.	7.4
	Configure the Bridging packet service. View Bridging MAC layer data.	5.3 5.4.2
	Configure the STWireless DHCP server/client.	11.3.3
	Configure the STWireless DNS server/client.	12.2
	Configure the STWireless WLAN parameters.	14
	Upgrade STWireless software.	15
	Save all changes made to persistent memory.	
	Open the 'CLI' web pages to allow detailed configuration of the STWireless .	19.1
	Pop up the STWireless online help pages.	

19 Maintenance – Speed Touch Wireless Command Line Interface

- Introduction** For advanced configurations, with full control over all the **STWireless** functions, the **STWireless** exhibits a low level interface, i.e. the Command Line Interface (CLI).
- As the CLI has far more configurational possibilities than the regular **STWireless** web pages, it is intended for experienced users only.
- The CLI is accessible via:
- ▶ The **STWireless** web pages
 - ▶ A Telnet session via Ethernet IP connectivity
 - ▶ The serial 'Console' port.
-

In this chapter


Topic	See
CLI via the Web Pages	19.1
Native CLI Access	19.2

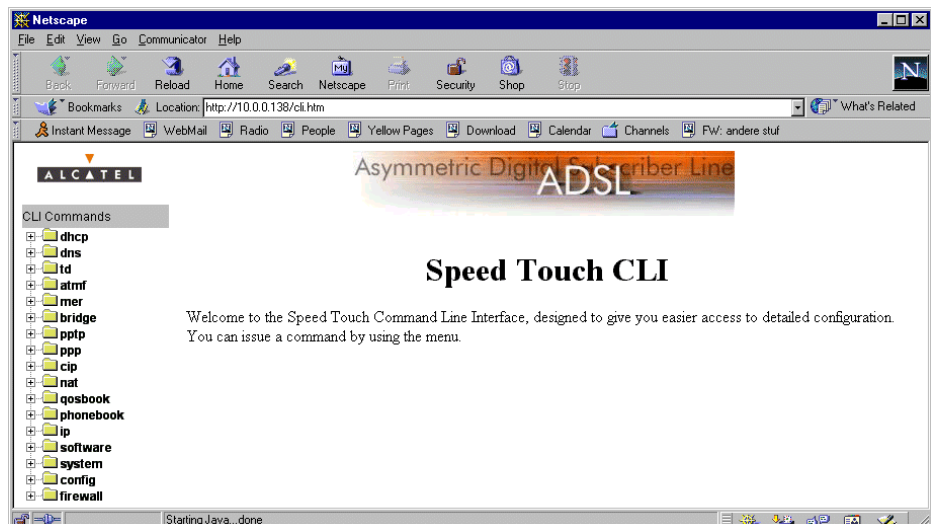
19.1 CLI via the Web Pages


- In this section**
- ▶ CLI Web Page Requirements
 - ▶ The **STWireless** 'CLI' Web Page
 - ▶ CLI Commands Basics
 - ▶ Example: Command Group Description
 - ▶ Executing Commands
 - ▶ Example: Command Execution
 - ▶ Detailed CLI Commands Description


- CLI web page requirements**
- To be able to access the 'CLI' web page, you need the following:
- ▶ Microsoft's Internet Explorer 4.0, or better
 - ▶ Netscape's Communicator 4.06, or better.
- Both web browsers must support JavaScript.

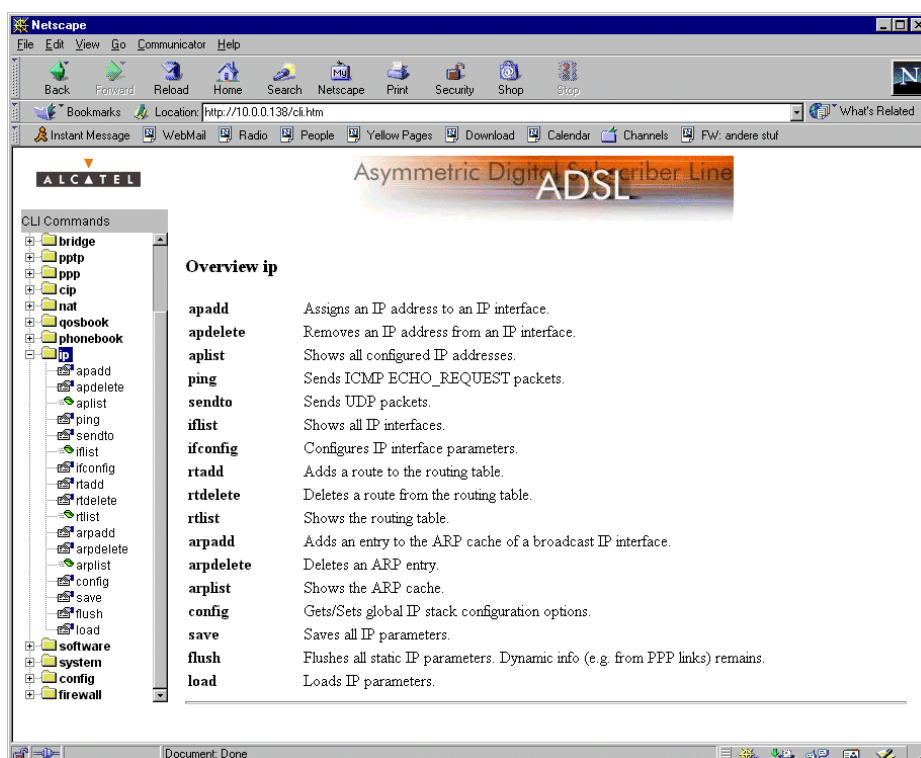
The STWireless 'CLI' web page




Clicking  in the left pane of the **STWireless** web pages, pops up the 'CLI' web page (See section 18.2 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.

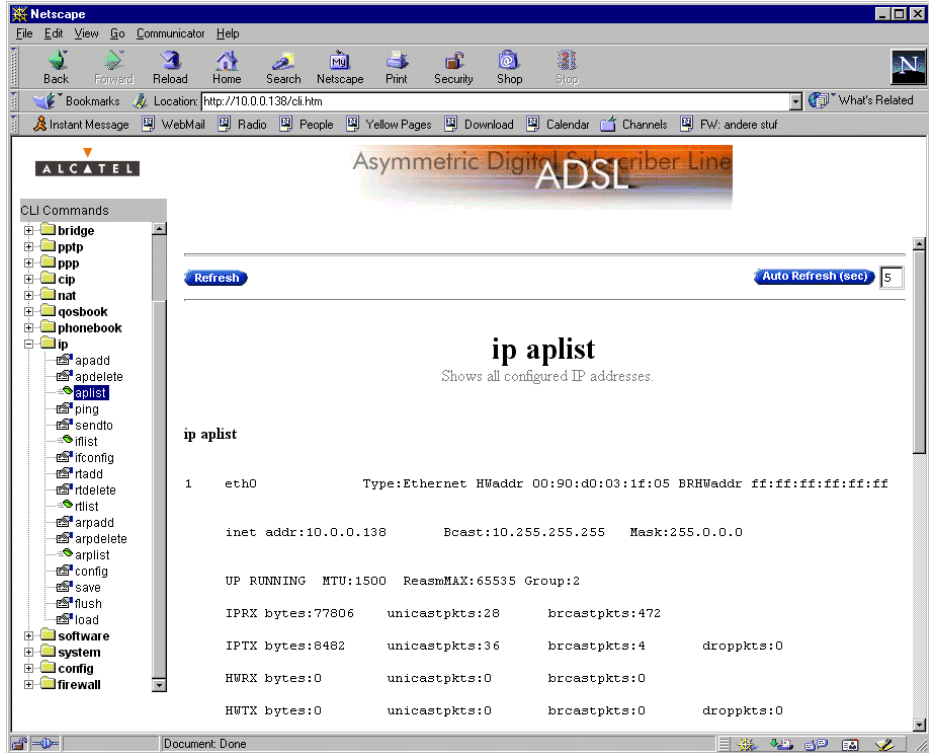
Example: command group description The following example shows the output if you click  next to the 'ip' group name:



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  to execute the command.

Example: command execution

Clicking 'aplist' in the 'ip' command group generates the following immediate output:



CLI Reference Manual

A CLI Reference manual with detailed CLI configuration description of all the commands can be found at:

<http://www.alcatel.com>

<http://www.alcateldsl.com>

19.2 Native CLI Access

Introduction Next to the CLI access via the **STWireless** web pages, you can use native access via the serial port, or 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	19.2.1
CLI via Serial Access	19.2.2
CLI Commands Basics	19.2.3

19.2.1 CLI through a Telnet Session

Introduction Via a PC, or terminal connected via the **STWireless** WLAN environment, or connected to the Ethernet interface of the **STWireless** you can execute CLI commands.
However, you must gain access to the **STWireless** first, by opening a TCP/IP Telnet session.

Note The examples throughout this section all refer to Microsoft Windows OSs. However, all the concepts remain equally valid for other OSs.

- In this section**
- ▶ Telnet Features
 - ▶ Telnet Requirements
 - ▶ Opening a Telnet Session to your **STWireless**
 - ▶ Closing a Telnet Session.
-

Telnet features Telnet is:



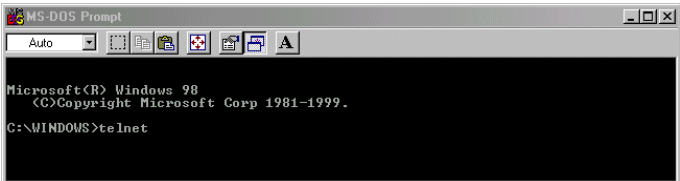
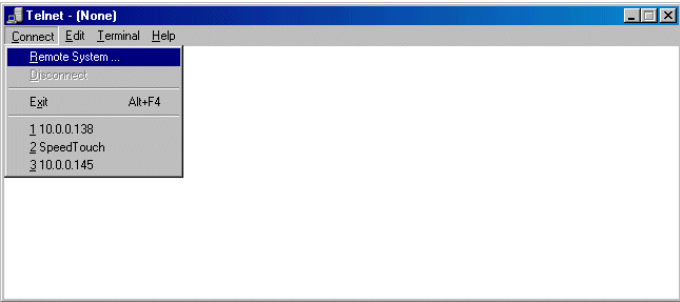
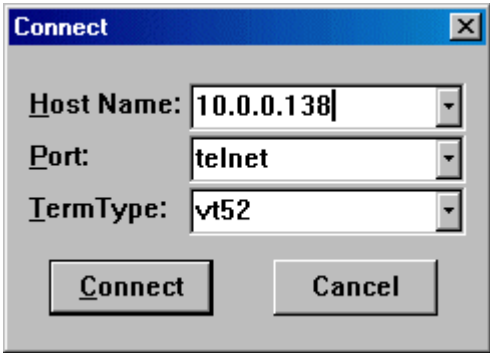
- ▶ A fairly general, bi-directional, eight-bit byte-oriented communication facility
- ▶ A standard method of interfacing terminal devices to each other.


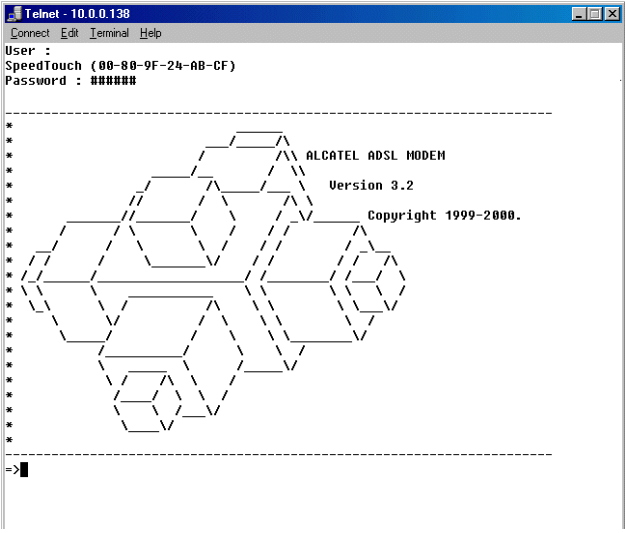
Telnet requirements Prior to using Telnet, you need:

- ▶ A connected, and configured **STWireless**, with known IP address, or DNS hostname, and, if applicable, the system password
- ▶ 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 **STWireless**.
- ▶ A TCP/IP suite installed on this PC, or terminal
- ▶ A Telnet session application installed on this PC, or terminal.

Opening a Telnet session to your STWireless

Proceed as follows:

Step	Action and Description
1	Click  from the system tray on your desktop.
2	Select 'Programs' and click  MS-DOS Prompt to open a DOS window.
3	<p>The DOS window pops up:</p>  <p>At the DOS prompt, enter: telnet.</p>
4	<p>The 'Telnet' window pops up:</p>  <p>In the toolbar, you select 'Connect', and click 'Remote System...'</p>
5	<p>The 'Connect' window pops up:</p>  <p>In the 'Host Name' field, enter the STWireless IP address, or its DNS hostname.</p> <p>Note: The default IP address is 10.0.0.138 The default DNS hostname is SpeedTouch.</p>

Step	Action and Description						
6	Click 						
7	The STWireless will prompt you with User :						
8	Press 'Enter'.						
9	The following step depends on the following: <table border="1" data-bbox="695 506 1372 757"> <thead> <tr> <th>If ...</th> <th>Then ...</th> </tr> </thead> <tbody> <tr> <td>A system password was set before</td> <td>You must supply the password, prior to gaining CLI access.</td> </tr> <tr> <td>No system password was set</td> <td>No passwords must be supplied, and you have immediate CLI access.</td> </tr> </tbody> </table>	If ...	Then ...	A system password was set before	You must supply the password, prior to gaining CLI access.	No system password was set	No passwords must be supplied, and you have immediate CLI access.
If ...	Then ...						
A system password was set before	You must supply the password, prior to gaining CLI access.						
No system password was set	No passwords must be supplied, and you have immediate CLI access.						
10	The STWireless CLI banner will appear: 						

Result At this point you reached the CLI prompt, preceded by the opening CLI banner:

=>

CLI commands can be executed now.

Closing a Telnet Session

CLI access to your **STWireless** is released, either via timeout, or by holding down the 'Ctrl' tab and pressing ']'.

To quit the Telnet application, enter **quit**, or hold down the 'Ctrl' tab and press 'C'.

Note You can perform a quick release from the CLI to your OS's prompt, by holding down the 'Ctrl' tab and pressing 'C' at the CLI prompt.

19.2.2 CLI via Serial Access

Advantages of the CLI via serial access

The CLI via serial access:

- ▶ Provides CLI command connectivity to the **STWireless**, without the need of a TCP/IP configuration
- ▶ Allows remote **STWireless** configuration via an intermediate POTS modem, or ISDN modem/router.

Serial access requirements

For serial access, you need:

- ▶ A serial cable.
- ▶ An ASCII terminal (VT100), or a PC with ASCII terminal emulation, for local configuration

or

- ▶ A POTS, or ISDN modem/router for remote configuration

Serial connection settings

Setup the serial interface of your ASCII terminal, or PC for:

- ▶ 9600 BAUD
- ▶ 8 databits
- ▶ no parity, 1 stopbit.

Accessing the CLI

As soon the connection is made, your terminal is ready for the CLI. Just press 'Enter' to pop up the CLI banner, possibly after supplying the **STWireless** system password.

19.2.3 CLI Command Basics

Introduction Although it is not the aim of this subsection to give a complete overview of all possible configurational **STWireless** items, this subsection describes some of the generalities of the native CLI environment.

General CLI information Once you accessed your **STWireless**, 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
?              : Displays this help information
exit          : Exits group selection.
..            : Exits group selection.
```

```
Following command groups are available :
```

```
dhcp          dns          td          atmf         mer
bridge        pptp         ppp         cip          nat
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 Manual A CLI Reference manual with detailed CLI configuration description of all the commands can be found at:

<http://www.alcatel.com>

<http://www.alcateldsl.com>

Speed Touch™ Wireless

Appendices

Abbreviations

ACCOMP	Address and Control field COMPression
ADSL	Asymmetric Digital Subscriber Line
ARIN	American Registry for Internet Numbers
ASP	ADSL Service Provider
CHAP	Challenge Handshake Authentication Protocol
CIP	Classical IP
CLI	Command Line Interface
DSSS	Direct Sequencing Spread Spectrum
DTE	Data Terminal Equipment
ETHoA	ETHernet over ATM
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
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
LAN	Local Area Network
LCP	Link Control Protocol
LIS	Logical IP Subnet
MAC	Medium Access Control
Mbps	Mega bits per seconds
MER	MAC Encapsulated Routing
NAPT	Network Address & Port Translation
NIC	Network Interface Card
NID	Network Interface Device
OS	Operating System
OSI	Open Systems Interconnection

PAP	Password Authentication Protocol
PC	Personal Computer
PIP	Packet Interception Point
POST	Power On Self Test
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol
PPPoA	PPP over ATM
PPTP	Point-to-Point Tunnelling Protocol
PT	Port Translation
QoS	Quality of Service
RAS	Remote Access Services
REN	Ringer Equivalence Number
ROW	Rest Of the World
RTSP	Real Time Stream Protocol
SP	Service Provider
SSID	Service Set ID
SVC	Switched VC
TCP	Transmission Control Protocol
URL	Uniform Resource Locator
VP	Virtual Path
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless LAN

AppendixA Troubleshooting

Introduction This appendix provides information on how to identify and correct some common problems you may encounter when using, and configuring the **STWireless**.

If the following troubleshooting tips have not resolved the problem, contact the company from which you purchased the **STWireless** for assistance.

Configuration problems In case you encounter ADSL connectivity problems due to misconfiguration, you might consider a reset to original defaults as described in chapter 17. However, be aware that a reset to original defaults destroys all configurational changes you made to the **STWireless** internal settings.

Trouble solving table The following table provides possible solutions to some problems:

Problem	Solution
STWireless does not work. (none off the LEDs lights up)	Make sure the STWireless is plugged into an electrical outlet.
	Make sure the power switch on the STWireless modem is turned on.
No Ethernet connectivity.	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.
No Wireless connectivity.	Make sure your WLAN adapter is compliant to the STWireless WLAN standards.
	Make sure both STWireless and WLAN adapter are configured for the same regulatory area.
Telnet session from a Windows PC is not possible.	The STWireless system password is longer than 8 characters. Change the STWireless system password.
Poor STWireless ADSL performance.	Make sure the STWireless is installed as instructed in this user manual.
Windows Error 730. (Windows98/98SE)	TCP/IP is not installed on your PC. Install the TCP/IP protocol suite on this PC.

AppendixB ADSL Connectivity

Introduction ADSL is state-of-the-art technology, used for unlocking the potential bandwidth of the widely available public telephone network.

In this appendix

Topic	See
ADSL Exposed	B.1
Preconditions	B.2
Splitter and Filters	B.3
Central Splitter	B.4
Distributed Filters	B.5
ADSL Line Pinning	B.6

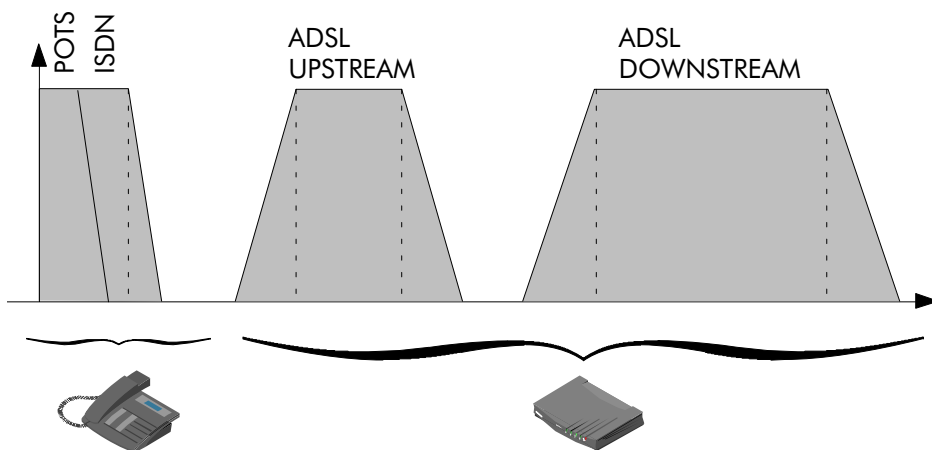
B.1 ADSL Exposed

ADSL ADSL is short for *Asymmetric Digital Subscriber Line*. This somewhat cryptic name is best explained in straightforward terms:

- ▶ **Line:** ADSL uses the ordinary existing copper line, known as “local loop”, running between your local premises and the telephone central office.
- ▶ **Subscriber:** That’s you, the end user. Because this is what service providers or operators call their customers.
- ▶ **Digital:** ADSL is a digital transmission technology. To a certain extend, digital information is not affected by impairments on the telephone line, thus achieving a higher reliability.
- ▶ **Asymmetric:** ADSL can transmit data much faster from the Internet towards the end user than vice versa.

ADSL vs. POTS As Plain Old Telephone Service (POTS) or Integrated Services Digital Network (ISDN), and ADSL occupy distinct frequency spectra, ADSL service can coexist with these conventional telephone services.

Frequency spectrum



B.2 Preconditions

Before you start using ADSL service

Prior to using the **STWireless**, you **MUST** contact your SP. The SP will inform you whether the ADSL service is already enabled. If not, the SP will advise you on how to proceed.

Requirements to use ADSL service

Your SP must provide you with:

- ▶ A telephone line (POTS, or ISDN) which supports ADSL service
 - ▶ Guidelines for in-house cabling
 - ▶ A splitter or filters to decouple conventional phone signals and ADSL signals.
-

STWireless and telephone service

Two variants of the **STWireless** models exist: a POTS variant, and an ISDN variant.

To identify your variant, see the marking label on your **STWireless**.

POTS, or ISDN vs. telephone equipment

In all cases you must use the appropriate equipment according your local telephone service, this to avoid damage to your equipment and the telephone line.

In case your local telephone line is POTS, only use:

- ▶ A POTS **STWireless** variant
- ▶ A POTS/ADSL splitter, or POTS/ADSL filters.

In case your local telephone service is ISDN, only use:

- ▶ A ISDN **STWireless** variant
 - ▶ A ISDN/ADSL splitter, or ISDN/ADSL filters.
-

B.3 Splitters and Filters

Mutual POTS/ADSL, or ISDN/ADSL interference

Next to existing POTS, or ISDN signals, ADSL signals are added to the wires in central telephony offices.

Although POTS, or ISDN and ADSL occupy distinct channels, they might influence one another.

Consequences of interference

In devices such as phones, modems, answering machines and fax machines (collectively referred to as telephony devices) ADSL signals can cause audible noise.

Telephony devices can in turn interfere with ADSL signals, causing deterioration in data throughput.

Solutions to avoid this interference

To avoid this mutual interference, an electronic central splitter, or distributed filters need to be installed.

Inside the STWireless

Inside the **STWireless**, dedicated filters remove the POTS, or ISDN signals. Consequently, only the ADSL signals remain to be processed by the **STWireless** ADSL router.

Home installation

As a variety of configurations are deployed, ask your ADSL provider for advice. He will usually prefer one solution rather than another.

In the following sections

Topic	See
Central Splitter	B.4
Distributed Filters	B.5

B.4 Central Splitter

Introduction In this section some configuration features of the central splitter are described.



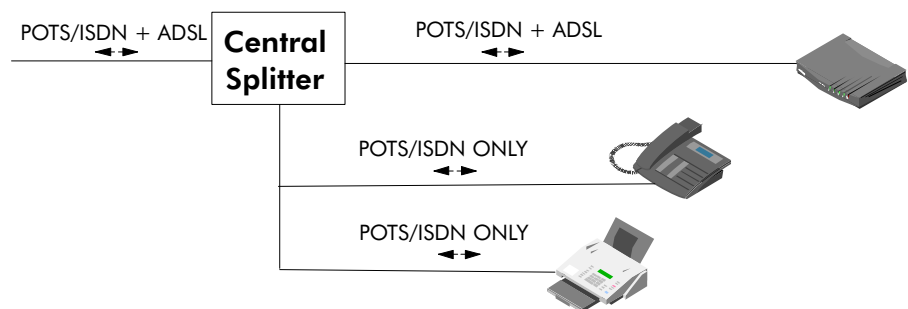
In all cases contact your ADSL service provider about splitter installation.

Public telephone lines carry voltages that **can cause electric shock**.

You may only install splitters yourself if the splitter model clearly stipulates that self-installation is allowed. All other splitters may only be installed by qualified service personnel.

- In this section**
- ▶ General Configuration
 - ▶ Splitter Installation and In-House Cabling
 - ▶ In-House ADSL Service
 - ▶ Splitter Locations
 - ▶ The Network Interface Device (NID)
 - ▶ Indoor Splitter Installation.

General configuration In the below configuration the public telephone line terminates into a central splitter.



Splitter installation and in-house cabling

The central splitter is installed as follows:

- ▶ The POTS/ADSL, or ISDN/ADSL line is connected to the splitter input
- ▶ One output, containing POTS, or ISDN signals only, is connected to the existing in-house POTS, or ISDN network for your ordinary telephone service
- ▶ The other output, containing POTS/ADSL, or ISDN/ADSL, is either connected to:
 - A dedicated spare wire pair in the existing telephone cable to connect to the **STWireless**
 - A newly installed cable to connect to the **STWireless** if no spare wire pair is available.

Note: Ensure that the installed cables are of sufficient quality.

In-house ADSL service

Depending upon the existing wiring and sockets, ADSL should now be present from all of your telephony wall sockets. When using a new dedicated cable, ADSL service is only present from the wall sockets attached to this cable.

Splitter Locations

The central splitter can be either external, or internal to your home.

The NID

An outdoor splitter is installed by the SP in what is often referred to as Network Interface Device, or NID.

The NID is mostly an outdoor enclosure terminating and securing the public telephone cable. For the telephone operator it is the demarcation point between the public and private section of your line.

Indoor splitter installation

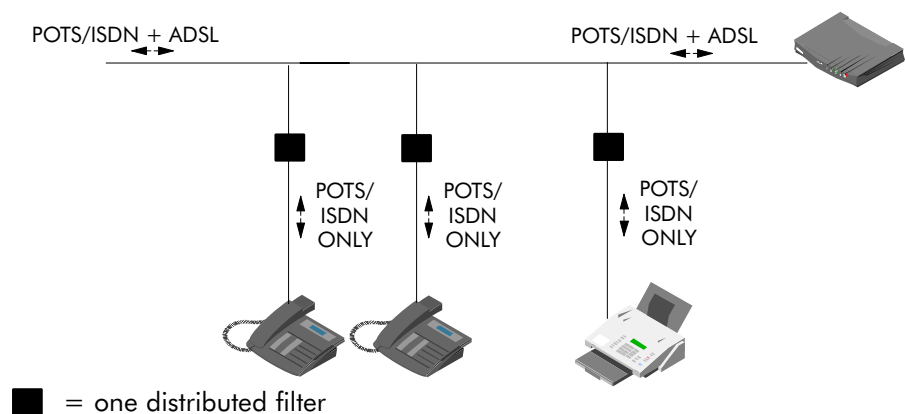
Depending on splitter type and your SP's instructions, you are allowed to install the indoor splitter yourself. For more information, check the manual, supplied with the indoor splitter.

B.5 Distributed Filters

Introduction In this section some configuration features of distributed filters are described.

- In this section**
- ▶ General Configuration
 - ▶ In-house ADSL Service
 - ▶ Filter Installation.

General configuration In this configuration, the combined POTS/ADSL, or ISDN/ADSL signals are distributed over the complete in-house wiring.



In-house ADSL service You can connect your **STWireless** to any wall outlet supporting POTS/ADSL, or ISDN/ADSL service.

Filter installation For optimum ADSL performance, and for telephony device protection from the ADSL signals, you must insert filters in front of any connected telephony device inside your house.

B.6 ADSL Line Pinning

Introduction This section provides information on the possible ADSL pinning terminations.

STWireless ADSL connector pinning, and included ADSL cable Depending on the model variant you purchased, ADSL is terminated on pins 2/5, or 3/4 of the ADSL port (See section F.2). To identify your model variant, see the marking label on your **STWireless**.
The included ADSL cable is a full wired RJ11/RJ11 cable.

Splitter/filter ADSL connector pinning In case a central splitter is installed, ADSL signals are present on pins 2 and 5 of the ADSL enabled wall socket.
POTS, or ISDN telephone service is terminated on pins 3 and 4 of the wall socket.
In case distributed filters are used, both ADSL and POTS, or ISDN, service is present on pins 3 and 4 of the wall sockets.

Crossover adapters Depending on how ADSL and POTS, or ISDN are distributed over your in-house wiring, and depending on your **STWireless** model variant, crossover adapters might be required.

AppendixC Microsoft Dial-Up Networking



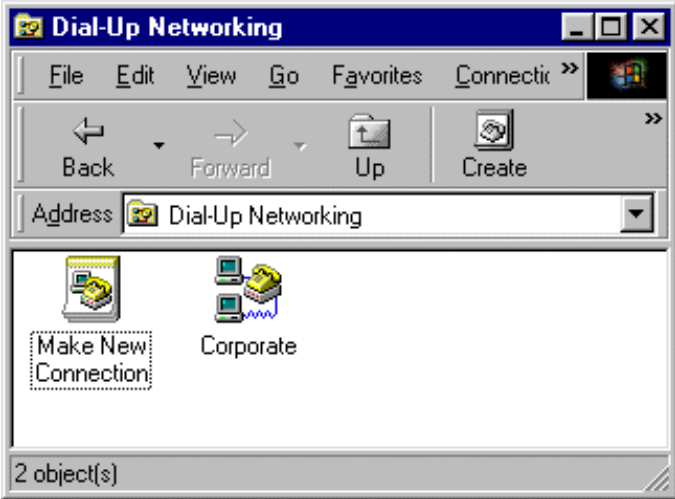


In this appendix

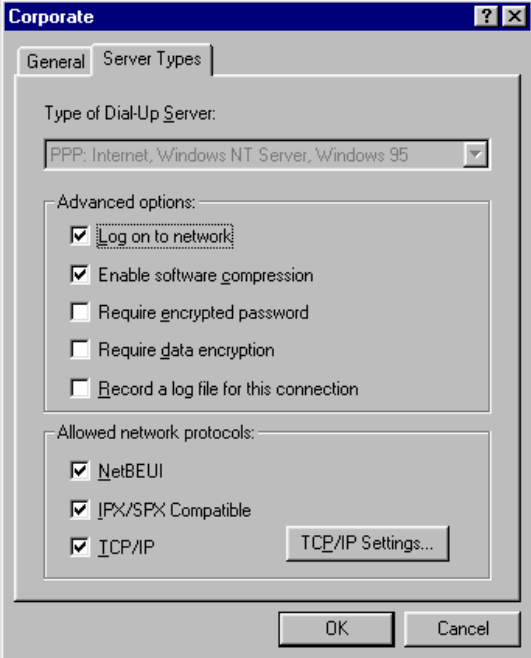
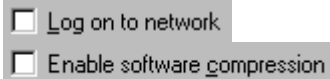
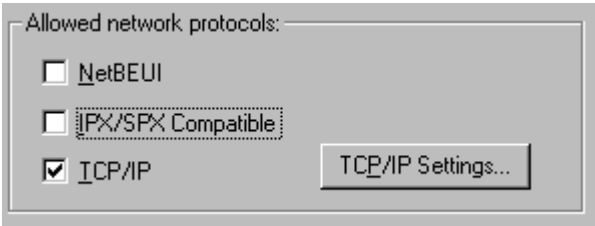

Topic	See
Adapting Dial-Up Networking Properties	C.1
Upgrade Procedure for MS Windows 95	C.2
Configuring PPTP Tunneling for Windows NT	C.3 ... C.6
Using PPTP Tunneling for Windows NT	C.7
Platform Limitations for Microsoft Dial-Up Networking	C.8

C.1 Adapting Dial-Up Networking Properties

Dial-Up connection properties procedure

Proceed as follows:

Step	Action and Description
1	<p>Double-click the 'My Computer' icon on your desktop.</p>  <p>My Computer</p>
2	<p>Double-click the 'Dial-Up Networking' icon.</p>  <p>Dial-Up Networking</p> <p>The 'Dial-Up Networking' window pops up.</p> 
3	<p>Right-click the Dial-Up connection icon 'Corporate' created via the previous procedure.</p>  <p>Corporate</p> <p>As a result, a selection box pops down:</p> 
4	<p>In the selection box, select 'Properties'.</p> <p>The 'Corporate' window appears.</p>

Step	Action and Description
5	<p>In the 'Corporate' window you select the 'Server Types' tab to pop up the following window:</p> 
6	<p>Ensure that 'Log on to the network' and 'Enable software compression' boxes are blank, i.e. not flagged:</p>  <p>In the 'Allowed network protocols' ensure that only 'TCP/IP' is selected, i.e. flagged (✓):</p> 
7	<p>Click  to finish the procedure.</p>

C.2 Upgrade Procedure for MS Windows 95

Introduction This section explains how to download and install the “*Windows Dial-Up Networking 1.3 Performance and Security Upgrade for Windows 95*” needed for the **STWireless**’s PPPoA-to-PPTP Relaying packet service.

PC/workstation requirements The Windows 95 PC(s)/workstation(s) must meet the following minimum requirements :

- ▶ Pentium-class processor 90MHz or higher
- ▶ 16MB of memory.

Download requirements For downloading the “*Windows Dial-Up Networking 1.3 Performance and Security Upgrade for Windows 95*” one PC needs to have Internet access via a voiceband modem.

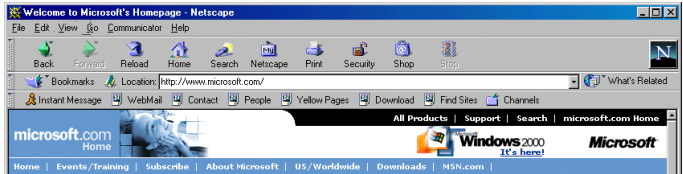
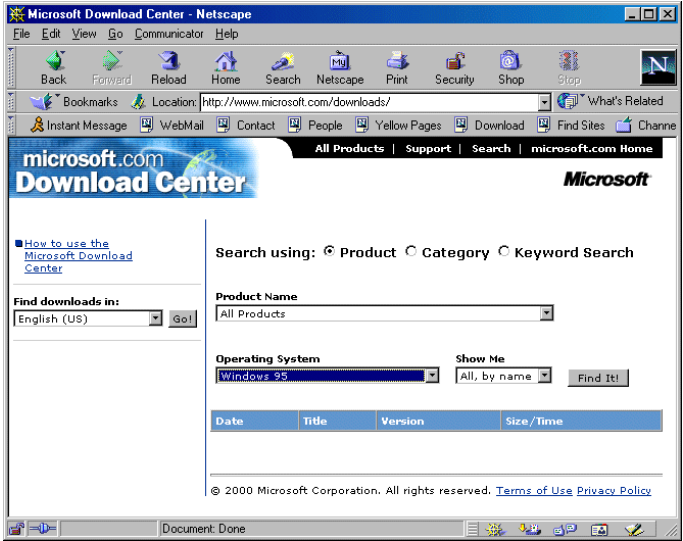


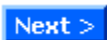
Prior to installing the upgrade If you have installed Windows 95 from a CD-rom, you will need to have the Windows 95 CD-rom ready prior to start the installation process.

To enable Windows95 VPN server support You must:

- ▶ Download the Dial-Up Networking Upgrade
- ▶ Install the Dial-Up Networking Upgrade

Download the Dial-Up Networking Upgrade


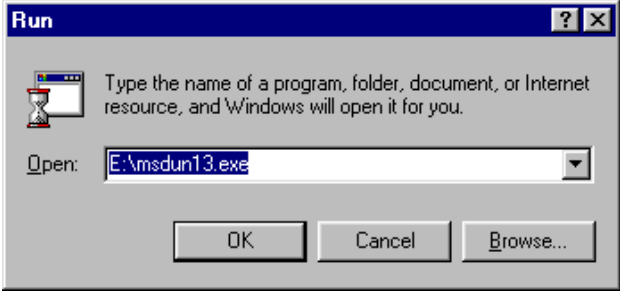


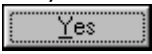


Proceed as follows:

Step	Action and Description
1	Browse to the Microsoft website at 'http://www.microsoft.com' by entering this address in the Uniform Resource Locator (URL) field of your Web browser: 
2	Click the 'Downloads' button in the Microsoft homepage's taskbar. You will be guided to Microsoft's 'Download Center'. 
3	In the 'Download Center' web page, select Windows 95 as OS: 
4	Click 
5	On the resulting web page all available downloads for Windows 95 are listed. In the list, look for the 'Dial-Up Networking Performance & Security Upgrade' and click it. <p style="text-align: center;">Dial-Up Networking Performance & Security Upgrade</p> <p>Note: You can also use Microsoft's Search Tool to locate the Upgrade file. Therefore, search on 'MSDUN13.EXE'.</p>
6	A 'Read me first' web page pops up, informing how the download will progress. to proceed, click 

Step	Action and Description
7	In the following web page, select the Dial-Up Networking Graphical User Interface (GUI) language. To proceed, click Download Now
8	The next web page allows you to choose the nearest download site. Select one, and click Download Now A 'Save As...' window pops up, asking you to specify a location for the MSDUN13.exe file to be downloaded. <div data-bbox="679 618 1366 1037" style="border: 1px solid gray; padding: 5px; margin: 10px auto; width: fit-content;"> </div>
9	Specify a location for the storage. To execute the download, click Save

Installing the Dial-Up Networking Upgrade

Proceed as follows:

Step	Action and Description
1	<p>Click 'Start' from the system tray on your desktop:</p>  <p>Note: All other applications must be closed.</p>
2	<p>Select 'Run' from the menu list.</p> <p>As a result the 'Run' window pops up:</p> 
3	<p>Specify the path (the one that you specified during the download procedure) for the MSDUN13.EXE file in the 'Open' box of the 'Run' window.</p> <p>Note: You can also browse to the file, by clicking </p>
4	<p>Click </p>
5	<p>The system will ask if you want to start the MSDUN13 installation. Click  to proceed.</p>
6	<p>An 'End-User License Agreement' window pops up. To accept, click </p> <p>As a result the installation starts.</p>
7	<p>During the installation, setup will ask you twice to restart your computer. To proceed each time, click </p> <p>Upon restart, the installer will rebuild your driver twice: once for Dial-Up-Networking and once to enable Virtual Private Networking.</p>

C.3 Configuring PPTP Tunneling for Windows NT

In this section The following overview summarizes the procedures to setup your Windows NT PC for the use of PPTP Dial-Up connections over standard telephone lines and Virtual Private Network connections over IP networks such as the Internet:

Step	Action	See
1	Make sure that <i>Microsoft Service Pack 3</i> has been installed on your PC(s).	
2	Configure a <i>Private</i> IP address on your PC	NO TAG
3	Install the PPTP Tunneling network protocol	C.4
4	Configure RAS for PPTP Tunneling	C.5
5	Create PPTP Dial-up phonebook entries	C.6




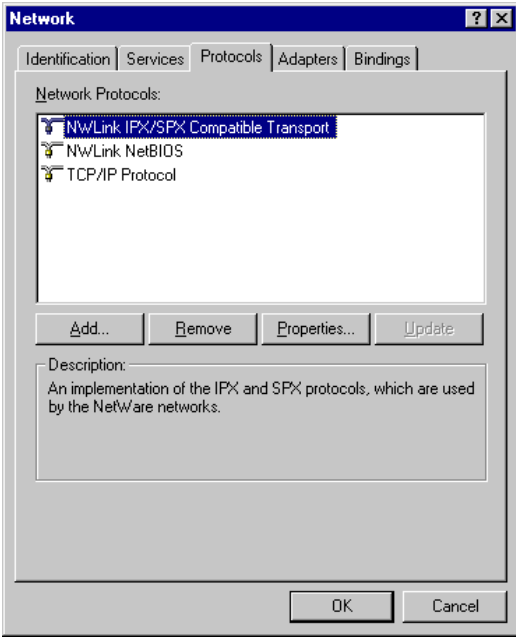



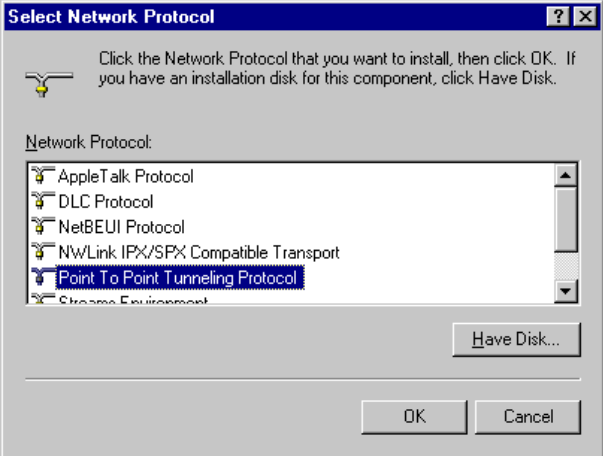


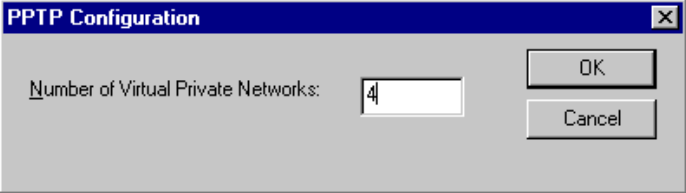


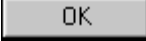
Microsoft Service Pack 3 Installation

Make sure that '*Microsoft Service Pack 3*' has been installed on your PC before you start creating tunnel sessions.

C.4 Installing the PPTP Tunneling Network Protocol (WinNT)


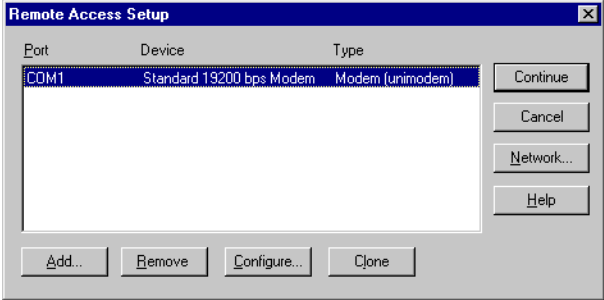
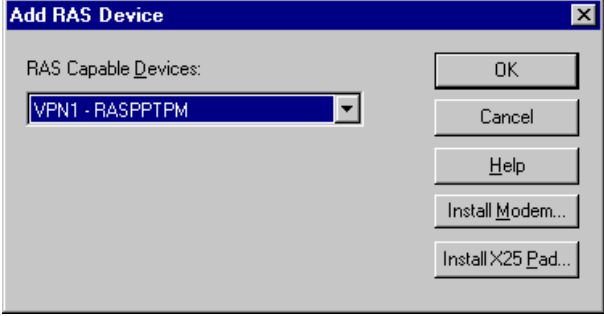


Procedure Proceed as follows:

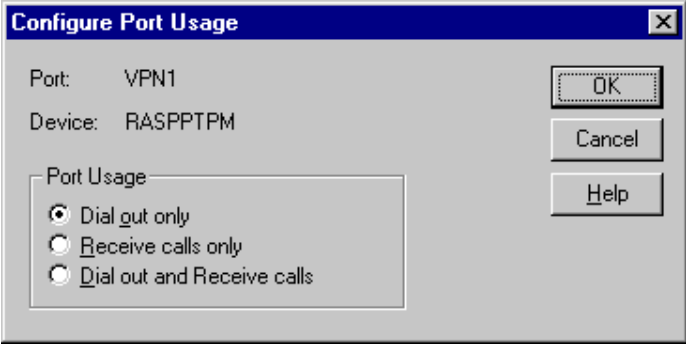




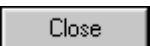

Step	Action and Description
1	<p>Double-click the 'My Computer' icon on your desktop.</p>  <p>My Computer</p>
2	<p>Double-click the 'Control Panel' icon.</p>  <p>Control Panel</p>
3	<p>In the 'Control Panel' folder, double-click the 'Network' icon.</p>  <p>Network</p> <p>As a result the 'Network' window pops up.</p> 

Step	Action and Description
4	<p>Select the 'Protocol' tab and click  to pop up the 'Select Network Protocol' window:</p> 
5	<p>Select the 'Point-to-Point Tunneling Protocol', and click </p>
6	<p>Setup now needs to copy some Windows NT files and prompts you for the proper path to the installation files.</p> <p>Specify the path and click </p> <p>The installation will load all necessary PPTP files.</p>
7	<p>The 'PPTP Configuration' box pops up.</p>  <p>This box presents you with a key question : how many VPNs do you want to enable for access to the Remote Access Services (RAS) server.</p> <p>Type the number of VPNs you want in the VPN field.</p>
8	<p>Click  to pop up the 'System Message' box:</p> 
9	<p>Click  to continue.</p>

C.5 Configuring RAS for PPTP Tunneling (WinNT)




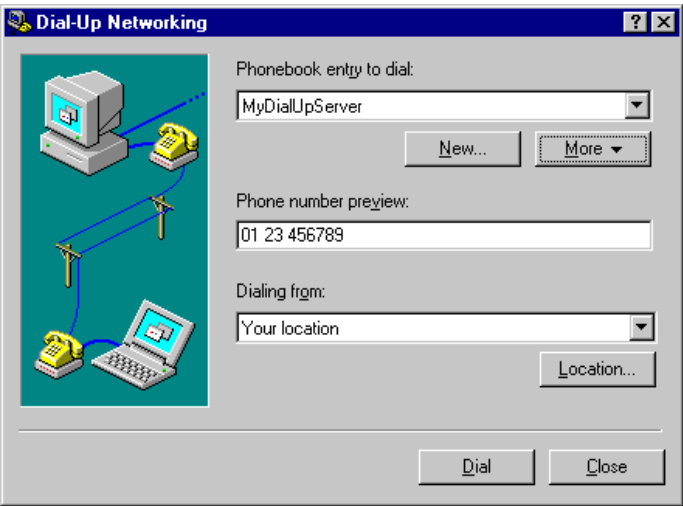

Procedure Proceed as follows:


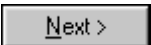
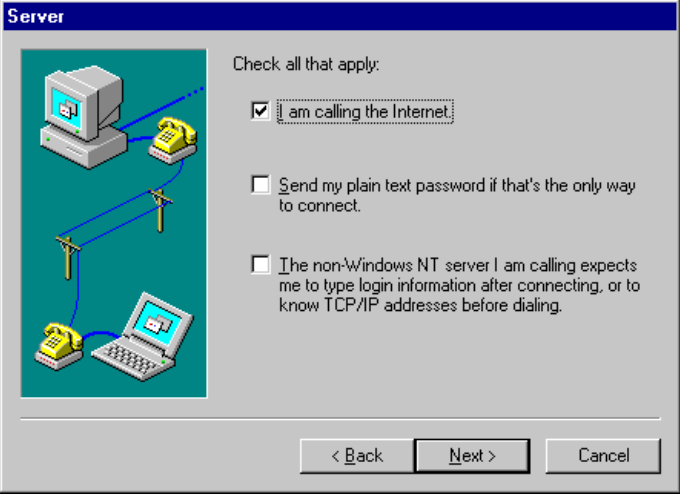

Step	Action and Description
1	<p>After the 'Installing the PPTP Tunneling Network Protocol' procedure, the 'Remote Access Setup' window pops up.</p> <p>Click  to add new created VPN ports to the RAS configuration.</p>  <p>In the example window, one (voiceband) modem is shown, which already was configured for RAS.</p>
2	<p>The 'Add RAS Device' window pops up.</p>  <p>You must add each port individually. To do so, double-click on the correct port and click </p>
3	<p>The 'Remote Access Setup' window reappears, now with the VPN port added to the device list.</p> <p>Repeat steps 1 and 2 until all VPN ports are listed in the 'Remote Access Setup' window.</p>
4	<p>At this point the ports are configured by default for dial-in only. To change this, select a port in the 'Remote Access Setup' window and click </p>

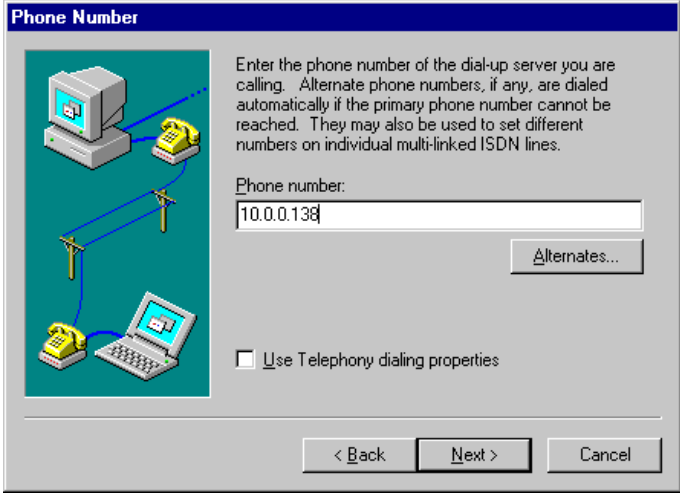


Step	Action and Description
5	<p>The 'Configure Port Usage' window pops up.</p>  <p>Select the 'Dial-out only' option and click </p>
6	<p>The 'Remote Access Setup' window returns.</p> <p>Repeat steps 4 and 5 until all VPN ports are configured for dial-out only.</p>
7	<p>In addition, you can also define which tunneled protocols you will allow through the VPNs.</p> <p>To do so, highlight each port and click </p>
8	<p>Enable, or disable the protocols in the 'Network Configuration' window and click </p> <p>Note: You can enable or disable IP, IPX or NETBEUI sessions for each port.</p>
9	<p>The 'Remote Access Setup' window returns.</p> <p>Repeat steps 7 and 8 until the network configuration for each VPN port is configured.</p>
10	<p>In the 'Remote Access Setup' window, click </p>
11	<p>Click </p>
12	<p>The RAS application will inform you it needs to be restarted in order for the changes to take effect.</p> <p>To restart, click </p>

C.6 Creating PPTP Dial-Up phonebook Entries (WinNT)

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 Note: If the Dial-Up phonebook was empty, a window appears to inform you that no entries exist in the phonebook. Click  to continue with step 4.
3	The 'Dial-Up Networking' window pops up.  The 'Phonebook entry to dial' box lists all existing entries. To add a new phonebook entry, click 

Step	Action and Description
4	<p>The 'New Phonebook Entry Wizard' window pops up.</p>  <p>Enter a name for the entry you are creating; the entry will be saved in the phonebook under this name.</p>
5	<p>Click </p>
6	<p>The 'Server' window pops up.</p>  <p>Activate all the options that apply, and click </p>

Step	Action and Description
7	<p>The 'Phone Number' window pops up.</p>  <p>Enter the 'Phone number', i.e. the IP address, or DNS hostname, of the STWireless.</p> <p>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. See section 7.5 for more information.</p>
8	<p>Click  to proceed. A window pops up, announcing the successful creation of a new tunnel.</p>
9	<p>Click  to finish the procedure.</p>

Creating multiple PPTP Dial-up phonebook entries

Per destination you can create a unique PPTP Dial-up phonebook entry. To do so, repeat the steps, starting with 3 of the previous procedure.

Specific VC and PPTP Profile



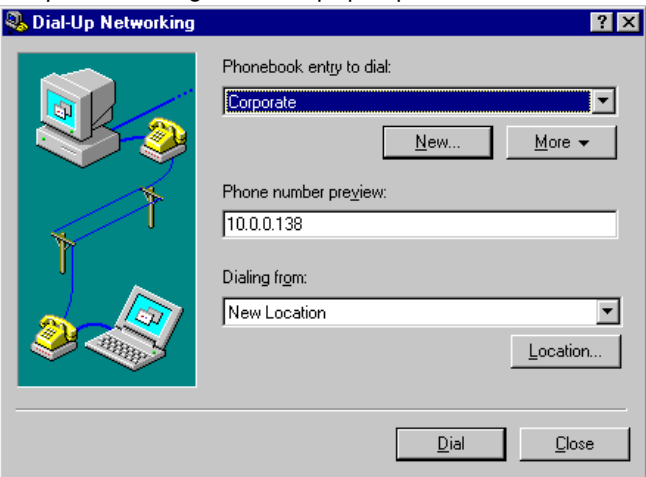

Using a specific PPTP phonebook entry and/or PPTP profile is described in section 7.5.




C.7 Using PPTP Tunneling for Windows NT

- In this section**
- ▶ Opening a PPTP Tunnel Session
 - ▶ NT Dial-Up Networking in Detail
 - ▶ Closing a PPTP Tunnel Session.

Opening a PPTP Tunnel session

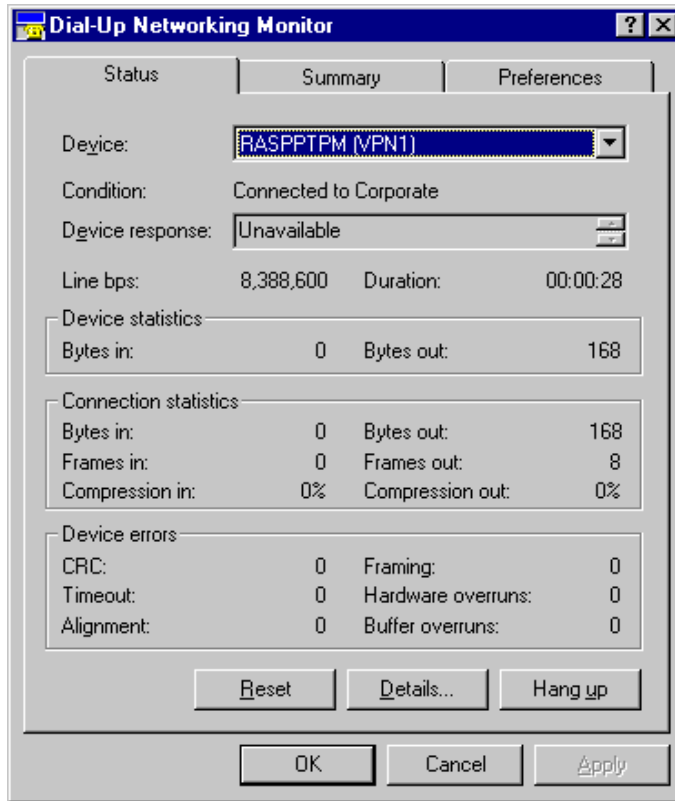
Proceed as follows:

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	The 'Dial-Up Networking' window pops up.  <p>Select the appropriate entry (e.g. 'Corporate') in the 'Phonebook entry to dial' listbox, and click </p>

Step	Action and Description
4	<p>The 'Connect To' window pops up.</p>  <p>Enter your user name and password for the VPN server.</p> <p>Enter the optional information in the 'Domain' box. This is only required by some Microsoft NT VPN servers.</p> <p>Note: To save your password, tick 'Save password' (✓).</p>
5	<p>Click </p> <p>Note: Steps 4 and 5 need only be executed the first time the tunnel is set up. After the tunnel is set up, the 'Connecting to' window will directly appear on your desktop.</p>
6	<p>The 'Connecting To' window pops up.</p>  <p>This window informs you of the status of the connection process.</p>
Result	<p>Once the connection is established, an MSDUN icon representing the Dial-Up connection appears on your system tray.</p>

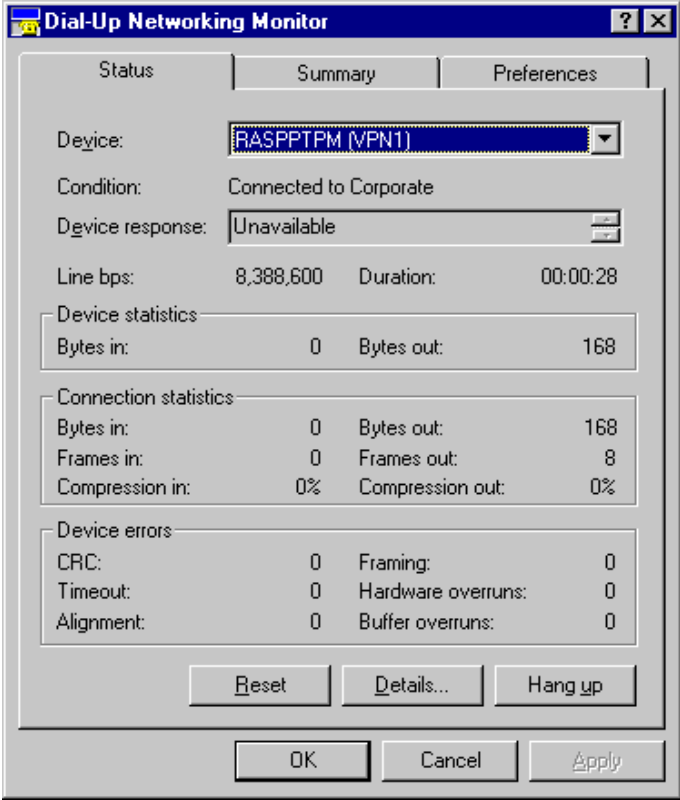
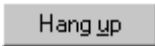
**NT Dial-Up Networking
in detail**

During your session, you can view the connection status by clicking the Dial-Up icon in the system tray. The following window will pop up:



Closing a PPTP Tunnel session

Proceed as follows:

Step	Action and Description
1	<p>Click the appropriate connection icon on your system tray to pop up the 'Dial-Up Networking Monitor' window:</p> 
2	<p>Click </p>
Result	<p>The connection to your SP no longer exists.</p>

C.8 Platform Limitations of Windows Dial-Up Networking

Windows 95/98 Three limitations exist when using the Windows 9x OS:

▶ **One Tunnel**

Windows 9x only allows you to set up one tunnel at a time. This implies that you cannot connect to both your ISP and your corporate simultaneously from one PC.

▶ **Tunneling within a Tunnel**

Tunneling within a tunnel is not possible with Windows 9x, due to its single tunnel limitation.

▶ **Local Connectivity is Lost**

After you set up a tunnel, communication with local LAN devices may be lost. This is because Windows 9x adds a new default gateway to its routing table. This new default gateway points to the tunnel. As TCP/IP is designed to use only one default gateway, connectivity through the original gateway will be lost.

As soon as the tunnel is terminated, connectivity through the original default gateway is again possible.

You can circumvent this problem by manually adding routes to local destinations in the routing table (See section 11.4).

Windows NT Windows NT does not share the first two limitations with Windows 9x:

▶ **Multiple Tunnels**

You can set up multiple tunnels; consequently you can connect to multiple remote destinations simultaneously.

▶ **Tunneling within a Tunnel**

A tunnel within another tunnel is also possible, assuring better end-to-end security.

AppendixD STWireless Layout and Behaviour

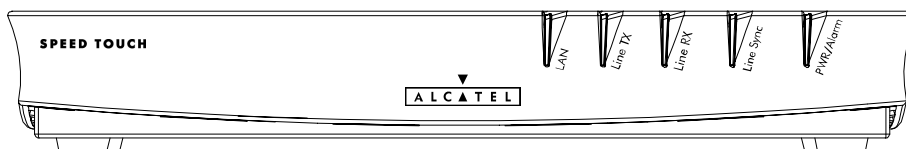
Introduction This appendix describes how your **STWireless** looks like, describes its LEDs description, and describes its start-up behaviour.

In this appendix

Topic	See
Front Panel Layout and LED Description	D.1
Rear Panel Layout	D.2
Power On/Off Behaviour	D.3

D.1 Front Panel Layout and LED Description

Front panel layout The **STWireless** features the following front panel:



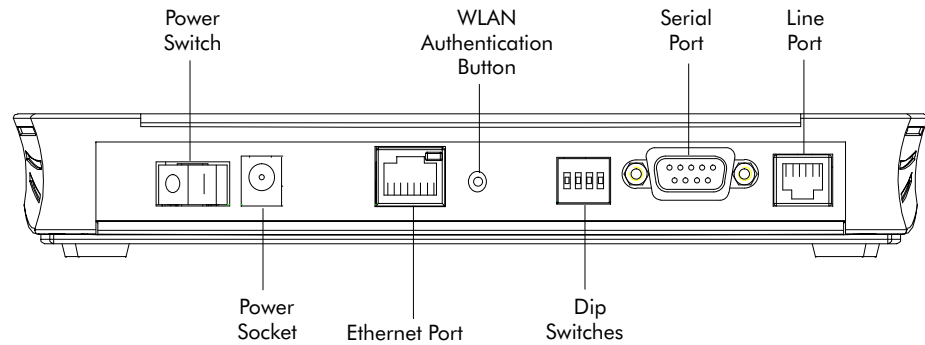
Five front panel LEDs The **STWireless** is equipped with 5 LEDs on its front panel, indicating the state of the device:

Indicator			Description
Name	Color	State	
LAN	Green	Flashing	Data is flowing from/to the Ethernet port, and/or WLAN hub.
		Off	No activity on both Ethernet interface and WLAN hub.
Line TX	Green	Flashing	ATM cells are being sent over the ADSL line.
		Off	No transmission activity.
Line RX	Green	Flashing	ATM cells are being received via the ADSL line.
		Off	No reception activity.
Line Sync	Green	Flashing	During initialization of the ADSL line.
		On	ADSL line synchronization achieved.
PWR/Alarm	Green	On	Power on, normal operation.
	Red	Flashing	Power on, POST(*) pending.
		On	Power on, POST(*) failed.

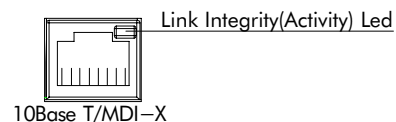
(*) Power On Self Test (POST)

D.2 Rear Panel Layout

Dual port model The **STWireless** features the following rear panel:



Ethernet port LED The Ethernet port on the rear panel has a LED:



Indication of link integrity If the **STWireless** and other LAN device(s) are properly connected and powered on, the particular green LED lights up.

Indication of link activity A flashing green LAN LED on the front panel, indicates reception of data (Rx) via the Ethernet port, and/or WLAN hub.

D.3 Power On/Off Behaviour

Turning on/off the STWireless You can turn the **STWireless** on (**I**), or off (**O**) with the power switch.

POST phases As soon your **STWireless** 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 red	POST failed
	Solid green	Normal operation

Your **STWireless** is ready for service.

Checking link integrity If the LAN device, directly connected to the **STWireless** Ethernet port is powered on, the link integrity/activity LED lights up green.

AppendixE STWireless Original Settings

Introduction This chapter lists all of the **STWireless** original settings. These settings apply at the time the **STWireless** leaves the factory and after a reset to original defaults.

In this chapter

Topic	See
General Settings	E.1
Wireless LAN Settings	E.2
IEEE802.1D Transparent Bridging Defaults	E.3
MAC Encapsulated Routing Defaults	E.4
PPPoA-to-PPTP Relaying Defaults	E.5
PPP Defaults	E.6
CIP Defaults	E.7
Global VPI/VCI Defaults	E.8

E.1 General settings

STWireless IP address 10.0.0.138

STWireless DNS name SpeedTouch

STWireless domain name lan

STWireless DNS server Active

STWireless DHCP server AutoDHCP

STWireless Firewall On (default settings)

E.2 Wireless LAN Settings

STWireless WLAN SSID STW_Alcatel

**STWireless WLAN
channel number** 6

E.3 IEEE802.1D Transparent Bridging Defaults

Phonebook entries

Name	VPI	VCI	State
Br1	8	35	Free
Br2	8	36	Free
Br3	8	37	Free
Br4	8	38	Free

ATM encapsulation RFC1483 LLC/SNAP for Bridged PDUs (FCS not preserved)

Aging Time 5 minutes (300 seconds)

E.4 MAC Encapsulated Routing Defaults

Phonebook entries

Name	VPI	VCI	State
Br1	8	35	Free
Br2	8	36	Free
Br3	8	37	Free
Br4	8	38	Free

ATM encapsulation RFC1483 LLC/SNAP for Bridged PDUs

E.5 PPPoA-To-PPTP Relaying Defaults

Phonebook entries

Name	VPI	VCI	State
RELAY_PPP1	8	48	Free
RELAY_PPP2	8	49	Free
RELAY_PPP3	8	50	Free
RELAY_PPP4	8	51	Free
PPP1	8	64	Configured (PPP & IP routing)
PPP2	8	65	Configured (PPP & IP routing)
PPP3	8	66	Free

ATM encapsulation RFC2364 VC-MUX for PPP PDUs

E.6 PPP Defaults

Phonebook entries

Name	VPI	VCI	State
RELAY_PPP1	8	48	Free
RELAY_PPP2	8	49	Free
RELAY_PPP3	8	50	Free
RELAY_PPP4	8	51	Free
PPP1	8	64	Configured (PPP & IP routing)
PPP2	8	65	Configured (PPP & IP routing)
PPP3	8	66	Free
DHCP_SPOOF	8	67	Configured (PPP to DHCP Spoofing)

ATM encapsulation RFC2364 VC-MUX of PPP PDUs

PPP configuration, authentication

Name	User	Password
PPP1	guest	guest
PPP2	guest	guest
DHCP_SPOOF	guest	guest

**PPP configuration,
routing**

Name	Connection Sharing	NAPT
PPP1	Everybody	✓
PPP2	Everybody	✓
DHCP_SPOOF	Only me	

**PPP configuration,
options**

Name	Mode	LCP echo	ACCOMP
PPP1	Dial-in	✓	✓
PPP2	Always-on	✓	✓
DHCP_SPOOF	Dial-in	✓	✓

E.7 CIP Defaults

Phonebook entries

Name	VPI	VCI	State
CIPPVC1	8	80	Configured
CIPPVC2	8	81	Free
CIPPVC3	8	82	Free
CIPPVC4	8	83	Free

ATM encapsulation RFC1577–RFC1483 LLC/SNAP for Routed non-ISO PDUs

CIP configuration

Enabled CIP member	cip0
CIP member IP address	172.16.1.1 (255.255.255.0)
VC explicitly assigned	CIPPVC1
VC's IP address	172.16.1.2
NAPT	disabled

E.8 Global Default VPI/VCI Values

Ethernet/WLAN

VPI	VCI	Service channel
8	35	IEEE802.1D Transparent Bridging MAC Encapsulated Routing
8	36	
8	37	
8	38	
8	48	PPPoA-to-PPTP Relaying PPP
8	49	
8	50	
8	51	
8	64	
8	65	
8	66	
8	67	
8	80	
8	81	
8	82	
8	83	
15	16	SNMP/ASAM agent communication channel for the Alcatel ASAM
15	64	Software download channel

AppendixF Hardware Reference

Introduction This appendix provides physical specifications and connector pin assignments for the **STWireless**.

In this appendix

Topic	See
Specifications	F.1
Connector Pin Assignments	F.2
Power Supply Adapter	F.3
LAN Cables Layout	F.4

F.1 Specifications

Physical specifications 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}
Frequency: 50/60 Hz
Power consumption: 8W_{max}

Hardware platform LAN interfaces: 1 10Base-T MDI-X Ethernet port
Wireless LAN hub
WAN interface: ADSL line (RJ11) port
Serial interface: RS232

ADSL router specifications Up to 8Mbps downstream
Up to 1Mbps upstream

ADSL standard compliancy:

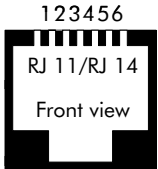
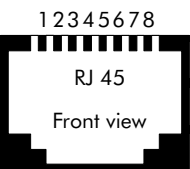
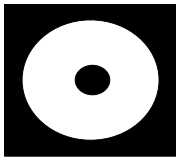
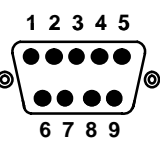
- ▶ ITU G.DMT (Full rate G.992.1 Annex A)
 - ▶ ITU G.LITE (Lite rate G.992.2)
 - ▶ Full rate ANSI T1.413 Issue2
 - ▶ ITU Automode
-

Wireless LAN specifications

- ▶ 11Mbps IEEE802.11b High Rate specification compliant WLAN
 - ▶ Wireless Ethernet Compatibility Alliance (WECA): Wi-Fi Interoperability compliancy certificated
 - ▶ Dynamic rate switching: 11, 5.5, 2, 1 Mbit/s
 - ▶ Coverage: 60m (200ft.) typically indoors
 - ▶ Antenna diversity support for maximum operating range and throughput
-

F.2 Connector Pin Assignments

STWireless port description

Port	Pin No.	Signal Name	Function	Model Reference
 <p>LINE</p>	2	Wire A	Subscriber line wire A	2/5 model
	3	Wire A	Subscriber line wire A	3/4 model
	4	Wire B	Subscriber line wire B	
	5	Wire B	Subscriber line wire B	2/5 model
 <p>10BASE-T MDI-X</p>	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* (-)	
 <p>DC</p>	Inner	+9V _{DC}	Power supply connection (+)	
	Outer	GND	Power supply connection (ground)	
 <p>console</p>	2	RD [RS232-9]	Received data	
	3	SD [RS232-9]	Transmitted data	
	5	DCD [RS232-9]	Signal common	

Note: (*) Data Terminal Equipment (DTE)

Free connector pins Connector pins not mentioned are not connected.

F.3 Power Supply Adapter

Power adapter use The **STWireless** 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	AULTInc. 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

Note: (*) Rest Of the World (ROW)

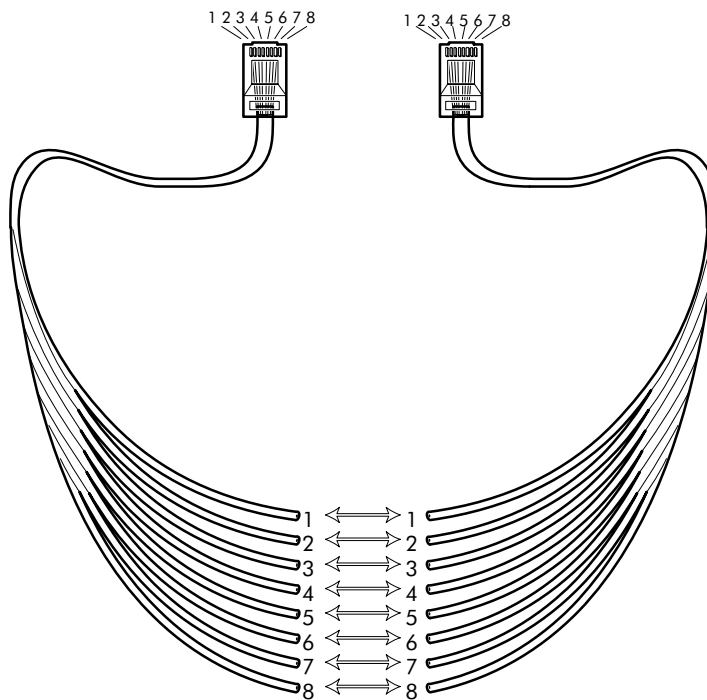
Output specifications The supplied adapter has the following output specifications:

- ▶ 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).

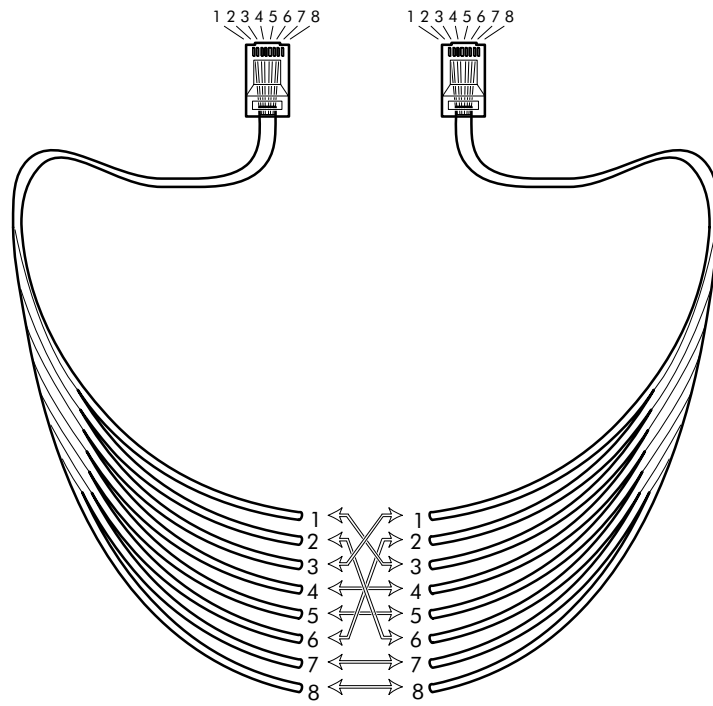
F.4 LAN Cables Layout

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:



AppendixG Wall Fixing Assembly

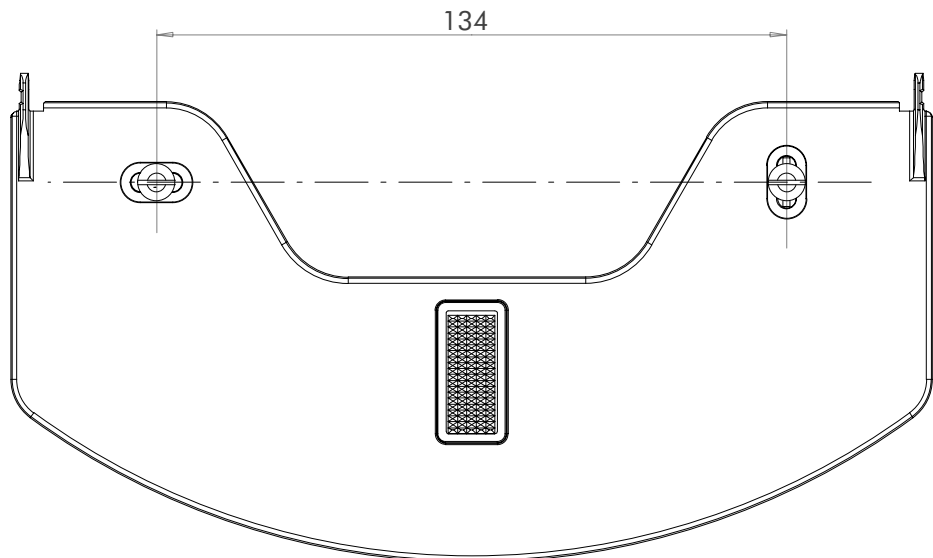
Introduction This appendix describes how to wall mount your **STWireless**, with the wall fixing assembly delivered in the package.

Before you start, check for the following items:

- ▶ The wall fixing assembly
- ▶ 2 screws and 2 wall plugs
- ▶ 1 Velcro sticker

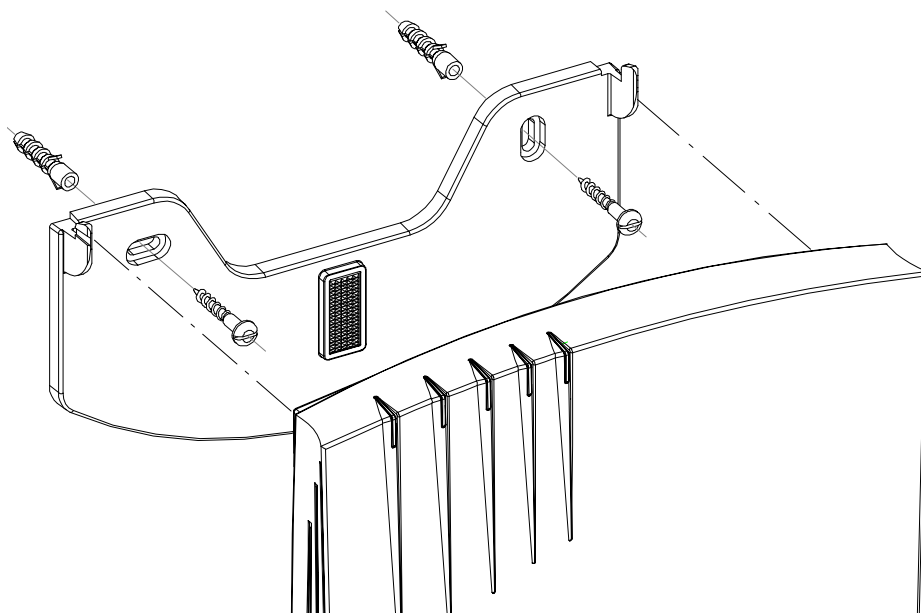
Preparing your wall fixing assembly

- 1.** Mark two hole positions horizontal at 134 mm (5.36 inches) distance:

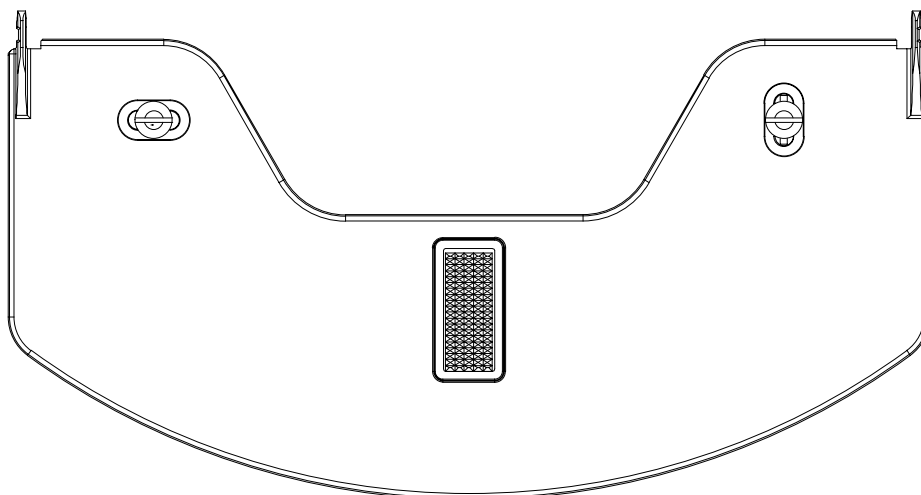


- 2.** Drill the marked holes with a 6mm (0.24 inches) diameter drill bit to a minimum depth of 35mm (1.38 inches).

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 **STWireless** over the two hooks and pull the box down until its firmly positioned, and sticking to the Velcro.

AppendixH 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	H.1
European Declaration of Conformity	H.2
Radio Frequency Interference Statement	H.3
Canadian Class B Notice	H.4



STORE THESE INSTRUCTIONS CAREFULLY



H.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 Appendix F.

Power sources The powering of this product must adhere to the power specifications indicated on the marking labels. If you are unsure 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.

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 ADSL performance.

Depending on your ADSL configuration and type of splitter/filters, installation must be carried out by qualified service personnel.

Consult your telephone service company or ADSL 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



H.2 European Community Declaration of Conformity



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.

H.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 (See Appendix F: Hardware Reference) for details.

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 complaint 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.

H.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.
