Examples of Topologies

For public Internet Access in The Netherlands

Nationaal Aftap Overleg (NAO) / Dutch National Lawful Interception Forum (NLIF)
Working Group Topology
Author: Pim van Stam (NLIP)
Date: January 22, 2001
State: Draft
Revision: 0.2

Content

History

Comment	Revision	Author	Date
First edit	Draft 0.0.1	Pim van Stam	01/17/2001
Edited NLIP	Draft 0.1	Pim van Stam	01/19/2001
Comment P. Bloemen	Draft 0.2	Pim van Stam	01/22/2001

1 Introduction

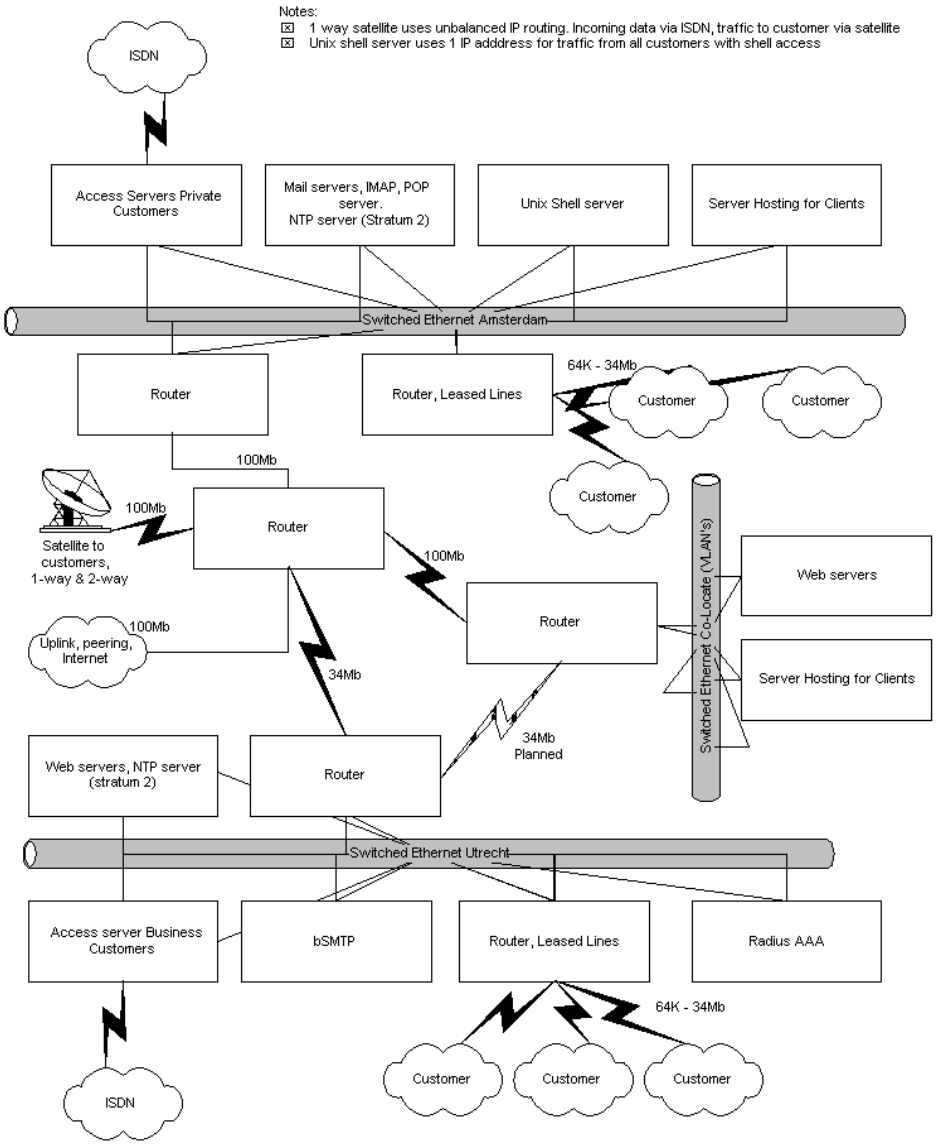
The Working Group Topology (WGT) has to deliver a document (this one) with some examples of the most common topologies from the networks of de Dutch Internet Service Providers. This document is written for suppliers of Lawful Interception Equipment (LIE).

The background for this document is the obligation from the Dutch law to make Lawful Interception possible on Internet.

The examples together with the following two documents[1] is the base for suppliers to build solutions for the Lawful Interception:

- TIIT document: Transport of Intercepted IP Traffic, Version 0.1.2 (October 19, 2000; EJ van Eijk, NFI).
- WAI/GT/FuncSpecs: Functional Specifications for lawful interception of Internet Traffic in The Netherlands, V1.0.1 (2000-06).

In this document three types of Internet network topologies and two E-mail topologies are descibed.



The previous figure shows several types of access to an Internet Service Provider. With this figure you can address the most problems according to lawful interception.

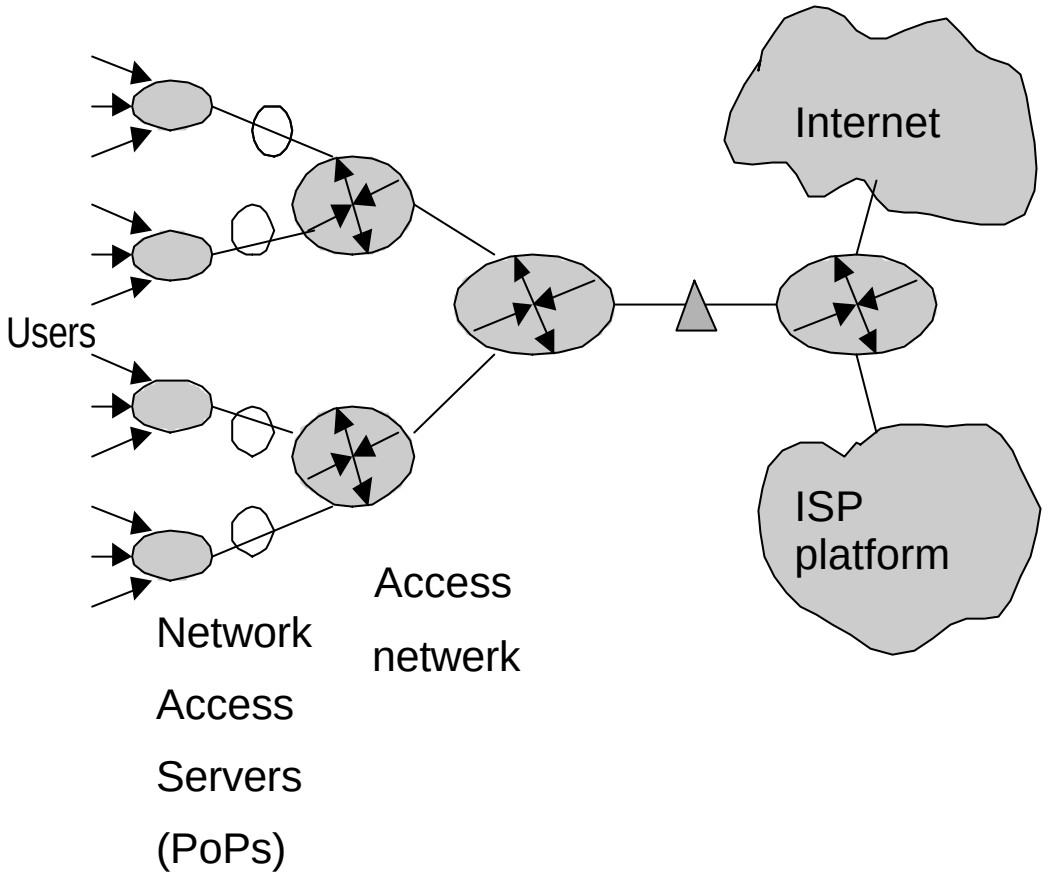
[1] Helpful could also be the ETSI document DEG/SEC-LI-00014 Security; Lawful Interception; IP Interception

1.1 Abbreviations

AAA	Authentication, Authorization and Administration
AP	Access Provider
ATM	Asynchronous Transport Mode
DHCP	Dynamic Host Configuration Protocol
HI	Handover Interface
HI1	Handover Interface (for Administrative Information)
HI2	Handover Interface (for Intercept Related Information)
HI3	Handover Interface (for Content of Communication)
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
LEA	Lawful Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
MAC	Media Access Control
MTA	Message Transfer Agent
MUA	Message User Agent
PoP	Point of Presence
PSTN	Public Switched Telephone Network
TCP	Transmission Control Protocol
TI	Target Identity

2 Example 1: Access network – Dialup / ISDN

2.1 Variant 1: Access network in ISP's control

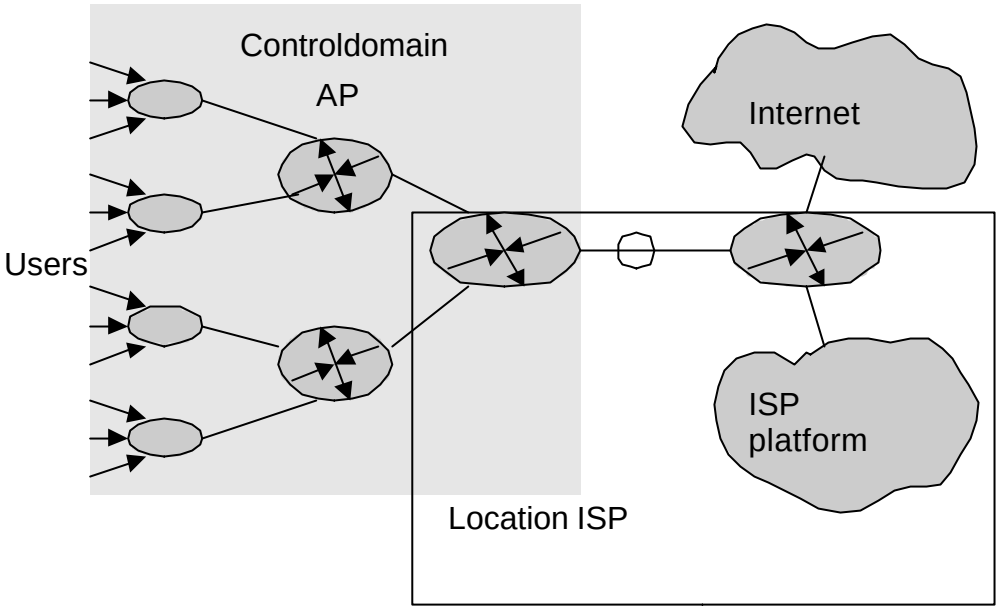


2.1.1 Characteristics

- The user connects to the PoP by means of the PSTN or ISDN network. These parts of the networks are not in control of the ISP, but of the Telecommunication Companies.
- Access is also possible via GSM, WAP and GPRS.
- In this example the ISP controls both the access network, the backbone and the ISP serverfarm (ISP platform). The ISP does the AAA-process (Authenitication, Authorization and Administration).
- The ISP platform contains the services like Radius, mail, website, hosting sites.
- In this topology is InterPoP traffic[2] possible.
- The circles and the triangle in the figure are possible places for the LEMF.
- In most cases dynamic IP-numbers are used.
- Identification of the target by means of login timestamp, assigned IP address, identification of the PoP en when possible the Caller ID (phone number) of the target. When dialling in with GPRS the identification of the radio mast is necessary.

[2] InterPoP traffic is the IP traffic between two users connected to the same Pop.

2.2 Variant 2: Access network subcontracted to Access Service Provider



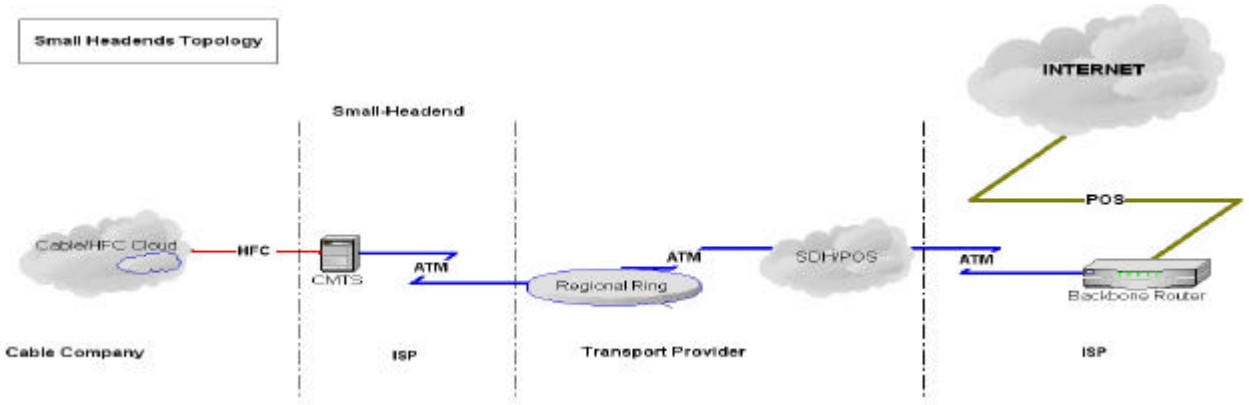
2.2.1 Characteristics

- Part of the Access Network is subcontracted to an Access Provider (AP). This can vary from only the modempool, where the ISP does the authentication and IP-addressing, to the whole connectivity. In this case the ISP has only his servers and is not involved in the user handling except when it comes to the user administration.
- The AAA-process can partly or as a whole be processed by the Access provider. Most of the times the ISP does the Administration and the Access Provider the Authorization. The AP or the ISP can do the Authentication.
- In some cases there is no Authorization, Authentication and Administration at all on the cable network. In this case the traffic data (statistics) stays in the cable network and doesn't come available for the ISP.
- Some AP's deliver services to more then one ISP with the same Access network.
- IntraPoP traffic is a more serious issue here[3].

[3] There is also IntraPoP traffic from the view of an ISP who sees the Acces Network as a super-PoP. More serious is the InterPoP traffic within a shared Access Network of two ISP's.

3 Example 2: Always on – Cable providers

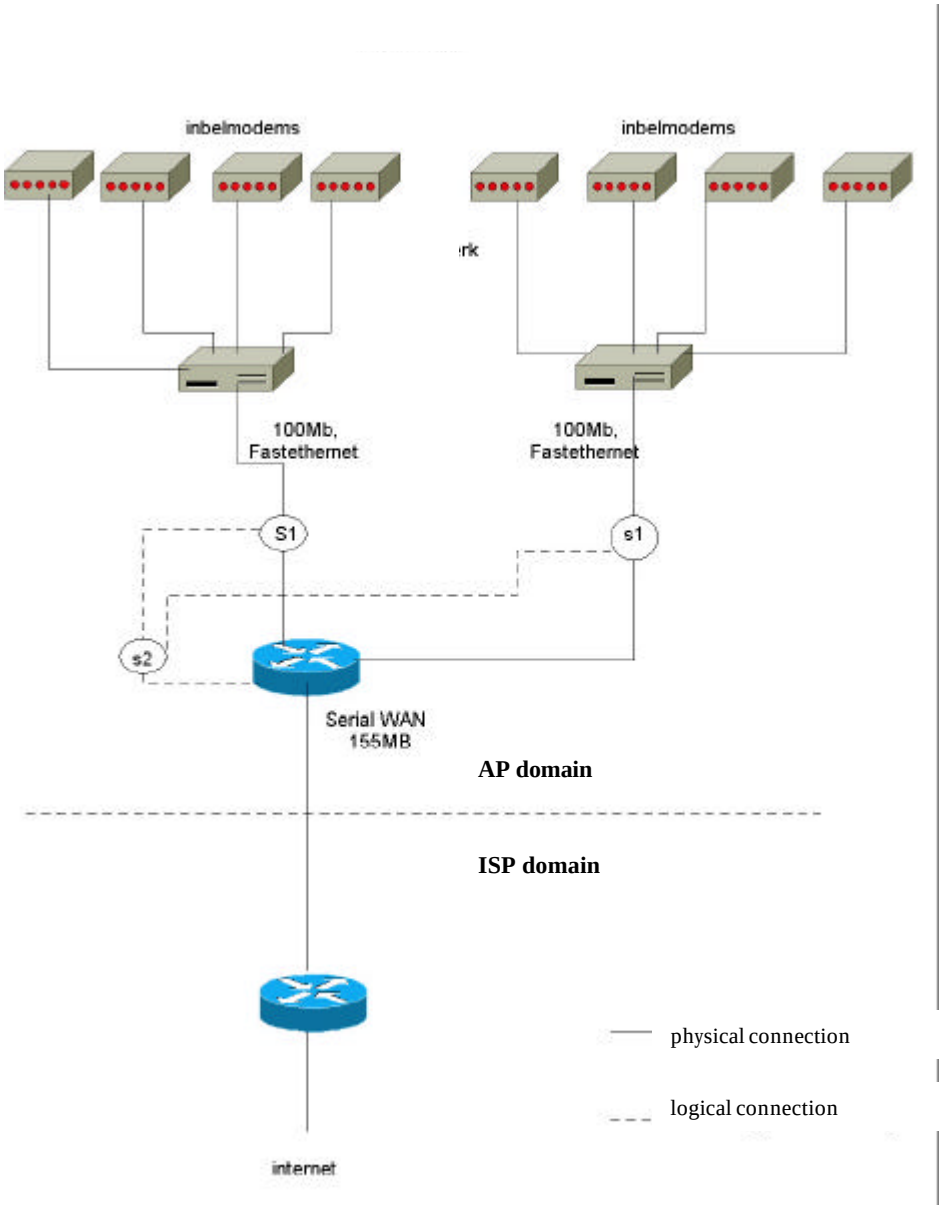
3.1 Variant 1: Cable network in control of the ISP



3.1.1 Characteristics

- The ISP is also the Cable Company. This means the ISP has full control of the cable itself.
- Bandwith (e.g. traffic load) is a challenge for interception.
- InterPoP traffic is an issue. Especially where users are on the same physical cable (e.g. live in one street).
- Not in all cases does authentication take place. Sometimes the access to Internet is granted by placing the right filter on the cable. In most other cases access is granted with the MAC-address of the cable modem.
- IP-spoofing: In most cases the Cable modems (or other user equipment) has a fixed IP-address. The ISP has this IP address in it's administration. However the user can take over some other IP-address.
- Some cable providers seem to use DHCP, so the IP-addresses should be dynamic. However, DHCP tends to reissue the same IP-address to a customer on request or renewal of the lease. Users also are making an effort in staying online and keep the IP-address.

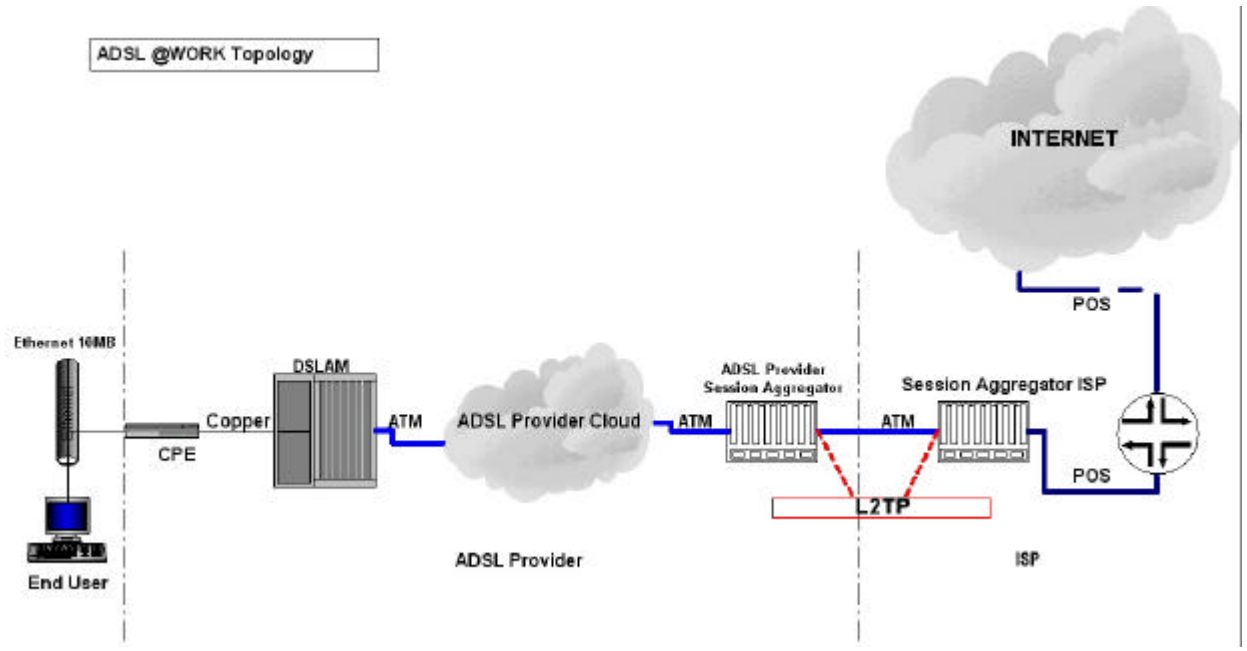
3.2 Variant 2: Cable network subcontracted to Cable Company



3.2.1 Characteristics

- The cable is owned by the Cable Company. The ISP uses the access network from the Cable Company. In this case the ISP has the user administration.
- Bandwith, IntraPoP and authentication is a problem.
- Also IP-spoofing is an issue.

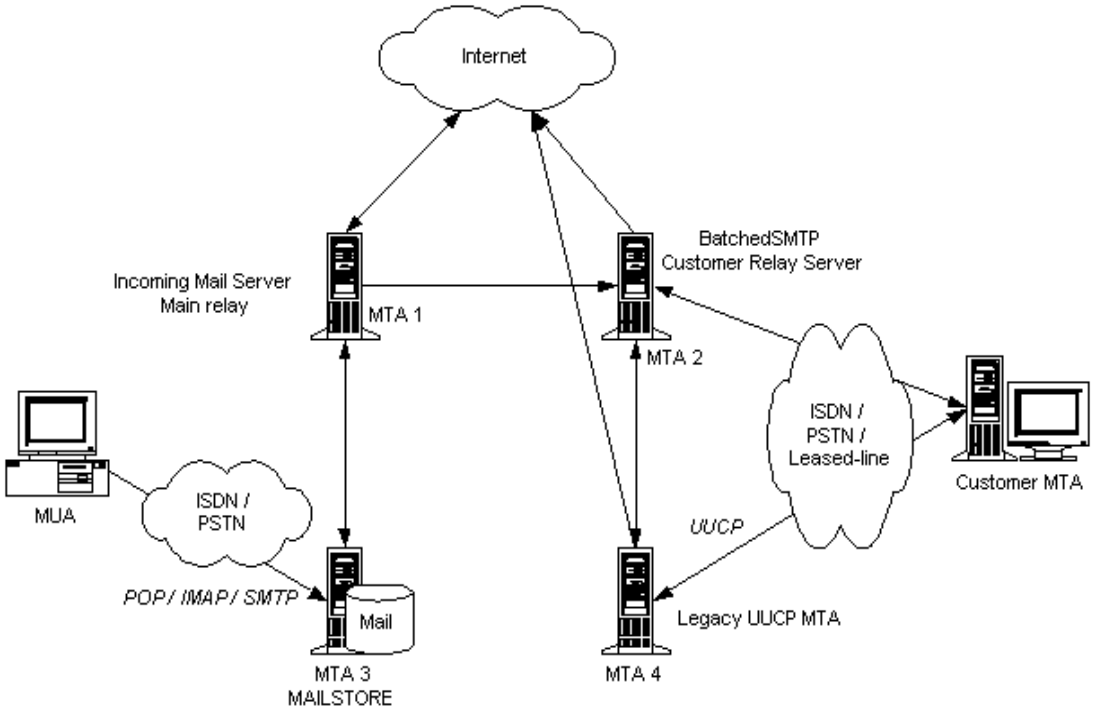
4 Example 3: Always on – ADSL



4.1 Characteristics

- By default the ADSL network is not owned by the ISP but the Telecom Company. So the Telecom Company deliver it's services to the ISP.
- Bandwith is an big issue.
- When intercepting in de ADSL provider cloud then technology is an issue.

5 Mail example 1: SMTP / POP3 / IMAP[4]



5.1 Charasteristics

- MTA vs. MUA[5]
  (Message Transfer Agent and Message User Agent)

  1. Webmail: both MTA and MUA at the ISP's mail server.
  2. Mail client, like Outlook: MTA from ISP, MUA on the user's side; send with SMTP, receive with, POP3/IMAP.
  3. User's own domain: MTA and MUA at user's side, MTA from ISP is an SMTP relay agent; send with SMTP, receive with SMTP or bSMTP, occasionally even POP3 (multi aliases with one (or more) mailbox(es)).
  4. MUA at the ISP and MTA within user's domain is not possible.

		MUA	
		ISP	User
MTA	ISP	Web mail	Mail client
	User	<not possible>	Local domain

- In the example MTA 1 is the relay agent for the other SMTP-servers. Users normally send their mail via MTA 1 (with SMTP). MTA 3 is the mailserver for end-users containing the mailboxes (read with POP3 or IMAP). MTA 2 is the mailserver for (business) customers with an own MTA (SMTP server). MTA 4 is an old fashioned UUCP mailserver for business customers.

[4] At this moment only received mail has to be intercepted.
[5] For ETSI members: more information can be found in the document "LEA requirements for the LI of email", November 2, 2000 TD011.

6 Mail example 2: Other technologies

Some ISP's use other platforms for the mailbackbone. Most common are:

- Netscape Messenger
  The Netscape Messenger system 'out of the box' does all four functions (SMTP, POP3, IMAP, web mail). For a larger set up functions are usually divided.
- Microsoft (e.g. Exchange server)
- Lotus Notes

- In most cases the transport protocols are STMP (send mail) and POP3/IMAP (receive mail). However the storage is the propriety solution.
- Netscape Messenger can be adapted with server side plugins. With such a plugin a mail LEMF is possibly to be made.