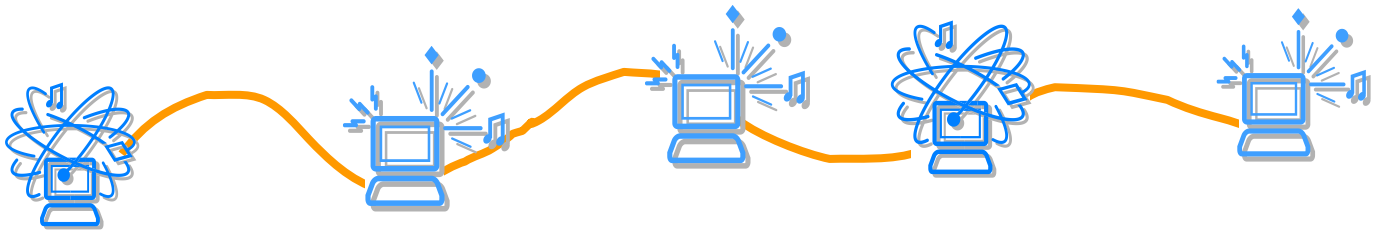
Segurança em Redes
VPN – L2TP (*Layer 2 Tunneling Protocol*)



Redes de Comunicação
Departamento de Engenharia da Electrónica e Telecomunicações e de Computadores
Instituto Superior de Engenharia de Lisboa

Baseado em:

- RFC 2661, “Layer Two Transport Protocol (L2TP)”, 1999
- Wikipedia [https://en.wikipedia.org/wiki/Layer_2_Tunneling_Protocol]
- “*VPNs A Beginner’s Guide*”, John Mairs, McGraw-Hill
- *M.Sc. in Information Security* - Royal Holloway, University of London
- Prof. Dr. Andreas Steffen - Zürcher Hochschule Winterthur
- Pascal Meunier, Symantec Corporation, Purdue Research Foundation
- Henric Johnson, Blekinge Institute of Technology, Sweden
- Fred Baker, VPNs

L2TP

L2TP extends the PPP model by allowing the L2/PPP endpoints to reside on different devices interconnected by a packet-switched network.

With L2TP, a user has an L2 connection to an access concentrator (e.g., modem bank, ADSL DSLAM, etc.), and the concentrator then tunnels individual PPP frames to the NAS. **This allows the actual processing of PPP packets to be divorced from the termination of the L2 circuit**.

One obvious benefit of such a separation is that instead of requiring the L2 connection terminate at the NAS (which may require a long-distance toll charge), the connection may terminate at a (local) circuit concentrator, which then extends the logical PPP session over a shared infrastructure such as frame relay circuit or the Internet. From the user's perspective, there is no functional difference between having the L2 circuit terminate in a NAS directly or using L2TP.

L2TP

L2TPv3, appeared as proposed standard **RFC 3931** in 2005 (L2TPv3 provides additional security features, improved encapsulation, and the ability to carry data links other than simply Point-to-Point Protocol (PPP) over an IP network (for example: Frame Relay, Ethernet, ATM, etc.).

The entire L2TP packet, including payload and L2TP header, is sent within a User Datagram Protocol (UDP) datagram. L2TP uses UDP port 1701. A virtue of transmission over UDP (rather than TCP; c.f. SSTP) is that it avoids the "TCP meltdown problem". It is common to carry PPP sessions within an L2TP tunnel.

L2TP does not provide confidentiality or strong authentication by itself. IPsec is often used to secure L2TP packets by providing confidentiality, authentication and integrity. The combination of these two protocols is generally known as L2TP/IPsec.

L2TP

- L2TP combina o protocolo *Cisco Layer-Two Forwarding* (L2F) com PPTP
- É uma extensão do PPP
- Só pode ser usado em VPN nó-a-nó devido a aplicação na camada de enlace (*data link*)
- Para funcionar extrêmo-a-extrêmo, todos os nós da rede (*routers*) precisam suportar L2TP

L2TP

The two endpoints of an L2TP tunnel are called:

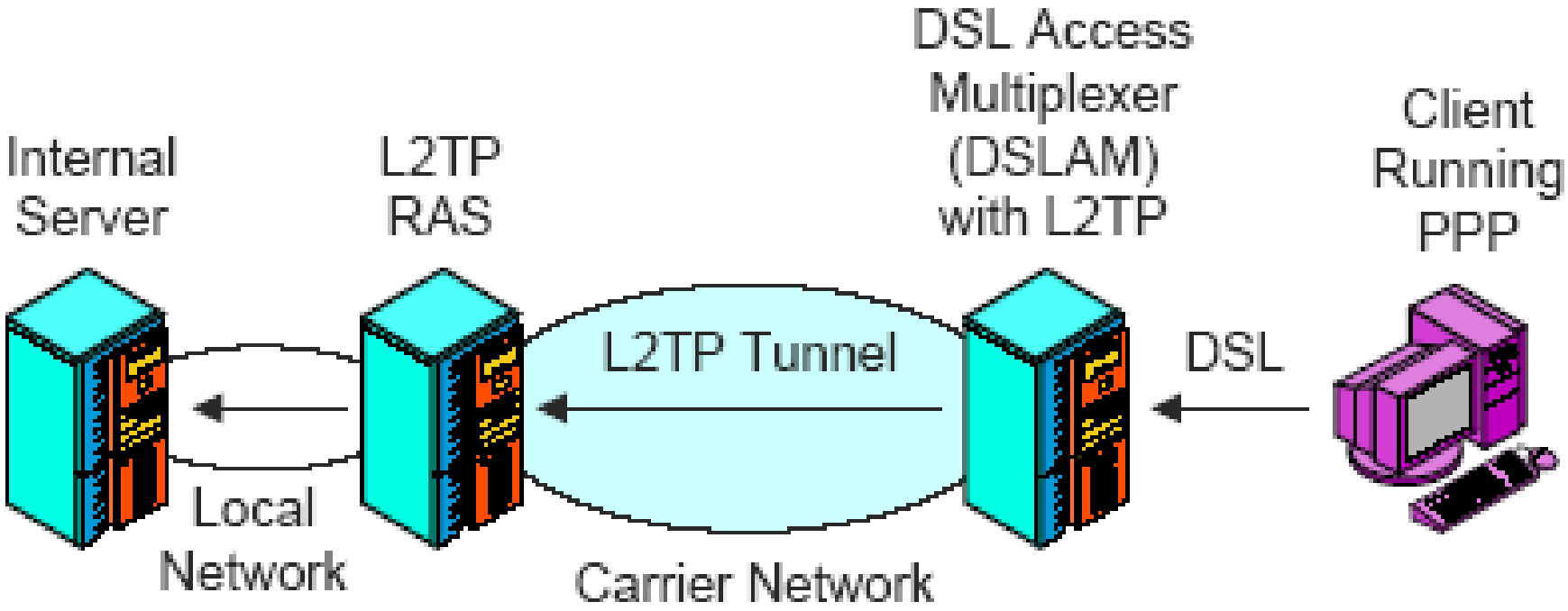
- LAC (L2TP Access Concentrator) and the
- LNS (L2TP Network Server).

The LNS waits for new tunnels. Once a tunnel is established, the network traffic between the peers is bidirectional. Either the LAC or LNS may initiate sessions (one tunnel may has one or more sessions).

The packets exchanged within an L2TP tunnel are categorized as either control packets or data packets.

L2TP provides reliability features for the control packets, but no reliability for data packets.

Layer 2 Tunnelling Protocol (L2TP)

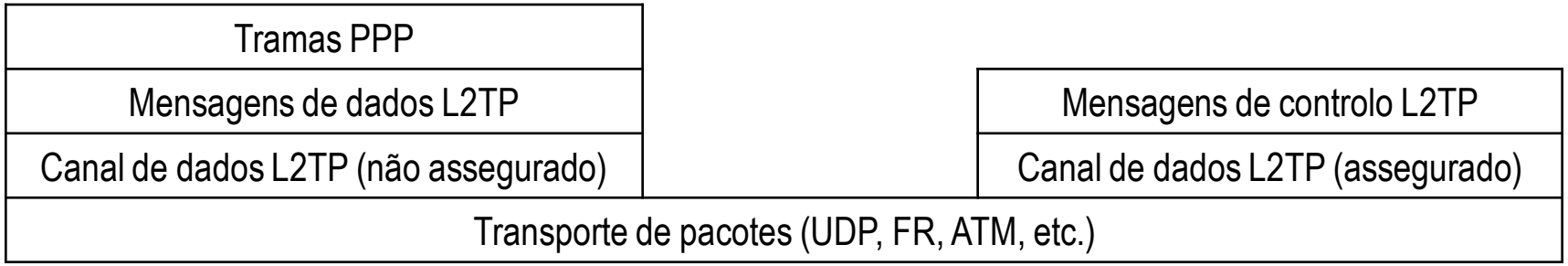


Note: L2TP does not provide security. It provides only tunneling. L2TP recommends the use of IPsec for security.

Exemplo: https://kitz.co.uk/adsl/equip.htm

Layer 2 Tunneling Protocol (L2TP)

- L2TP estende o modelo PPP ao permitir que o nível 2 e os extremos PPP existam em diferentes equipamentos interligados por uma rede IP.
- O utilizador tem uma ligação de nível 2 até um concentrador de acessos que envia as tramas PPP através de um túnel até ao NAS.
- L2TP define dois canais, para transmissão assegurada de dados (mensagens de controlo) e não assegurada (mensagens de dados).



L2TP message format

- **Flags:**
  - **T**: controlo/dados.
  - **L**: indica a presença do campo Length.
  - **S**: indica a presença dos campos de sequência Ns e Nr.
  - **O**: indica a presença dos campos de *offset*.
  - **P**: indica tratar-se de uma mensagem prioritária

1	1	1	1	1	1	1	1	1	1	1	1	4	16
T	L	x	x	S	x	O	P	x	x	x	x	Ver	Length (opt)
Tunnel ID													Session ID
Ns (opt)													Nr (opt)
Offset Size (opt)													Offset pad (opt)

L2TP message format

Flags and version

Control flags indicating data/control packet and presence of length, sequence, and offset fields.

Length (optional)

Total length of the message in bytes, present only when length flag is set.

Tunnel ID

Indicates the identifier for the control connection.

Session ID

Indicates the identifier for a session within a tunnel.

Ns (optional)

Sequence number for this data or control message, beginning at zero and incrementing by one (modulo 2^{16}) for each message sent. Present only when sequence flag set.

Nr (optional)

Sequence number for expected message to be received. Nr is set to the Ns of the last in-order message received plus one (modulo 2^{16}). In data messages, Nr is reserved and, if present (as indicated by the S bit), MUST be ignored upon receipt.

L2TP message format

Offset Size (optional)
Specifies where payload data is located past the L2TP header. If the offset field is present, the L2TP header ends after the last byte of the offset padding. This field exists if the offset flag is set.
Offset Pad (optional)
Variable length, as specified by the offset size. Contents of this field are undefined.
Payload data
Variable length (Max payload size = Max size of UDP packet − size of L2TP header)

L2TP: Mensagens

Controlo da ligação

1	SCCRQ	*Start-Control-Connection-Request*
2	SCCRP	*Start-Control-Connection-Reply*
3	SCCCN	*Start-Control-Connection-Connected*
4	StopCCN	*Stop-Control-Connection-Notification*

Gestão de ligação

7	OCRQ	*Outgoing-Call-Request*
8	OCRP	*Outgoing-Call-Reply*
9	OCCN	*Outgoing-Call-Connected*
10	ICRQ	*Incoming-Call-Request*
11	ICRP	*Incoming-Call-Reply*
12	ICCN	*Incoming-Call-Connected*
14	CDN	*Call-Disconnect-Notify*

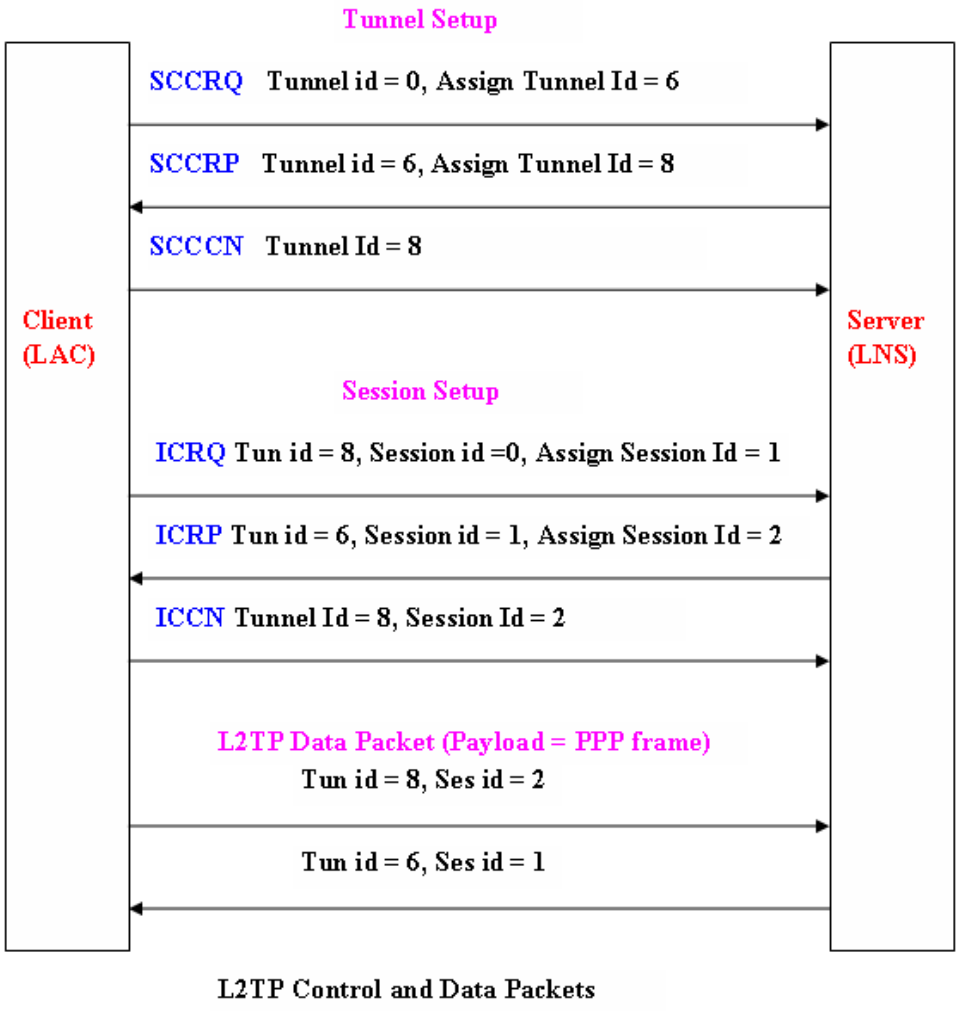
Error Reporting

15	WEN	*Call-Disconnect-Notify*

PPP Session Control

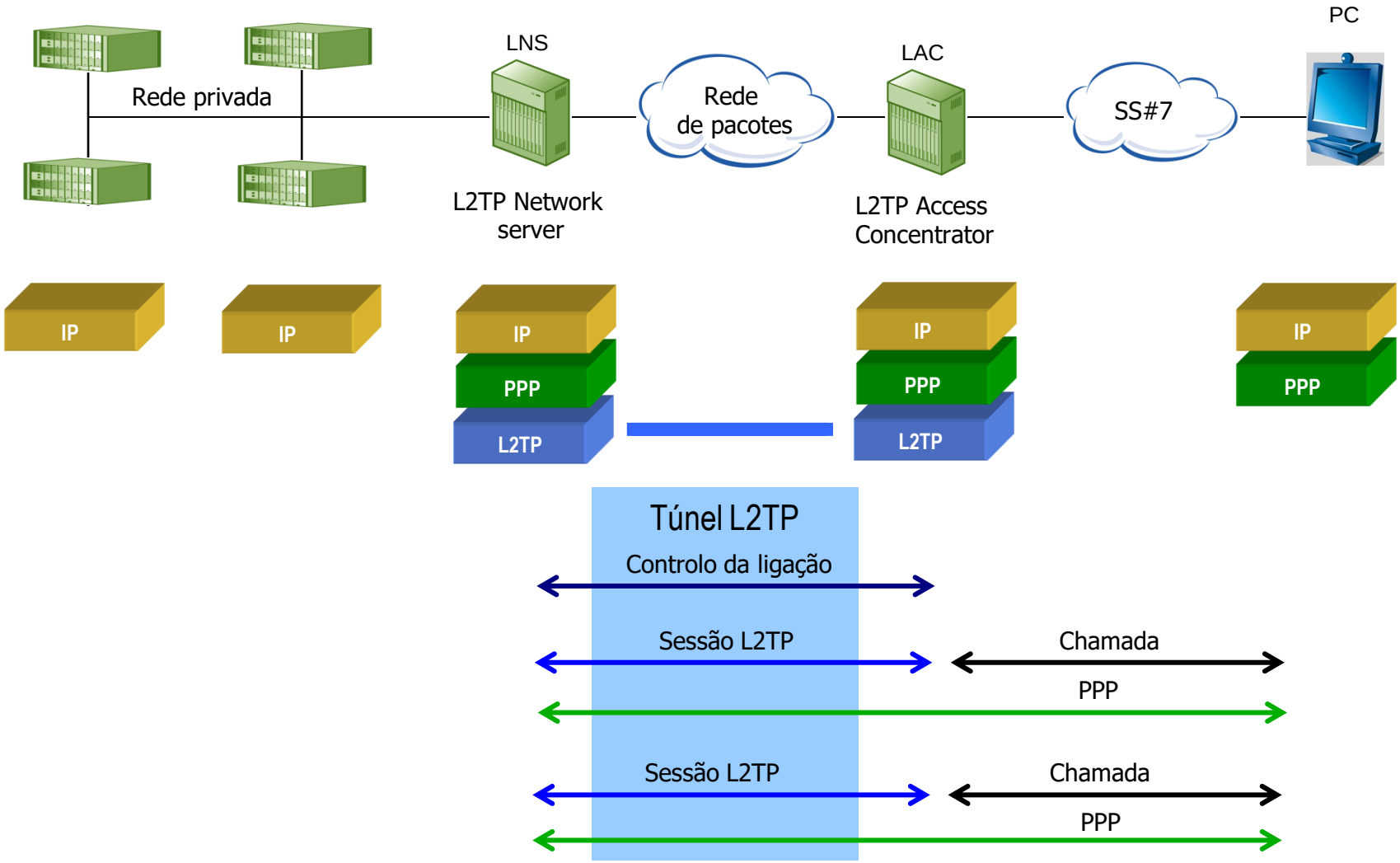
16	SLI	*Set-Link-Info*

L2TP Control and data packets



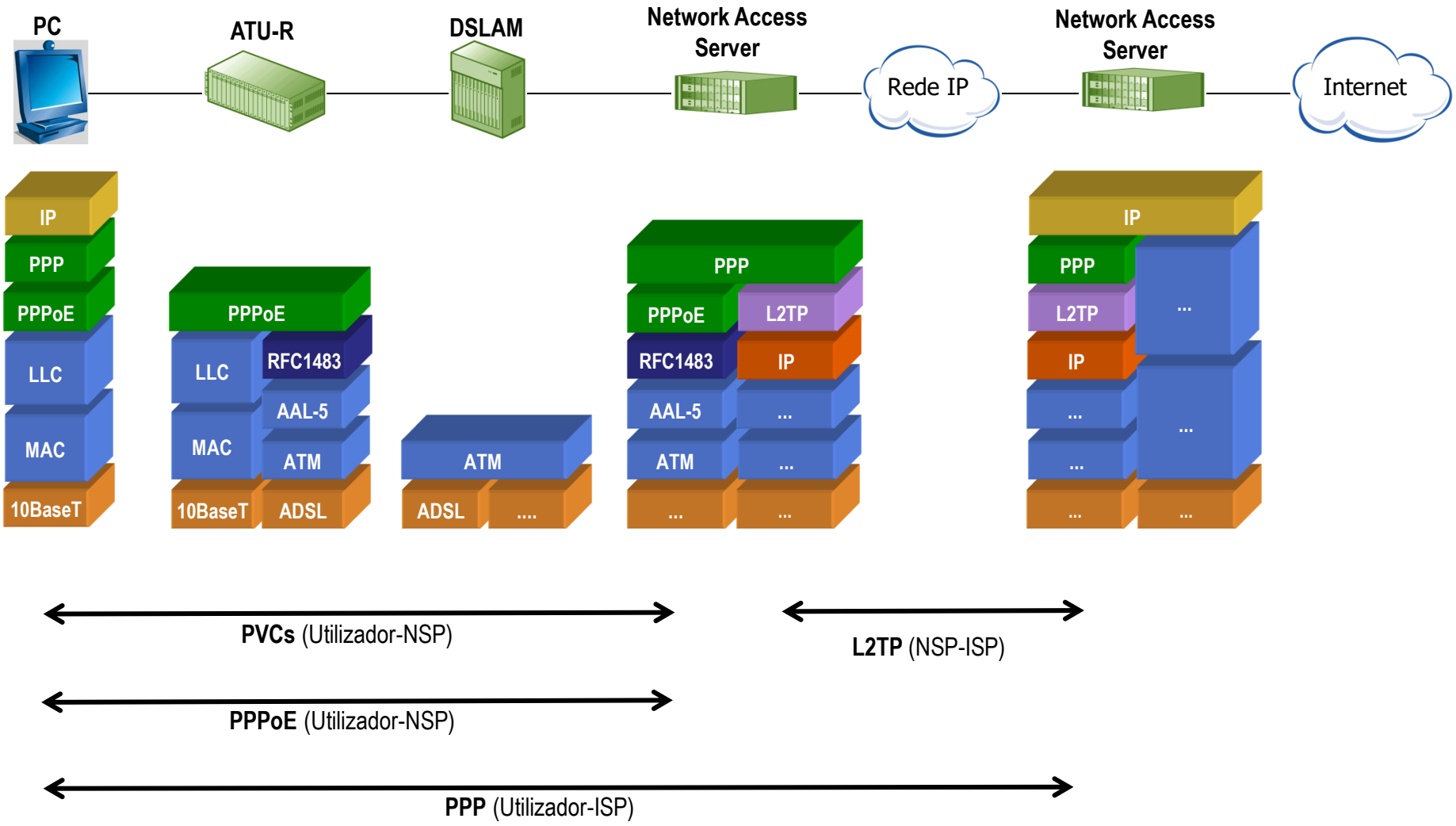
L2TP Control and Data Packets

L2TP: Túnel PPP

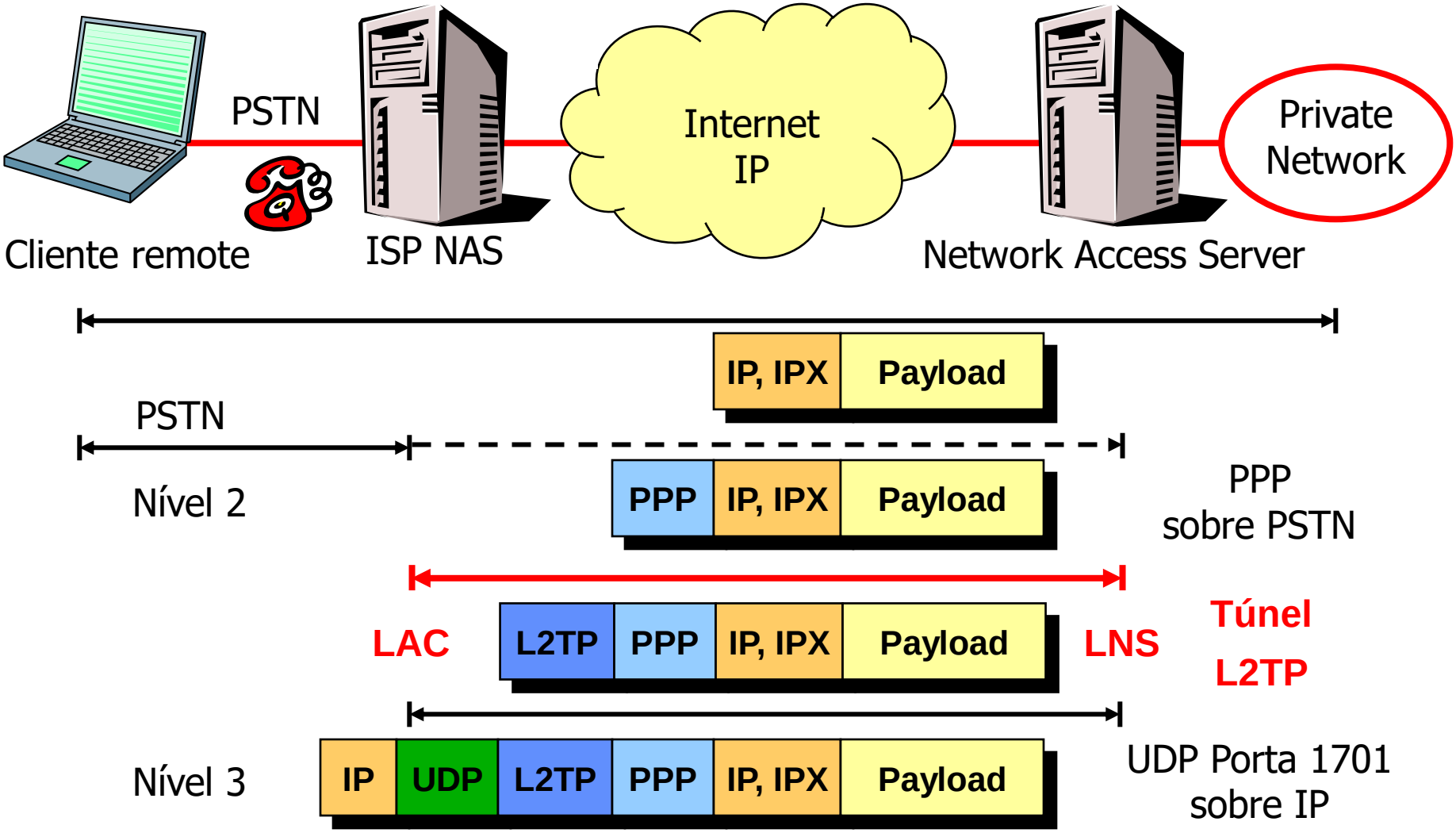


Caso 2: Sessão PPP sobre PPPoE

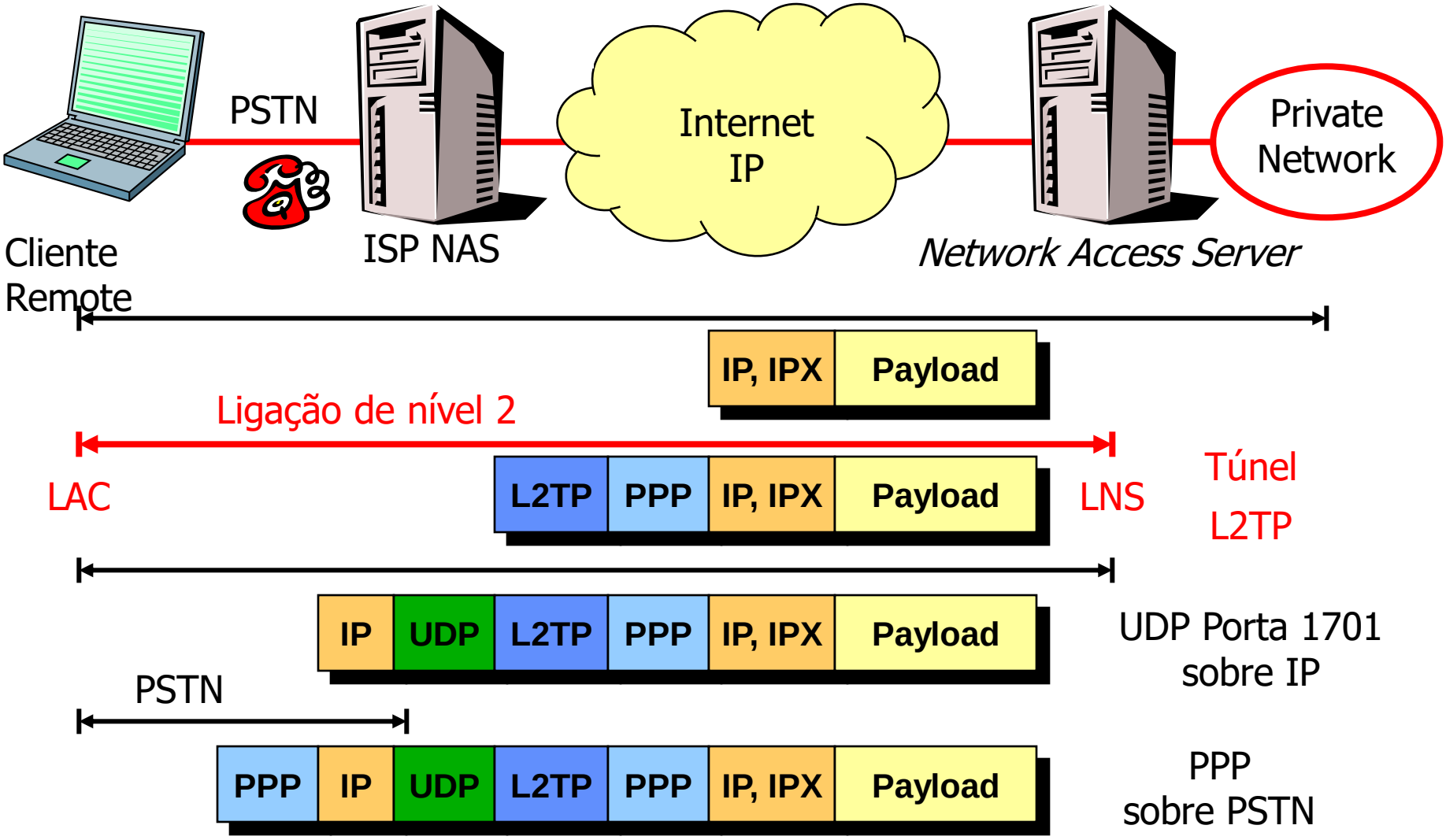
Network Service Provider com rede IP



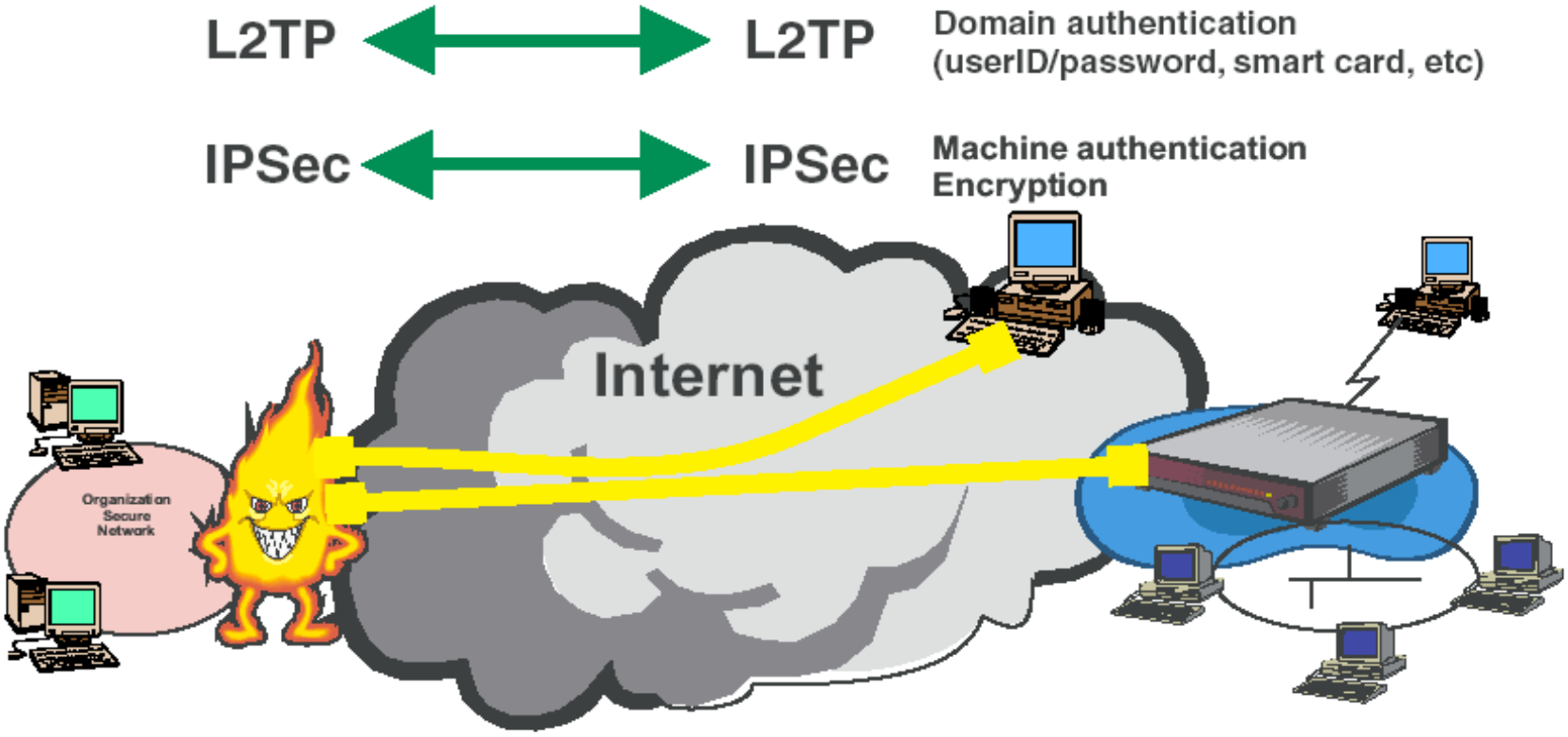
Layer 2 Tunneling Protocol (L2TP) - Modo compulsivo



Layer 2 Tunneling Protocol (L2TP) - Modo voluntário



Camada de ligação: L2TP para VPDN (*Vir Pvt Dial Net*)



IPSec IKE negotiation
Establish IPSec ESP for L2TP UDP port 1701
L2TP tunnel setup, management over IPSec
User authentication to domain

PPTP Versus L2TP

	PPTP	L2TP
Tunneling?	Yes	Yes
Security?	Yes	No. Use IPsec or some other system for security
Limited to IP internet?	Yes	No. Also Frame Relay, etc.

Problemas

- Não existem mecanismos de protecção do túnel L2TP definidos ⇒ expõe tanto os pacotes de dados quanto os pacotes de controle a vulnerabilidades como:
  - Obtenção da identidade do utilizador
  - Modificação dos pacotes de dados e controle
  - Sequestro do túnel L2TP ou da ligação PPP
  - Interrupção da negociação PPP ECP ⇒ remoção da protecção de confidencialidade
  - Interrupção ou enfraquecimento do processo de autenticação PPP ⇒ acesso à senha do utilizador