VPN

VIRTUAL PRIVATE NETWORKS

OVERVIEW OF VIRTUAL PRIVATE NETWORK TECHNOLOGY AND VPN PROTOCOLS SUCH AS PPTP, IPSEC AND L2TP

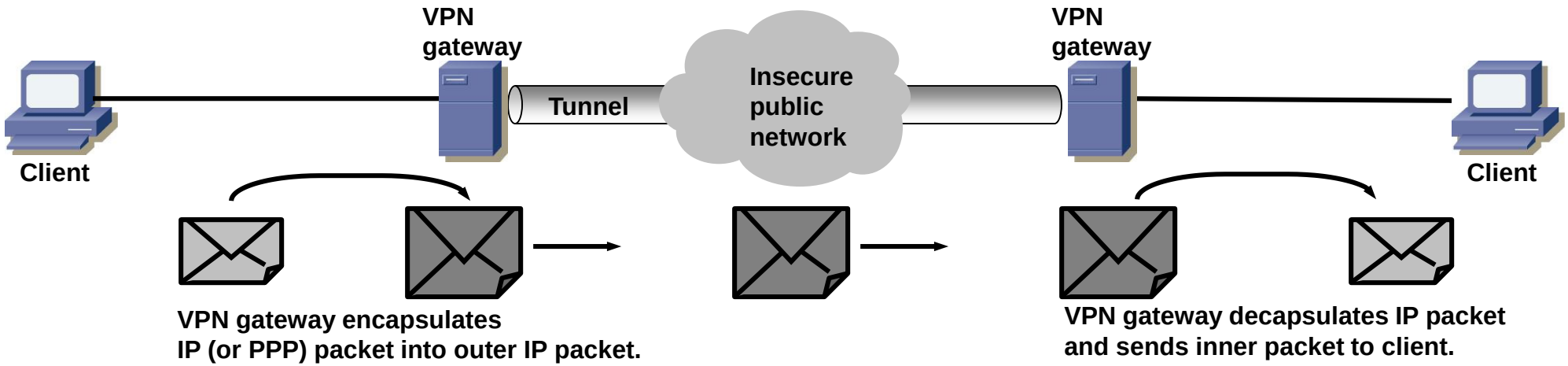
Peter R. Egli
peteregli.net

Contents

1. Virtual Private Network VPN purpose

1. Secure communication over insecure links / networks:

A. Tunnelling of protocols like PPP:

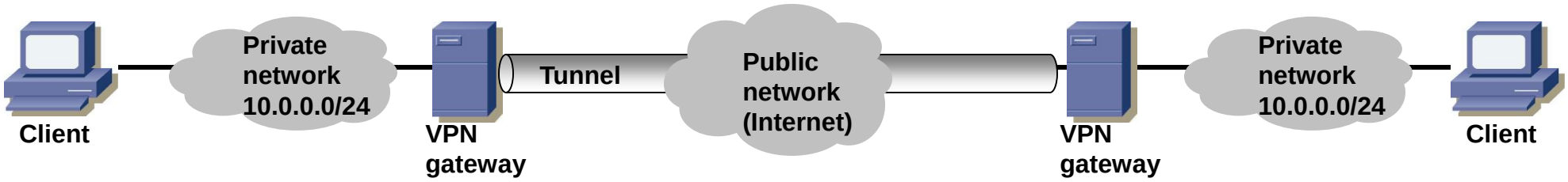


B. Encryption: Tunnel may use encryption to provide secrecy/confidentiality.
C. Authentication: Tunnel may be authenticated thus granting access to VPN only to authorized clients.
D. Access control / authorization: VPN gateways ascertain and enforce level of access for VPN client.
E. Auditing (monitor, log, intervene): VPN gateways monitor usage of VPN and react in case of anomality.

---

2. Private addressing and protocols on top of public addresses:

Tunnelling of private IP addresses (10.0.0.0, 172.16.0.0, 192.168.0.0) through public network (Internet).



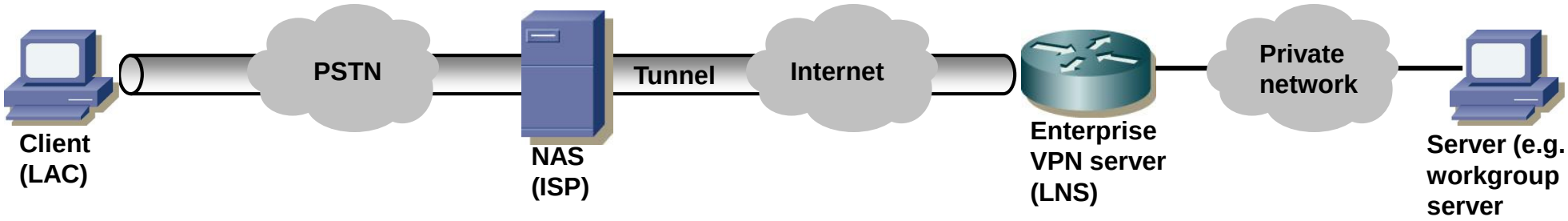
2. Types of Virtual Private Networks (1/3)

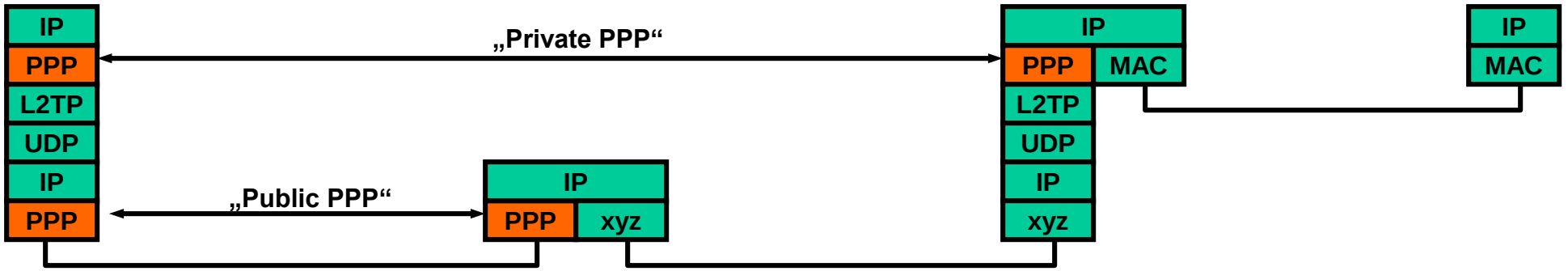
1. Access VPN client initiated (=voluntary tunnel):

➔ VPN client is located on client machine. NAS only delivers public IP address to client via PPP („public PPP session“ between client and NAS).

➔ On top of that client creates a VPN connection (e.g. L2TP) to get private IP and this way is hooked into the private network just as it were directly connected to the private network („private PPP session“ between client and server).

➔ This VPN mode is called „voluntary“ since the VPN is under control of the client itself (client can decide if it establishes the VPN tunnel or not).





NAS Network Access Server
LNS L2TP Network Server
ISP Internet Service Provider
PSTN Public Switched Telephony Network
LAC L2TP Access Concentrator
L2TP Layer 2 Tunnelling Protocol
PPP Point to Point Protocol

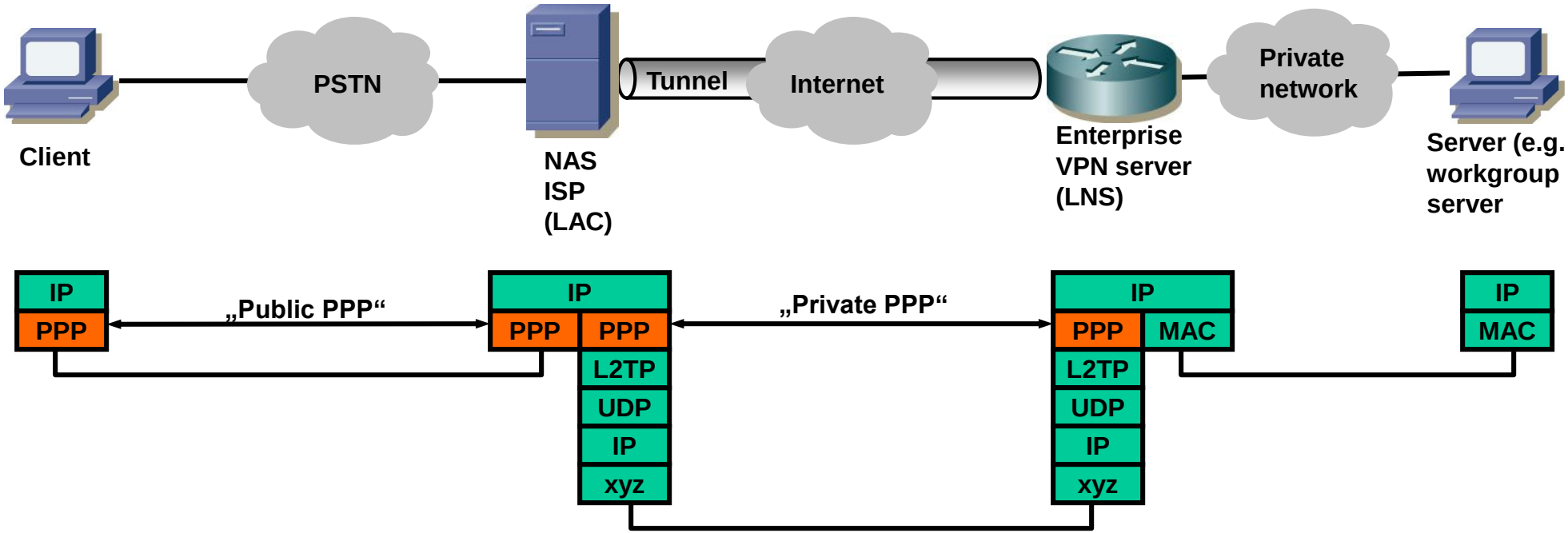
2. Types of Virtual Private Networks (2/3)

2. Access VPN NAS initiated (=compulsory tunnel):

➔ NAS opens VPN tunnel to enterprise VPN server on behalf of client.

➔ Unlike the client initiated VPN the access part is not private (no encryption, no private IP).

➔ This VPN mode is called „compulsory“ since the VPN is not under control of the client itself (client can not decide if it establishes VPN tunnel or not – VPN tunnel is always established irrespective of client settings).

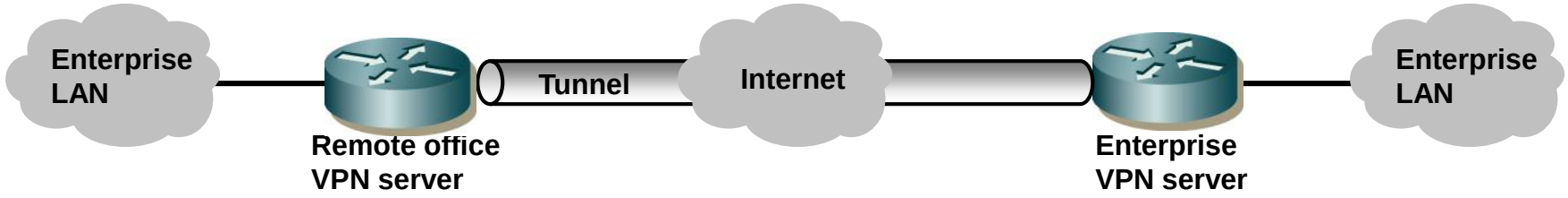


2. Types of Virtual Private Networks (3/3)

3. Intranet VPN:

➔ Enterprise VPN server and branch office VPN server connect LANs to each other thus forming an Intranet (Intranet = private network based on Internet protocols).

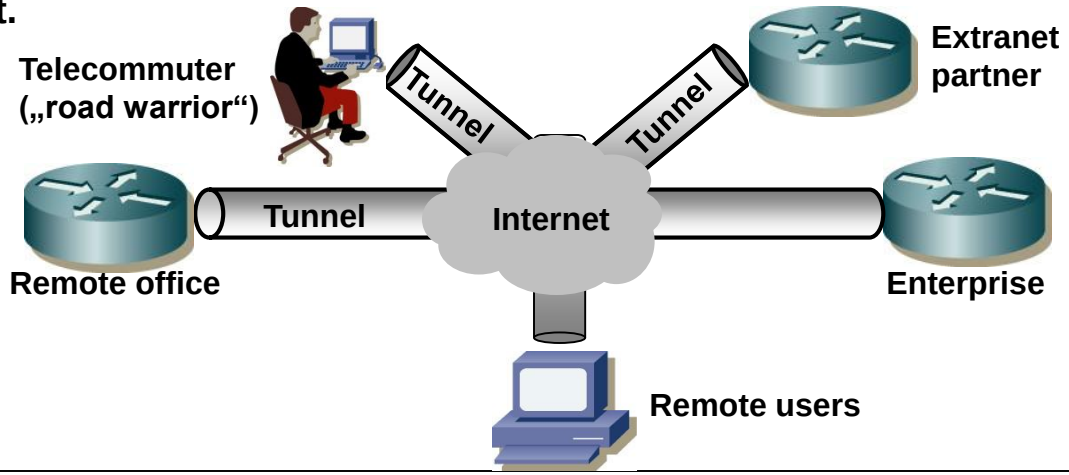
➔ The VPN gateways establish a virtual connection (tunnel) between the 2 sites and thus the remote / branch office is virtually hooked up directly to the enterprise LAN.



4. Extranet VPN:

➔ An extranet is either a hub and spoke VPN (central VPN gateway establishing VPN connections with all extranet members) or a meshed VPN with a VPN tunnel between any 2 VPN members.

➔ An extranet is a „semi-private“ network that gives the extranet members access to each other thus forming a virtual network outside of the Intranet.



3. Comparison VPN Layer 2 tunnelling vs. Layer 3 tunnelling VPNs

➔ Layer 2 tunnelling protocols allow the tunnelling of layer 2 protocols (e.g. PPP).

➔ Layer 3 tunnelling protocols can be used for the tunnelling of layer 3 protocols (e.g. IPSec).

	Layer 2 tunnelling	Layer 3 tunnelling
Tunnelling	PPP over xyTP over UDP over IP	IP over IP
Tunnel setup	Dynamic	Static
User authentication	PPP	None or ISAKMP
IP address	Dynamic (PPP)	Static
Data compression	PPP (CCP)	None
Data encryption	PPP (ECP)	Various
Encryption key	Periodic key refreshment	ISAKMP
Multiprotocol	Yes	No (IP only)
Examples	L2TP, GRE, L2F	IPSec

• **The most important tunnelling protocols:**

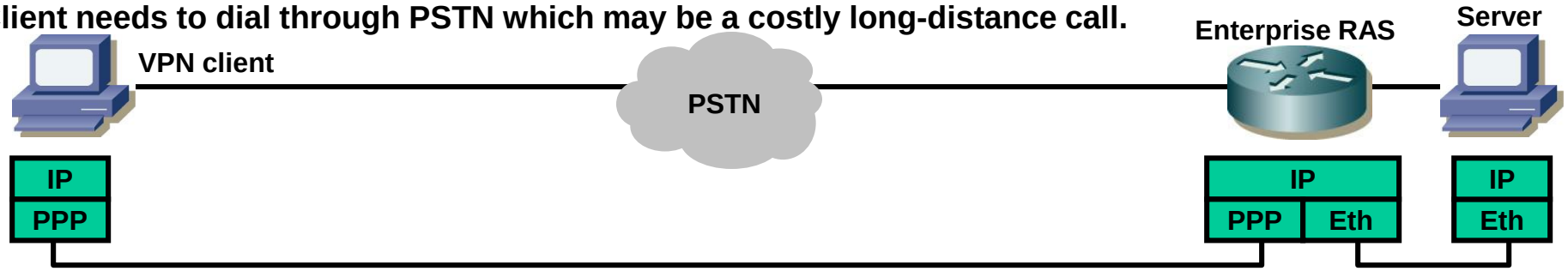
A. PPTP - Point to Point Tunnelling Protocol
B. GRE - Generic Routing Encapsulation
C. L2F - Layer 2 Framing Protocol
D. L2TP - Layer 2 Tunnelling Protocol
E. IPSec / IP in IP
F. SSH - Secure SHell
G. SSL/TLS - Secure Socket Layer based VPNs
H. PPPoE - PPP over Ethernet
I. MPLS - MultiProtocol Label Switching
K. MIP - Mobile IP

4. PPTP Point to Point Tunnelling Protocol RFC2637 (1/2)

Key:
RAS Remote Access Server

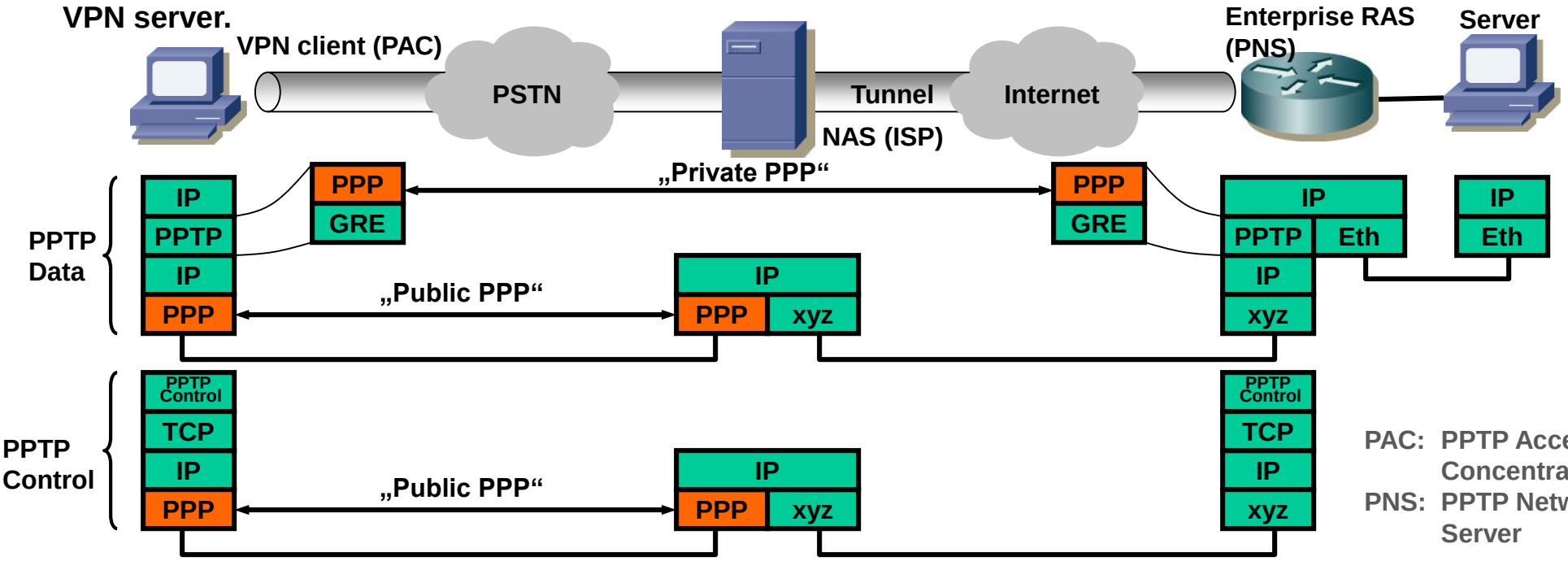
A. Remote access in the old days (dial-up):

Client needs to dial through PSTN which may be a costly long-distance call.



B. Remote access with PPTP (client initiated voluntary tunnel mode):

VPN clients establish "public PPP" session with NAS and on top of that "private PPP" session with enterprise VPN server.



PAC: PPTP Access Concentrator
PNS: PPTP Network Server

4. PPTP Point to Point Tunnelling Protocol RFC2637 (2/2)

➔ PPTP was originally used for remote access via an ISP (PPTP = remote access solution). PPTP was devised by Microsoft as a RAS (Remote Access Service) protocol.

➔ PPTP is the most widely used VPN tunnelling protocol but will be supplanted by L2TP / IPSec in the long run.

➔ PPTP is based on and uses the services of PPP (Point to Point Protocol). By using PPP various authentication (PAP, CHAP, MSCHAP, EAP) and encryption (ECP with preshared keys, RC4, DES) standards compined with compression (CCP) are possible with PPTP.

➔ PPTP provides multiprotocol encapsulation through usage of GRE for data packets; this means that the tunnel between client and server is transparent for applications (applications do not „see“ the tunnel); client is virtually within enterprise LAN.

➔ GRE, as its name implies, is basically an encapsulation protocol that allows transport of layer 2 (e.g. PPP) and 3 (IP) protocols. In PPTP GRE is used for the transport of data frames while PPTP control frames are used for setting up the GRE connection.

➔ PPTP uses a PPTP control connection (TCP) to establish a PPTP data tunnel (GRE) with the following control connection messages:

PPTP_START_SESSION_REQUEST / _REPLY
PPTP_ECHO_REQUEST / _REPLY
PPTP_WAN_ERROR_NOTIFY
PPTP_SET_LINK_INFO
PPTP_STOP_SESSION_REQUEST / _REPLY

➔ The PPTP control connection is neither authenticated nor integrity-checked;

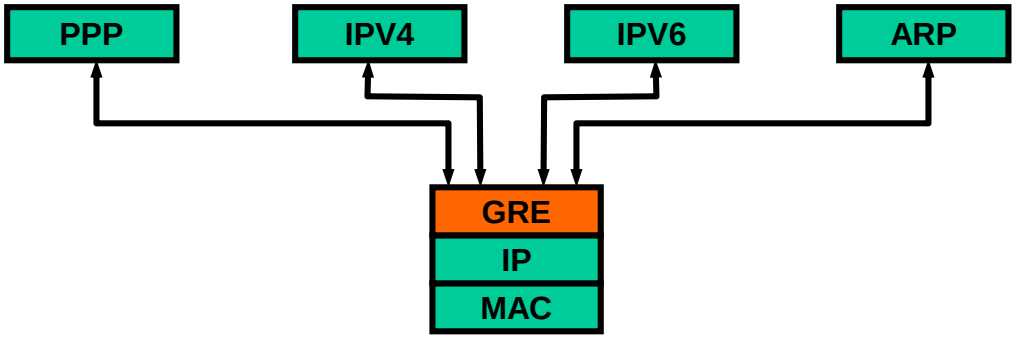
➔ Eavesdropping is possible.

➔ Connection hijacking is possible (GRE not encrypted).

➔ PPTP can usually be made to pass through NAPT / NPAT since it uses GRE as encapsulation protocol. But the NAPT must have an ALG for GRE (also called NAT Editor).

5. GRE Generic Routing Encapsulation RFC1701 / RFC1702

➔The purpose of GRE is to provide a generic protocol for encapsulation (tunnelling) of a protocol X in a protocol Y. Prior to GRE a range of RFCs were written defining how to encapsulate protocol X in protocol Y thus leading to a O(n^2) complexity. GRE solved this problem by providing a standard way to encapsulate different protocols in others (multi-protocol support).



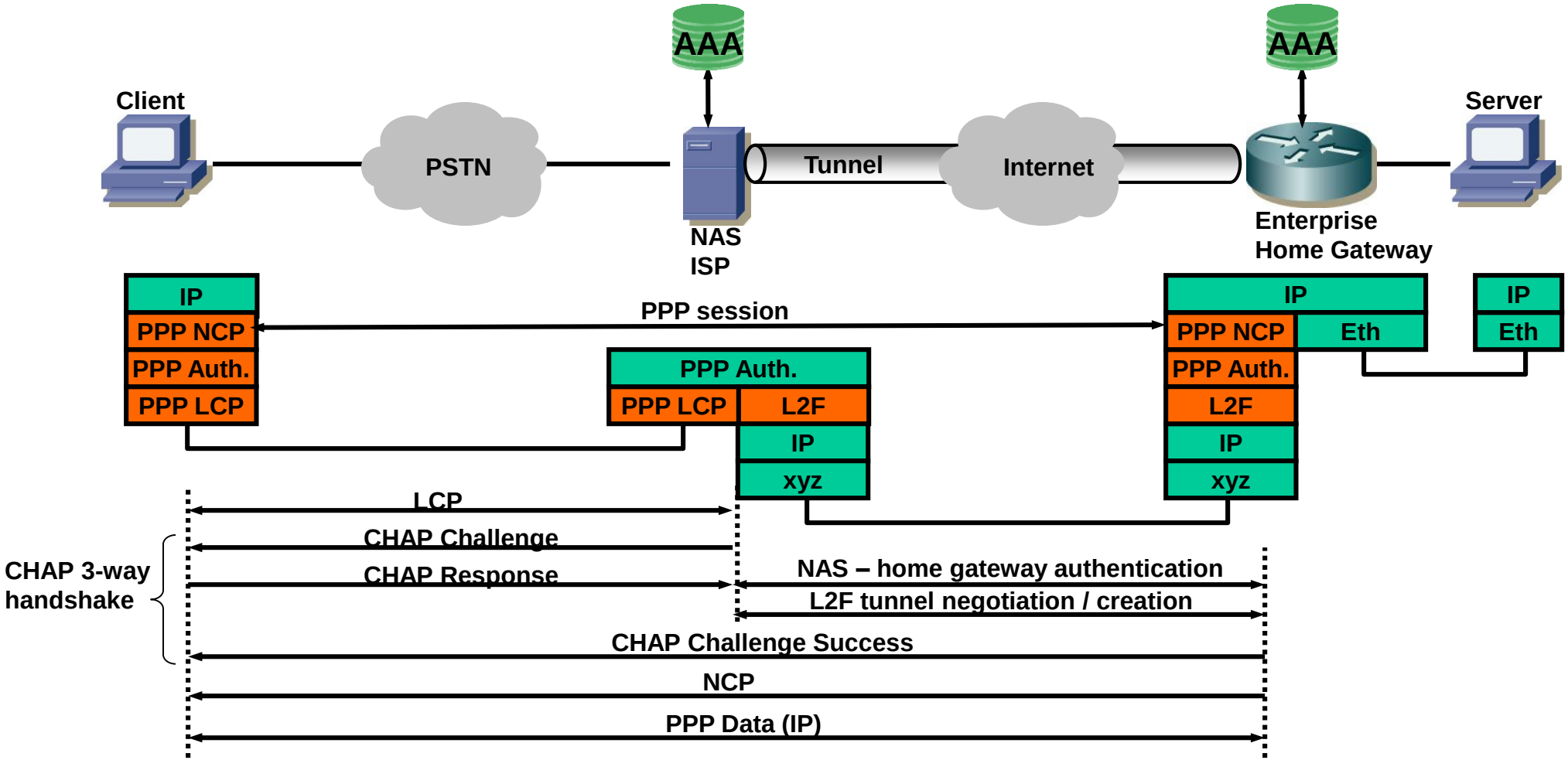
➔ Another reason for GRE is the fact that RFC1700 does not define PPP as payload of IP (type field in IP header) since normally IP is carried in PPP and not PPP in IP. GRE allows encapsulation of PPP frames in IP packets.
➔ GRE provides sequencing (restore correct order at destination).
➔ GRE has a low overhead; thus it is suited for high speed tunnelling.
➔ GRE allows multicasts which is required for routing protocol updates.
➔ Even though GRE is a tunnelling it does not provide security (encryption etc.).
➔ GRE and NAPT: GRE does not have a transport protocol, but certain NAPTs can be made to pass GRE (based on protocol ID in IP header); these NAPTs are called „NAPT editors“ or „ALG“ Application Level Gateway.

6. L2F Layer 2 Forwarding

➔ L2F allows the tunnelling of layer2 protocol such as PPP.

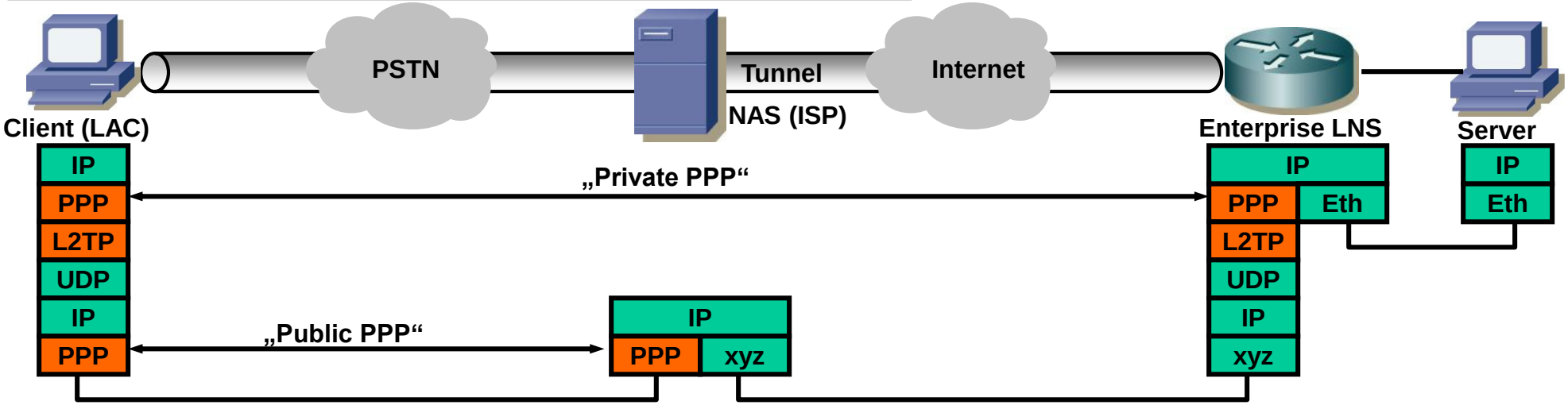
➔ L2F was designed for NAS initiated compulsory tunnel.

➔ Once the L2F tunnel is established, the NAS acts as a PPP forwarder.

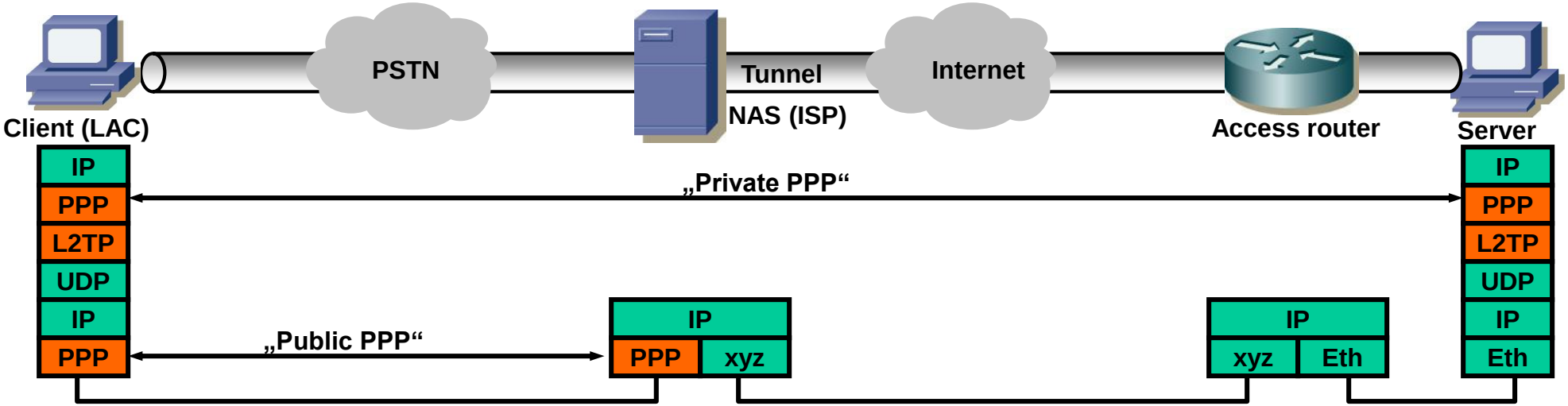


7. L2TP Layer 2 Tunnelling Protocol RFC2661 (1/3)

Scenario 1: Client (LAC) to enterprise VPN server (LNS):



Scenario 2: End-to-end tunnel (LNS on server):

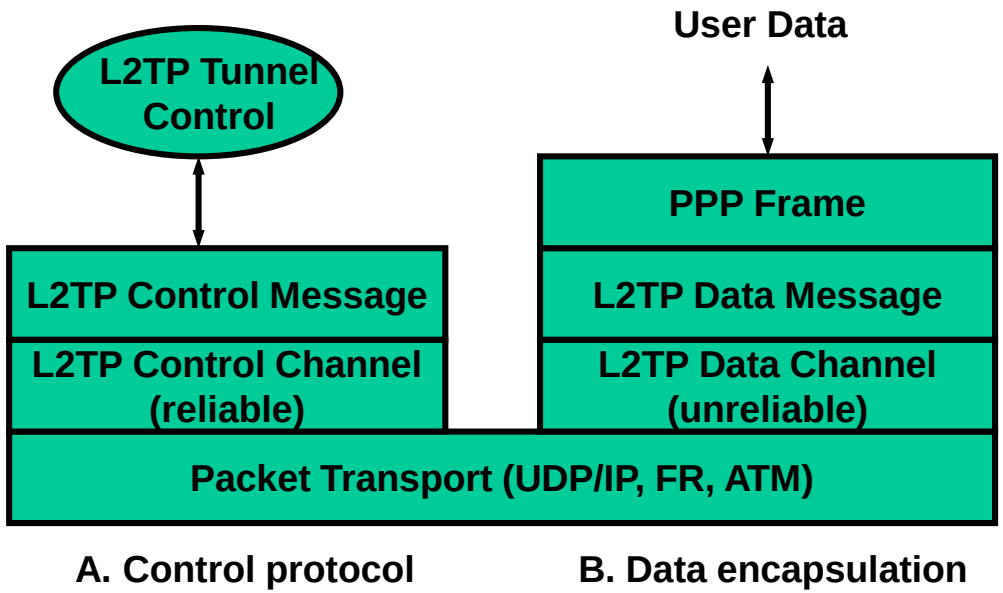


7. L2TP Layer 2 Tunnelling Protocol RFC2661 (2/3)

➔ **L2TP is:**

A. A control protocol to dynamically setup and teardown connections (tunnels); this control protocol uses a reliable transport (that uses the Ns and Nr sequence numbers for reliability).

B. Data encapsulation for tunnelling user data frames (PPP); the data packet transport is unreliable, that is makes not use of Ns and Nr sequence numbers.



7. L2TP Layer 2 Tunnelling Protocol RFC2661 (3/3)

➔ L2TP is the „merger“ of PPTP (Microsoft) and L2F (Cisco) and thus is the best of the two whilst incorporating additional features:

- L2TP is multiprotocol (PPTP was bound to IP as transport protocol). L2TP allows to tunnel PPP over any packet switched network.
- L2TP allows end-to-end tunnels (along with the client initiated voluntary VPN mode); L2F supports only the NAS initiated VPN model.
- L2TP only uses one single format (L2TP header over UDP) for data and tunnel maintenance. PPTP had a data (IP over PPP over GRE) and a control (TCP) channel.
- L2TP allows user and tunnel authentication (tunnel auth. with L2TP, user authentication with PPP authentication). PPTP only allowed user authentication.
- L2TP allows an arbitrary number of tunnels (useful for enabling QoS). L2F and PPTP only allowed to open 1 tunnel between 2 endpoints.
- L2TP is run over UDP/IP to make it pass through firewalls.
- L2TP affords sequencing and flow control (required since transported over unreliable UDP).

➔ L2TP has its deficiencies:

- L2TP has no built-in confidentiality. This leaves the L2TP tunnel vulnerable to attacks (with PPP only payload but not tunnel data is authenticated / encrypted). To overcome this L2TP can be combined with IPSec. Pure L2TP voluntary and compulsory mode see previous slides.

8. IPSec IP Security RFC2401 et.al. (1/13)

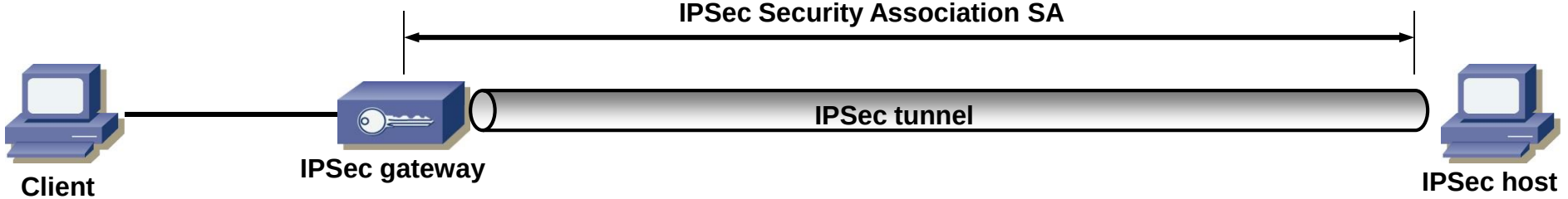
➔ IPSec implements security at the IP layer; thus IPSec is transparent to applications.

➔ An IPSec „connection“ (security association, see below) is static; this means that there is no setup and teardown of a „connection“.

➔ IPSec RFCs:

* IPSec RFC2401.
* Encapsulating Security Payload ESP RFC2406.
* Authentication Header AH RFC2402.
* Various encryption algorithms, e.g. AES (FIPS PUB 197).
* Various authentication algorithms, e.g. HMAC-MD5 RFC2403 or HMAC-SHA-1 RFC2404.
* Key management, e.g. ISAKMP or PKI.

➔ IPSec architecture and terms:



Security Association SA:	An SA spans between security relationship between 2 IPSec endpoints.
Client:	An IPSec client terminates IPSec and consumes data.
Gateway:	Terminates IPSec and forwards data to its destination.
Tunnel:	Encapsulation of IP in IP in order to disguise original IP addresses.
Transport mode:	No tunnel used (that is original IP header is used as IP header).
Tunnel mode:	Old IP packet is encapsulated into new IP packet (IP in IP).
AH:	Authentication Header (one of the IPSec protocols).
ESP:	Encapsulating Security Payload (one of the IPSec protocols).

8. IPSec IP Security RFC2401 et.al. (2/13)

➔ Authentication Header AH is used for authentication.

AH provides:

a. Data integrity (MD5, SHA-1 HMAC Hashed Message Authentication Codes).

b. Data origin authentication (MD5, SHA-1 with shared secret as input).

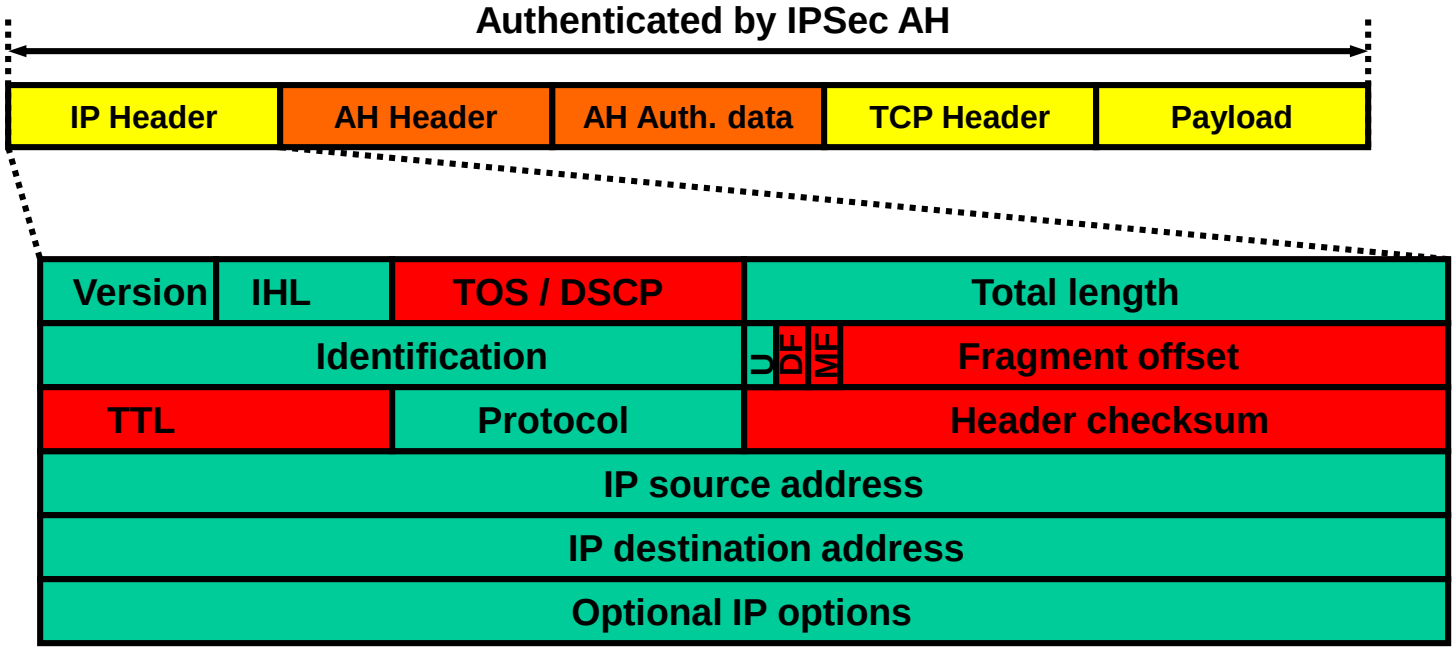
c. Sequence integrity / replay protection (MD5, SHA-1 with serial number as input).

d. Non-repudiation („Nicht-Rückweisbarkeit").

e. Header forward authentication.

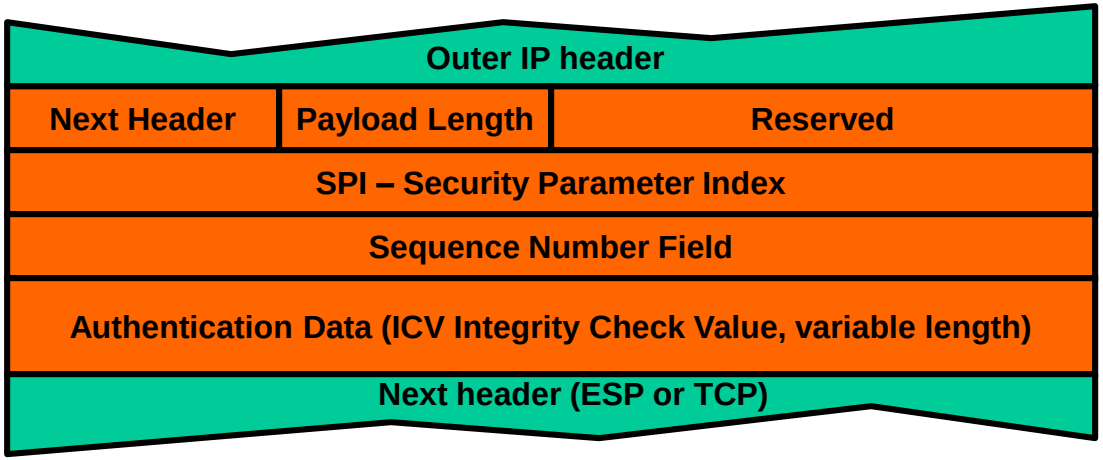
➔ a. thru e. are commonly referred to as „authentication".

➔ AH provides „forward header authentication", i.e. it authenticates the immutable fields of the outer header as follows (green IP header fields, red fields are not authenticated since they may change during transit):



8. IPSec IP Security RFC2401 et.al. (3/13)

➔ Authentication Header AH fields:



Next Header: Identifies the protocol (header) following the AH Authentication Data.

Payload Length: Length of AH header and AH data.

SPI: Identifier for identifying the AH security association.

Sequence Number Field: Counter for packets to foil replay attacks.

Authentication Data (ICV): Authentication value based on MD5 hash (or other algorithm).

8. IPSec IP Security RFC2401 et.al. (4/13)

➔ **Encapsulating Security Payload ESP is used for encryption.**

ESP provides:

a. Confidentiality (encryption).

b. Data integrity.

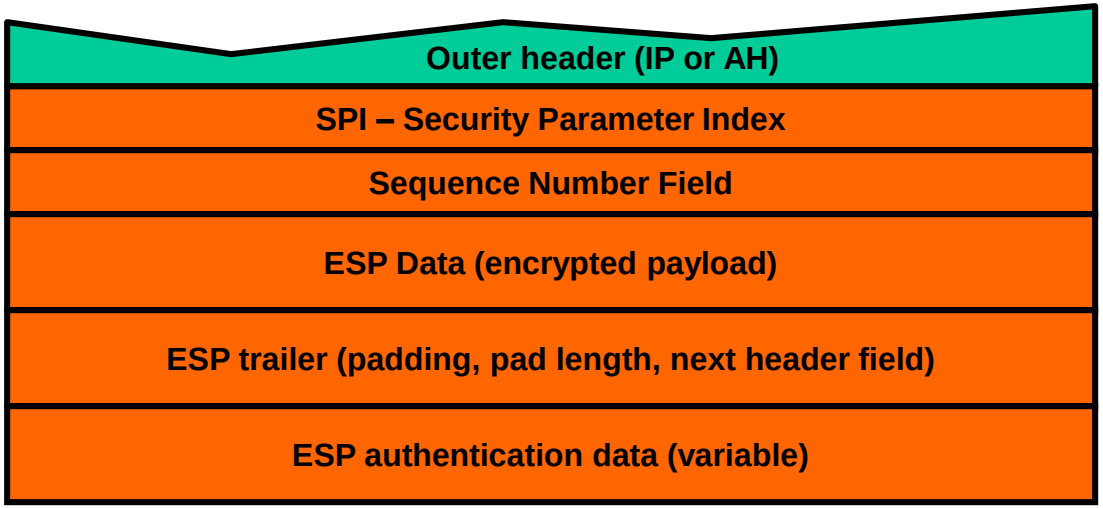
c. Data origin authentication (optional, usually not used since already provided by AH).

d. Replay protection.

➔ ESP does not provide header forward authentication.

➔ ESP authentication is optional and makes only sense if ESP extends AH (e.g. AH terminated at access server but ESP reaching into the LAN to a server).

➔ **ESP header and trailer fields:**



SPI: Identifier for identifying the ESP security association.

Sequence Number Field: Counter for packets to foil replay attacks.

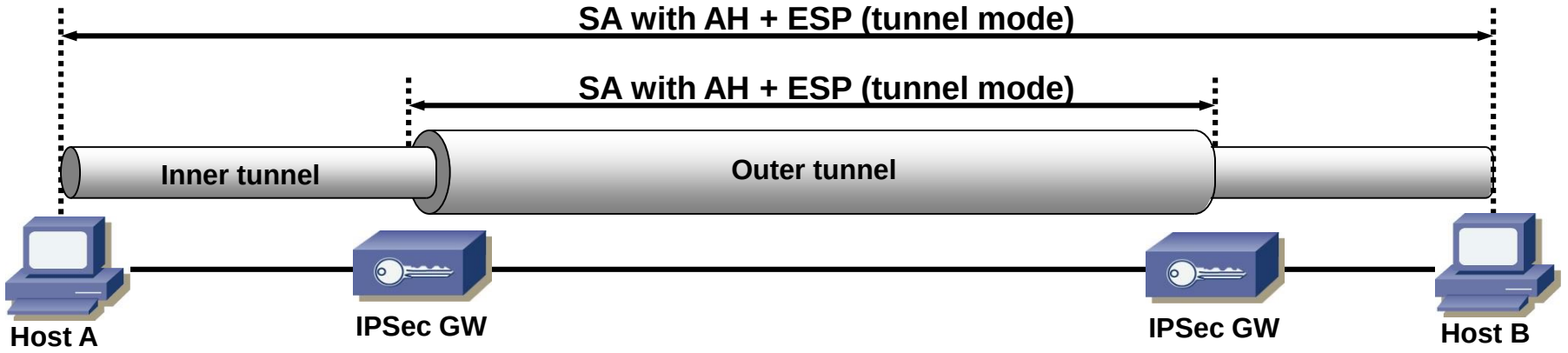
ESP Data: Enrypted TCP header and APDU.

ESP trailer:
a. Padding: Some encryption algorithms require that the data be a multiple of some number of bytes.
b. Next header: Identifies the protocol following the trailer, e.g. ESP authentication header (!= AH).

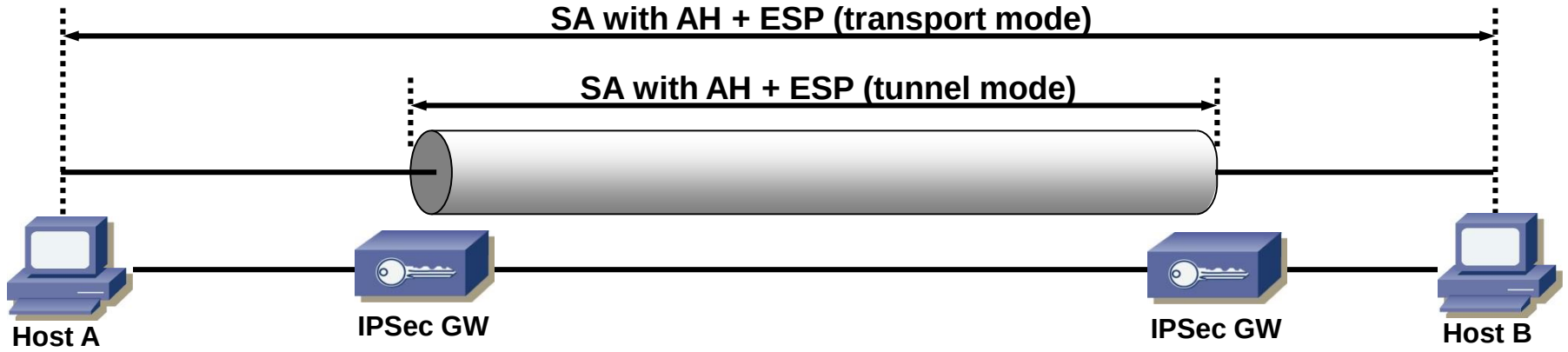
ESP authentication data:
Optional data for ESP authentication (is not the same as IPSec AH authentication data!).

8. IPSec IP Security RFC2401 et.al. (5/13)

➔ AH and ESP in tunnel mode, nested SAs:



➔ AH and ESP in transport and tunnel mode, nested SAs:



N.B.: More than 2 tunnels (e.g. tunnel in tunnel in tunnel) is usually impractical and thus not employed.

8. IPSec IP Security RFC2401 et.al. (6/13)

➔ Why have AH and ESP?

a. AH provides authentication, ESP provides encryption (separation). This separation is useful since in many cases authentication provides enough security and encryption would be too costly and in some cases not even allowed by the government.
b. In many cases AH provides enough security, and ESP (encryption) would consume too much processing power.
c. The authentication provided by ESP could have been designed to cover the IP header as well (forward authentication), but ESP is more complicated since it requires strong encryption and thus has a more complicated format than AH. (N.B.: IPSec processing is done per packet!)
➔ Thus AH and ESP can be used individually or combined.

➔ Some general IPSec design rules:

a. If one of the IPSec endpoints is a gateway, use tunnel mode.
b. If both IPSec endpoints are hosts, use transport mode (outer IP header would be the same as the inner IP header thus IP header is exposed anyway).
c. If protection of the entire IP packet (including header) is required, then use tunnel mode. This hides the source and destination IP addresses to a potential attacker.
d. If AH and ESP are to be combined, AH is the outer protocol, ESP the inner (first authenticate, then decrypt; if authentication fails IPSec does not need to perform costly decryption).
e. If AH and ESP are to be combined, both use the same mode (transport or tunnel mode).

8. IPSec IP Security RFC2401 et.al. (7/13)

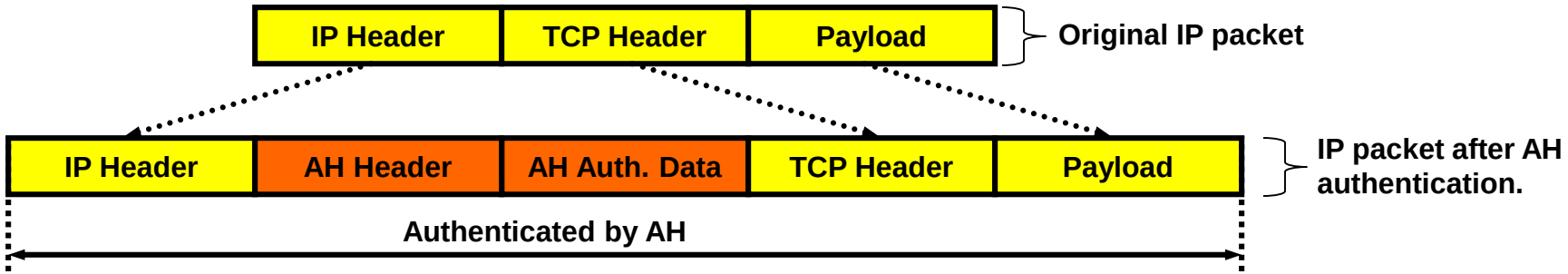
➔ **IPSec Transport Mode:**

1. Transport mode only protect upper layer protocols (TCP and above).
2. Devices implementing only transport mode are called *IPSec hosts*.

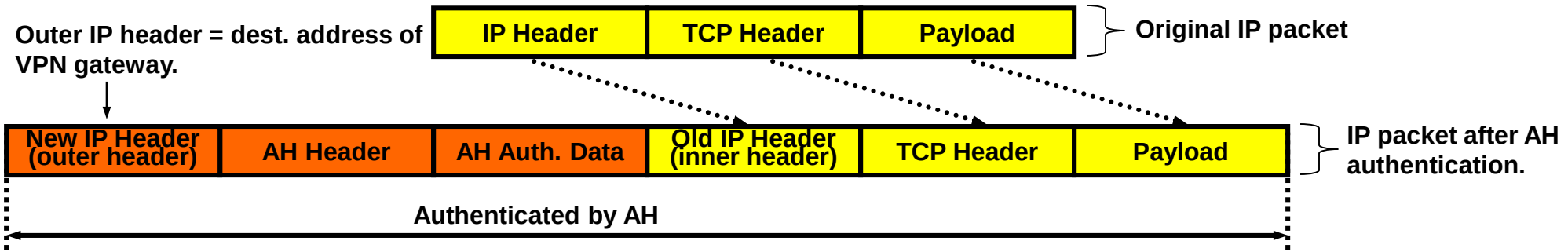
➔ **IPSec Tunnel Mode:**

1. Tunnel mode protects the entire IP packet and tunnel in a secured transport path.
2. Devices implementing tunnel mode are called *IPSec gateways*.

➔ **IPSec AH Transport Mode:**

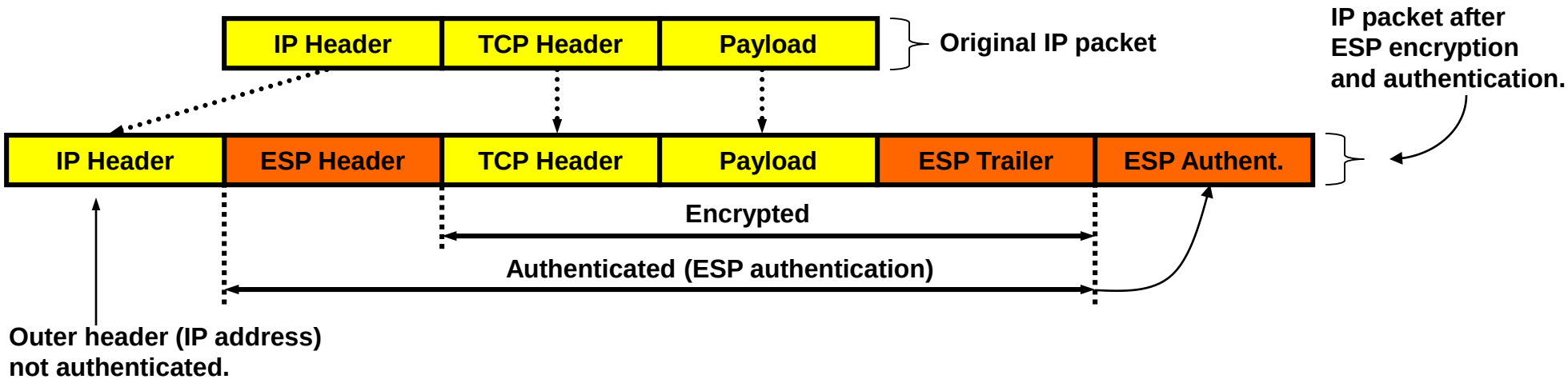


➔ **IPSec AH Tunnel Mode:**

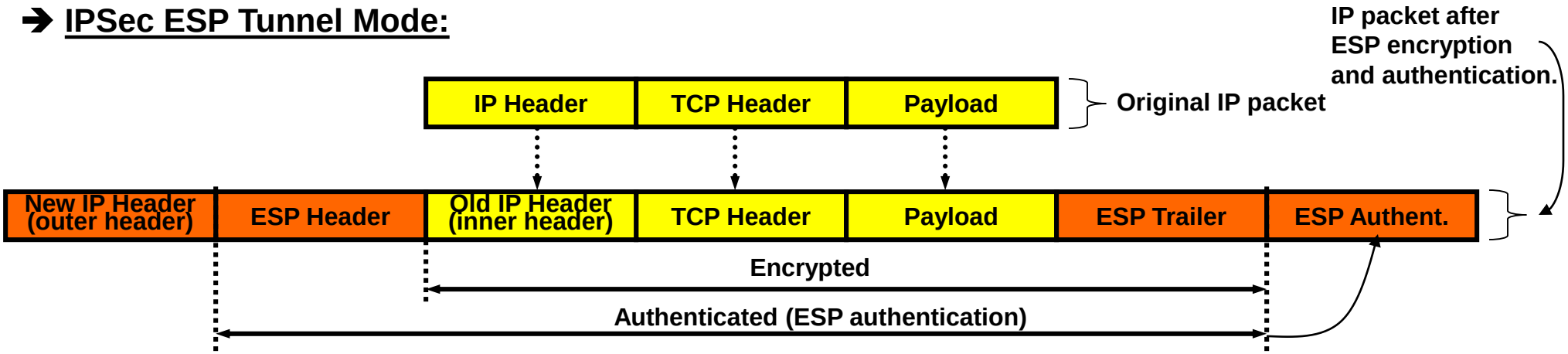


8. IPSec IP Security RFC2401 et.al. (8/13)

➔ IPSec ESP Transport Mode:

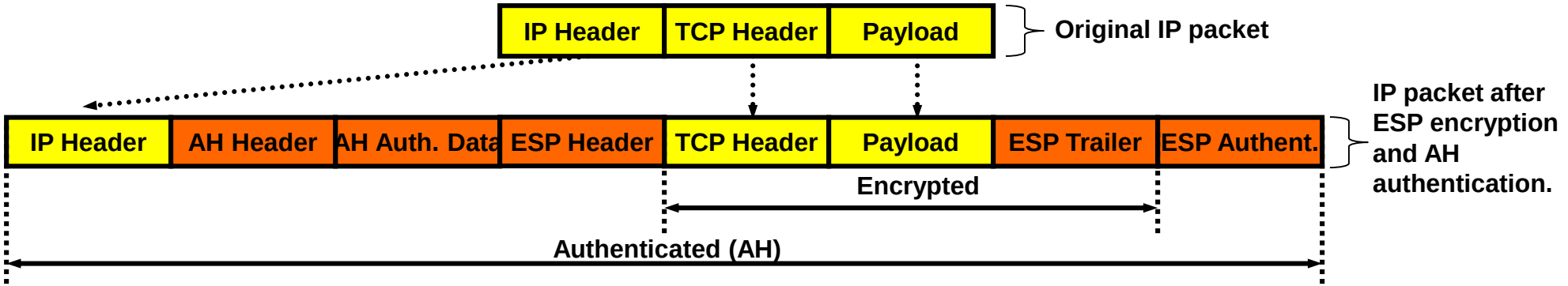


➔ IPSec ESP Tunnel Mode:

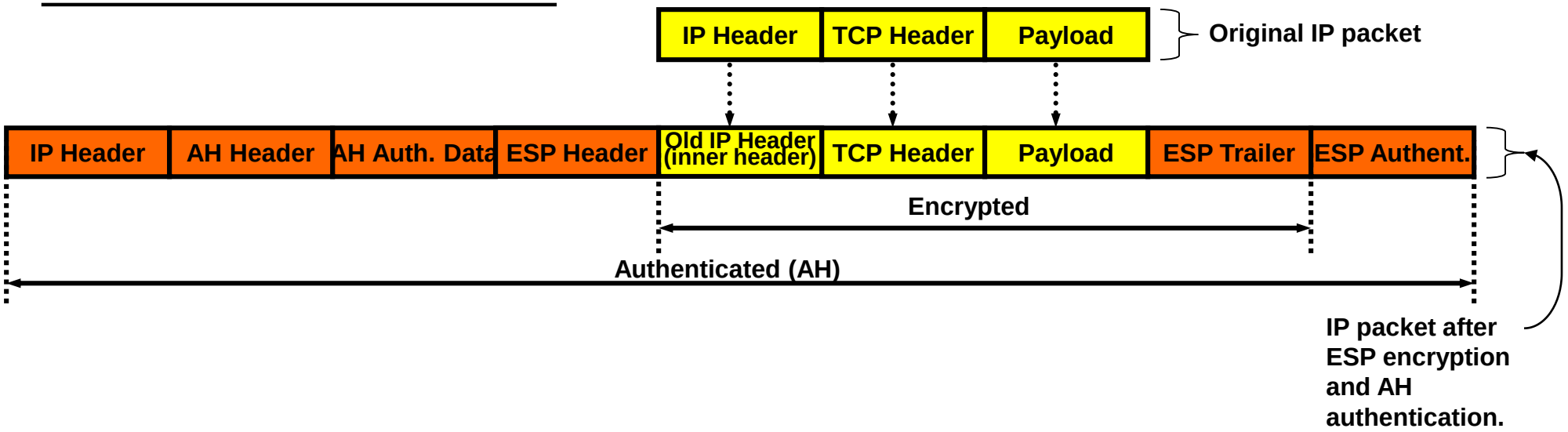


8. IPSec IP Security RFC2401 et.al. (9/13)

➔ IPSec AH and ESP Transport Mode (called „Transport Adjacency“):



➔ IPSec AH and ESP Tunnel Mode:



8. IPSec IP Security RFC2401 et.al. (10/13)

➔ **AH and ESP overview:**

	AH	ESP	AH+ESP
Encryption	**No**	**Yes**	**Yes**
Sender and receiver authentication	**Yes**	**Yes (IPSec tunnel mode only)**	**Yes**
Data integrity	**Yes**	**Yes**	**Yes**
Replay protection	**Yes**	**Yes**	**Yes**
Sender and receiver confidentiality	**No**	**Yes (IPSec tunnel mode only)**	**Yes (IPSec tunnel mode only)**

With AH most of the security needs can be usually satisfied (authentication). IPSec can then be added (encryption) in situations with higher security demands.

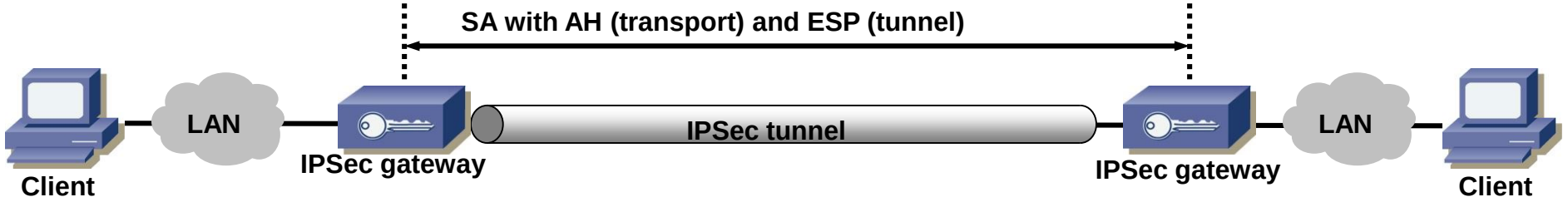
8. IPSec IP Security RFC2401 et.al. (11/13)

➔ Examples of typical IPSec architectures (1):

1. Simple SA (no security layering):

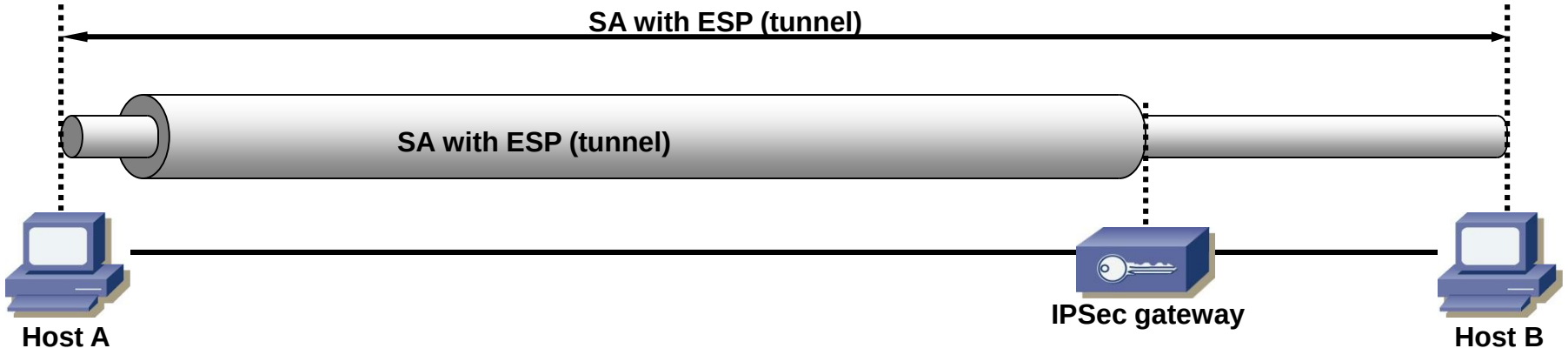
➔ LANs are considered secure thus no encryption or authentication used in LANs.

➔ E.g. VPN between different sites of a company with secure tunnels between each pair of sites.



2. Bundled SA (hierarchic SAs, multilayer security):

➔Access networks (LANs, dial-up network) are considered insecure. An inner tunnel provides end-to-end security between host A and host B. The 2 tunnels have different endpoints.



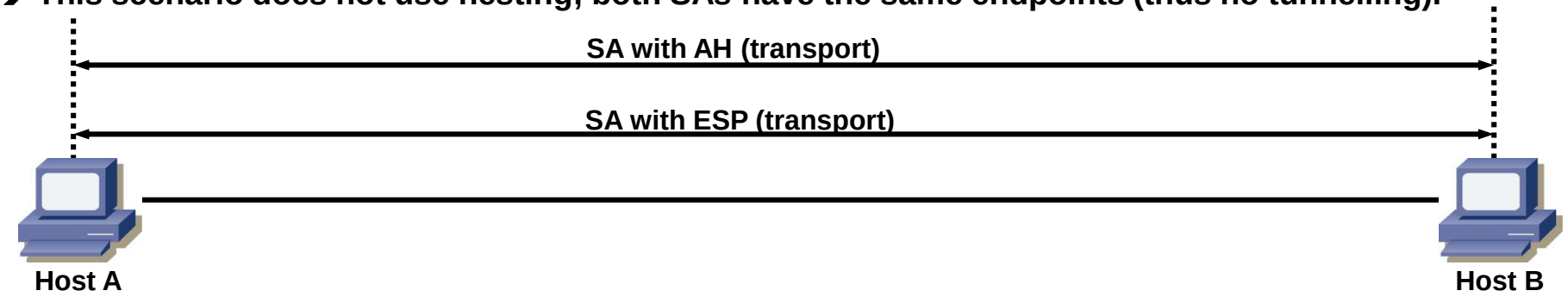
8. IPSec IP Security RFC2401 et.al. (12/13)

➔ Examples of typical IPSec architectures (2):

3. Bundled SA (transport adjacency, single level security):

➔ This example provides end-to-end encryption and authentication. The original IP header is still visible (transport mode).

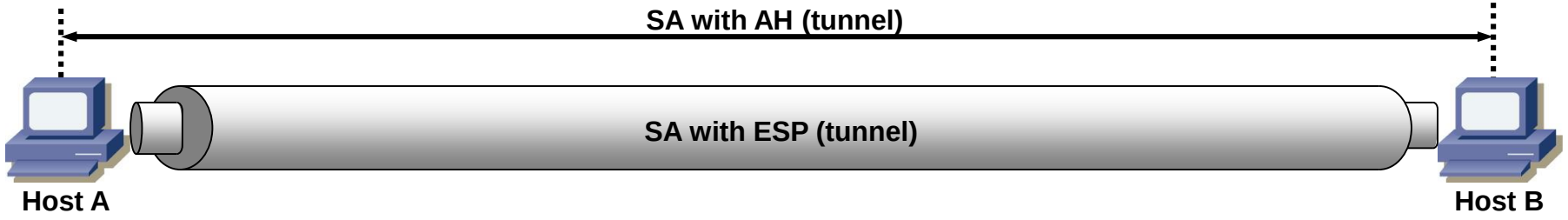
➔ This scenario does not use nesting; both SAs have the same endpoints (thus no tunnelling).



4. Bundled SA (iterated tunnelling, multilayer security):

➔This scenario uses end-to-end security with encryption and authentication. The original IP header is not visible (tunnel mode).

➔ The 2 nested tunnels have the same endpoints.



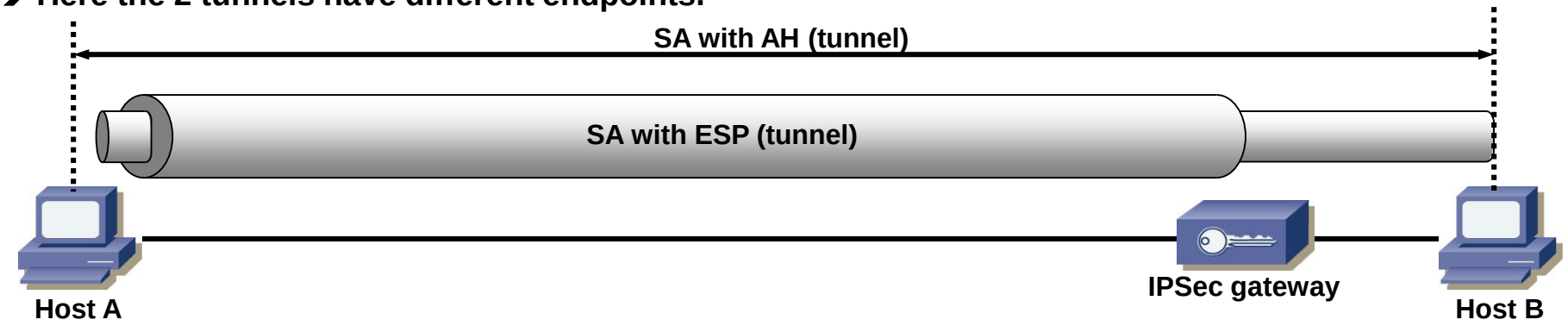
8. IPSec IP Security RFC2401 et.al. (13/13)

➔ Examples of typical IPSec architectures (3):

5. Bundled SA (iterated tunnelling):

➔ This scenario provides end-to-end security; the endpoint IP addresses are not visible.

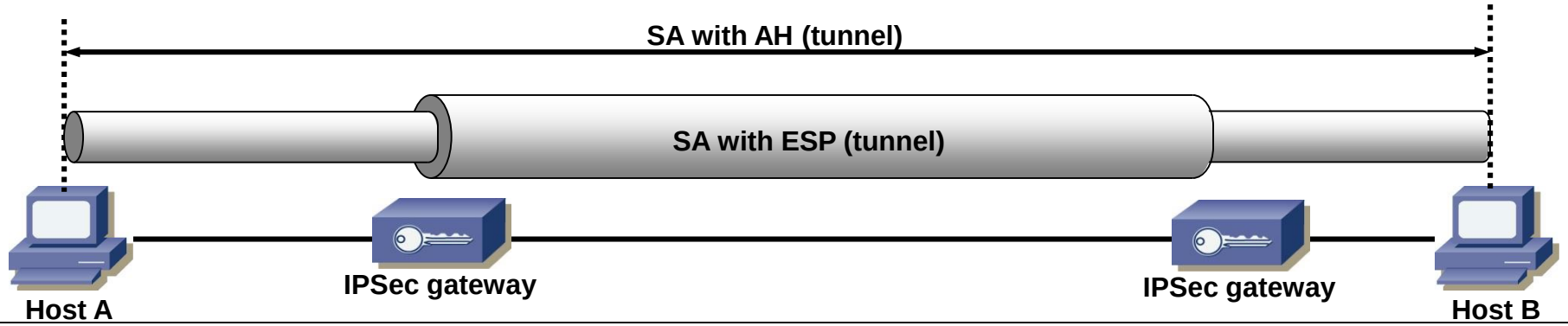
➔ Here the 2 tunnels have different endpoints.



6. Bundled SA (iterated tunnelling):

➔ The 2 nested tunnels have different endpoints.

➔ Secure connectivity (nested tunnel) in secure connection between 2 networks.

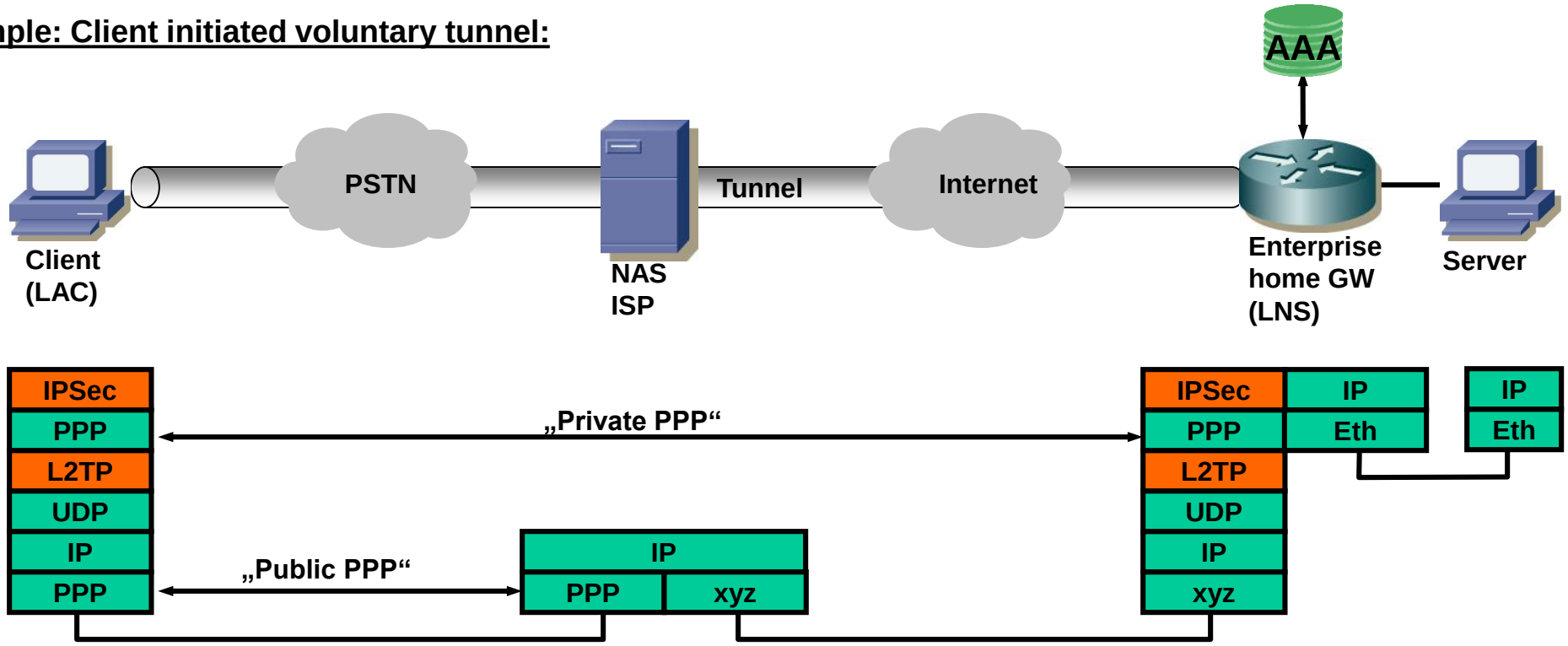


9. Combining different VPN protocols (1/6)

1. IPSec over L2TP:

➔ L2TP offers multiprotocol transport over IP and non-IP based transport networks (which IPSec doesn‘t).
➔ IPSec affords true security with forward header authentication etc. (when it comes to security, IPSec is the choice).
➔ NAPT in the transmit path does not pose a problem (L2TP uses UDP and is thus ‚NAPTable‘, IPSec is not ‚NAPTable‘).
➔ IPSec over L2TP does not provide user authentication but machine authentication instead.

Example: Client initiated voluntary tunnel:



9. Combining different VPN protocols (2/6)

2. L2TP over IPSec RFC3193:

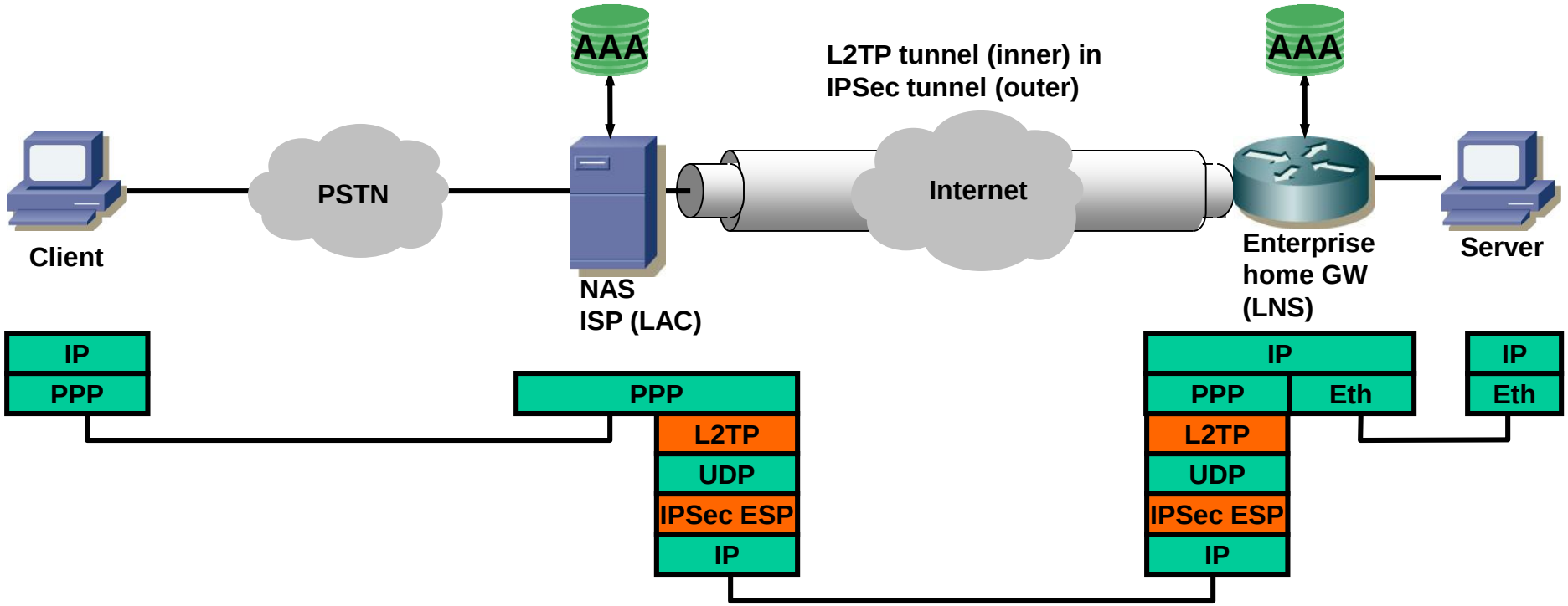
➔ A layer 2 tunnel (L2TP) is established on top of a secure layer 3 tunnel (IPSec).

➔ First the secure IPSec tunnel is established. Second the L2TP is established providing PPP and multiprotocol services.

➔ In order to get through NATs in the Internet IPSec in turn may be run over UDP (NAT-T, see below).

➔ IPSec provides machine to machine security (secure tunnel between machines). PPP is used for user authentication (login to server). In order to get PPP across the Internet an L2TP tunnel is established.

Example: NAS initiated compulsory tunnel:



9. Combining different VPN protocols (3/6)

➔ L2TP over IPSec versus IPSec over L2TP:

L2TP over IPSec:

- Provider based security
  LAC ➔➔ LNS.
- Fully protected L2TP tunnel construction.
- NAT is not possible on IPSec. Firewalls may cause problems.
- PPP password exchange is fully protected.
- Microsoft's way of constructing tunnels (Legacy PPP dial in is still in use and working with NT passwords).
- Client is not involved in IPSec (unless client and LAC are in same router / Win2k client)
- Better scaleability.

IPsec over L2TP

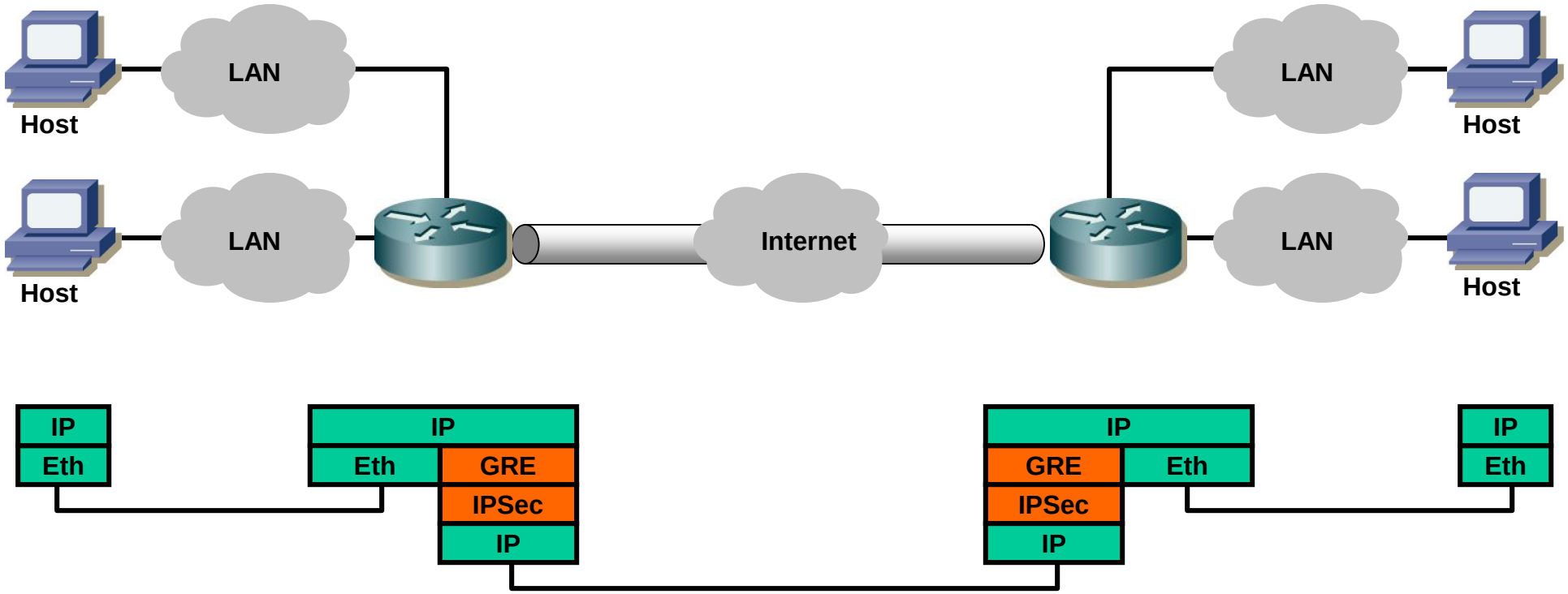
- Client based security
  Client ➔➔ LNS/Client.
- Unprotected L2TP tunnel construction.
- L2TP will go trough NAT and most firewalls.
- 'only' PPP like security on session construction.
- Cisco way of constructing VPN's.
- LAC is not involved in IPSec.

9. Combining different VPN protocols (4/6)

3. Multiprotocol over IPSec using GRE (Cisco):

➔ This combination is often used for site-to-site VPNs.

➔ The configuration is simplified since 1 GRE tunnel replaces N*M IPSec tunnels (from each network to each other network an IPSec tunnel is required).



9. Combining different VPN protocols (5/6)

4. IPSec over UDP RFC3947/RFC3948 (NAT-T = NAT-Traversal):

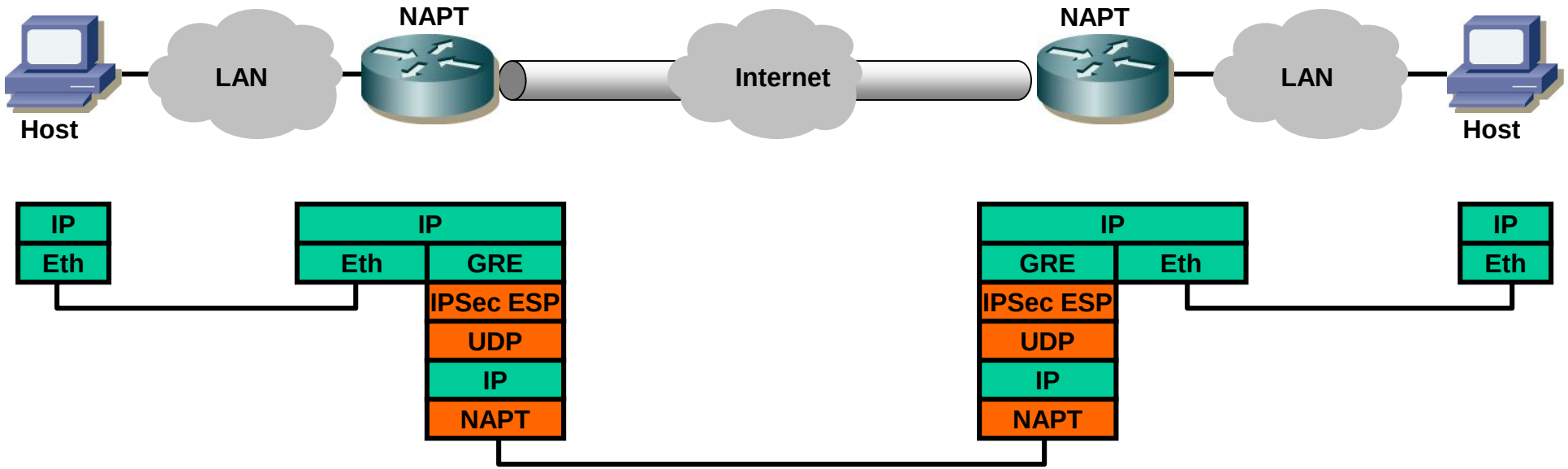
➔ IPSec AH does not pass through a NAPT / NPAT since AH authenticates immutable fields of the IP header including the source IP address which is manipulated by NAPT.

➔ IPSec ESP passes through NAT since ESP does not use IP header fields; but ESP will not pass through NAPT/NPAT since ESP uses (TCP, UDP) port numbers.

➔ Solution: IPSec AH + ESP over UDP RFC3948 (also dubbed „IPSec pass-through“ or „NAT traversal“).

➔ IPSec over UDP uses the same port number as IKE (IPSec Key Exchange protocol), 500, in order to only open 1 hole in the NAT.

➔ Even though „ESP over UDP RFC3948“ works with IPV6 it is seen as a temporary solution since IPV6 does away with the IP address scarcity problem and thus renders NAPT useless (we will see...).



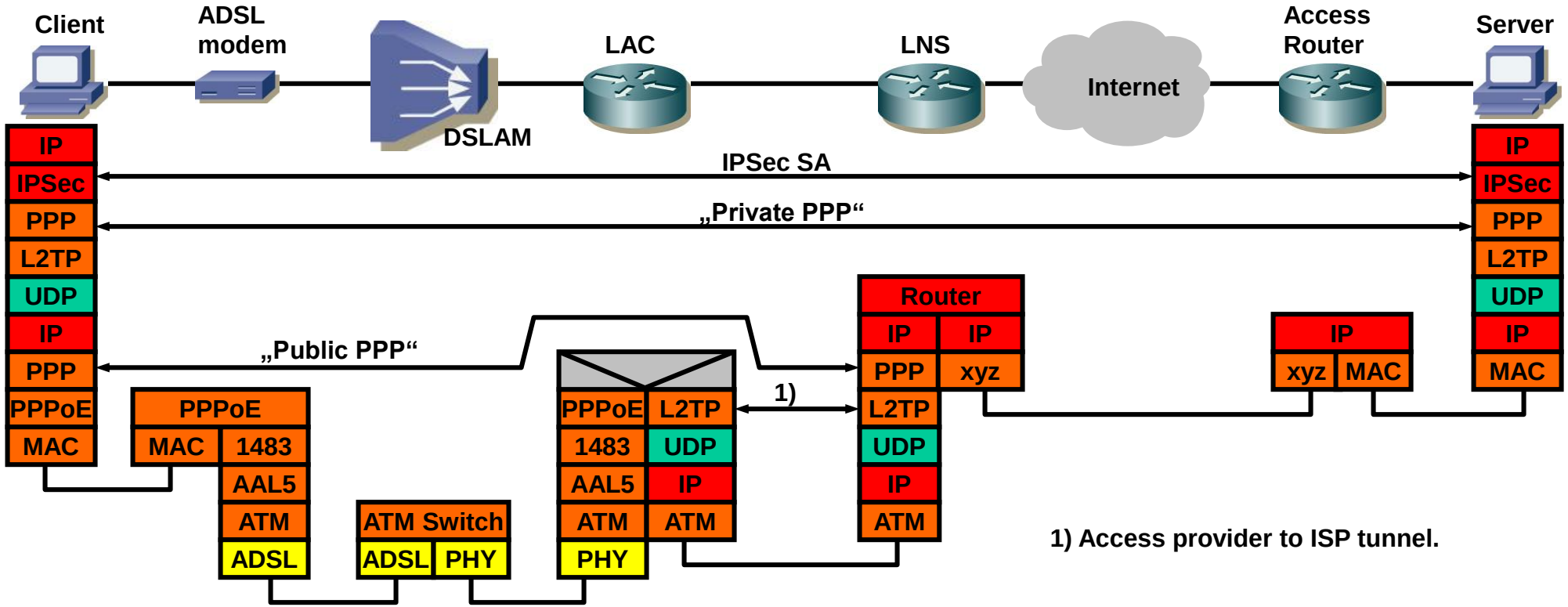
9. Combining different VPN protocols (6/6)

5. IPSec over L2TP over L2TP based access network:

➔ VPN and tunnelling protocols can be combined in a „Lego“-fashion with the following building blocks:

A. IP address assignment, authentication, link negotiation etc.: PPP.
B. Tunnelling of layer 2 protocols: L2TP with UDP for NAPT traversal.
C. Security (encryption, authentication, message integrity etc.): IPSec.
D. NAPT-traversal for IPSec: L2TP.
E. Transport of PPP over Ethernet, layer 2 access protocols: PPPoE over ATM (RFC1483, AAL5).

➔ N.B.: Protocol hierarchy (OSI layering) is reversed (e.g. layer 2 protocol over layer 3 protocol).



10. IPSec Key Management (1/3)

➔ IPSec can be used with static pre-shared keys (statically configured keys on IPSec endpoints). It is however more secure to occasionally replace keys with newer ones. This means that a dynamic key exchange protocol between IPSec endpoints is needed.

➔ Important key exchange protocols are:

1. ISAKMP RFC2408 Internet Security Association and Key Management Protocol:
   - ➔ General framework for key exchange and management (N.B.: ISAKMP does not itself define a particular key exchange procedure).
2. Oakley: Key management according to ISAKMP:
   - ➔ Key generation.
   - ➔ Identity protection.
   - ➔ Authentication.
3. SKEME: Secure Key Exchange Mechanism:
   - ➔ Anonymity.
   - ➔ Non-repudiation.
   - ➔ Quick key refreshment.
4. IKE Internet Key Exchange RFC2409: The key management protocol used within IPSec:
   - ➔ IKE is a combination of ISAKMP, Oakley and SKEME.
   - ➔ IKE is used for periodic key exchange.
   - ➔ IKE is a key management protocol.
   - ➔ IKE is also used for IPSec protocol negotiation (AH or ESP).

10. IPSec Key Management (2/3)

➔ **IKE Internet Key Exchange RFC2409 (1):**

IKE has 2 phases:

Phase 1:

Creation of secure ISAKMP SA (which is bidirectional) for IKE protection itself:

a. IKE SA negotiation (algorithms for secure IKE SA).

b. Key exchange for IKE SA.

c. Peer authentication (using certificates, pre-shared keys or public key encryption).

Phase 1 is executed only once in the lifetime of an IKE/IPSec association.

Phase 2:

Phase 2 starts only after phase 1 is finished.

Phase 2 comprises the negotiation of IPSec protection (keys etc.) using the Diffie-Hellman algorithm thus affording PFI (*Perfect Forward Security*) which means that new keys are in no way dependent on old keys; this means that even if an attacker can break a key he would not be able to break the next key since it is not dependant on the old key.

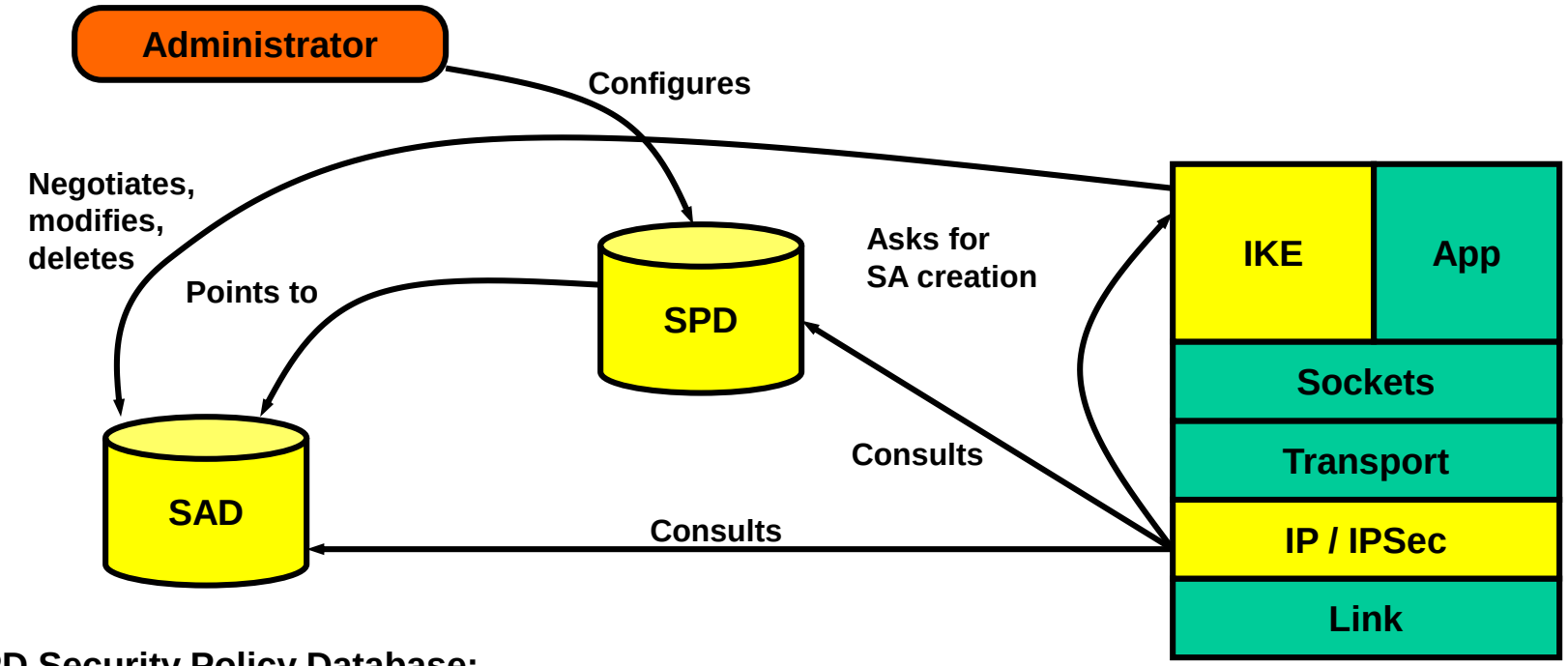
During an IPSec session phase 2 (re-negotiation of session keys) is repeated more often than phase 1 (re-negotiation of IKE keys).

➔ **IPSec key lifetime < IKE key lifetime.**

10. IPSec Key Management (3/3)

➔ IKE Internet Key Exchange RFC2409 (2):

Components and architecture:



SPD Security Policy Database:

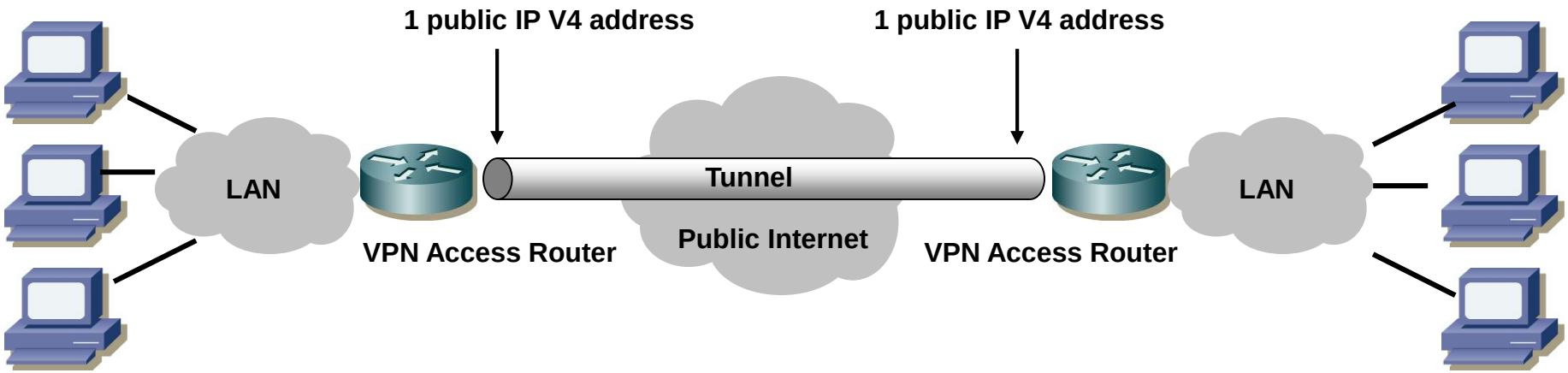
The SPD contains general policies (e.g. let user X pass, user Z no IPSec).
The SPD entries are static (set up administratively).
The SPD entries are similar to firewalls access control lists ACL.

SAD Security Association Database:

The SAD contains SA data (outer header IP, IPSec proto, SN counter etc.).
Its entries are dynamic for active connections (come and go with SAs).

11. IPV4 addresses: how many are there?

➔ In principle 2^32=4‘294‘967‘295 (at least for IPv4), but:



➔ This setup creates a „network in the network“ where 16’777’216 + 1’048’576 + 65’536 = 17‘891‘328 hosts can communicate with each other. The VPN (tunnel) creates some kind of application context using private IP addresses. Note that the VPN hosts can still communicate with hosts in the Internet. The tunnels allow to pass any protocol through VPN access routers that run NAPT and other firewall functions.