HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

4 Virtual Private Networks

Prof. Dr. Andreas Steffen

Institute for Internet Technologies and Applications (ITA)

Layer 2 versus Layer 3 versus Layer 4

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

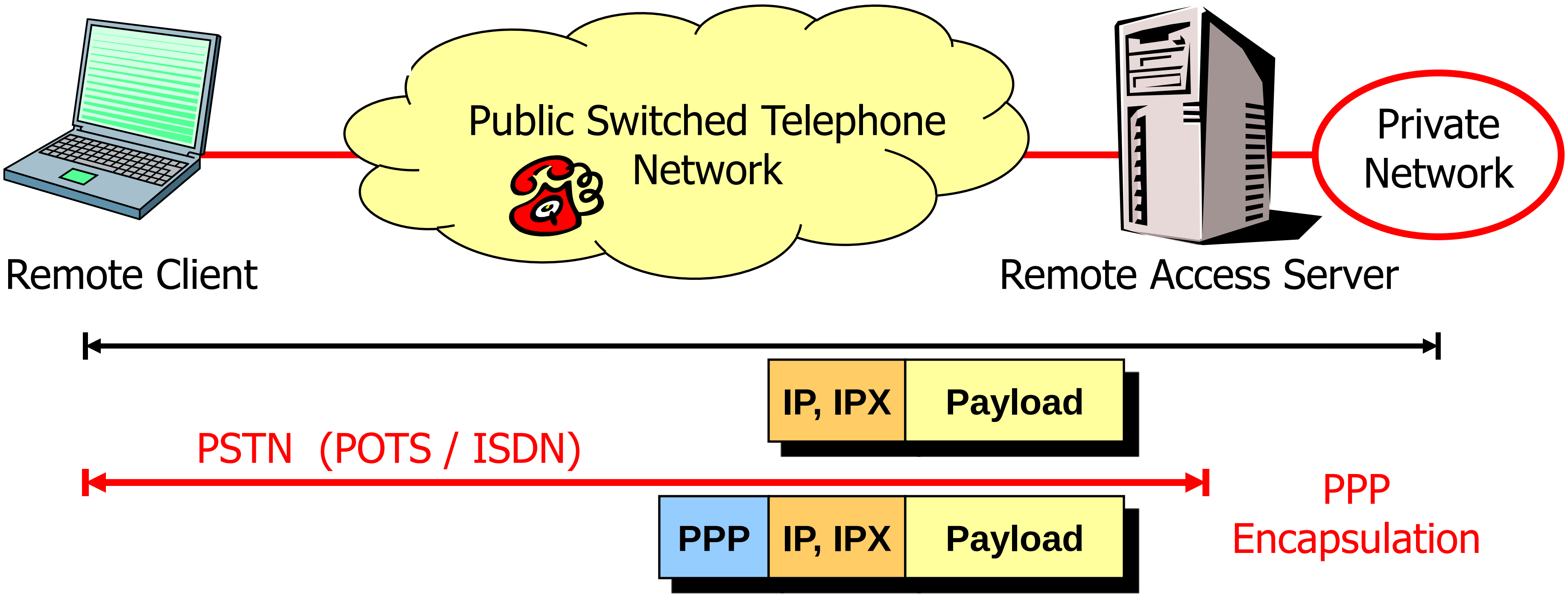
Communication layers	Security protocols
Application layer	ssh, S/MIME, PGP, Kerberos, WSS
Transport layer	TLS, [SSL]
Network layer	IPsec
Data Link layer	[PPTP, L2TP], IEEE 802.1X, IEEE 802.1AE, IEEE 802.11i (WPA2)
Physical layer	Quantum Communications

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

4.1 Point-to-Point Protocol (PPP)

PPP–based Remote Access using Dial–In

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz



- Authentication using PAP (password), CHAP (challenge/response), or the Extensible Authentication Protocol (EAP) supporting e.g. token cards
- Optional PPP packet encryption (ECP) using preshared secrets
- Individual PPP packets are not authenticated
- The Link Control Protocol (LCP), as well as EAP and ECP are not protected !!

The PPP Encryption Control Protocol (ECP)

0x8053	Code	ID	Length	ECP Options (algorithm, IV)

- The Encryption Control Protocol (ECP, RFC 1968) uses the same packet exchange mechanism as the Link Control Protocol (LCP, RFC 1661).
- ECP packets may not be exchanged until PPP has reached the Network-Layer Protocol phase and should wait for an optional Authentication phase.
- Exactly one ECP packet is encapsulated in the PPP Information field, where the PPP Protocol field indicates type `0x8053`.

0x0053	Seq. Nr	Ciphertext

- An encrypted packet is encapsulated in the PPP Information field, where the PPP Protocol field indicates type `0x0053` (Encrypted datagram).
- Compression may also be negotiated using the Compression Control Protocol (CCP, RFC 1962).
- ECP implementations should use the PPP Triple-DES Encryption Protocol (3DESE, RFC 2420). DES-EDE3-CBC with a 168 bit key is used.

The PPP Extensible Authentication Protocol (EAP)

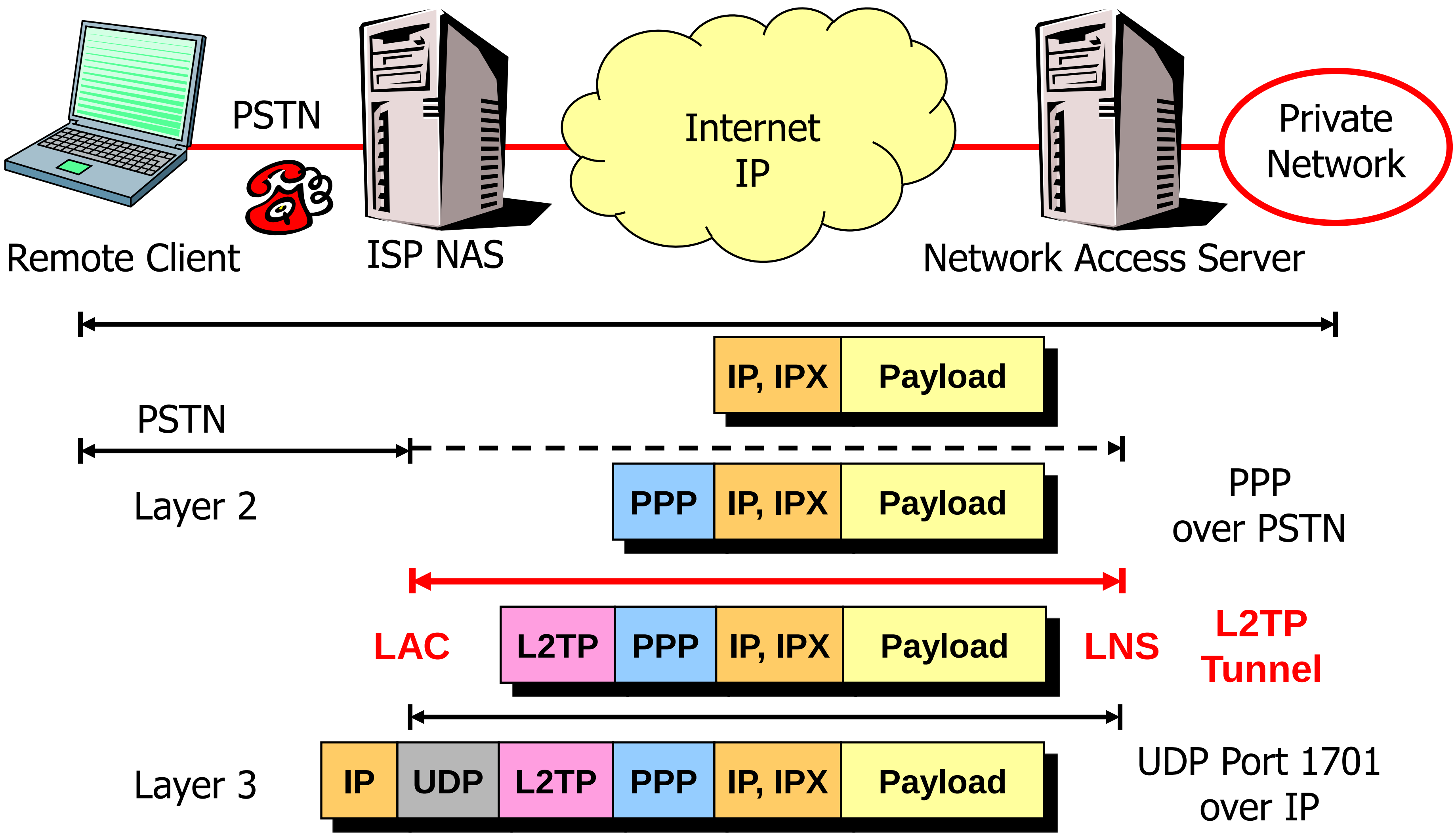
0xC227	Code	ID	Length	Type	Data

- Some of the authentication types supported by EAP (RFC 2284):
  - 1 Identity
  - 4 MD5-Challenge
  - 5 One-Time Password (OTP, RFC 2289)
  - 6 Generic Token Card
  - 9 RSA Public Key Authentication
  - 13 EAP-TLS (RFC 2716, supported by Windows XP)
  - 15 RSA Security SecurID EAP
  - 17 EAP-Cisco Wireless
  - 18 Nokia IP smart card authentication
  - 23 UMTS Authentication and Key Argreement
  - 24 EAP-3Com Wireless
  - 25 PEAP (Protected EAP, supported by Windows XP)
  - 29 EAP-MSCHAP-V2 (supported by Windows XP)
  - 35 EAP-Actiontec Wireless
  - 36 Cogent Systems Biometrics Authentication EAP

4.2 Layer 2/3/4 VPNs

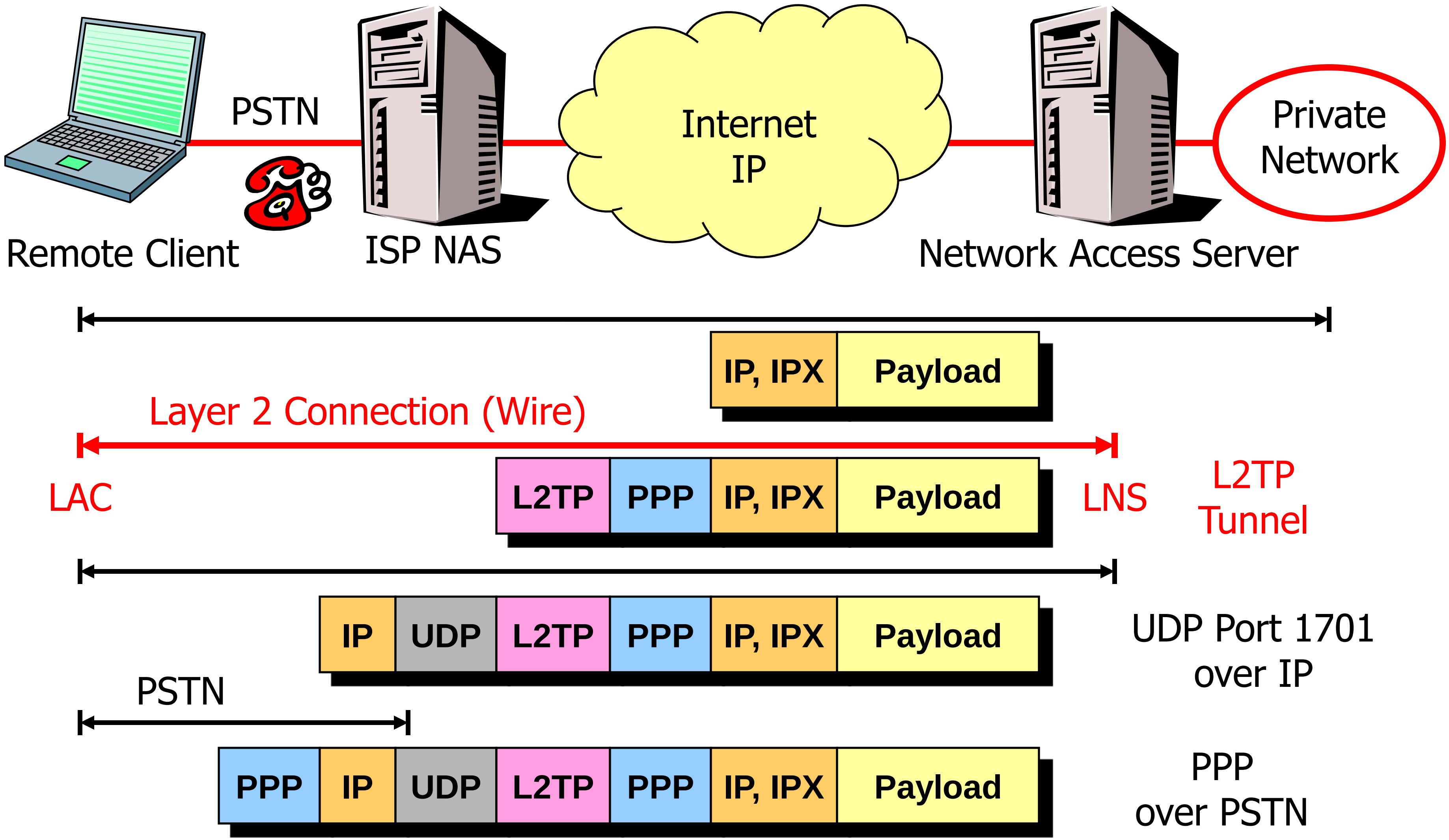
Layer 2 Tunneling Protocol (L2TP)
Compulsory Mode

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

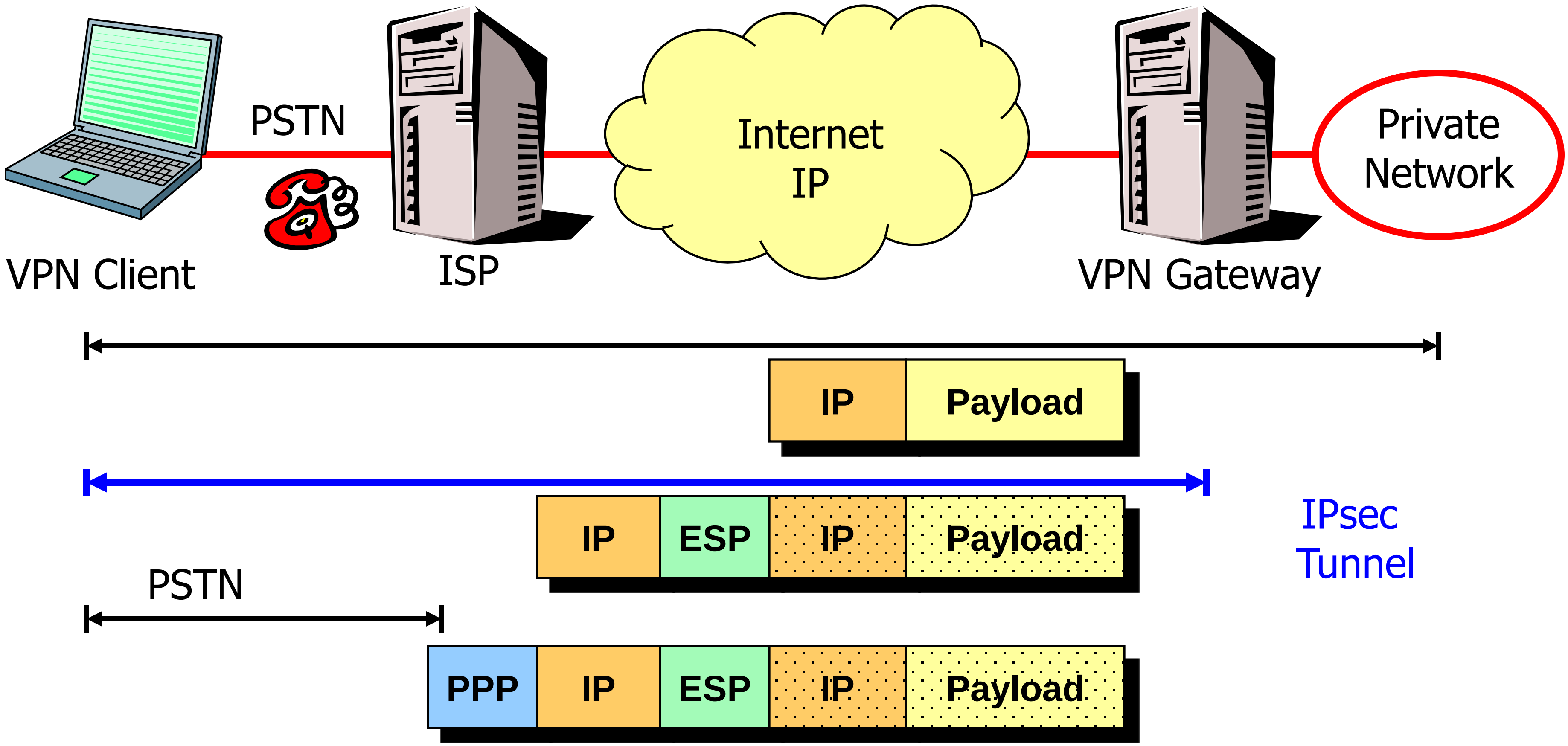


Layer 2 Tunneling Protocol (L2TP)
Voluntary Mode

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

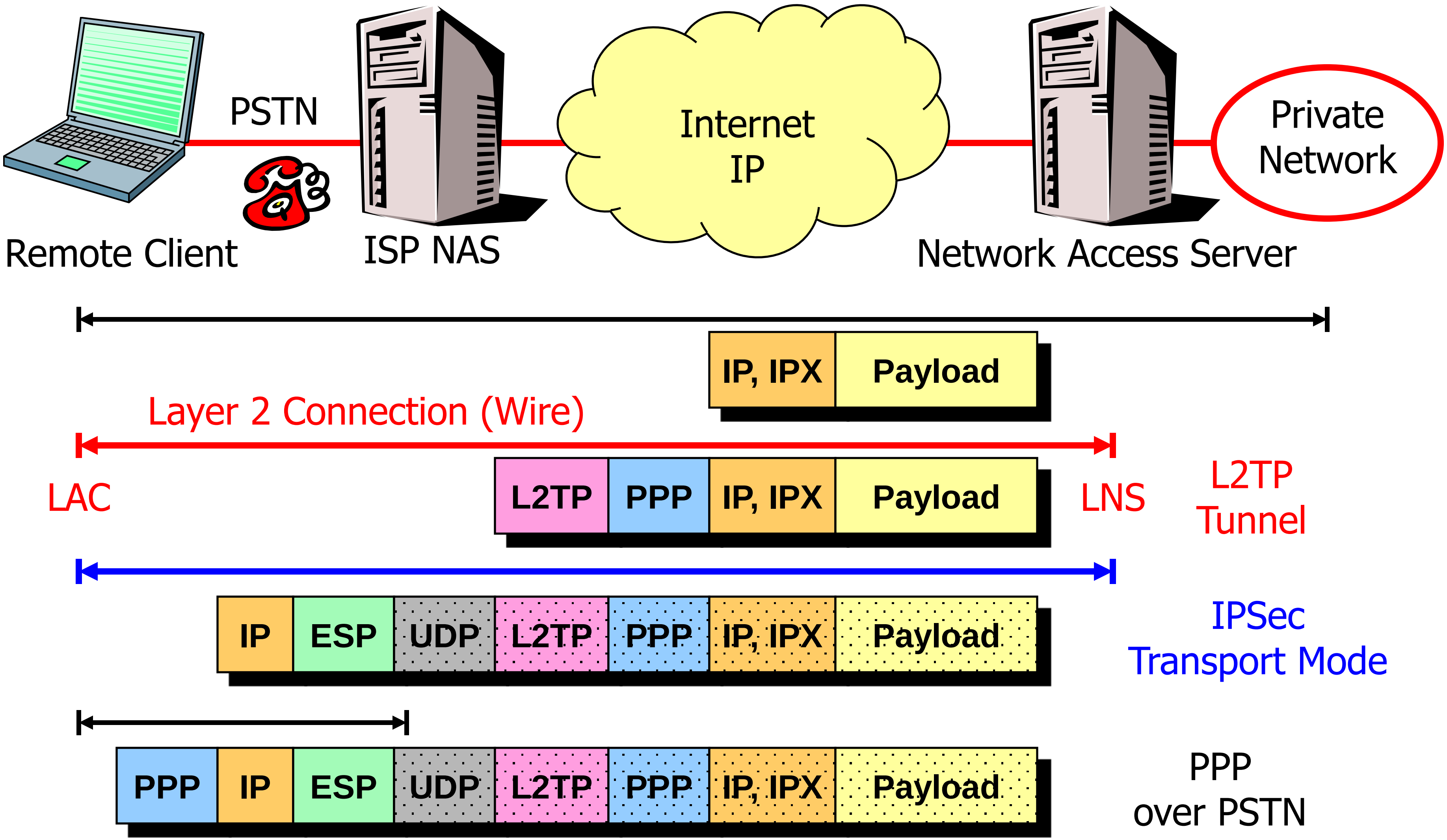


Layer 3 Tunnel based on IPSec

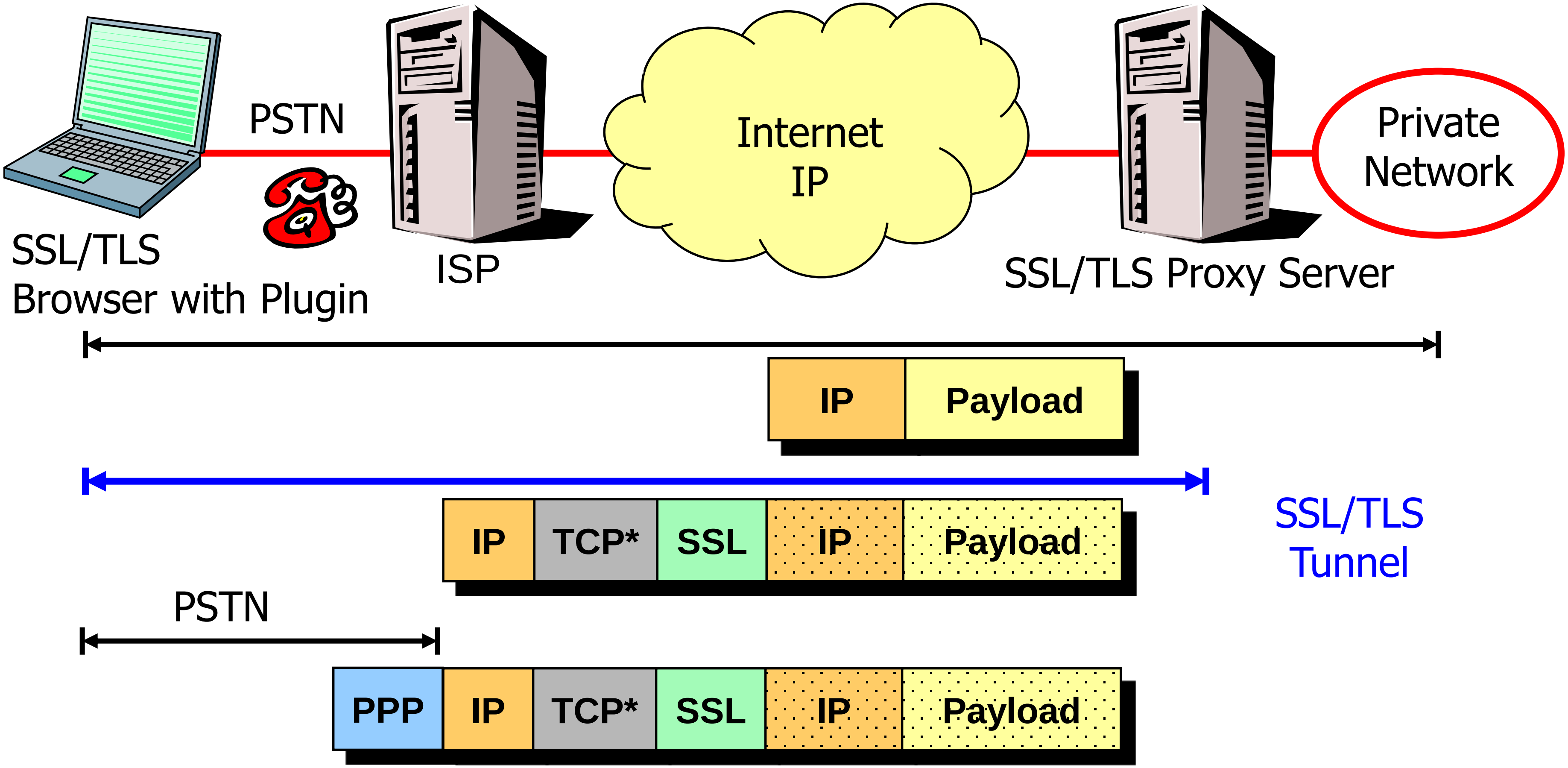


L2TP over IPsec (RFC 3193) – Voluntary Mode

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz



Layer 4 Tunnel based on SSL/TLS



*OpenVPN uses SSL over UDP

Layer 2/3/4 VPNs – Pros and Cons

- Layer 2 – L2TP
  - ↗ Same login procedure as PPP (preshared secrets, RADIUS, etc.)
  - ↗ Same auxiliary information as with PPP (virtual IP, DNS/WINS servers)
  - ↘ No strong security without IPsec, LCP can be cheated into establishing no encryption. Non-authenticated L2TP packets prone to replay attacks.
- Layer 3 – IPSec
  - ↗ Cryptographically strong encryption and authentication of VPN tunnel
  - ↗ Can negotiate and enforce complex VPN access control policies
  - ↗ XAUTH and IKEv2-EAP authentication offer PPP-like features
  - ↘ Does not allow the tunneling of non-IP protocols (IPX, etc.)
  - ↘ Complex connection setup, PKI management overhead
- Layer 4 - TLS
  - ↗ Clientless and simple: Internet Browser plus Java Applets or Plugin.
  - ↗ Cryptographically strong encryption and authentication of VPN tunnel
  - ↘ Access to certain applications need special plugin (still clientless?)

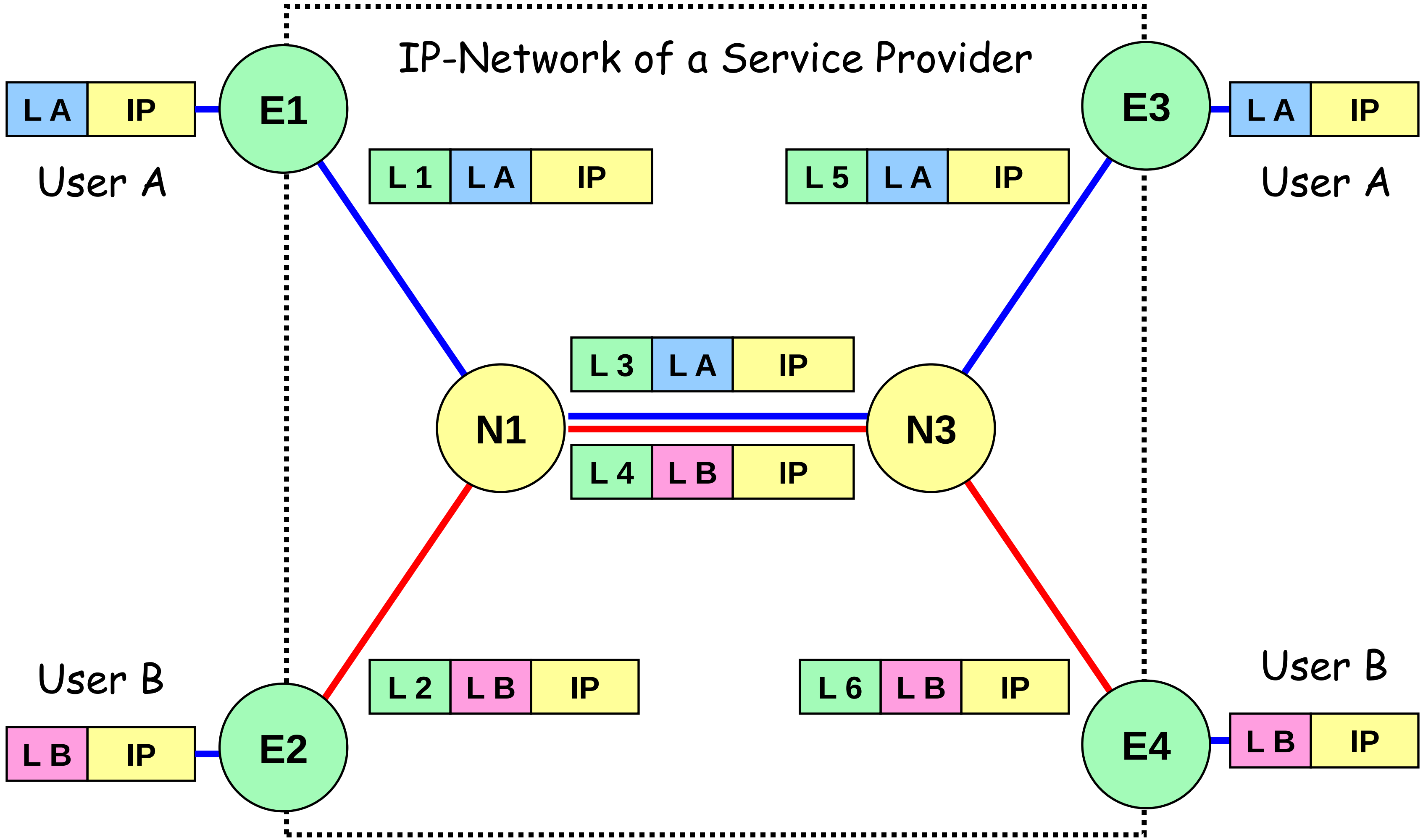
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

4.3 Multi-Protocol Label Switching (MPLS)

MPLS based Virtual Private Networks

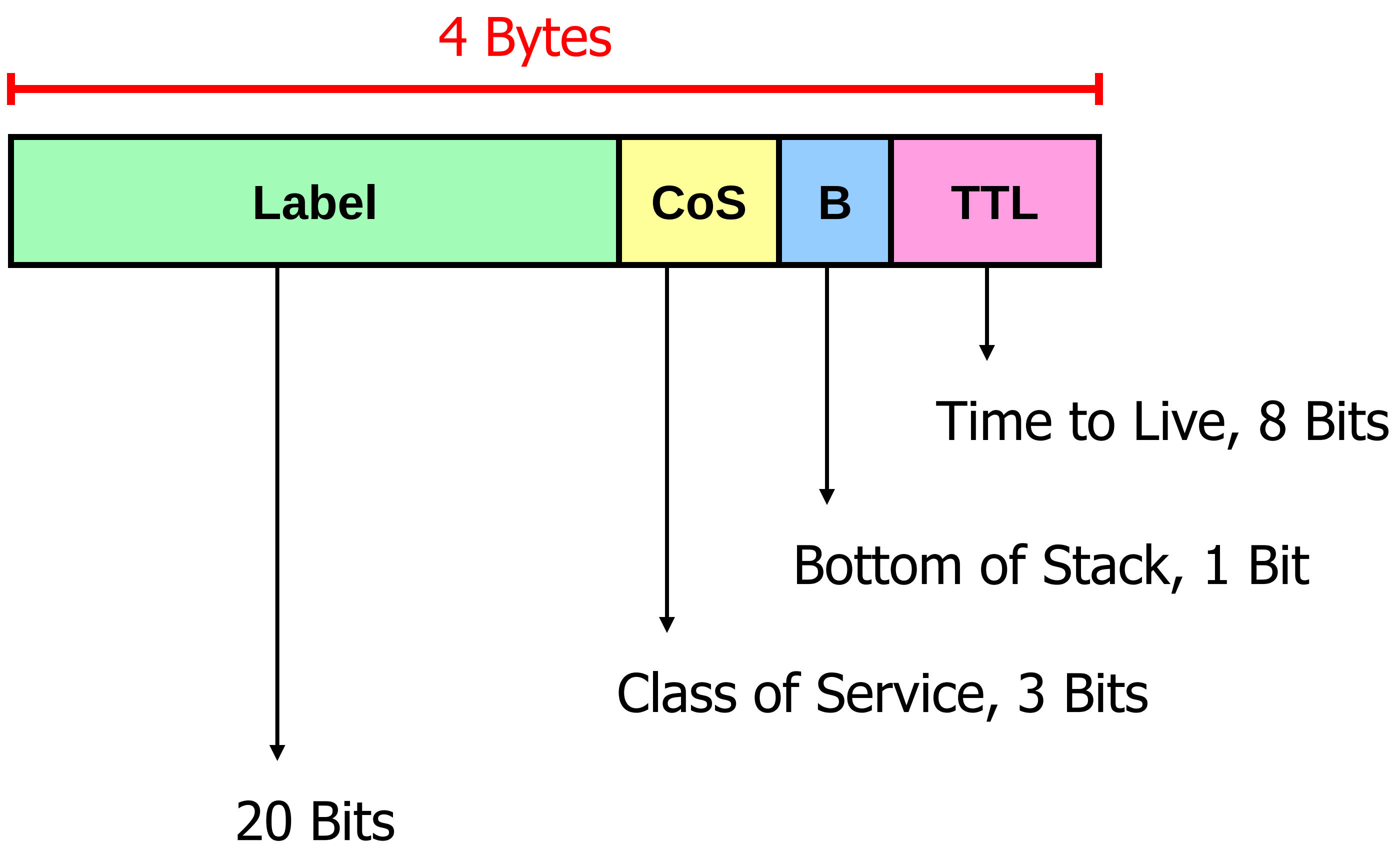
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz



MPLS Layer 2 Shim Header (RFC 3032)

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz



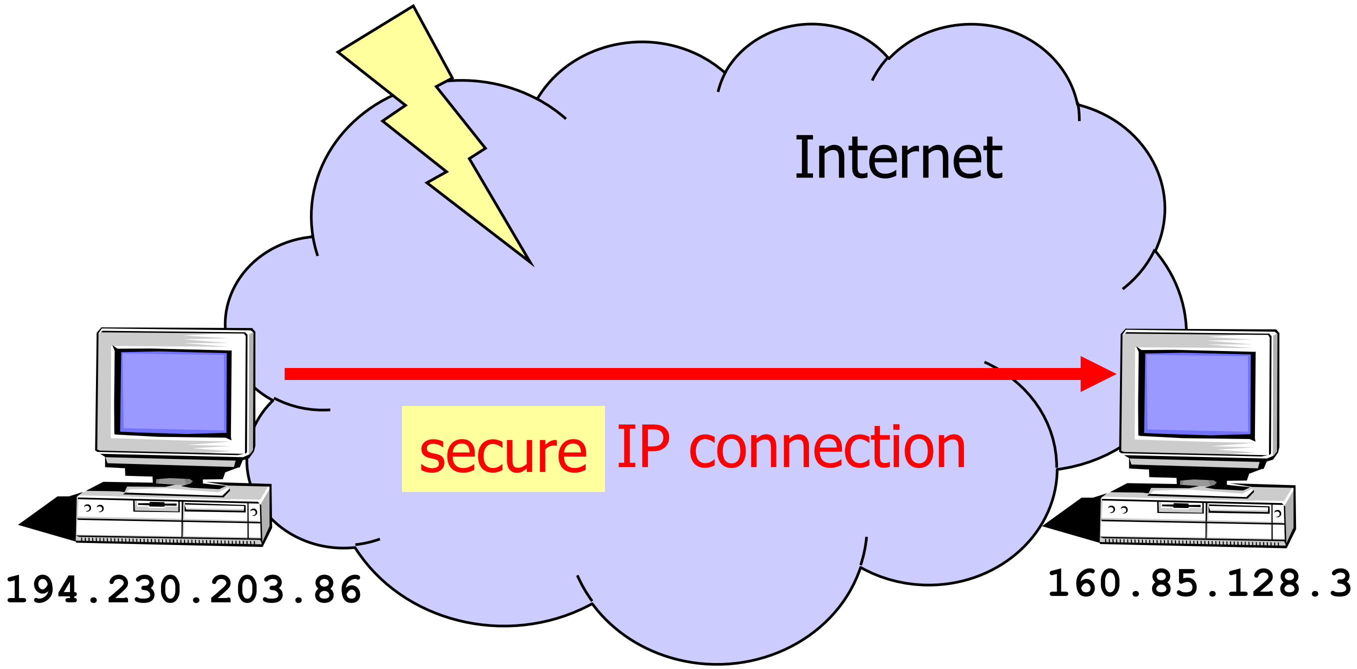
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

4.4 IPsec Transport Mode

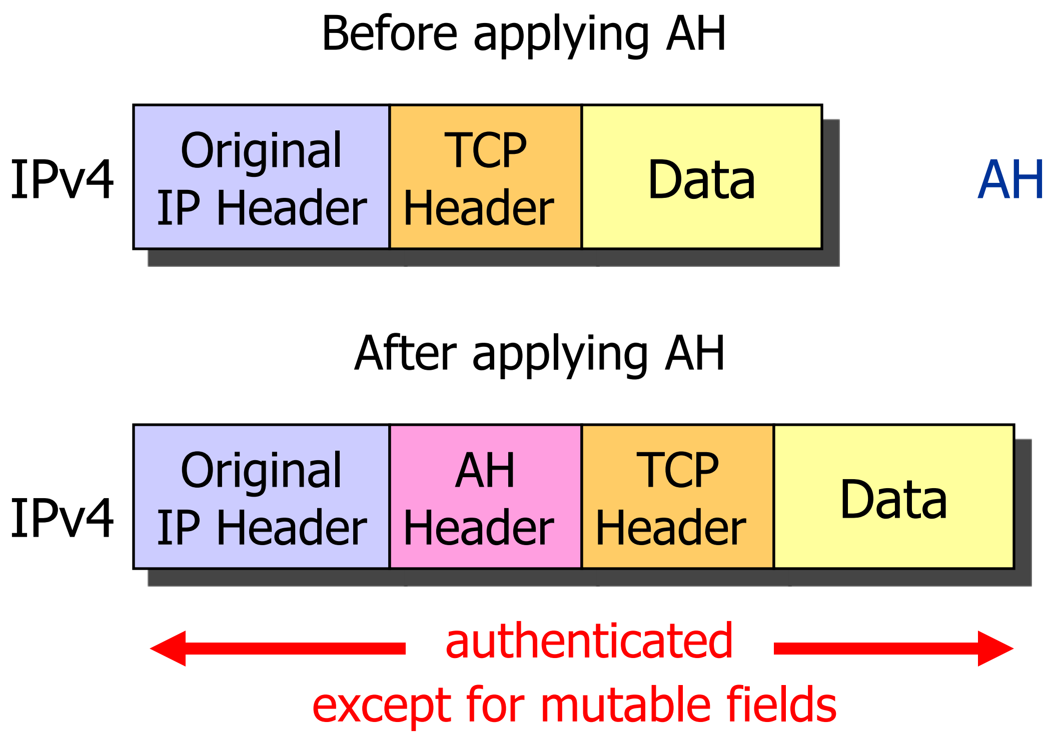
IPsec – Transport Mode

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz



- IP datagrams should be authenticated
- IP datagrams should be encrypted and authenticated

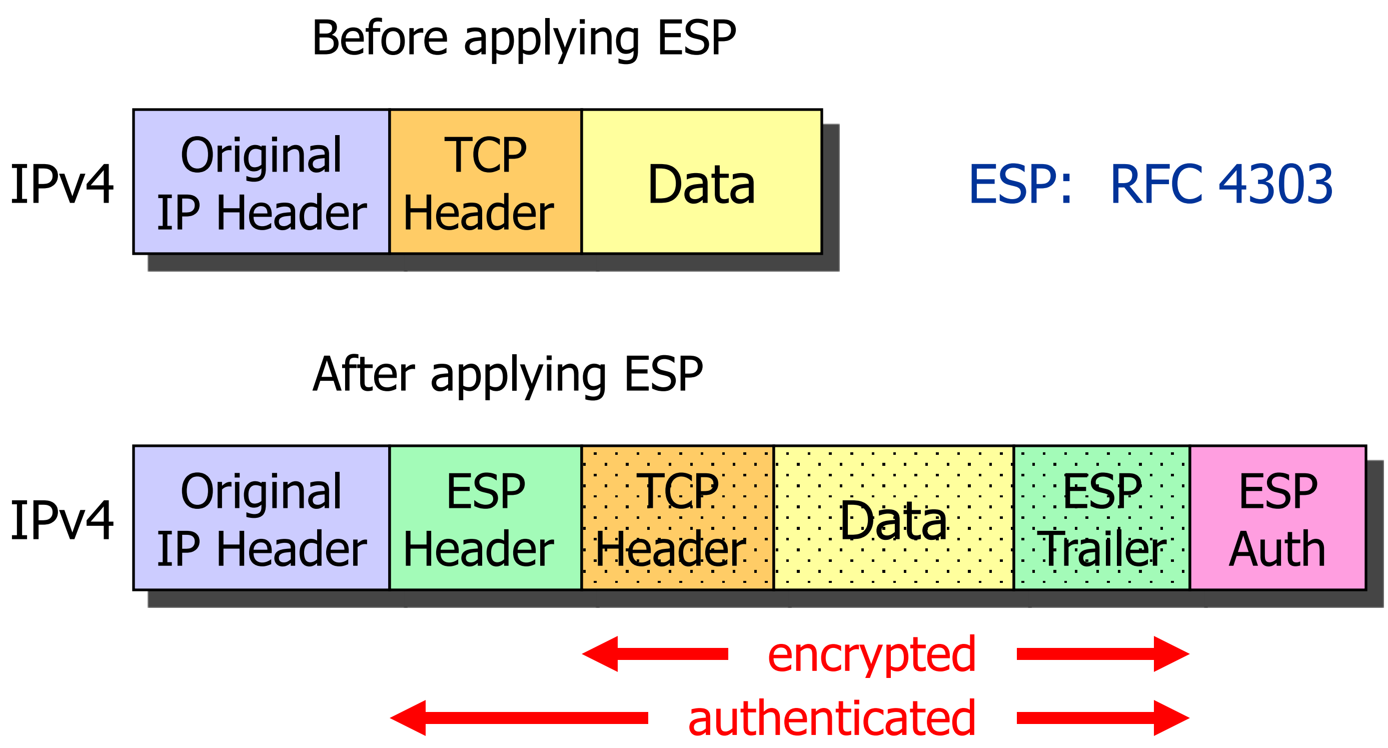
IPsec – Transport Mode
IP Authentication Header (AH)



AH: RFC 4302

- IP protocol number for AH: 51
- Mutable fields: Type of Service (TOS), Fragment Offset, Flags, Time to Live (TTL), IP header checksum

IPsec – Transport Mode
IP Encapsulating Security Payload (ESP)



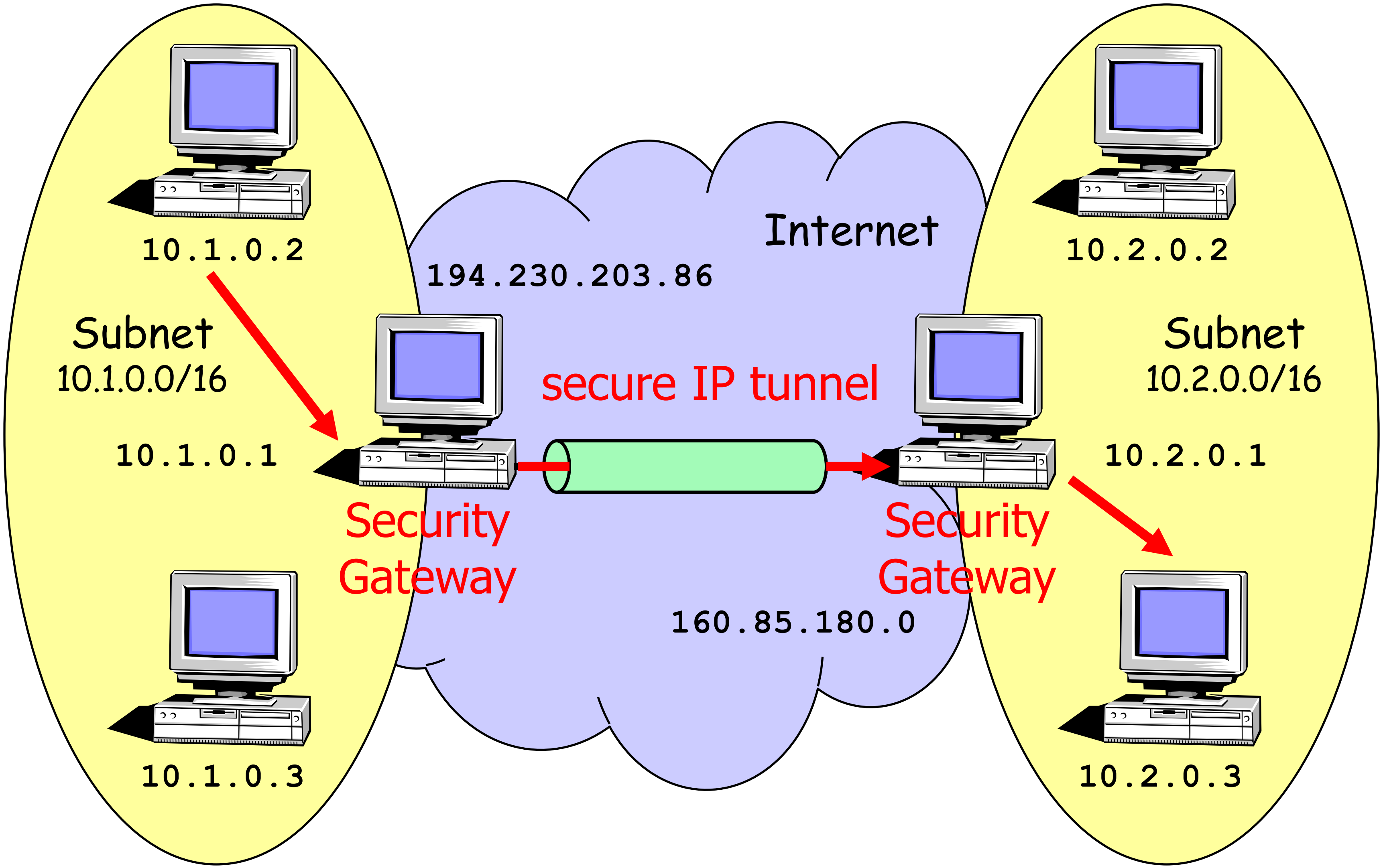
ESP: RFC 4303

- IP protocol number for ESP: 50
- ESP authentication is optional
- With ESP authentication the IP header is not protected.

4.5 IPsec Tunnel Mode

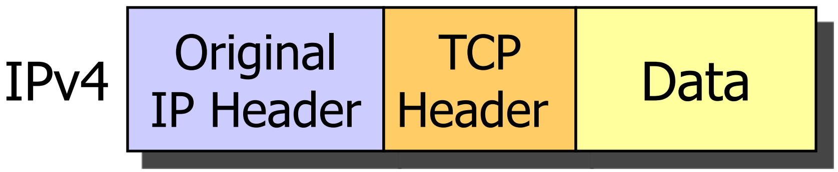
IPsec – Tunnel Mode
Virtual Private Network (VPN)

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz



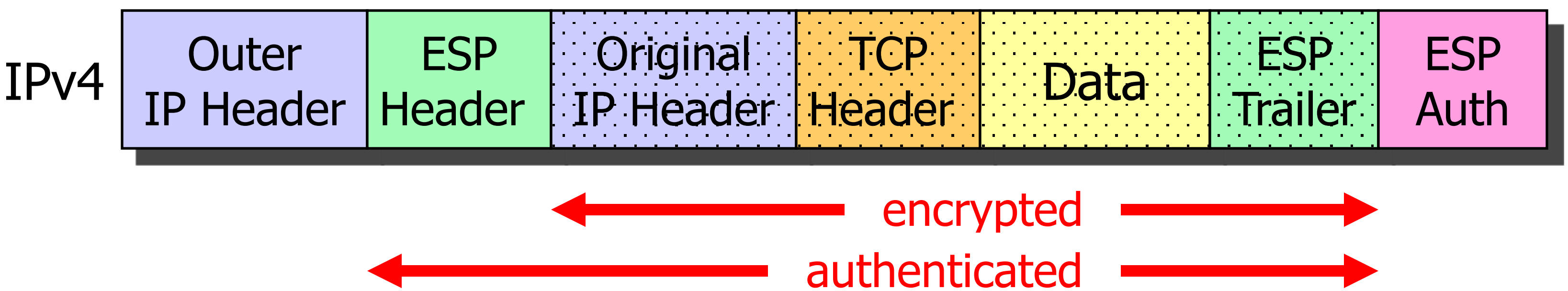
IPsec Tunnel Mode using ESP

Before applying ESP



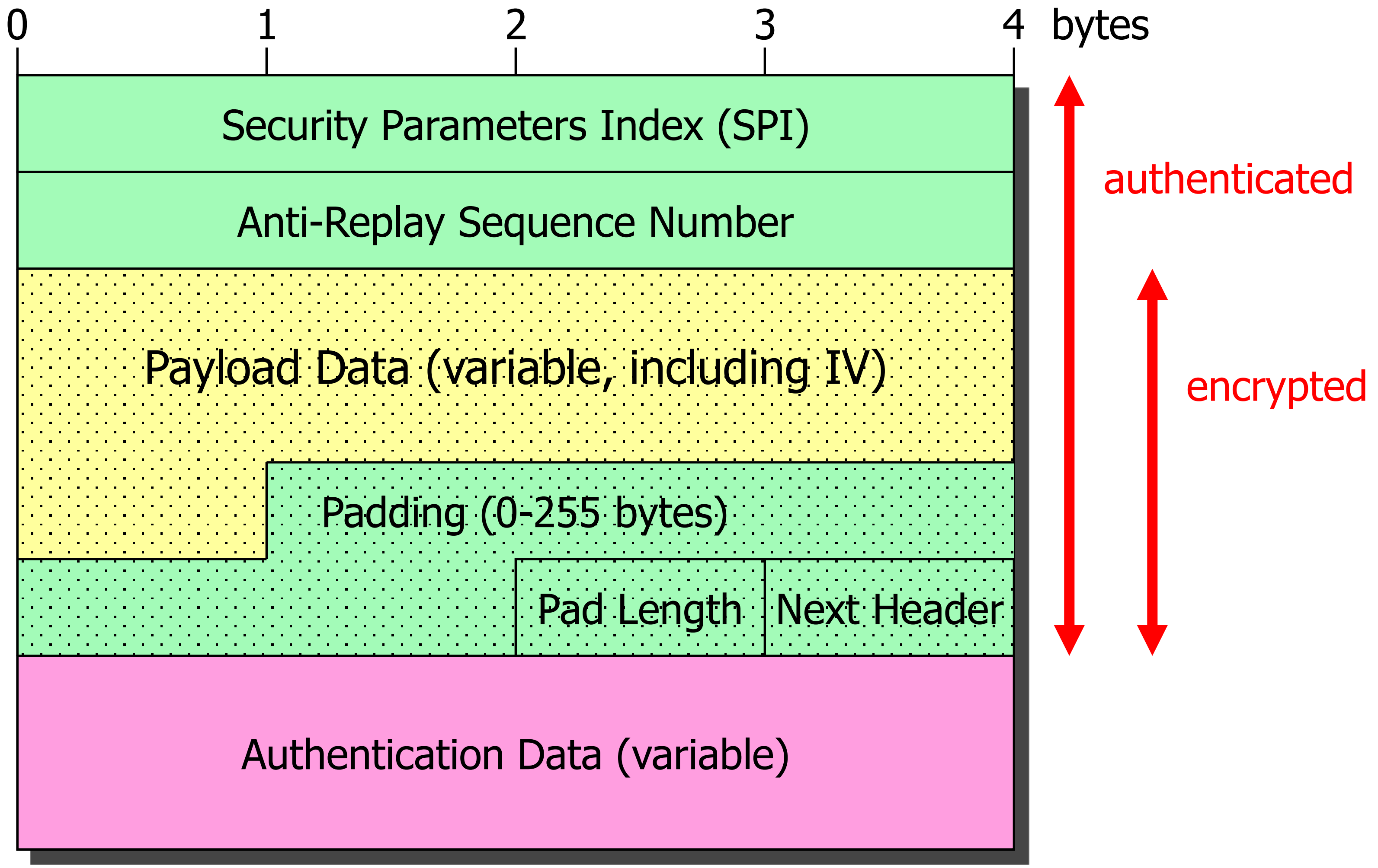
Encapsulating Security Payload (ESP): RFC 4303

After applying ESP



- IP protocol number for ESP: 50
- ESP authentication is optional but often used in place of AH
- Original IP Header is encrypted and therefore hidden

ESP Header (Initial Header / Payload / Trailer)



IPsec Tunnel Mode CBC Packet Overhead

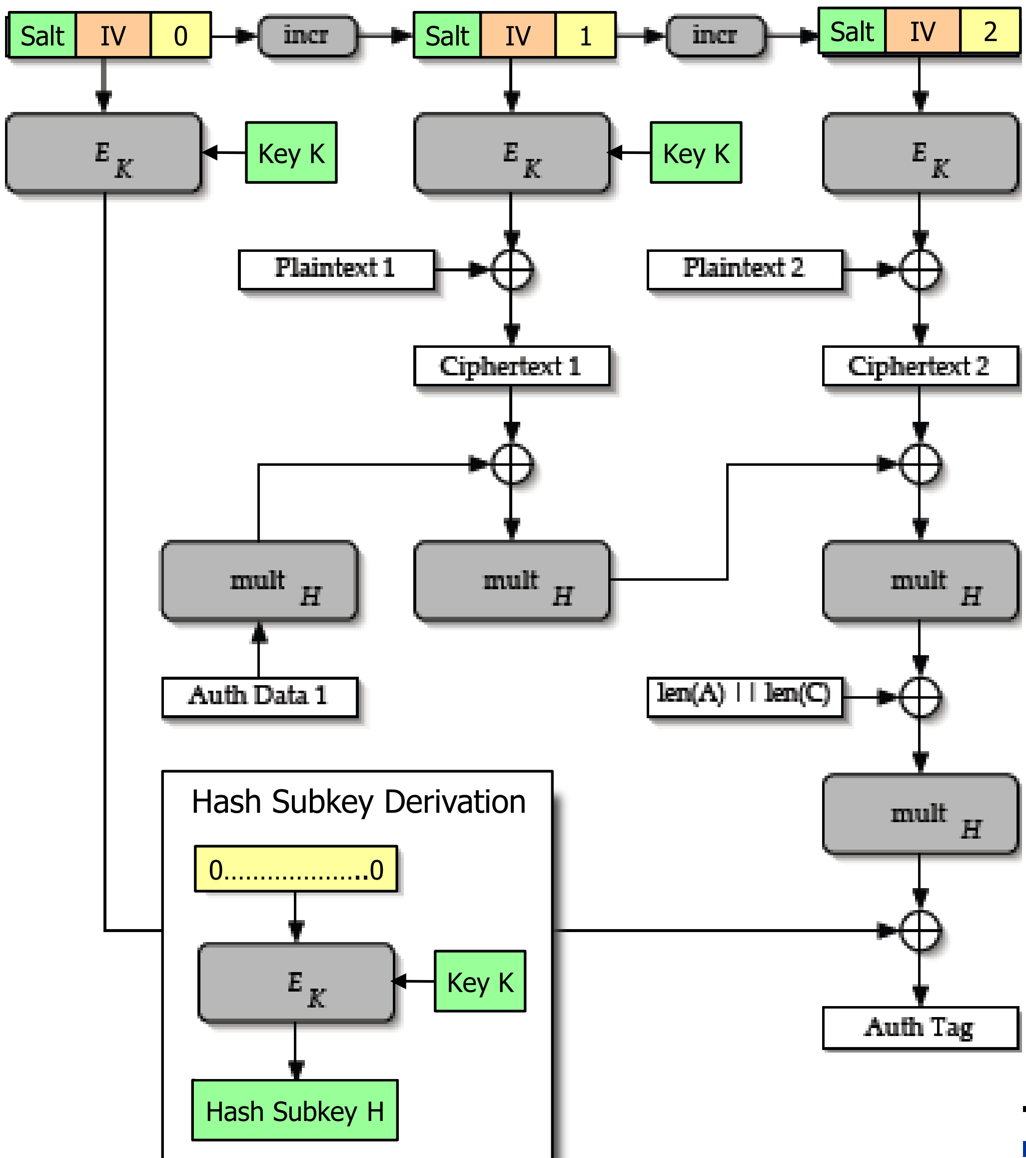
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

Outer IP Header	20	20	20	20	20	20	20	20	20	20	20
SPI / Seq. Number	8	8	8	8	8	8	8	8	8	8	8
3DES_CBC IV	8	8	8	8	8	8					
AES_CBC IV	16						16	16	16	16	16
3DES_CBC max Pad	7	7	7	7	7	7					
AES_CBC max Pad	15						15	15	15	15	15
Pad Len / Next Header	2	2	2	2	2	2	2	2	2	2	2
HMAC_SHA1_96	12	12					12				
AES_XCBC_96	12		12					12			
HMAC_SHA2_256_128	16			16					16		
HMAC_SHA2_384_192	24				24					24	
HMAC_SHA2_512_256	32					32					32
Best Case Overhead		50	50	54	62	70	58	58	62	70	78
Worst Case Overhead		57	57	61	69	77	73	73	77	85	93

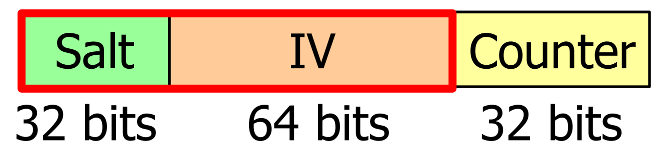
Bytes

Authenticated Encryption with Associated Data (AEAD)

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz



- AEAD is based on special block cipher modes:
- Block size: 128 bits
- Key size: 128/256 bits
- Tag size : 128/96/64 bits
- Nonce size: 96 bits



- Recommended AEAD Modes:
  AES-Galois/Counter Mode
  AES-GMAC (auth. only)
- Alternative AEAD Modes:
  AES-CCM
  CAMELLIA-GCM
  CAMELLIA-CCM

IPsec Tunnel Mode AEAD Packet Overhead

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

Outer IP Header	20	20	20	20
SPI / Seq. Number	8	8	8	8
AES_GCM IV	8	8	8	8
AES_CNT max Pad	3	3	3	3
Pad Len / Next Header	2	2	2	2
AES_GCM_64 Tag	8	8		
AES_GCM_96 Tag	12		12	
AES_GCM_128 Tag	16			16
Best Case Overhead		46	50	54
Worst Case Overhead		49	53	57

Bytes

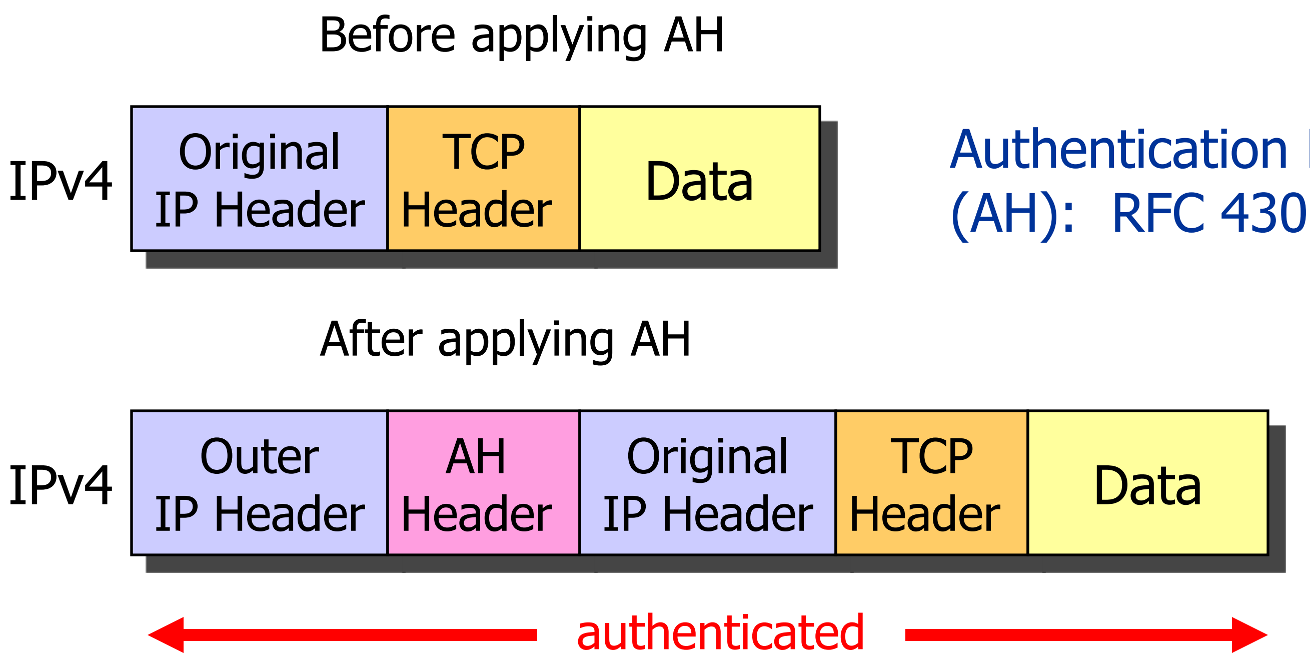
Additional Authenticated Data:

0	1	2	3
Security Parameter Index			
Sequence Number			

or

0	1	2	3
Security Parameter Index			
Extended Sequence Number			

IPsec Tunnel Mode using AH



Authentication Header (AH): RFC 4302

- IP protocol number for AH: 51
- Mutable fields: Type of Service (TOS), Fragment Offset, Flags, Time to Live (TTL), IP header checksum
- ESP can be encapsulated in AH