

# 9 Virtual Private Networks

---

Prof. Dr. Andreas Steffen

Institute for Internet Technologies and Applications (ITA)

---

■ Andreas Steffen, 23.01.2006, 9-VPN.ppt 1

## 9 Virtual Private Networks

### 9.1 Point-to-Point Protocol (PPP)

- PPP-based remote access using dial-in
- PPP encryption control protocol (ECP)
- PPP extensible authentication protocol (EAP)

### 9.2 Layer 2/3/4 VPNs

- Layer 2 tunneling protocol (L2TP) – compulsory mode / voluntary mode
- Layer 3 tunnel based on IPsec
- L2TP over IPsec
- Layer 4 tunnel based on SSL/TLS
- Layer 2/3/4 VPNs – Pros and cons

### 9.3 Multi-Protocol Label Switching

- MPLS-based virtual private networks, MPLS layer 2 shim header

### 9.4 IPsec Transport Mode

- IPsec authentication header (AH)
- IPsec encapsulating security payload (ESP)

### 9.5 IPsec Tunnel Mode

- IPsec-based virtual private networks
- IPsec encapsulating security payload (ESP)
- IPsec authentication header (AH)



# 9.1 Point-to-Point Protocol (PPP)

---







## 9.2 Layer 2/3/4 VPNs

---









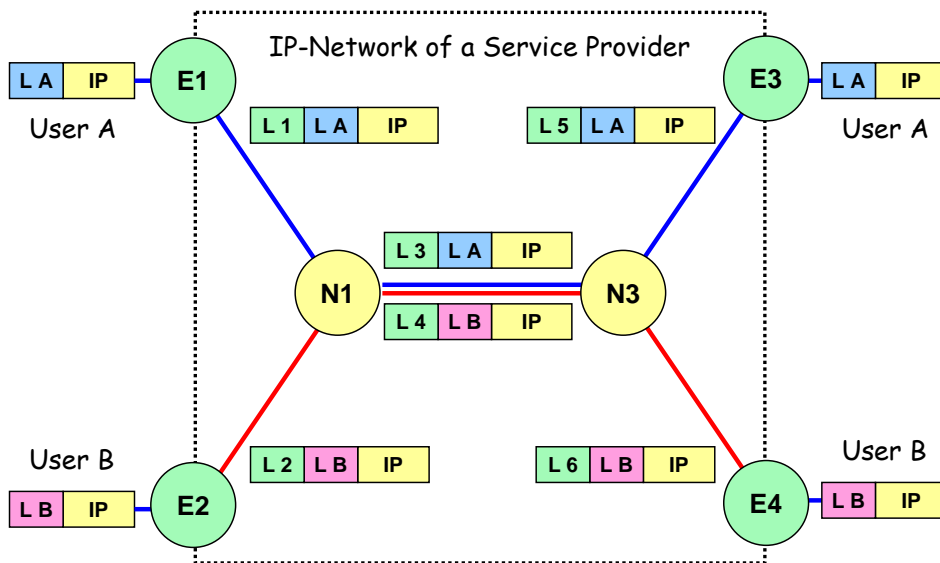




## 9.3 Multi-Protocol Label Switching (MPLS)

---

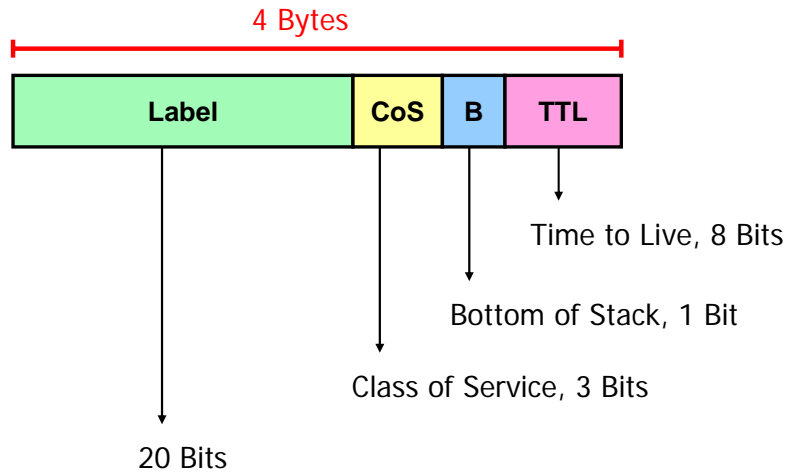
## MPLS based Virtual Private Networks



### Virtual Private Network (VPN) based on MPLS

- By prepending a user label LA in front of each IP packet the whole IP-traffic from user A can be transported from ingress node E1 (e.g. home office) to egress node E3 (e.g. company headquarters) without examining the IP headers along the route. Even private network addresses (e.g. 10.x.x.x) could be transported.
- From hop to hop an outer switching label (L1, L3, L5) that defines the label switched path is pushed onto the label stack at the beginning of a hop and popped again after the switching decision at the end of a hop.
- Labelling client traffic also allows efficient billing based on the number of transmitted IP-packets.

## MPLS Layer 2 Shim Header (RFC 3032)



### Shim Header

- The shim header is carried after the data link layer header (layer 2) and before the IP header (layer 3).

### Label

- Multiple encapsulations may exist, i.e. labels may be stacked to an arbitrary depth:
- Stacking maintains identity of several streams when they are aggregated into a single Label Switched Path (LSP)
- Labels are a generalization of ATM's concept of a dual hierarchy established by VPCs and VCCs.

### Class of Service

- The Class of Service (CoS) field is similar to the seldom used Type of Service (TOS) field in the IP header. MPLS uses these experimental bits for QoS purposes.

### Time to Live

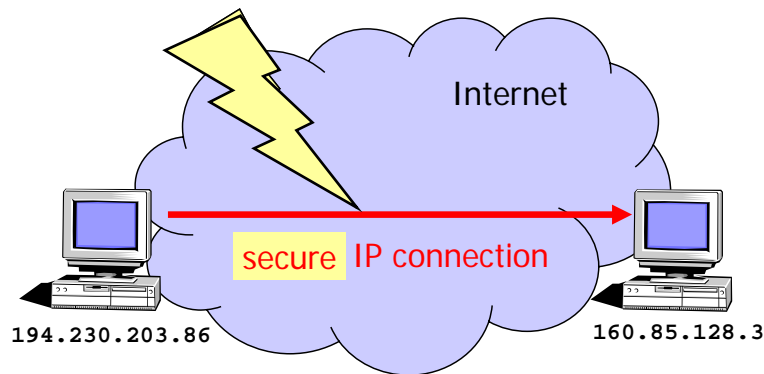
- The Time to Live (TTL) field takes over the function of the TTL field in the IP header hidden by encapsulation.

Source: Hans Weibel, ZHW Course „Kommunikationsnetze“, May 2000

## 9.4 IPsec Transport Mode

---

## IPsec – Transport Mode



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

### Authenticity of IP connections

- In order to prevent IP spoofing and connection hijacking, as well as to secure the content of IP datagrams against any unauthorized modifications, all IP datagrams sent over the Internet should be authenticated.

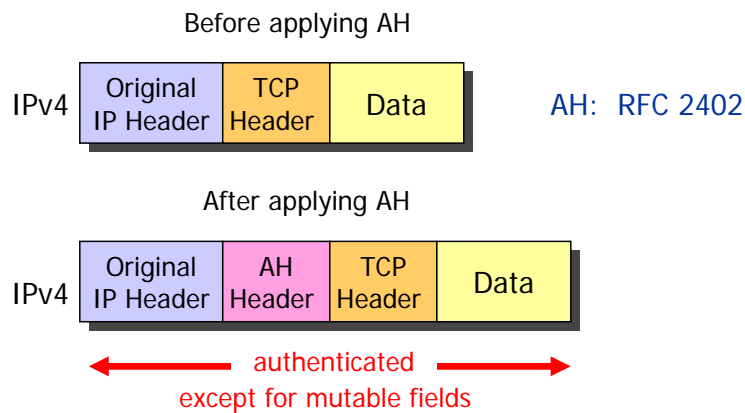
### Privacy of IP connections

- In order to guarantee privacy, all IP datagrams sent over the Internet should be encrypted by employing strong cryptography.

### Encryption and Authentication

- It is desirable to have both encryption and authentication applied to IP datagrams.

## IPsec – Transport Mode IP Authentication Header (AH)



AH: RFC 2402

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

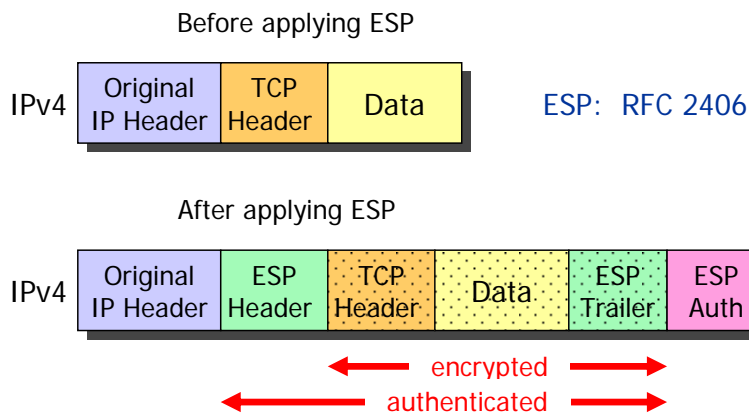
### IP Authentication Header (AH)

- The IPsec AH Protocol is specified in RFC 2402.
- AH protects both IP header and IP payload against modifications by computing a **keyed message authentication code (MAC)** over most octets of the IP datagram.
- Excluded from the cryptographic checksum are the following mutable header fields:
  - Type of Service (TOS)
  - Fragment Offset (always zero since AH is applied to non-fragmented packets, only)
  - Flags
  - Time to Live (TTL)
  - IP header checksum

The above header fields could possibly get modified by intermediate routers **en-route** from source to destination.

- The secured checksum is transmitted in the AH header, together with an arbitrary 32 bit Secure Parameters Index (SPI) uniquely identifying the Security Association and a 32 bit Sequence Number preventing replay attacks.
- The AH header has the structure of an IPv6 extension header but can also be carried over IPv4.
- Not only TCP and UDP but any transport layer protocol can be protected by AH. The **Protocol field** in the original IP header is set to the decimal value **51**, designating the AH protocol and the **Next Header field** in the AH header carries the original protocol number (e.g. 1 for ICMP, 6 for TCP, 17 for UDP), identifying the transport layer payload carried in the IP datagram.

## IPsec – Transport Mode IP Encapsulating Security Payload (ESP)



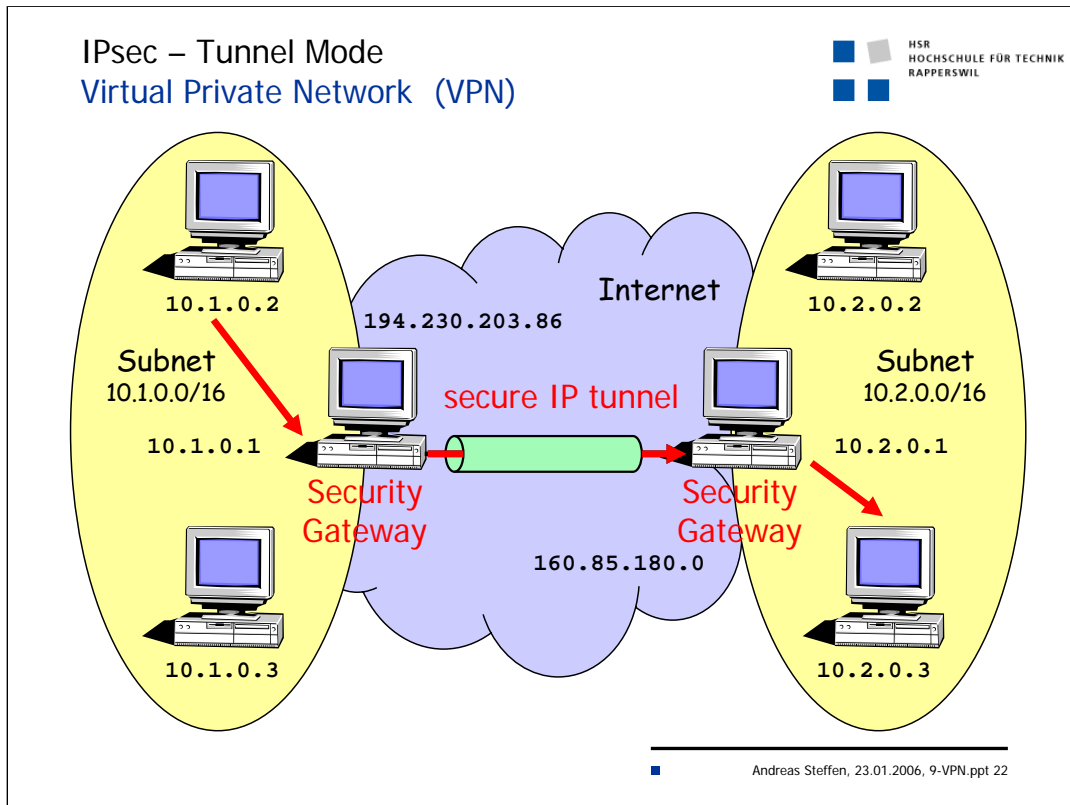
- IP protocol number for ESP: 50
- ESP authentication is optional
- With ESP authentication the IP header is not protected.

### IP Encapsulating Security Payload (ESP)

- The IPsec ESP Protocol is specified in RFC 2406.
- ESP encrypts the transport payload of the IP datagram using a strong symmetric encryption algorithm (IDEA, 3DES, AES, etc.).
- An ESP trailer is appended prior to encryption in order to align the payload data to a 4-byte boundary required by the ESP packet format. It may also be used to adapt the plaintext size to the block size of the block cipher (e.g. 64 bits for 3DES).
- Since IP packets could get lost, the encrypted payload is usually preceded by an initialization vector (IV) that is used by the receiver to initialize the block cipher algorithm used for the decryption of each IP payload.
- The ESP header has the structure of an IPv6 extension header but can also be carried over IPv4. Similar to the AH header it contains a 32 bit Secure Parameters Index (SPI) and a 32 bit Sequence Number.
- Any transport layer protocol can be encapsulated by ESP. The **Protocol field** in the original IP header is set to the decimal value **50**, designating the ESP protocol and the **Next Header field** in the ESP header carries the original protocol number identifying the transport layer protocol carried in the encrypted IP payload.
- Optionally the ESP payload can be authenticated by computing a keyed message digest over the body of the IP datagram and appending the MAC value as authentication data at the end of the encrypted payload. The IP header is not included in the checksum and therefore is not protected.
- In the case of an IPsec transport mode application where besides encryption also the protection of the IP header is required, the ESP and AH protocols can be cascaded by first encrypting the original IP payload using ESP and then authenticating both the original IP header and the ESP payload using AH.

## 9.5 IPsec Tunnel Mode

---



### Virtual Private Networks

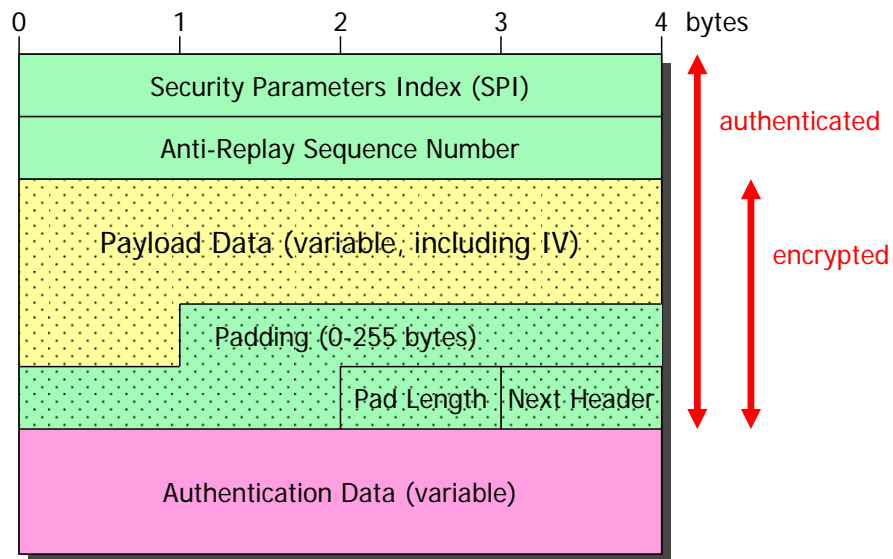
- A Virtual Private Network (VPN) can be used by an enterprise to connect its subnets or individual hosts located at various sites over shared public or semi-public communication channels. Compared to dedicated leased lines a VPN solution can offer significant cost savings without incurring any compromises regarding security requirements.
- VPNs can be realised using the **Layer 2 Tunneling Protocol (L2TP)** defined by the IETF or the now obsolete **Point-to-Point Tunneling Protocol (PPTP)**. Layer 2 tunnels are often transported over IP based networks using UDP as a transport medium but emulating a link layer dial-in line from source to destination.
- An elegant and increasingly popular VPN solution is based on layer 3 mechanisms using secure IP tunnels based on the IPsec protocol suite.

### IPsec Tunnels

- Two enterprise subnets can be securely connected with each other over the public Internet using an encrypted and authenticated IPsec tunnel. IP packets from a host on the local subnet to a host on the remote subnet are forwarded to the local **Security Gateway (SG)** which in turn tunnels the IP packets to the Security Gateway on the remote end of the IPsec tunnel where they are delivered to the destination host. The hosts belonging to the subnets are not aware of any security mechanisms. For them the Security Gateways have the function of simple routers.
- The encapsulation provided by the IPsec tunnels allows the use of private network addresses (e.g. 10.0.1.0/24 in one subnet and 10.0.2.0/24 in the second subnet) which are normally not routable over the Internet.



## ESP Header (Initial Header / Payload / Trailer)



ESP Overhead	3DES	AES	
• SPI	4	4	
• Sequence Number	4	4	
• IV	8	16	
• Padding (worst-case)	7	15	
• Pad Length / Next Header	2	2	
• Authentication Data	12	12	
	--	--	
<b>IPsec Transport Mode</b>	<b>37</b>	<b>53</b>	<b>bytes</b>
• Outer IP Header	20	20	
	--	--	
<b>IPsec Tunnel Mode</b>	<b>57</b>	<b>73</b>	<b>bytes</b>
<b>MTU</b>	<b>1443</b>	<b>1427</b>	<b>bytes</b>
	====	====	

Usually Path MTU discovery based on "fragmentation needed" ICMP messages" automatically reduces the MTU from a standard LAN MTU of 1500 bytes down to a payload data size that does not lead to fragmentation when the IPsec overhead is added.

