Zusammenfassung Netzwerk betreiben und erweitern

Modul 145

Titel	Zusammenfassung Netzwerk betreiben und erweitern	**Internet**	www.janikvonrotz.ch	**Status**	
Thema	Modul 145	**Typ**		**Version**	01.1
Autor	contact@janikvonrotz.ch	**Klasse**	öffentlich	**Freigabe Datum**	14.05.2012
Ablage/Name	D:\SkyDrive\education\bbzs\4.lehrjahr\sba\Modul145\Modul145_Netzwerk_Protokolle.docx				
Schlüsselwörter					
Kommentare					

Dokumentverlauf

Version	Datum	Autor	Beschreibung der Änderung	Status
1.0	15.04.2012	Janik von Rotz	Erstellen Dokument	In Bearbeitung
1.01	05.05.2012	Janik von Rotz	Freigabe	Bearbeitung beendet
1.2	14.05.2012	Janik von Rotz	Anpassen Formatvorlagen	Fertiggestellt

Referenzierte Dokumentes

Nr.	Dok-ID	Titel des Dokumentes / Bemerkungen	Ablage / Link

Lizenz

Inhaltsverzeichnis

1 Einleitung

In diesem Dokument werden die wichtigsten Protokolle, die im Rahmen der SBA-Prüfungen gefordert sind, behandelt.

Des Weiteren wird den Anforderungen entsprechend das Vorgehen zur Planung von IP-Netzwerken erläutert.

2 OSI Layer

Layer	Name	Einheit
1	Physical	Bits
2	Data Link	Frame
3	Network	Paket
4	Transport	UDP: Datagramm TCP Segment
5	Session	Data / Message
6	Presentation	Data
7	Application	Data

3 Protokolle

4 PPP

Point to Point Protocol

- Protocol type: Link layer protocol.

4.1 Beschreibung

Das PPP Protokoll ist eine standardisiert Einkapselungsmethode, die Funktionen auf der Verbindungsschicht umfasst, die vergleichbar mit der LAN-Einkapselung sind. PPP stellt Dienste für die Abgrenzung, Protokollidentifikation und Integritätsüberprüfung auf Bitebene bereit.

PPP bietet folgende Funktionen:

- **Verkapselung**
  - Eine Einkapselungsmethode auf der Verbindungsschicht, die für eine Verbindung mehrere Protokolle gleichzeitig unterstützt
- **Ordnungsgemässer Verbindungsaufbau**
  - Aushandeln des Authentifizierungsverfahren mit dem LCP[1]-Protokoll
- **Authentifizierungsmethoden**
  - Authentifizierung am Radius Server
- **Dynamische Protokolleigenschaften**
  - Protokollkonfiguration mit den NCP[2]-Protokollen

4.2 Frame

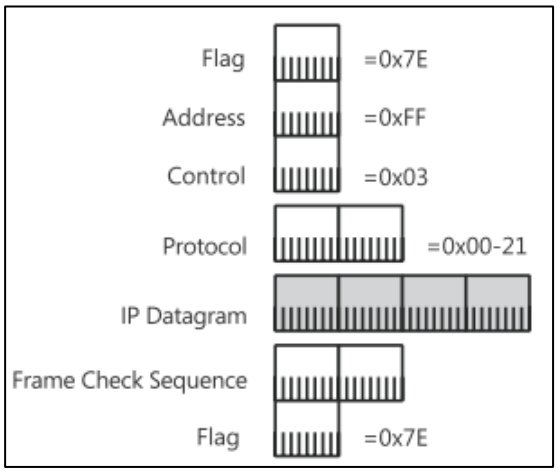


Abbildung 1: HDLC-Frame

[1] Siehe Kapitel: 19 LCP

[2] Siehe Kapitel: 20 NCP

4.2.1 Frame fields

Field	Description
Flag	Zeigt Beginn und Ende des Frames an
Adresse (Nur im HDLC Standard)	unnötig, da es sich meistens um Festverbindungen handelt
Control (Nur im HDLC Standard)	Nebenprodukt des HDLC Standards
Protokoll	Zeigt das eingekapselte Protokoll an: • 0x00-21 >> IP-Datagramm • 0x00-29 >> AppleTalk-Datagramm
FCE	Frame Check Sequence

4.3 Prozesse

- 4.3.1 Netzwerk-Architektur
- 4.3.2 WAN Configuration
- 4.3.3 Breitbandübetragung auf einer Telefonleitung
- 4.3.4 Leistung von ATM
- 4.3.5 PPP-Caputre
- 4.3.6 PPoE Capture Aufbau
- 4.3.7 PPP over Ethernet – Suchvorgang
- 4.3.8 PPP – Verbindungskonfigurations-Aufbau

4.3.1 Netzwerk-Architektur

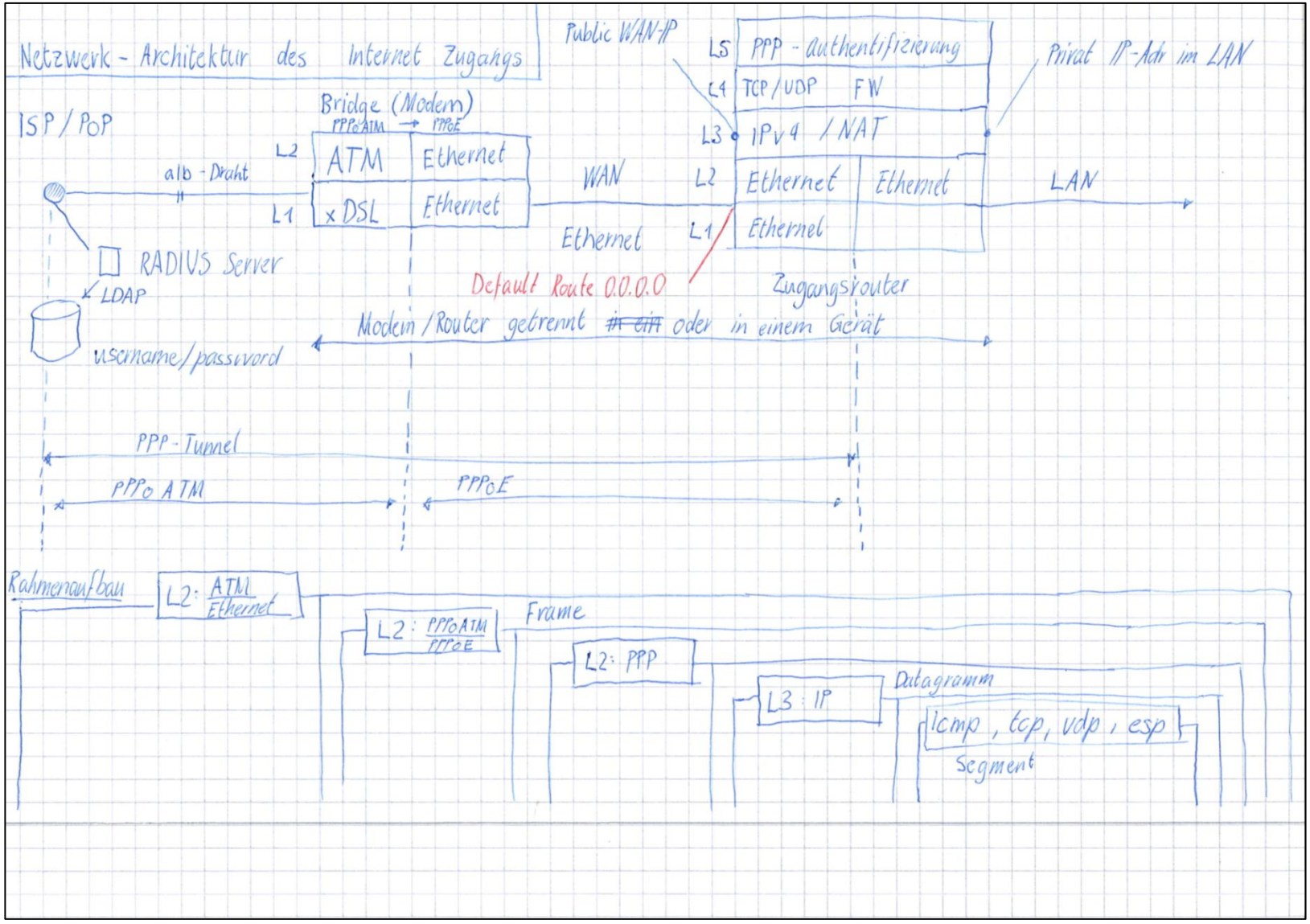


Abbildung 2: PPP Netzwerkarchitektur

4.3.2 WAN Configuration

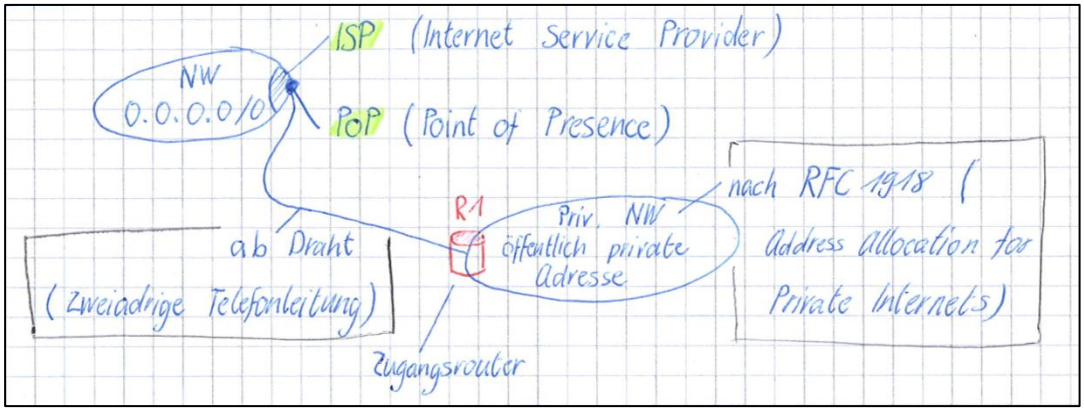


Abbildung 3: PPP WAN Configuration

1. Verwendung des Routers R1 als Default-Gateway für den Zugang ins Internet aus dem privaten Netz.
2. PPP konfiguriert den Router für die Kommunikation mit dem ISP, also die WAN-Schnittstelle, dazu gehört:
    a. IP-Adresse
    b. Default Route (Default Gateway)

4.3.3 Breitbandübetragung auf einer Telefonleitung

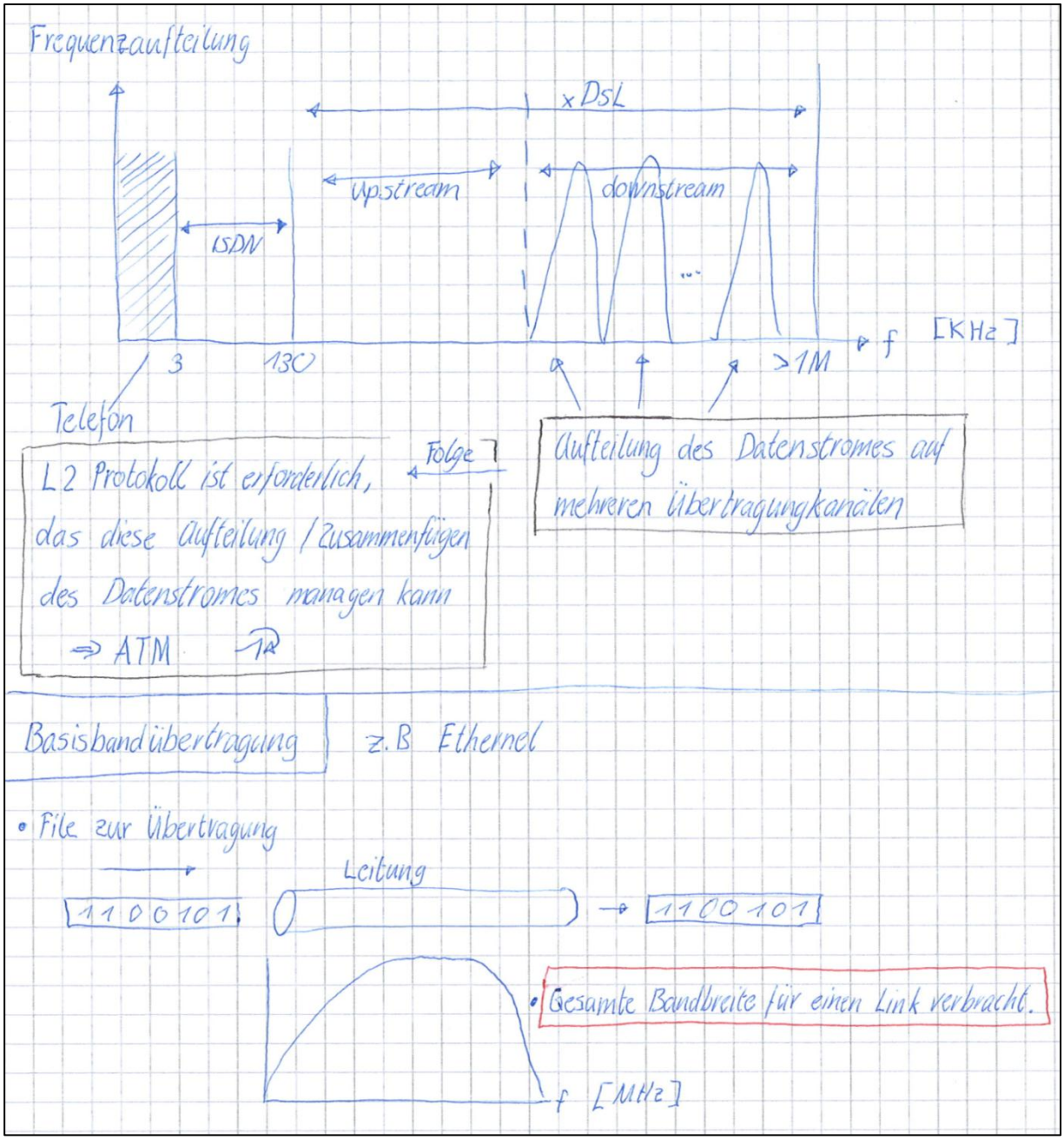


Abbildung 4: Schema Breitbandübertragung

4.3.4 Leistung von ATM[3]

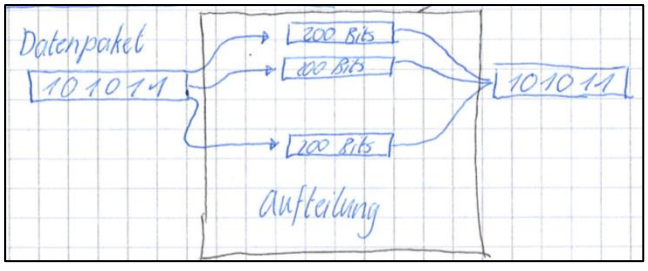


Abbildung 5: Leistung von ATM

[3] Siehe Kapitel: 21 ATM

4.3.5 PPP-Caputre

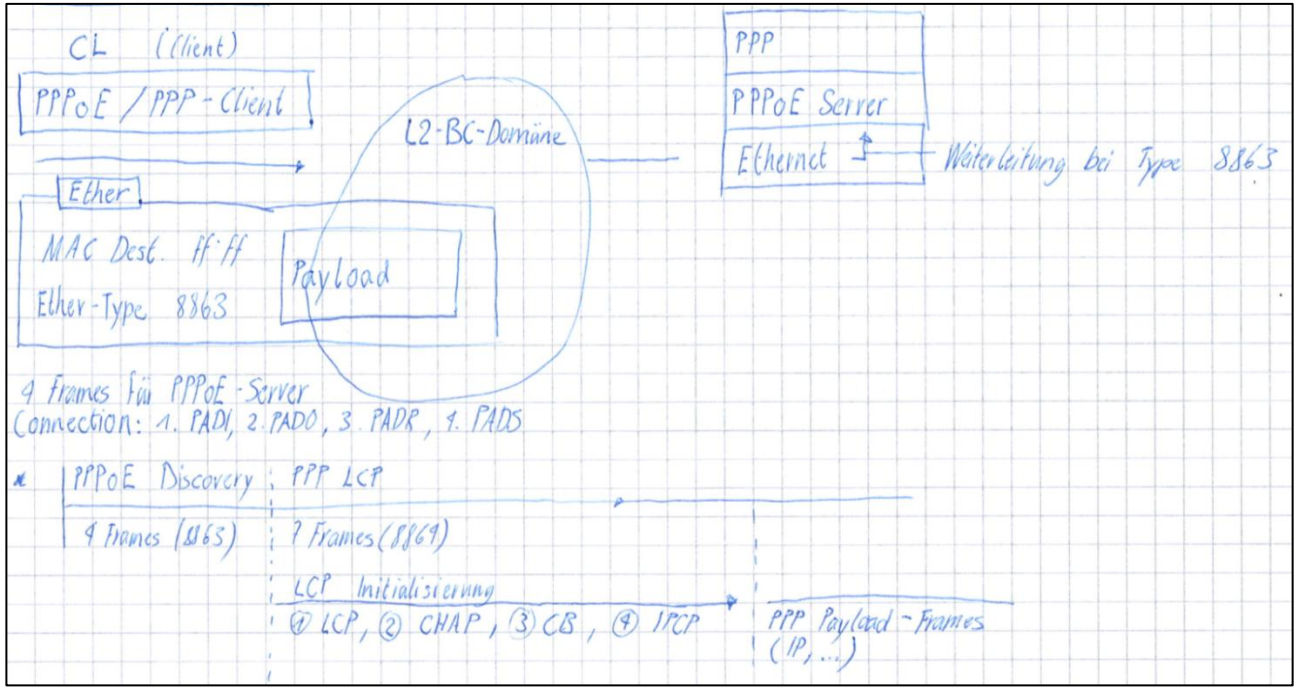


Abbildung 6: Aufbau PPP-Capture

4.3.6 PPoE Capture Aufbau

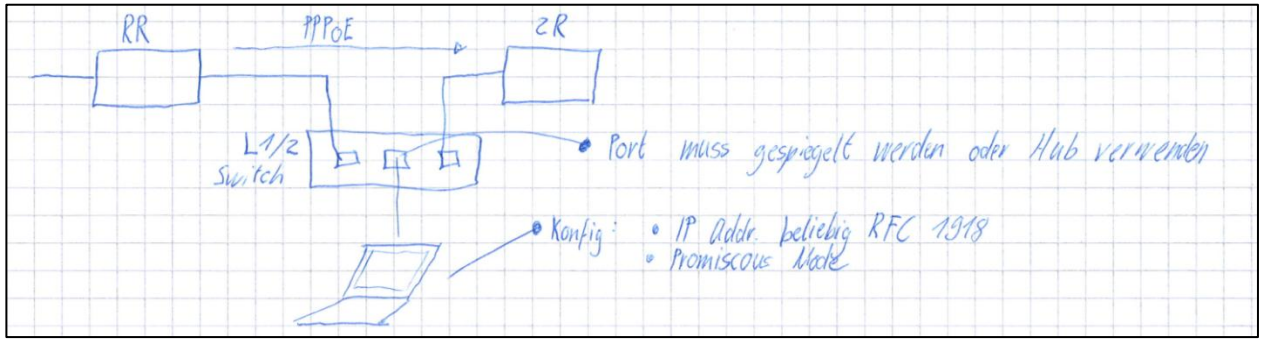


Abbildung 7: Capturing PPoE

4.3.7 PPP over Ethernet – Suchvorgang

In dieser Phase sucht der PPPoE-Client einen PPPoE-Ethernet-Server in der gleichen OSI-Layer 1,2 Infrastruktur und handelt mit diesem die PPPoE-Verbindungs-Parameter aus.

Ethernet					**PPP-over-Ethernet Discovery**					
Frame Nr	**Phasen Bezeichnung**	**Dest Adr**	**Src Adr**	**Ether Type**	**Version**	**Type**	**Code**	**Sitzungs-ID**	**Dienstname**	**Weitere PPPoE-Tags, die Werte enthalten**
1	PADI	ff:ff:ff:ff:ff:ff	Microsoft_af:6d:93	8863	1	1	9	0	-	Host-Uniq: 0100000001000000
2	PADO	Microsoft_af:6d:93	Microsoft_34:9a:49	8863	1	1	7	0	-	AC-Name: TEMPLATE Host-Uniq: 0100000001000000 AC-Cookie: 525350450003ffaf6d9360716ff7ba5fca01
3	PADR	Microsoft_34:9a:49	Microsoft_af:6d:93	8863	1	1	19	0	-	Host-Uniq: 0100000002000000 AC-Cookie: 525350450003ffaf6d9360716ff7ba5fca01
4	PADS	Microsoft_af:6d:93	Microsoft_34:9a:49	8863	1	1	65	2	-	Host-Uniq: 0100000002000000

Damit ist die PPP over Ethernet-Suchphase abgeschlossen

Das heisst: Es ist eine Layer 1,2 – Verbindung zwischen PPPoE-Client und PPPoE-Server aufgebaut.

Bei WAN-PPP Strecken (z.B PPPoATM bei der „ADSL-Verbindung“ wird die Layer 1,2 Verbindung ebenfalls formell aufgebaut. Bei gewissen ADSL-Routern gibt es dazu eine spezielle Anzeige-LED.

4.3.8 PPP – Verbindungskonfigurations-Aufbau

Dieser Vorgang ist technologie-unabhängig. Er erfolgt beim PPP-Verbindungsaufbau über ADSL/ATM, Ethernet oder auch über eine Telefon-Modem Verbindung.

Der PPP-Verbindungs-Konfigurationsvorgang erfolgt in vier Phasen, wobei die Phase 3 (Callback) in der Regel nicht stattfindet.

4.3.8.1 PPP-Phase 1: PPP-Konfiguration mit LCP

Konfigurations-Vereinbarungen, die in dieser Phase ausgehandelt werden:

- MRU (Maximum Receive Unit)
- ACCM (Asynchronous Control Character Map)
- Authentifizierungsprotokoll
- Zufallszahl (Magic Number)
- Protokollkoprimierung
- Adress- und Steuerfeldkomprimierung
- (Callback)

4.3.8.2 PPP-Phase 2: Authentifizierung mit dem PPP-Authentifizierungsprotokoll (Challenge Handshake Authentication Protocol)

Authentication protocol: CHAP (Challenge Handshake Authentication Protocol (0xc223))

4.3.8.3 PPP-Phase 3: Rückruf -> Callback Control Protocol

Diese Phase wird nicht durchgeführt.

4.3.8.4 PPP-Phase 4: Konfiguration der Netzwerkstueuerungsprotokolle Network Control Protocols

Aushandeln folgender IP-Konfigurationen:

```
⊟ Microsoft PPC: Supported Bits: 0x00000041
    .... .... .... .... .... .... .... ...1 = Desire to negotiate MPPC
    .... .... .... .... .... .... ...0 .... = Obsolete (should ALWAYS be 0)
    .... .... .... .... .... .... ..0. .... = 40-bit encryption OFF
    .... .... .... .... .... .... .1.. .... = 128-bit encryption ON
    .... .... .... .... .... .... 0... .... = 56-bit encryption OFF
    .... ...0 .... .... .... .... .... .... = Stateless mode OFF
```

Abbildung 8: PPP Options

```
⊟ Options: (6 bytes)
    IP address: 192.168.1.155
```

Abbildung 9: PPP Options IP-Config

Es werden normalerweise folgende Konfigurationen vorgenommen:

- Public Ip
- dGW
- IP NS 1,2
- Subnetmaske

Damit ist der „PPP-Bootvorgang“ (PPP-Konfiguration) abgeschlossen

Anschliessend können Nutzdaten übergeben übertragen werden

4.4 Summary

PPP wird für die Verbindungsaushandlung und Netzwerkprotokollaushandlung, sowie für die Einkapselung von Netzwerkprotokollpaketen verwendet, die über eine Festverbindung gesendet werden.

Der PPP-Verbindungsprozess umfasst vier Phasen:

1. Verbindungsaushandlung
2. Authentifizierung
3. Rückrufaushandlung (Callback)
4. Netzwerkprotokollaushandlung

Während der Verbindungsaushandlung legen die PPP-Kommunikationspartner fest, auf welche Weise PPP-Frames gesendet werden.

Während der der Authentifizierung werden unter Verwendung von PPP-Authentifizierungsprotokollen, beispielsweise MS-CHAP v2 oder EP-TLS, die Anmeldeinformationen des anrufenden oder des antwortenden PPP-Kommunikationspartners überprüft.

Während der Rückrufaushandlung legen der anrufende und der antwortende PPP-Kommunikationspartner fest, ob der antwortende PPP-Partner den anrufenden Kommunikationspartner zurückrufen soll und welche Telefonnummer dieser dabei verwenden muss.

Während der Netzwerkprotokollaushandlung werden unter Verwendung von NCPs, beispielsweise IPCP, CCP und ECP, die Verwendung und Konfiguration von TCP/IP, die Verwendung der Komprimierung und die Verwendung der Verschlüsselung festgelegt.

PPPoE ist eine Methode zum Einkapseln von PPP-Frames, damit diese über ein Ethernet-Verbindung gesendet werden können. Der PPPoE-Verbindungsprozess besteht aus zwei Phasen:

1. PPPoE-Suchphase
2. PPPoE-Sitzungsphase

Nachdem während der Suchphase eine PPPoE-Verbindung ausgehandelt wurde, werden in der PPPoE-Sitzungsphase mit PPP eine Verbindung ausgehandelt und Netzwerkprotokollframes gesendet.

4.5 Glossar

Bezeichnung	Wert	Beschreibung
Phase PPPoE Verbindungsaufbau	PADI	PPPoE Active Discovery Initiation
	PADO	PPPoE Active Discovery Offer
	PADR	PPPoE Active Discovery Request
	PADS	PPPoE Active Discovery Session-confirmation
Ether Type	8863	PPPoE Discovery
Code	9	Active Discovery Initiation

5 CHAP

Challenge Handshake Protocol

- Protocol type: PPP link control protocol, Authentication.
- PPP protocol: 0xC223.

5.1 Beschreibung

Das Authentifizierungs-Protokoll CHAP basiert auf folgenden Grundlagen:

- Der Benutzer muss über über einen Benutzernamen und ein Passwort verfügen.
- Der Authentifizierungsserver hat diese beiden Angaben zum Benutzerkonto in einer Datenbank (z.B. in einem LDAP-Directory) eingespeichert.
- Zu Beginn der Authentifizierung sendet der Authentifizierungsserver dem Client eine sogenannte Challenge-Message (CM), die aus einer Sitzungs-ID und einem zufällig gebildeten Challenge-String (CS), besteht.
- Der Client verwendet die CM und ergänzt diese mit dem Benutzerpasswort (PW). Anschliessend bildet der Client einen Hash H_{Client} nach der Formel:

  $H_{Client} = MD5(CM + PW)$
- Ein Angreifer kann zwar die CM mitlesen und daraus einen MD5-Hash H_{Hacker} nach der Formel

  $H_{Hacker} = MD(CM)$
- berechen.
- Aufgrund der extremen Unlinearität der Hash-Funktion kann er aber mit analytischen Mitteln auf keinen Fall den Hash des PW berechnen weil

  $MD5(PW) \mathbf{<>} MD5(CM + PW) – MD5(CM)$
- Daher kann ein Angreifer den Hash des Passwortes nicht zurückrechnen und schon gar nicht das Passwort selbst.

5.2 Prozesse

5.2.1 Ablauf CHAP-Verfahren

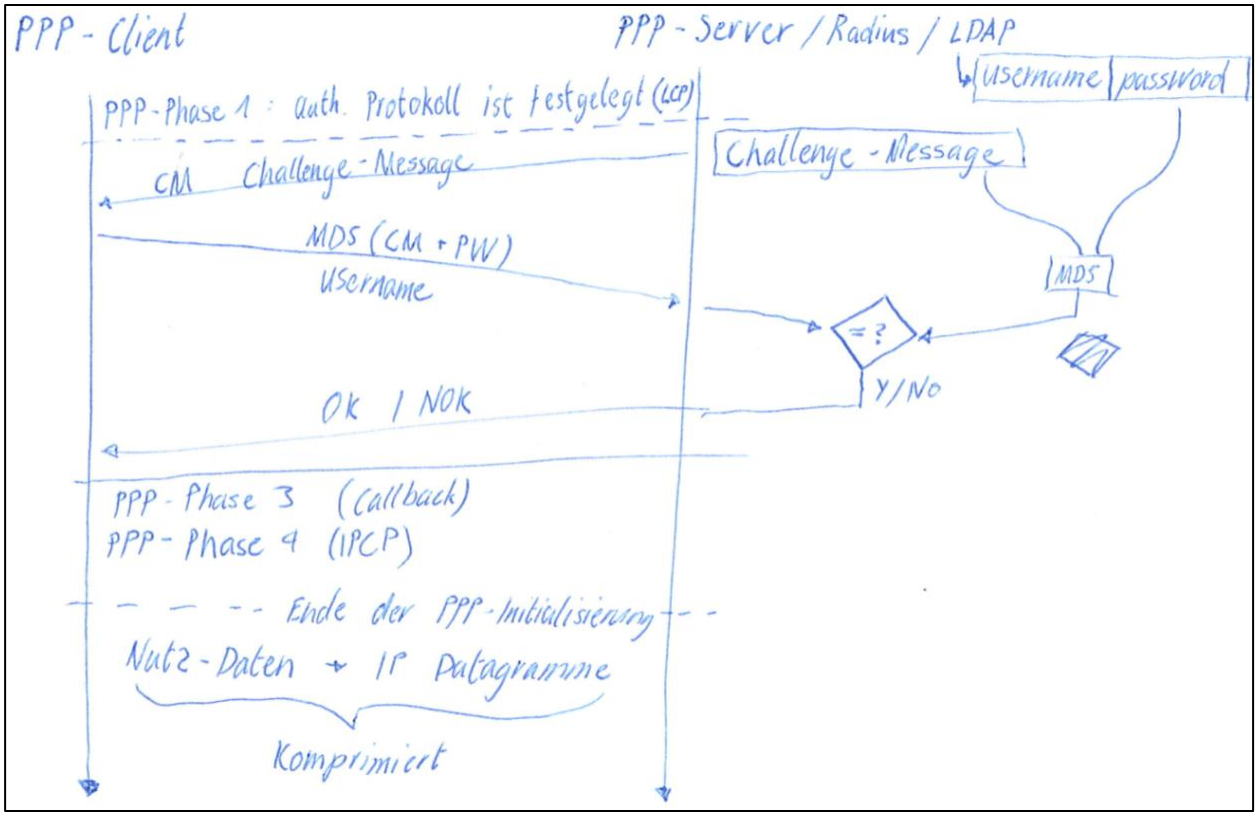


Abbildung 10: CHAP Verfahren

6 EAP

Extensible Authentication Protocol

- Protocol type: PPP link Control protocol.
- PPP protocol: 0xC227.

6.1 Beschreibung

EAP wurde als Erweiterung von PPP entwickelt, um bei der Implementierung von Authentifizierungsmethoden für PPP-Verbindungen die Erweiterbarkeit und Flexibilität zu verbessern.

Bei PAP, CHAP und MS-CHAP v2 beruht der Authentifizierungsprozess auf einem festgelegten Austausch von Nachrichten.

Mit EAP kann der Authentifizierungsprozess aus einer unbefristeten Konversation bestehen, in der alle PPP-Kommunikationspartner Nachrichten nach Bedarf senden.

Im Gegensatz zu den bisher in diesem Kapitel beschriebenen PPP-Authentifizierungsprotokollen werden bei EAP in der Phase 1 der Verbindung keine Authentifizierungsmethoden ausgewählt.

Stattdessen wird die EAP-Authentifizierungsmethode während der Phase 3 der Verbindung festgelegt. In der Phase 1 werden die entsprechenden LCP-Optionen (0xC2-27) angegeben.

6.2 Message

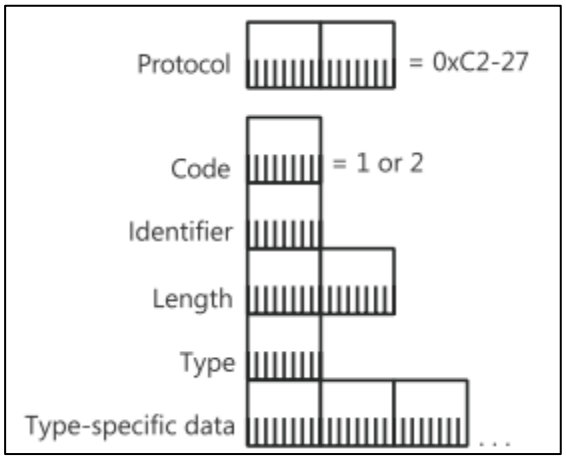


Abbildung 11: EAP-Message

6.3 Message fields

Field	Description
Code	Gibt den Typ der EAP-Nachricht an.
Type	Gibt den EAP-Typ an, z.B. Wert 29 für EAP-MS-CHAP v2
Type-specific data	Enthält die Daten der EAP-Nachrichten

6.4 Prozesse

- 6.4.1 EAP Anwendungsbeispiel

6.4.1 EAP Anwendungsbeispiel

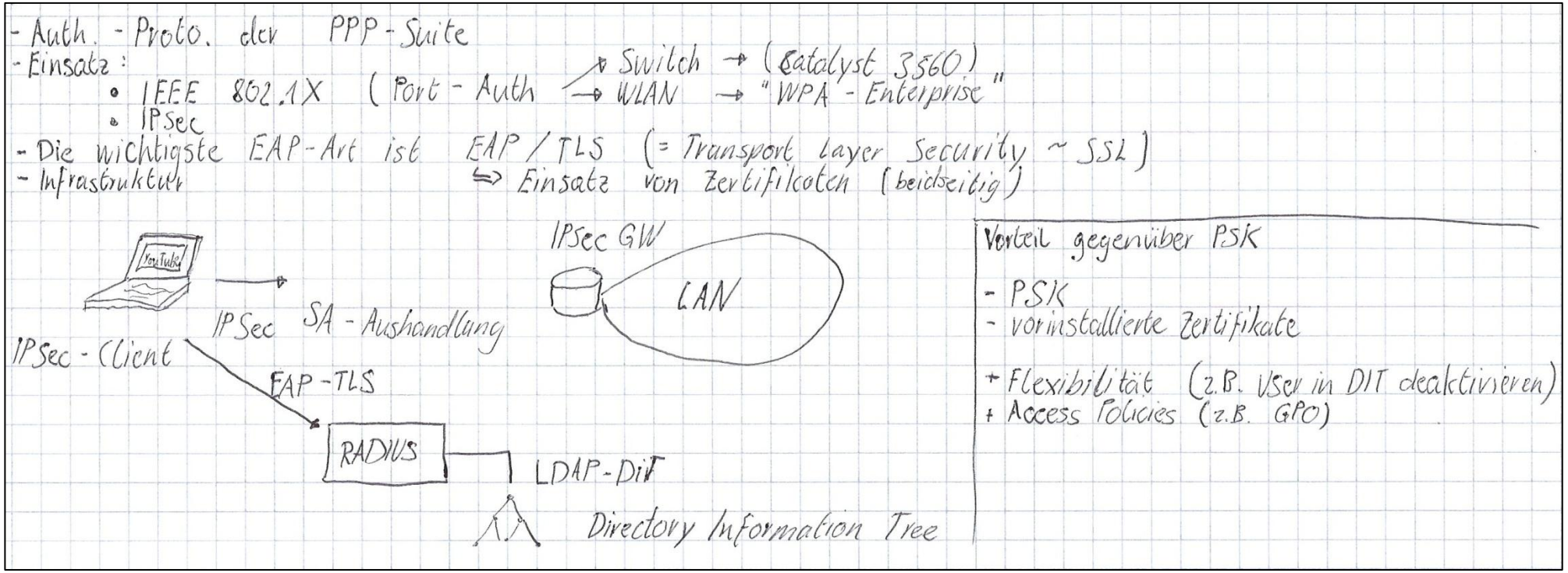


Abbildung 12: EAP Anwendungsbeispiel

7 TCP

Transmission Control Protocol

- Protocol type: Transport layer connection oriented byte stream protocol.
- IP Protocol: 6

7.1 Beschreibung

Grundlegende Eigenschaften von TCP sind:

- **3-Way-Handshake**
  - Server-Client-Verbindung wird über 3-Way-Handshake aufgebaut
- **Zuverlässig**
  - TCP-Verbindungen sind zuverlässig, d.h. es findet eine Kontrolle der übertragenen und empfangenen Segmente statt.
- **Vollduplex**
  - Der Datenaustausch erfolgt bidirektional
- **Direkte Übertragung**
  - Es sind nur 1:1 Verbindungen möglich
- **Bytestrom**
  - Der eingehende und der ausgehende Kanal ist ein kontinuierlicher Datenstrom. Die Analyse der Datenstroms erfolgt über das Anwendungsprotokoll

7.2 Segment

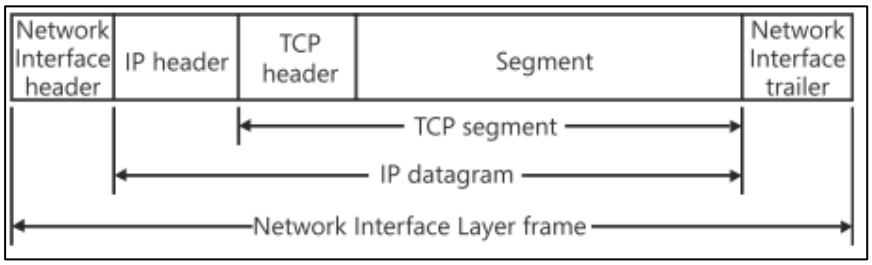


Abbildung 13:TCP Segment

7.3 Header

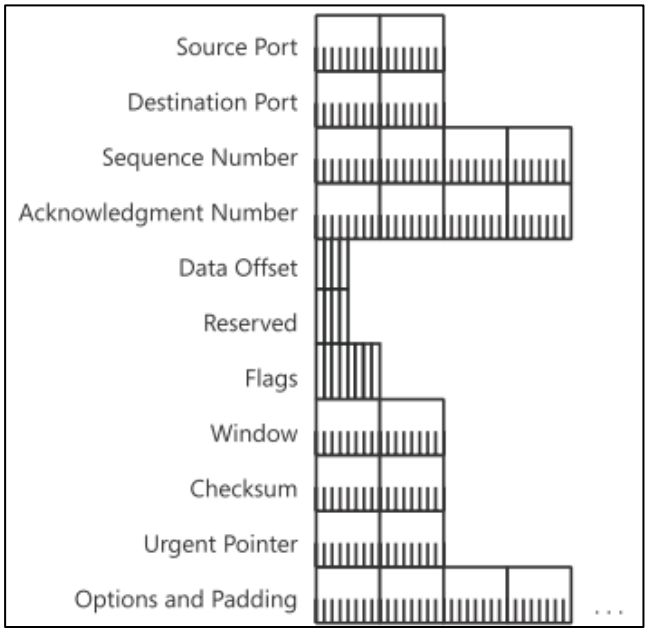


Abbildung 14: TCP Header

7.3.1 Header fields

Bezeichnung	Beschreibung	Grösse
Source Port	Quell Port / Quellprotokoll	2 Byte
Destination Port	Ziel Port / Zielprotokoll	2 Byte
Sequence Number	Nummerierung des TCP Segments	4 Byte
Flags	TCP Flags: • SYN: Verbindungsanforderung • ACK: Bestätigung Sender/ Empfänger • PSH: Leerung des Empfangspuffer	1Byte

7.4 Frame

```
+ Ethernet: Etype = Internet IP (IPv4)
+ Ipv4: Next Protocol = TCP, Packet ID = 57288, Total IP Length = 1500
- Tcp: Flags=....A..., SrcPort=FTP data(20), DstPort=1163, Len=1460, Seq=1038577021 -
 1038578481, Ack=3930983524, Win=17520 (scale factor not found)
    SrcPort: FTP data(20)
    DstPort: 1163
    SequenceNumber: 1038577021 (0x3DE76D7D)
    AcknowledgementNumber: 3930983524 (0xEA4E0C64)
  - DataOffset: 80 (0x50)
     DataOffset: (0101....) (20 bytes)
     Reserved:   (....000.)
     NS:         (.......0) Nonce Sum not significant
  - Flags: ....A...
     CWR:    (0.......) CWR not significant
     ECE:    (.0......) ECN-Echo not significant
     Urgent: (..0.....) Not Urgent Data
     Ack:    (...1....) Acknowledgement field significant
     Push:   (....0...) No Push Function
     Reset:  (.....0..) No Reset
     Syn:    (......0.) Not Synchronize sequence numbers
     Fin:    (.......0) Not End of data
    Window: 17520 (scale factor not found)
    Checksum: 46217 (0xB489)
    UrgentPointer: 0 (0x0)
    TCPPayload:
+ Ftp: Data Transfer To Client,DstPort = 1163,size = 1460 bytes
```

Abbildung 15: TCP Frame

7.5 Prozesse

- 7.5.1 TCP- / UDP-Port zur Adressierung
- 7.5.2 3-Way Handshake
- 7.5.3 SYN-Flood Attacke

7.5.1 TCP- / UDP-Port zur Adressierung

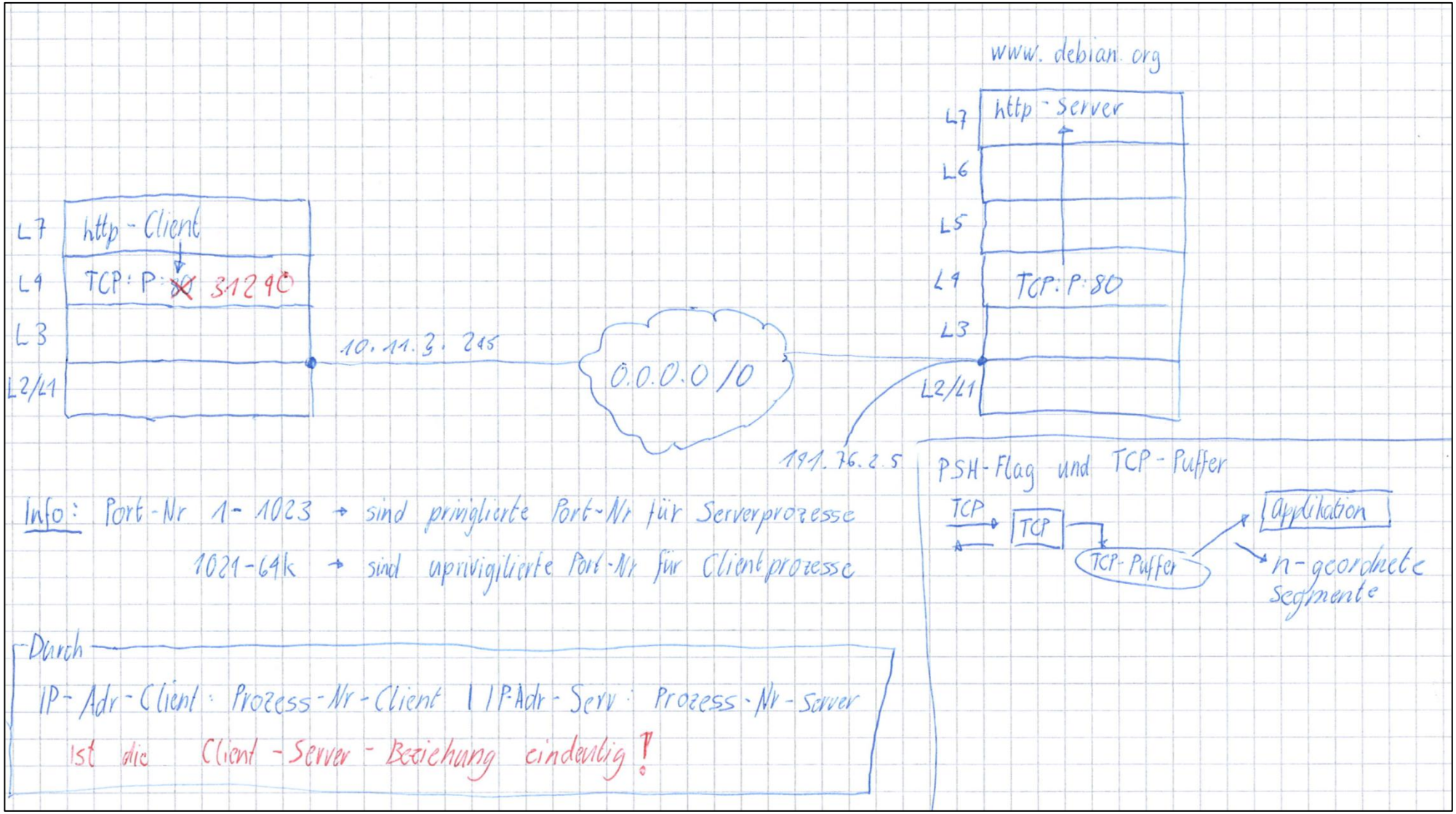


Abbildung 16: TCP/UDP Port Adressierung

7.5.2 3-Way Handshake

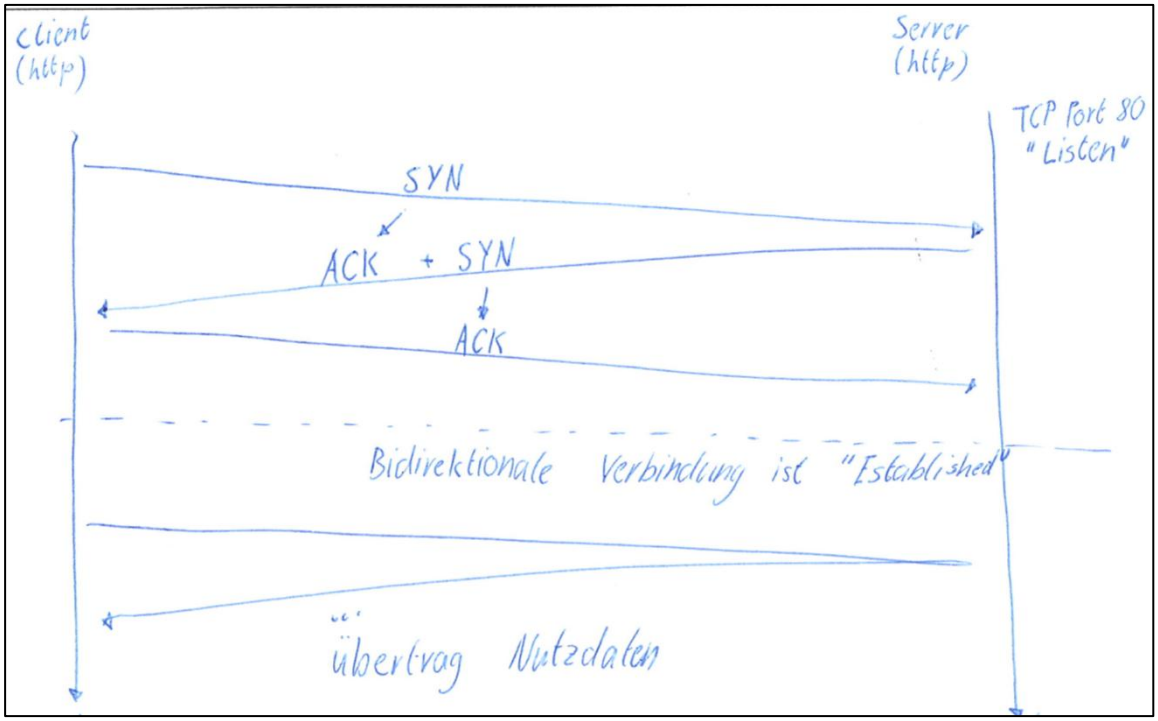


Abbildung 17: TCP 3-Way-Handshake

7.5.3 SYN-Flood Attacke

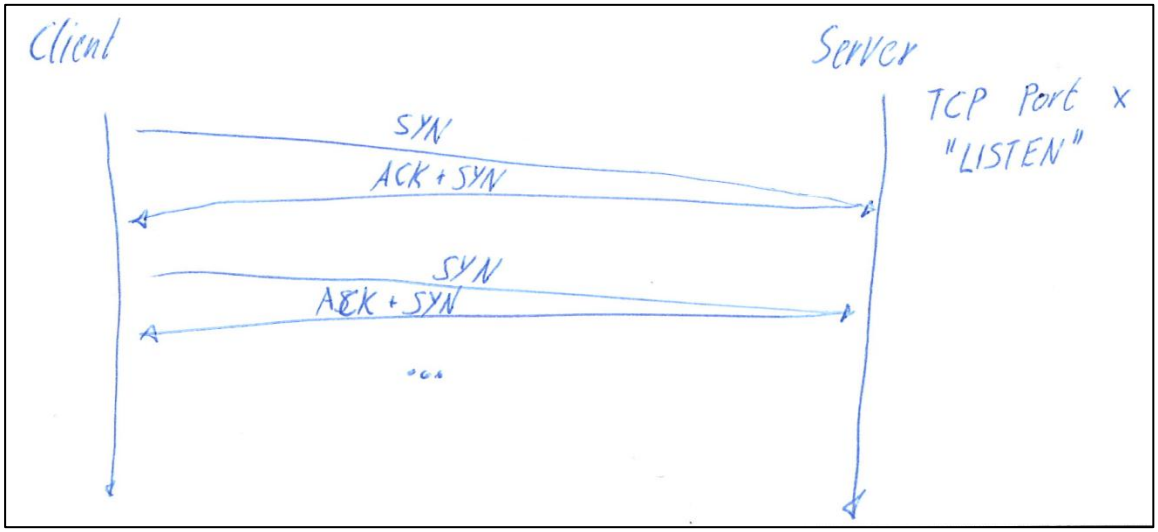


Abbildung 18: TCP SYN-Floot-Attack

Es werden so viele halboffene Verbindungen eröffnet bis der RAM-Speicher des Servers überfüllt ist.

7.6 TCP Ports

Port	Beschreibung
20	FTP Server (data channel)
21	FTP Server (control channel)
23	Telnet Server
25	Simple Mail Transfer Protocol (SMTP)
69	Trivial File Transfer Protocol (TFTP)
80	Hypertext Transfer Protocol (HTTP; Web Server)
139	NetBIOS Session Service
443	HTTP protocol over Transport Layer Security (TLS)
445	Direct-Hosted Server Message Block (SMB) (also known as Microsoft-DS)

7.7 Summary

TCP-Verbindungen werden über einen ausdrücklichen Prozess für den TCP-Verbindungsaufbau hergestellt. Dabei tauschen die beiden TCP-Kommunikationspartner SYN-Segmente aus und bestimmen die Anfangssequenznummern, Fenstergrössen, Fensterskalierungsfaktoren, die maximalen Segmentgrössen und andere TCP-Optionen.

TCP-Verbindungen können durch den Austausch von regelmässigen Keepalive-Segmenten gewartet werden, obwohl dies nicht üblich ist.

U eine TCCP-Verbindung ordnungsgemäss abzubauen, muss jeder TCP-Kommunikationspartner ein FIN-Segment senden das vom anderen Partner bestätigt wird.

TCP-Kommunikationspartner können ein TCP-Segment zum Zurücksetzen der Verbindung verwenden, um eine aktuelle Verbindung abzubrechen oder einen Verbindungsversuch abzulehnen.

8 UDP

User Datagram Protocol

- Protocol type: Connectionless transport layer protocol.
- IP Protocol: 17

8.1 Beschreibung

Die grundlegenden Eigenschaften von UDP sind:

- **Verbindungslos**
  - Die Kommunikation erfolgt verbindungslos
- **Unzuverlässig**
  - Es findet keine Sequenzierung und Bestätigungskontrolle der übertragenen Daten statt.
- **Identifizierung der Anwendungsschicht**
  - UDP umfasst ein Methode zum Senden on Nachrichten an ein bestimmten Protokoll der Anwendungsschicht
- **Prüfsumme**
  - UDP-Nachrichten erhalten eine Prüfsumme

8.2 Datagramm

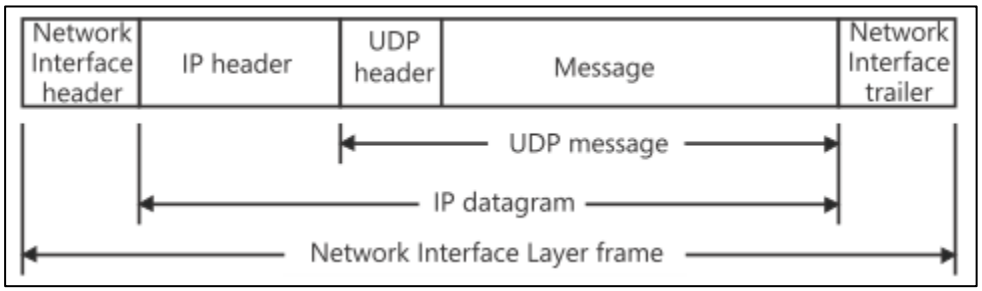


Abbildung 19: UDP Message

8.3 Header

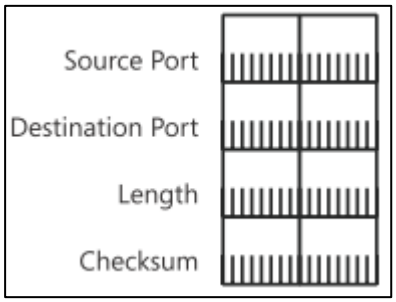


Abbildung 20: UDP Header

8.4 Frame

```
  Frame:
+ Ethernet: Etype = Internet IP (IPv4)
+ Ipv4: Next Protocol = UDP, Packet ID = 16385, Total IP Length = 58
- Udp: SrcPort = DNS(53), DstPort = DNS(53), Length = 38
    SourcePort: DNS(53), 53(0x35)
    DestinationPort: DNS(53), 53(0x35)
    TotalLength: 38 (0x26)
    Checksum: 27297 (0x6AA1)
+ Dns: QueryId = 0x2, QUERY (Standard query), Query  for  www.acme.com of type Host Addr on
class Internet
```

Abbildung 21: UDP Frame

8.5 UDP Ports

Port	Number Application Layer Protocol
53	DNS
67	BOOTP server (Dynamic Host Configuration Protocol [DHCP])
6	BOOTP Client (DHCP)
69	TFTP
137	NetBIOS Name Service
138	NetBIOS Datagram Service
161	Simple Network Management Protocol (SNMP)
445	Direct hosting of Server Message Block (SMB) datagrams over TCP/IP
520	RIP
1812, 1813	Remote Authentication Dial-In User Service (RADIUS)

8.6 Summary

UDP stellt einen verbindungslosen und unzuverlässigen Übertragungsdienst für Anwendungen bereit, die den zuverlässigen Übertragungsdienst von TCP nicht benötigen.

Protokolle der Anwendungsschicht können UDP bei einfachem Kommunikationsbedarf mit geringem Aufwand verwenden, beispielsweise zur Übertragung von Broadcast- und Multicastdaten oder wenn die Anwendungsschichtprotokolle zuverlässige Übermittlungsdienste bereitstellen.

Der UDP-header zeigt eine Prüfsumme sowie die Quell- und Zielportnummern an, die benötigt werden, um die UDP-Daten an die passenden Protokolle der Anwendungsschicht zu übergeben.

9 VLAN

Virtual Local Area Networks

9.1 Beschreibung

Ein Virtual Local Area Network (VLAN) ist ein logisches Teilnetz innerhalb eines Switches oder eines gesamten physischen Netzwerks. Es kann sich über einen oder mehrere Switches hinweg ausdehnen. Ein VLAN trennt physische Netze in Teilnetze auf, indem es dafür sorgt, dass VLAN-fähige Switches die Frames (Datenpakete) eines VLANs nicht in ein anderes VLAN weiterleiten und das, obwohl die Teilnetze an gemeinsame Switches angeschlossen sein können.

9.1.1 Vorteile

- **Performance**
  - Weniger BC und MC als in einem herkömmlichen LAN
- **Einfache Integration**
  - in ein LAN, Switches müssen IEEE 802.1q-fähig sein
- **IP Netzwerkplanung**
  - kann ohne Rücksicht auf die Broadcastdomänen geplant werden

9.2 Prozesse

- 9.2.1 IEEE 802.1q Virtuelle lokale Netzwerke
- 9.2.2 Redesign auf Layer 2
- 9.2.3 IP-Netzwerk auf einen Switch patchen
- 9.2.4 EEE 802.1q Tag – Ein- und Aus-taggen von Frames
- 9.2.5 Aufbau des VLAN Tags
- 9.2.6 IEEE 802.1q VLAN- und IPv4-Teilnetzplanung
- 9.2.7 Beispiel VLAN-Kommunikation

9.2.1 IEEE 802.1q Virtuelle lokale Netzwerke

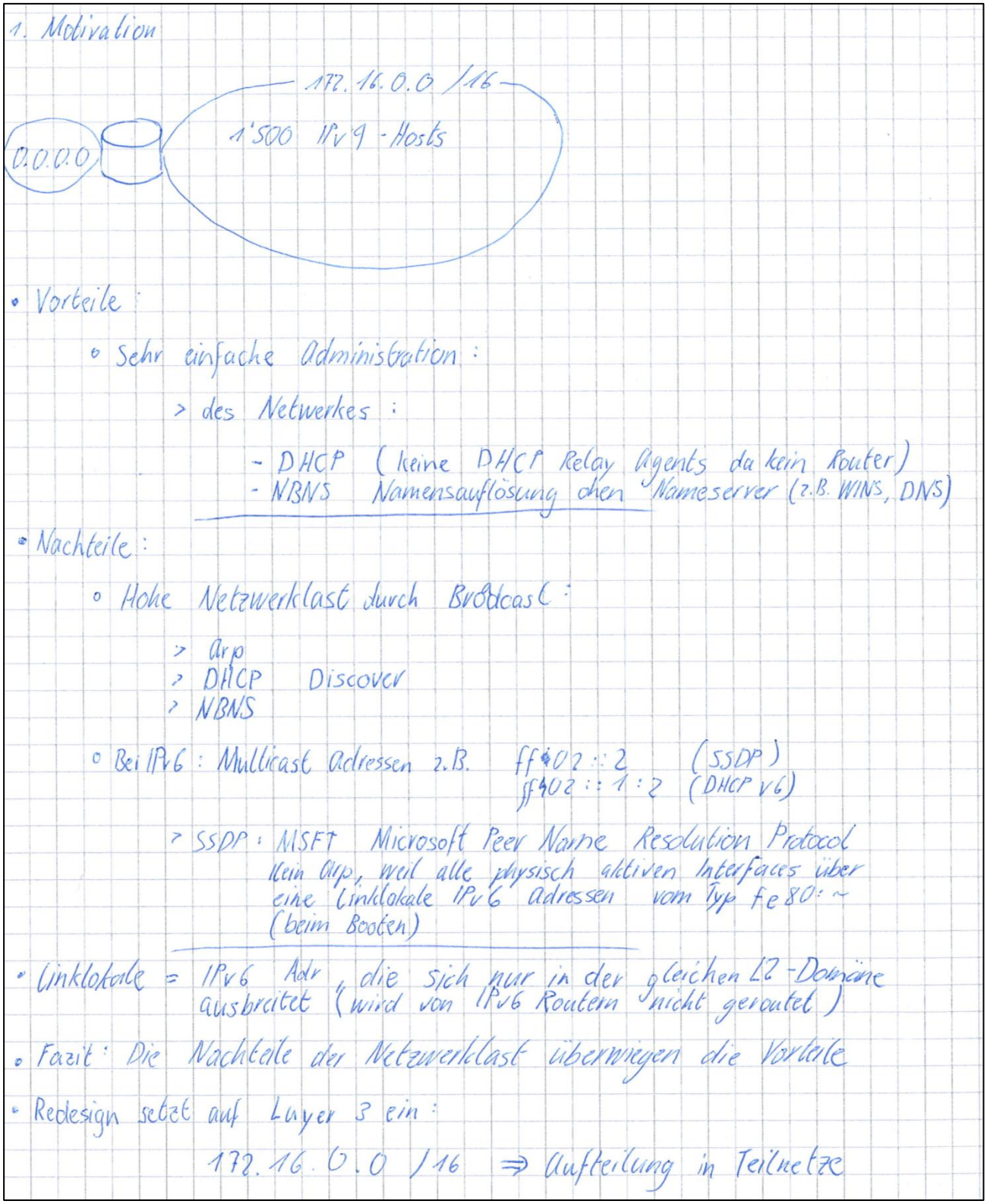


Abbildung 22: IEEE 802.1q Virtuelle lokale Netzwerke

9.2.2 Redesign auf Layer 2

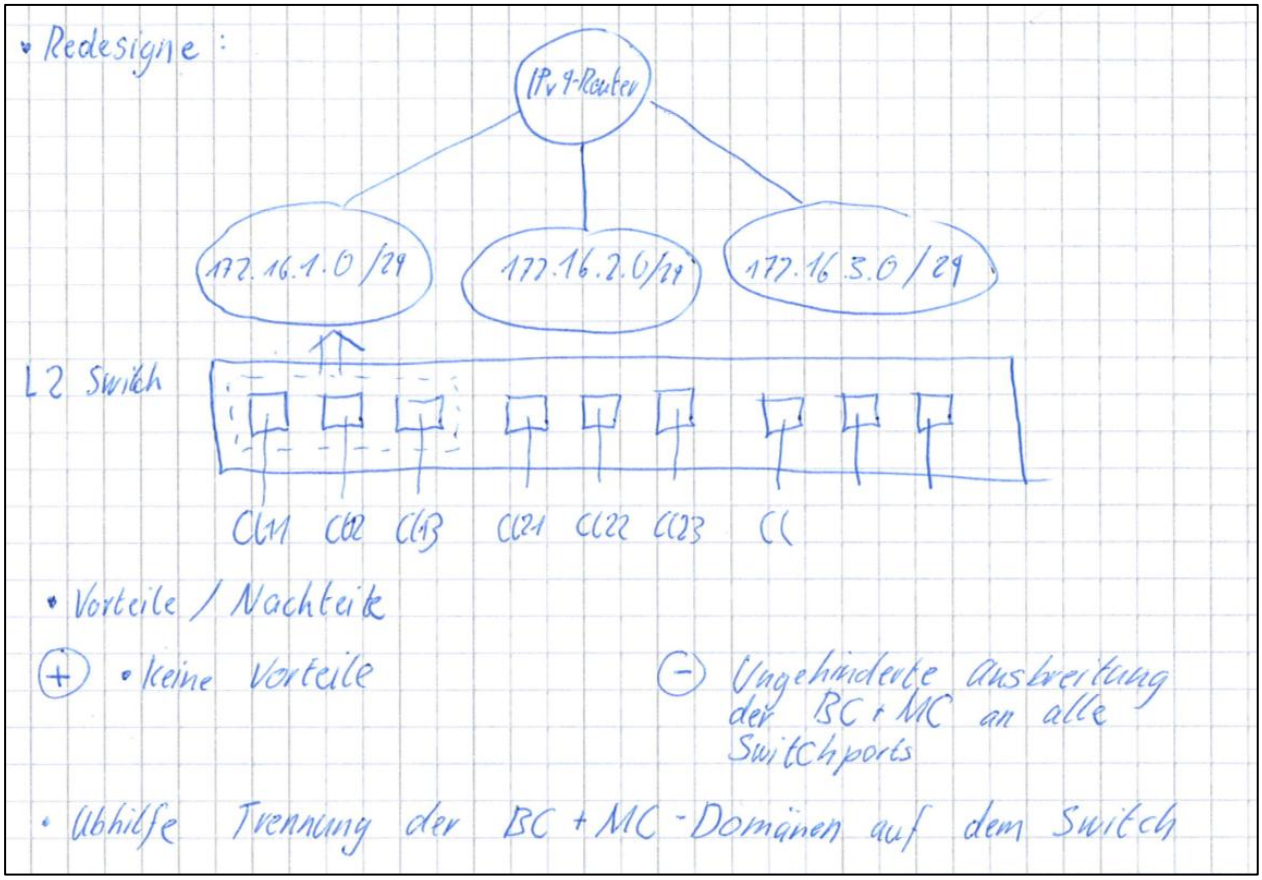


Abbildung 23: VLAN Redesign auf Layer 2

9.2.3 IP-Netzwerk auf einen Switch patchen

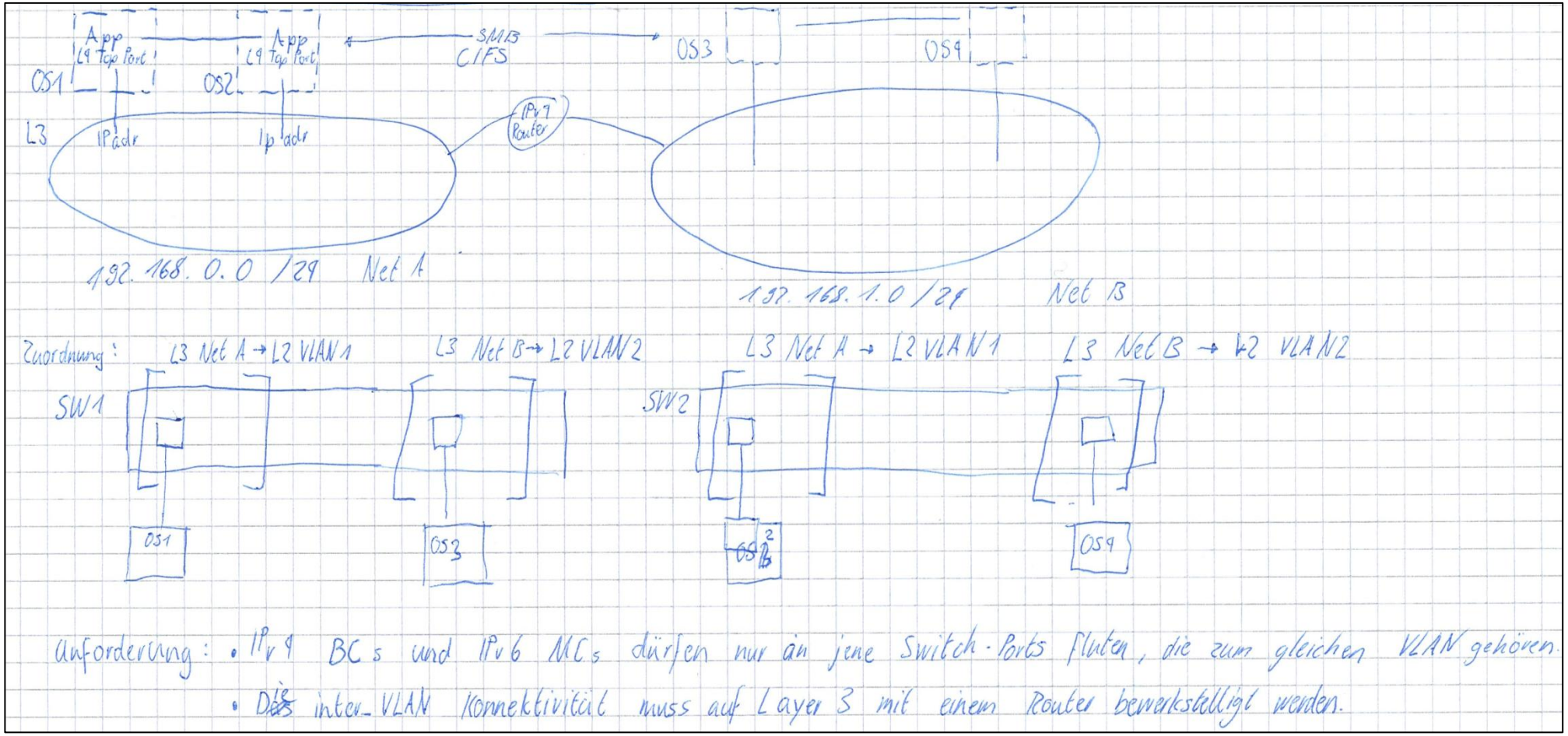


Abbildung 24: VLAN IP-Netzwerk auf einen Switch patchen

9.2.4 EEE 802.1q Tag – Ein- und Aus-taggen von Frames

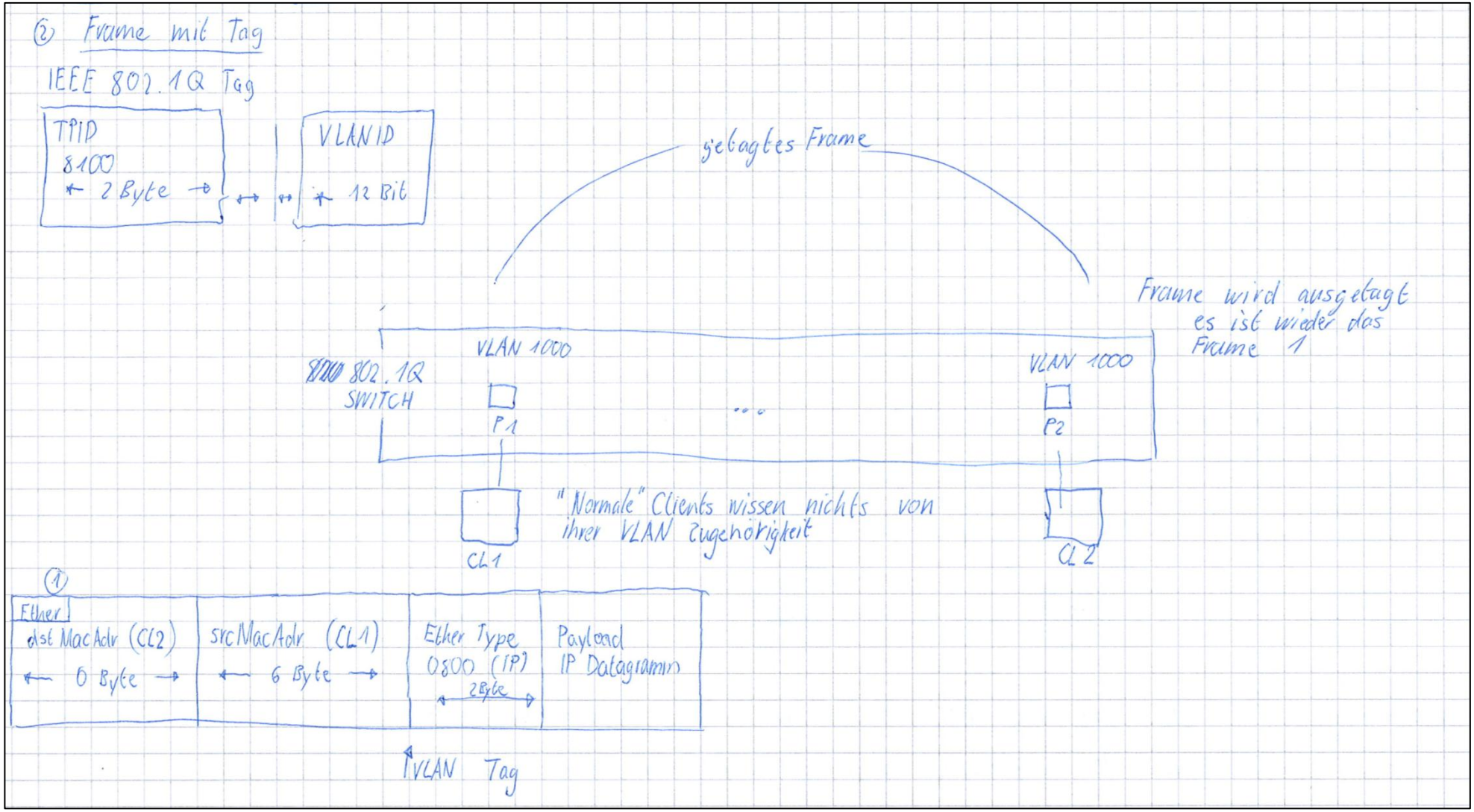


Abbildung 25: EEE 802.1q Tag – Ein- und Aus-taggen von Frames

9.2.5 Aufbau des VLAN Tags

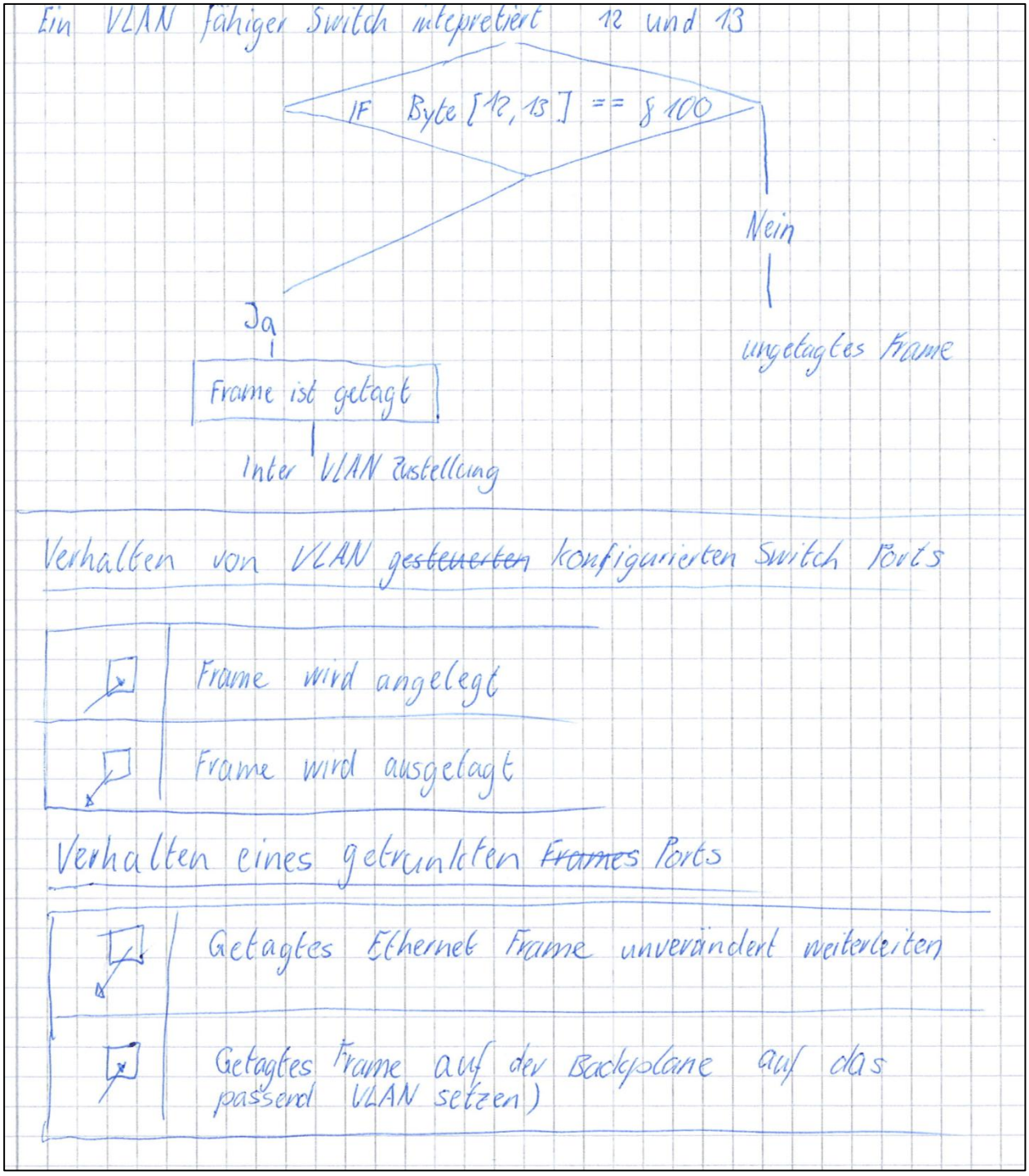


Abbildung 26: Aufbau des VLAN Tags

9.2.6 IEEE 802.1q VLAN- und IPv4-Teilnetzplanung

Im IPv4 Supernetz 192.168.12.0 /22 sollen

- 3 Client NW mit je 25%
- 1 Server NW mit12.5%
- 1 Management NW 6.25 %

liegen.

Bezeichnung	Anteil an Supernetz	IPv4 Addr	Broadcast	Gateway	VLAN-ID
Client NW 1	25%	192.168.12.0 /24	192.168.12.255/24	192.168.12.1	1224
Client NW 2	25%	192.168.13.0 /24	192.168.13.255/24	192.168.13.1	1324
Client NW 3	25%	192.168.14.0 /24	192.138.14.255/24	192.168.14.1	1424
Server NW 1	12.5%	192.168.15.0 /25	192.168.15.127 /25	192.168.15.1	1525
Management NW 2	6.25%	192.168.15.128 /26	192.168.15.191 /26	192.168.15.129	1526

192.168.12.0 /22 Supernetz

Besteht auf folgenden Teilnetzen:

- 192.168.12.0 /24
- 192.168.13.0 /24
- 192.168.14.0 /24
- 192.168.15.0 /24
- ~~192.168.16.0 /24~~ => wäre im nächsten Subnetz

9.2.7 Beispiel VLAN-Kommunikation

IP-Netz-Adr /SN	VLAN ID
192.168.8.0 /24	80
192.168.9 /24	90
192.168.10 /24	100

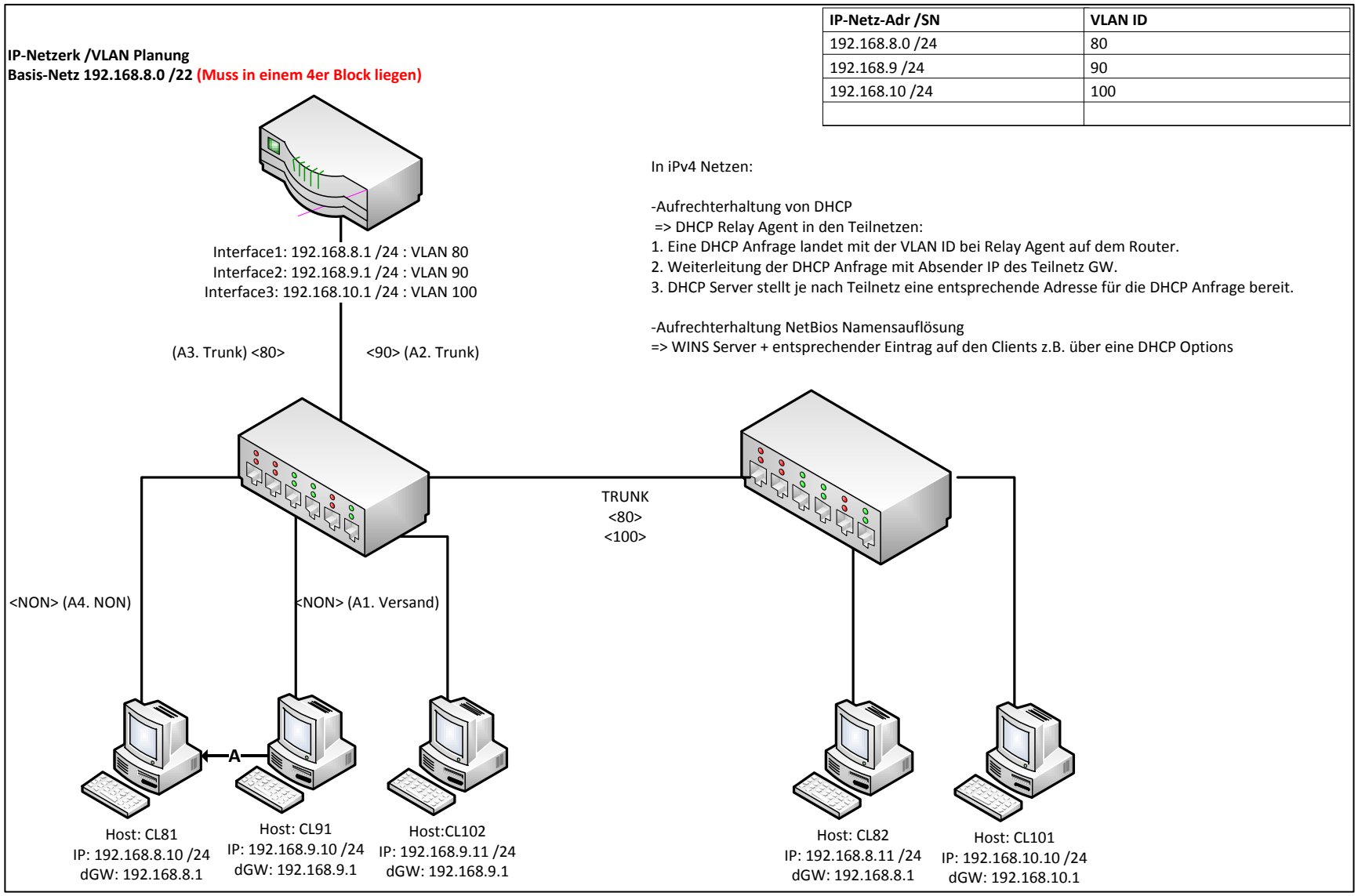


Abbildung 27: Beispiel VLAN Kommunikation

10 ICMP

Internet Control Message Protocol

- Protocol type: Transport layer control protocol.
- IP Protocol: 1

10.1 Beschreibung

ICMP ist ein erweiterbares Protokoll, das Funktionen zum Überprüfen von IP-Verbindungen umfasst. Es dient dazu Fehlermeldungen für Fehler auf dem Transport-Layer auszugeben.

Es besitzt folgende Eigenschaften:

- **Keine IP Verbesserung**
  - Mit ICMP wird IP nicht zuverlässiger
- **Keine Fehlerbehandlung**
  - Es gibt keine Richtlinien wie Fehler behandelt werden sollen
- **Unzuverlässig**
  - ICMP Nachrichten werden unzuverlässig übertragen
- **Erweiterbar**
  - ICMP kann um diverse Funktionen ergänzt werden

10.2 Paket

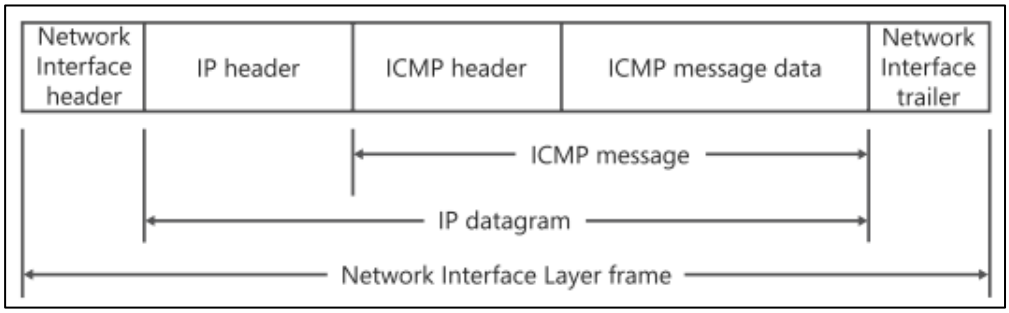


Abbildung 28: ICMP Paket

10.3 Header

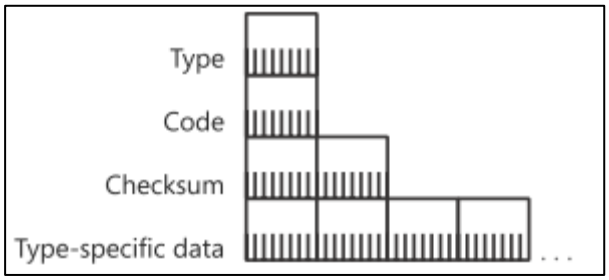


Abbildung 29: ICMP Header

10.3.1 Header fields

Field	Description
Typ	Typ der ICMP-Nachricht (siehe Kapitel: 10.3.2 ICMP Message Type)
Code	ICMP-Typ und Code bestimmen gemeinsam den Typ der Nachricht
Checksum	16-Bit Prüfsumme
Type-specific data	Optionale Daten für alle ICMP-Typen

10.3.2 ICMP Message Type

ICMP Type	Description
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect
8	Echo (also known as an Echo Request)
9	Router Advertisement
10	Router Solicitation
11	Time Exceeded
12	Parameter Problem

10.3.3 ICMP-Code von Type 3

Value	Description
0	Netzwerk nicht erreichbar
1	Host nicht erreichbar
2	Protokoll nicht erreichbar
3	Port nicht erreichbar
4	Fragmentierung erforderlich und DF festlegen
5	Quellroute fehlgeschlagen
6	Zielnetzwerk unbekannt
7	Ziel Host unbekannt
8	Quellhost isoliert
9	Kommunikation mit Zielnetzwerk administrativ untersagt
10	Kommunikation mit Ziel Host administrativ untersagt
11	Netzwerk für diesen Diensttyp (Type Of Service, TOS) nicht erreichbar
12	Host für diesen TOS nicht erreichbar
13	Kommunikation administrativ untersagt

10.4 Prozesse

- 10.4.1 Einbettung von ICMP im OSI-Modell
- 10.4.2 Verkapselung der ICMP-Nachricht
- 10.4.3 ICMP Pakete
- 10.4.4Prinzip von Tracert
- 10.4.5 Capture Filter für Whireshark
- 10.4.6 Beispiel ICMP Frames

10.4.1 Einbettung von ICMP im OSI-Modell

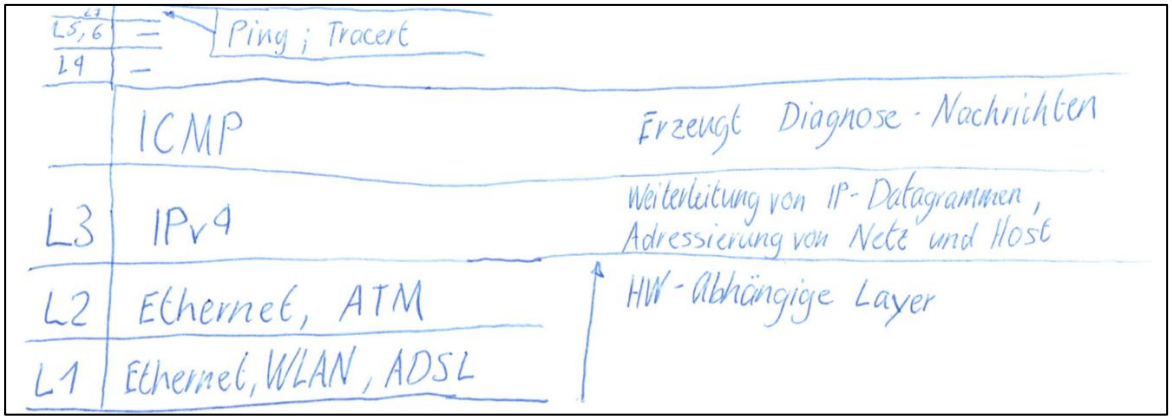


Abbildung 30: ICMP im OSI-Modell

10.4.2 Verkapselung der ICMP-Nachricht

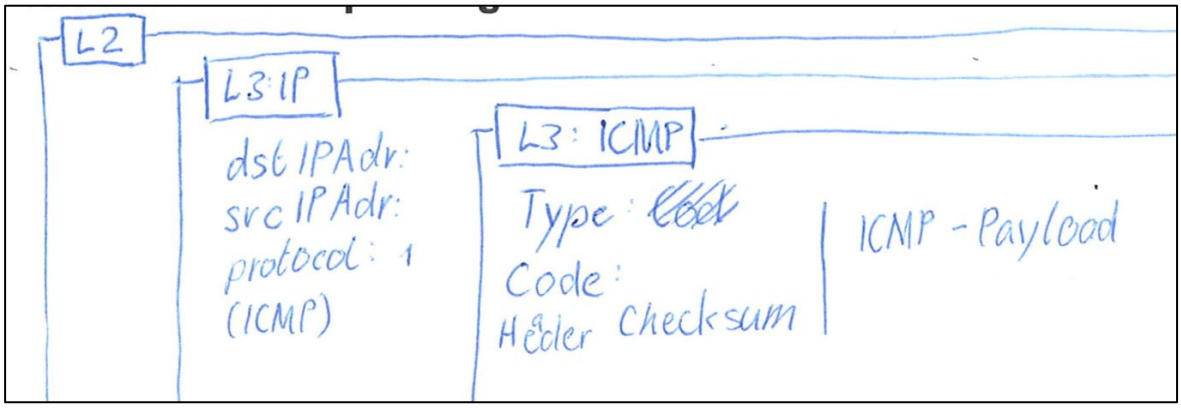


Abbildung 31: Verkapselung ICMP-Nachricht

10.4.3 ICMP Pakete

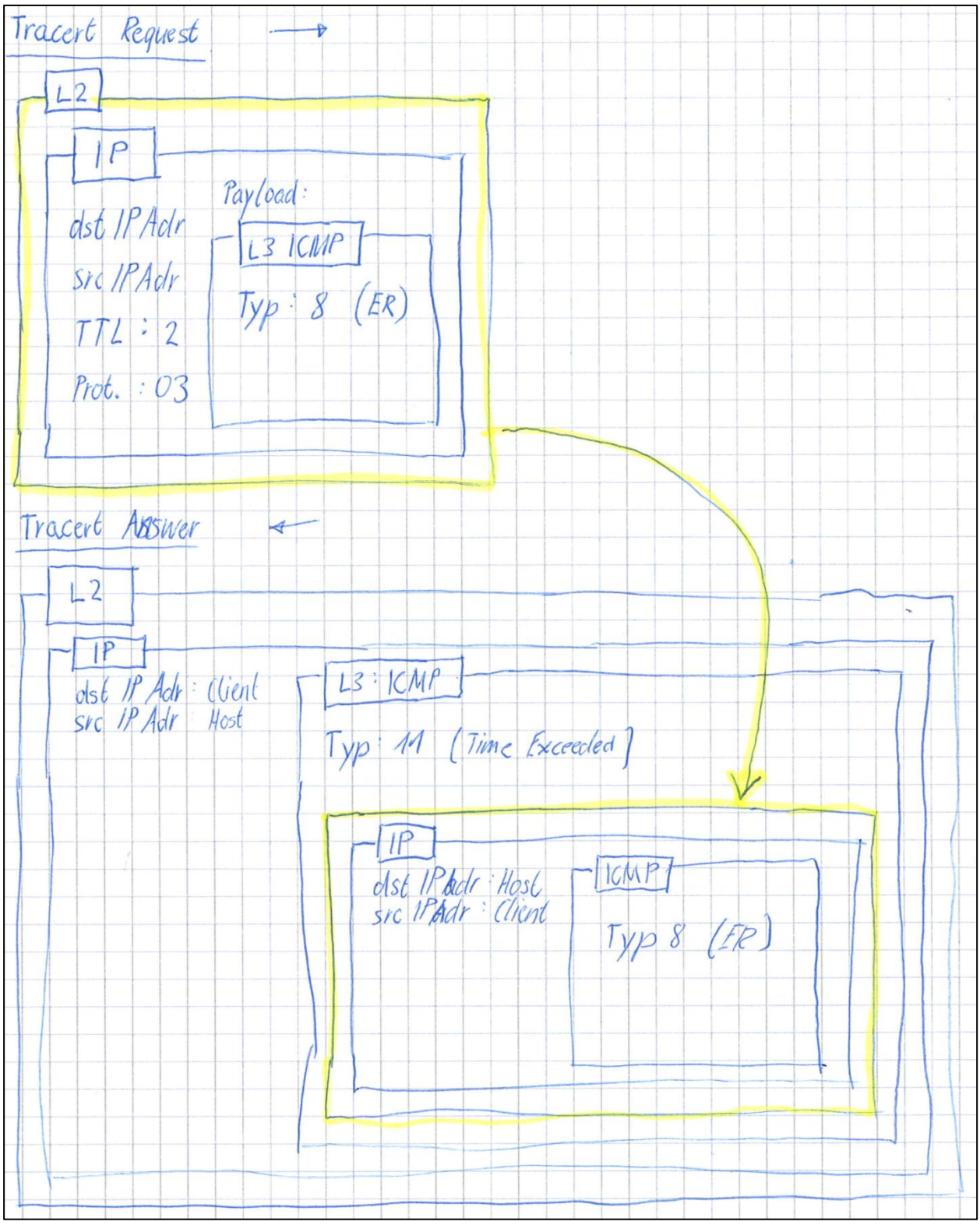


Abbildung 32: ICMP Tracert Paket

10.4.4 Prinzip von Tracert

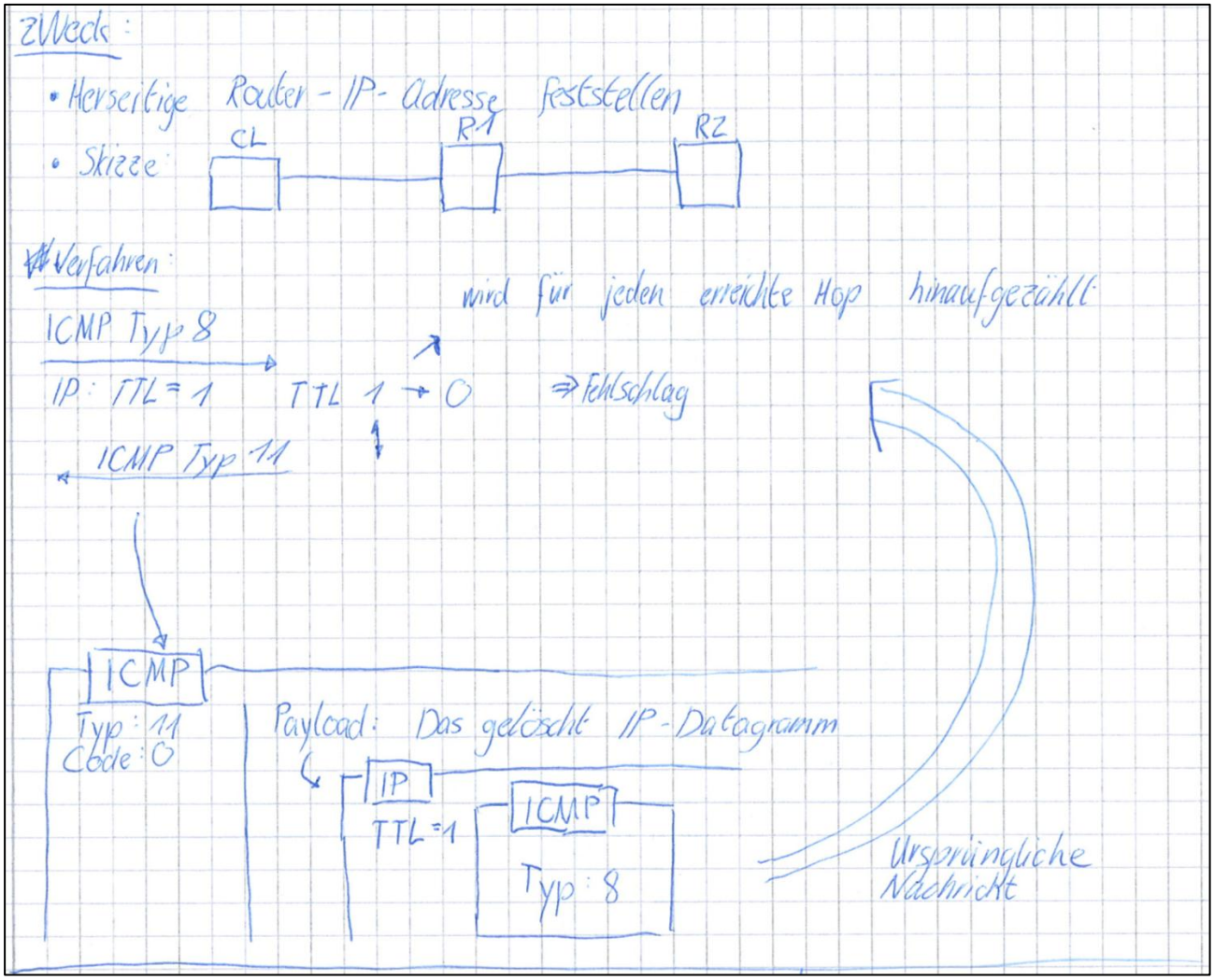


Abbildung 33: ICMP Prinzip von Tracert

10.4.5 Capture Filter für Whireshark

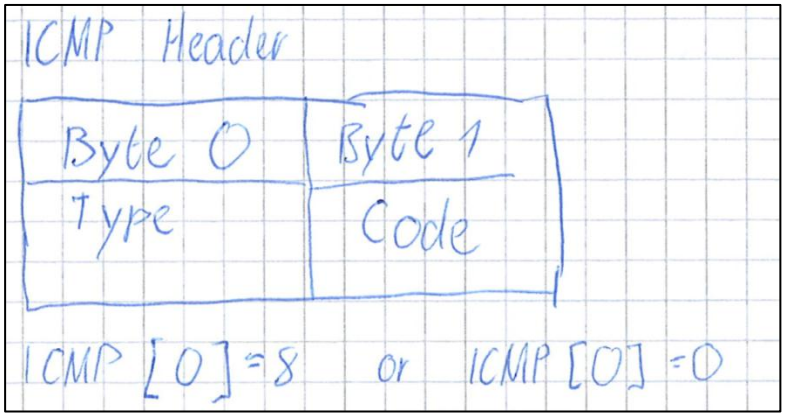


Abbildung 34: Capture Settings ICMP Whireshark

10.4.6 Beispiel ICMP Frames

10.4.6.1 ICMP-Echonachricht

```
  Frame:
+ Ethernet: Etype = Internet IP (IPv4)
- Ipv4: Next Protocol = ICMP, Packet ID = 35331, Total IP Length = 60
  + Versions: IPv4, Internet Protocol; Header Length = 20
  + DifferentiatedServicesField: DSCP: 0, ECN: 0
    TotalLength: 60 (0x3C)
    Identification: 35331 (0x8A03)
  + FragmentFlags: 0 (0x0)
    TimeToLive: 32 (0x20)
    NextProtocol: ICMP, 1(0x1)
    Checksum: 9898 (0x26AA)
    SourceAddress: 134.39.89.236
    DestinationAddress: 10.0.0.1
- Icmp: Echo Request Message, From 134.39.89.236 To 10.0.0.1
    Type: Echo Request Message, 8(0x8)
  - EchoReplyRequest:
     Code: 0 (0x0)
     Checksum: 7004 (0x1B5C)
     ID: 256 (0x100)
     SequenceNumber: 12544 (0x3100)
     ImplementationSpecificData: Binary Large Object (32 Bytes)
```

Abbildung 35: ICMP Echonachricht

10.4.6.2 ICMP Ziel nicht erreichbar – Host nicht erreichbar

```
  Frame:
+ Ethernet: Etype = Internet IP (IPv4)
- Ipv4: Next Protocol = ICMP, Packet ID = 31401, Total IP Length = 56
  + Versions: IPv4, Internet Protocol; Header Length = 20
  + DifferentiatedServicesField: DSCP: 0, ECN: 0
    TotalLength: 56 (0x38)
    Identification: 31401 (0x7AA9)
  + FragmentFlags: 0 (0x0)
    TimeToLive: 252 (0xFC)
    NextProtocol: ICMP, 1(0x1)
    Checksum: 47690 (0xBA4A)
    SourceAddress: 168.156.1.33
    DestinationAddress: 134.39.89.236
- Icmp: Destination Unreachable Message, 134.39.89.236
    Type: Destination Unreachable Message, 3(0x3)
  - DestinationUnreachable:
     Code: Host Unreachable 1(0x1)
     Checksum: 42914 (0xA7A2)
     Unused: 0 (0x0)
   - Data: Next Protocol = ICMP, Packet ID = 35331, Total IP Length = 60
    + Versions: IPv4, Internet Protocol; Header Length = 20
    + DifferentiatedServicesField: DSCP: 0, ECN: 0

          TotalLength: 60 (0x3C)
          Identification: 35331 (0x8A03)
        + FragmentFlags: 0 (0x0)
          TimeToLive: 28 (0x1C)
          NextProtocol: ICMP, 1(0x1)
          Checksum: 10922 (0x2AAA)
          SourceAddress: 134.39.89.236
          DestinationAddress: 10.0.0.1
          OriginalIPPayload: Binary Large Object (8 Bytes)
```

Abbildung 36: ICMP Ziel nicht erreichbar

10.5 Summary

ICM stützt sich auf eine Reihe von Nachrichten, um die Dienste bereitzustellen, die nicht Bestandteil von IP sind.

ICMP umfasst die folgenden Dienste:

- Diagnose
    - Echo Request
    - Echo Reply
- Fehleerberichte
    - ziel nicht erreichbar
    - Zeit abgelaufen
    - Quelle stilllegen
    - Umleitungsnachrichten
- Router Ermittlung
    - Router Ankündigung
    - Router Anforderung
- Erkennung IP-Headerproblemen
- Adressmaskenermittlung

11 SNMP

Simple Network Management Protocol

- Protocol type: Application layer network management protocol.
- Ethertype: 0x814C.
- Ports:
    - 161 (TCP, UDP) Server.
    - 162 (TCP, UDP) traps.
    - 5161 (TCP, UDP) over SSH.
    - 5162 (TCP, UDP) traps over SSH.

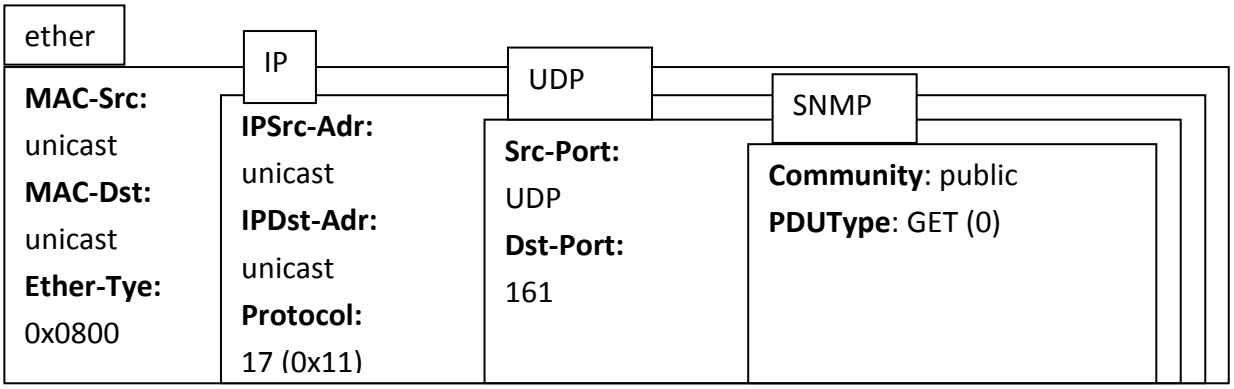
11.1 Beschreibung

SNMP ist ein Netzwerkverwaltungsprotokoll sowie eine Netzwerkverwaltungsinfrastruktur, die in IP-Netzwerken vielfach eingesetzt wird. Entwickelt wurde sie zuerst von Internetanwendern zur Überwachung von Routern und Bridges und zur Behebung technischer Probleme dieser Geräte. Mit SNMP können Netzwerkadministratoren Netzwerkgeräte (Arbeitsstationen bzw. Servercomputer, Router, Switches, Drahtloszugriffspunkte) verwalten.

SNMP eignet sich für folgende Zwecke:

- **Fernkonfigurierung von Netzwerkgeräten**
    - Konfigurieren Sie mit SNMP und einem zentralen Verwaltungscomputer über das Netzwerk Geräte.
- **Überwachung der Netzwerkleistung**
    - Fragen Sie mit SNMP systematisch und regelmäßig die Leistungszahlen von Geräten ab und überwachen Sie so den Netzwerkdurchsatz.
- **Erfassen von Netzwerkfehlern oder Zugriffsverletzungen**
    - Geräte können per SNMP bei Eintreten bestimmter Ereignisse Nachrichten versenden. Zu häufig auftretenden Störungen, die an Verwaltungssysteme gesendet werden, zählen das Herunterfahren und Neustarten von Geräten, nicht erstellte Router Verbindungen, Zugriffsverletzungen und Speicherplatzengpässe auf Dateiservern.

11.2 Frame



11.3 Prozesse

11.3.1 Management von Netzwerkgeräten

11.3.2 SNMP-Server-Client Architektur

0

MIB

11.3.4 OID

11.3.1 Management von Netzwerkgeräten

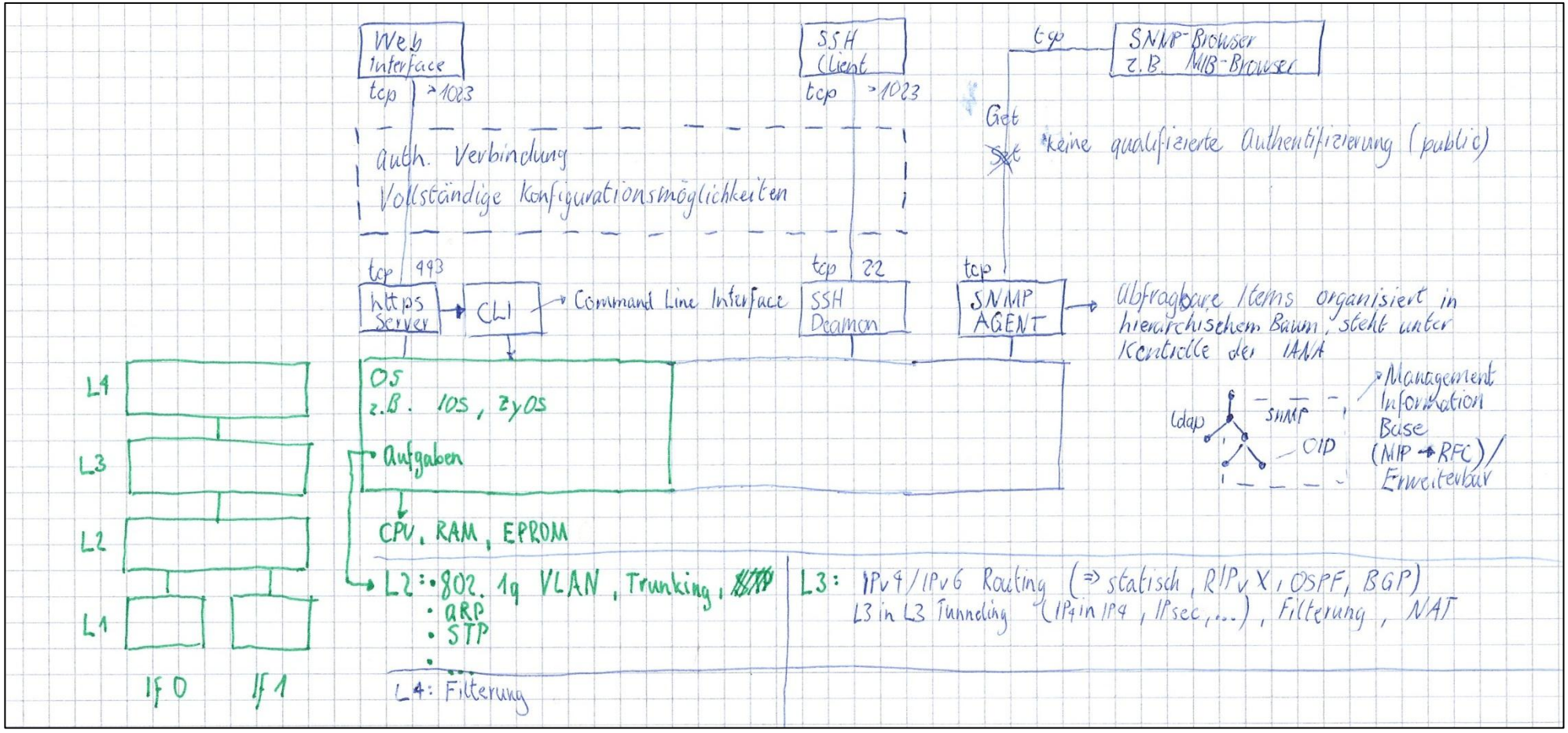


Abbildung 37: SNMP Management von Netzwerkgeräten

11.3.2 SNMP-Server-Client Architektur

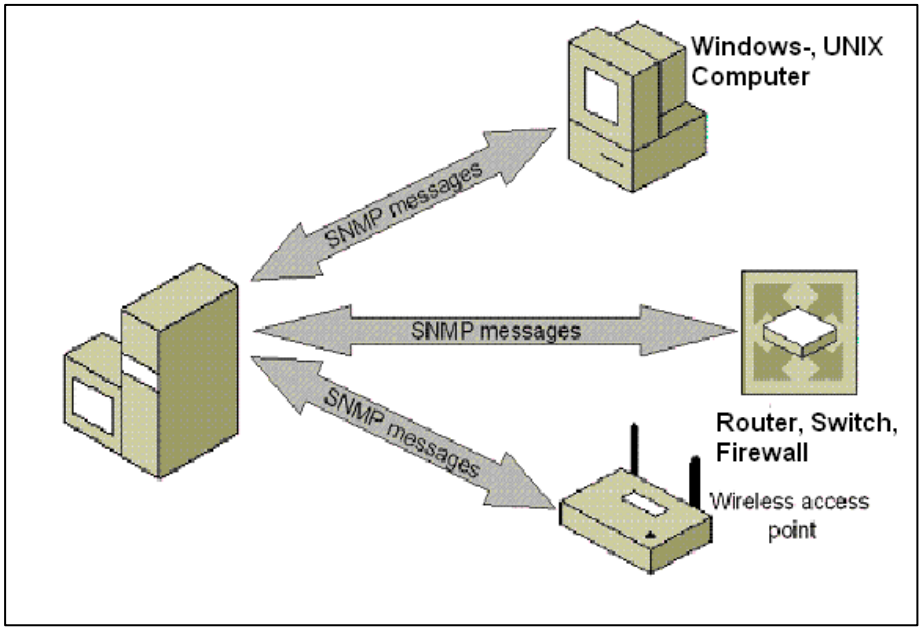


Abbildung 38: SNMP Client-Server-Architektur

Aus welchen beiden Komponenten besteht die SNMP-Server-Client Architektur?

Bezeichnung	Aufgabe
Agent (auf SNMP-fähigen Clients: Switch, Router, Server,...)	Stellt die Werte gemäss MIB oder eigener MIB-Erweiterung am UDP-Port 161 zur Verfügung Kann über UDP-Port 162 Traps aussenden (Client-Software für SNMP)
SNMP-Management System	Auf der Basis der Standard MIB2 und den Agent-typischen Erweiterungen kann das System: • die eingetragenen Agents periodisch abfragen • auf den eingetragenen Agents Werte setzen • von den eingetragenen Agents Traps empfangen Zudem kann das System die Daten darstellen und oder gar archivieren.

11.3.3 MIB

Manage Information Base

Die IANA definiert in zwei RFCs den plattformübergreifend gültigen Umfang der MIB:

- in einer Basisversion (einfach als MIB bezeichnet)
- und für einen erweiterten und heute allgemein verwendeten Umfang, der als MIB-2 bezeichnet wird.

Ergänzen Sie die folgende Tabelle:

MIB-Version	RFC-Nr	Titel des RFC
MIB	1212	Concise MIB Definition
MIB-2	1213	Management Information Base for Network Management of TCP/IP-based internets: MIB-II

11.3.4 OID

Die einzelnen Informationsinhalte der MIB werden als Objekte bezeichnet.

Die Objekte werden in einer baumartig aufgebauten Hierarchie abgelegt. Durch diese Art der Gliederung wird das Informationssystem praktisch unendlich erweiterbar.

Die einzelnen Informationsobjekte tragen Nummern.

Das MIB-Objekt für die SNMP-Information „sysUpTime“ hat die Nummer 1.3.6.1.2.1.1.3.0.

Diese MIB-Objektnummern werden als OID (Object-Identifier) bezeichnet.

Die IANA verwaltet im gleichen Inforationsbaum nicht nur die OIDs für SNMP sondern auch noch für das Directory-System LDAP, das z.B. von Active Directory eingesetzt wird.

Hier ein Beispiel eines OID-Trees:

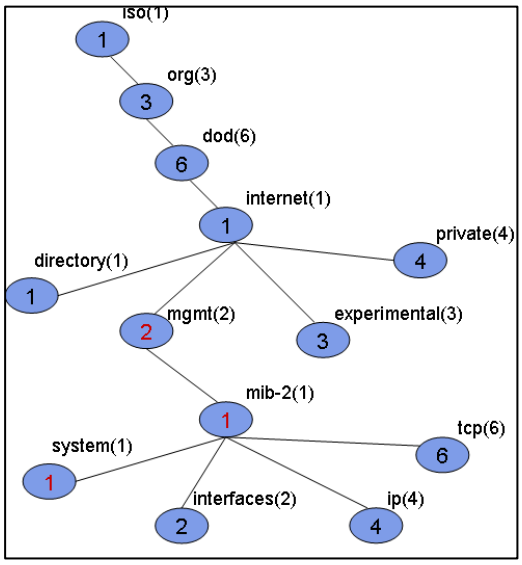


Abbildung 39: SNMP OID Tree

Und hier einige OIDs:

MIB-2 Bezeichnung	MIB-2 OID	Beschreibung
sysDescr	1.3.6.1.2.1.1.1	Systembeschreibung
sysObjectID	1.3.6.1.2.1.1.2	Hersteller-abhängige Id
sysUPTime	1.3.6.1.2.1.1.3	Zeit, seit dem letzten Bootvirgang
sysContact	1.3.6.1.2.1.1.4	Name einer Person, die für das Gerät zuständig ist.

12 RADIUS

Remote Authentication Dial-In User Service

- Protocol type: Application layer protocol.
- Ports:
  - 1646 (UDP) obsolete.
  - 1812 (UDP) Server.
  - 1813 (UDP) accounting.
  - 3799 dynamic authorization.

12.1 Beschreibung

RADIUS ist ein Client/Server-Protokoll, das Authentifizierungs-, Autorisierungs-, Konfiguration- und Abrechnungsinformation zwischen einem Netzwerkzugriffsserver (Network Access Server) und einem zentralisierten Server überträgt.

Netzwerkzugriffsserver umfassen beispielsweise IEEE 802.11-Drahtloszugriffspunkte und Server, die über RAS-Verbindungen den Zugriff auf ein Firmennetzwerk oder das Internet ermöglichen.

12.2 Data – RADIUS – Nachrichtenstruktur

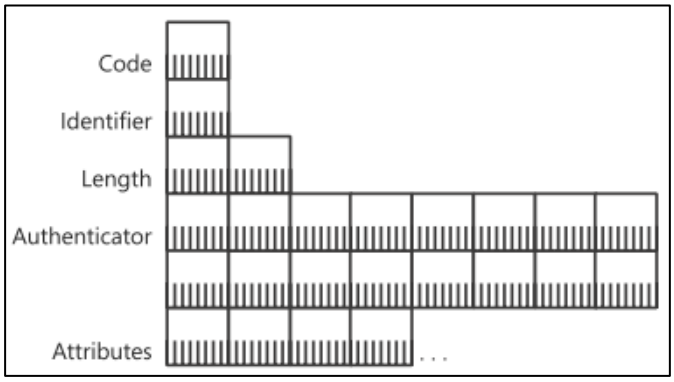


Abbildung 40: RADIUS Nachrichtenstruktur

12.2.1 Data fields

Field	Description
Code	RADIUS Nachrichtentyp
Identifier	Identifiziert den RADIUS-Nachrichtenaustausch
Length	Gibt die Länge der RADIUS-Nachricht an
Authenticator	RADIUS-Client authentifiziert die RADIUS-Antwort anhand dieser Information

12.2.2 Code values

Code	Message
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge

12.3 Frame – Access Request

```
  Frame:
+ Ethernet: Etype = Internet IP (IPv4)
+ Ipv4: Next Protocol = UDP, Packet ID = 30882, Total IP Length = 277
- Udp: SrcPort = 3065, DstPort = 1812, Length = 257
    SourcePort: 3065, 3065(0xbf9)
    DestinationPort: 1812, 1812(0x714)
    TotalLength: 257 (0x101)
    Checksum: 42833 (0xA751)
- Radius: Access Request, Id = 12, Length = 249
    MessageType: Access Request, 1(0x01)
    Identifier: 12 (0xC)
    AllLength: 249 (0xF9)
    Authenticator: DB 60 44 6A  2B 19 83 57  FF 75 F1 1D  19 2C 1A 7F
  + AttributeNasIPAddress: 10.10.1.150
  + AttributeServiceType: Framed, 2(0x2)
  + AttributeFramedProtocol: PPP, 1(0x1)
  + AttributeNasPort: 128
  + AttributeVendorSpecific:
  + AttributeVendorSpecific:
  + AttributeRadiusNASPortType: Virtual, 5(0x5)
  + AttributeTunnelType: Point-to-Point Tunneling Protocol (PPTP), 1(0x1)
  + AttributeTunnelMediumType: IPv4, 1(0x1)
  + AttributeStationID: 10.10.1.62
  + AttributeTunnelClientEndpoint:
  + AttributeVendorSpecific:
  + AttributeVendorSpecific:
  + AttributeUserName: KAPOHO\tfl
  + AttributeVendorSpecific:
  + AttributeVendorSpecific:
```

Abbildung 41: RADIUS Access Request

12.4 Summary

Alle RADIUS-Nachrichten verwenden eine einheitliche Struktur, die aus einem Abschnitt fester Grösse und einem Abschnitt variabler Grösse besteht. Der Abschnitt fester Grösse enthält Feder, die in allen RADIUS-Nachrichten vorkommen. Der variable Abschnitt enthält RADIUS-Attribute, bei denen es sich um Standardattribute oder anwenderspezifische Attribute handeln kann.

RADIUS-Attribute enthalten Daten, die für die Authentifizierung, Autorisierung und Abrechnung des Netzwerkzugriffs verwendet werden.

13 IPIP (und IP)

IP in IP tunneling

- Protocol type: Transport layer protocol.
- IP Protocol: 4
- IPSec: IP-Protocol: 50
- IPv6 in IPv4 Tunneling: IP Protocol: 41

13.1 Beschreibung

Mit dem IP-Tunneling erfahren werden IP-Datagramme von einem Netzwerk über ein Zwischennetzwerk an ein anderes Netzwerk übertragen, damit können die folgenden wichtigen Zwecke erreicht werden:

- Transparenz: Transparente Verknüpfung von RFC 1918 Netzwerken über das 0.0.0.0 /0 Netzwerk
- Erweiterte Sicherheit: Schutz der Vertraulichkeit und Integrität mit IPsec
- IPv6: Verbindung von global adressierten IPv6 Netzwerken über das 0.0.0.0 /0 Netzwerk

13.2 Prozesse

- 13.2.1RFC 1918 Netzwerk
- 13.2.2IP in IP tunneling nach RFC 1853

13.2.1 RFC 1918 Netzwerk

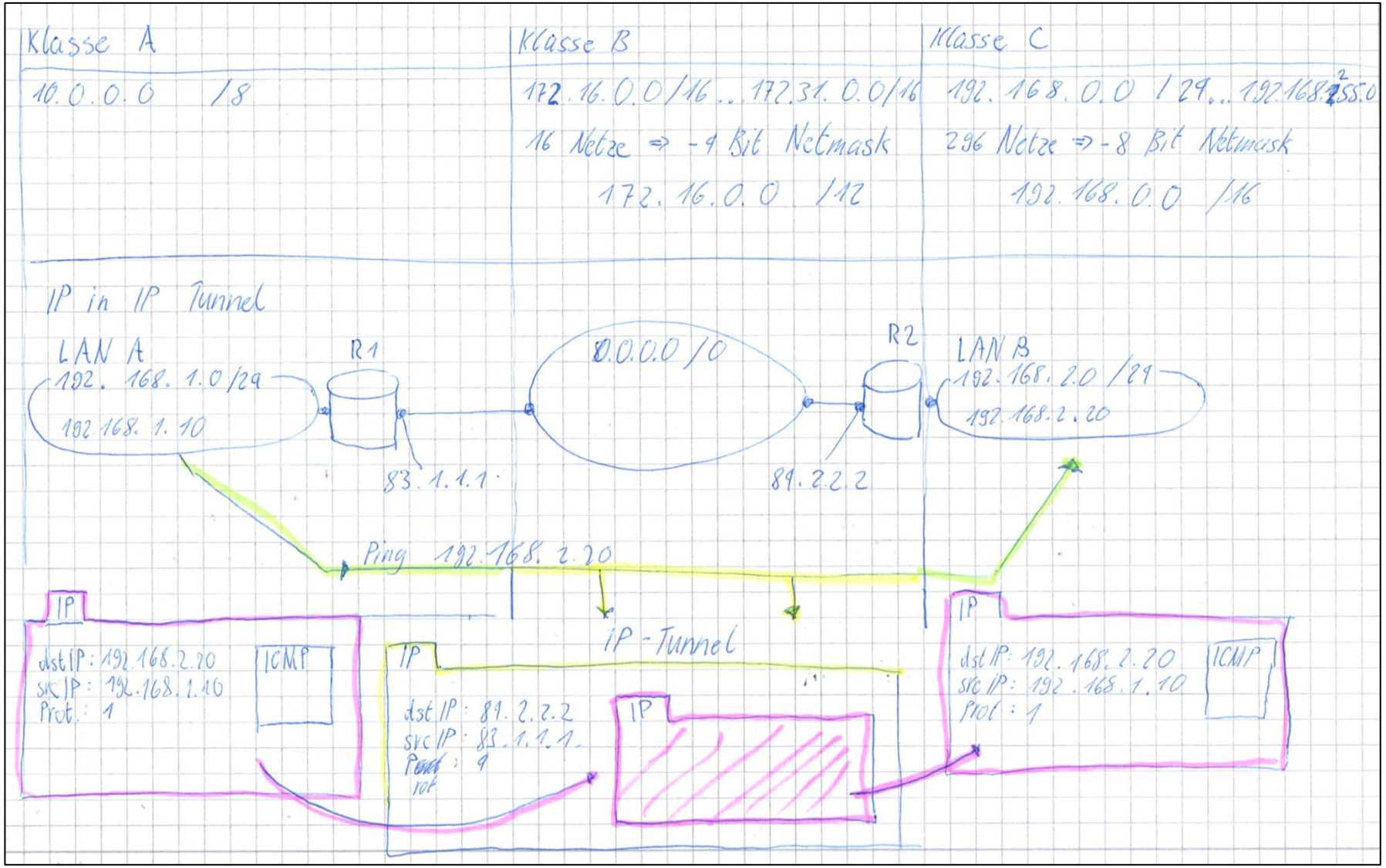


Abbildung 42: RFC 1918 Netzwerk

13.2.2 IP in IP tunneling nach RFC 1853

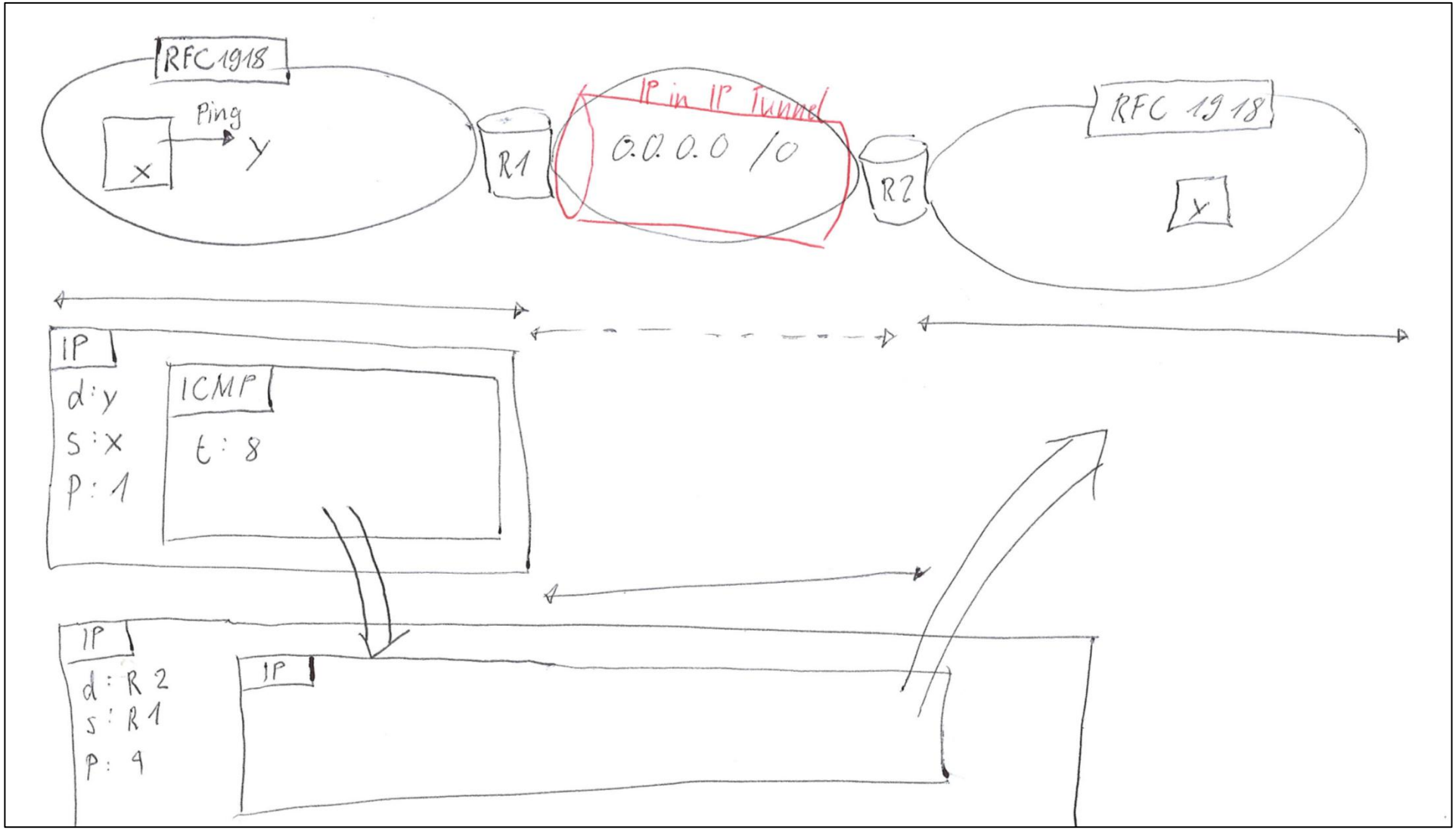


Abbildung 43: IPIP nach RFC 1853

14 IPSec

Internet Protocol Security

14.1 Beschreibung

IPSec kapselt die I-Nutzlast mit einem zusätzlichen Header oder Trailer ein, der die Informationen enthält, die sowohl für die Authentifizierung der Datenquelle und den Schutz vor Wiederholungsangriffen als auch zum Sicherstellen der Datenintegrität und der Vertraulichkeit der Daten erforderlich sind.

Der IPSec-Header umfasst folgende Elemente:

- AH (Siehe Kapitel: 15)
- ESP (Siehe Kapitel: 16)

Mit diesen Elementen kann ein IP-Datagramm in ein sicheres Datagramm umgewandelt werden.

Wichtigste Merkmale von IPSec:

- **Vertraulichkeit**
  - Verschlüsselung mit symmetrischen Schlüssen.
  - Verfahren: 3DES, AES, …
  - Erzeugen des Vorschlüssels mit DH
- **Integrität:**
  - Erkennen von Veränderungen während dem Transport
  - Verfahren: Hash-Bildung mit MD5/SHA256
- **Authentifizierung der Tunnelendpunkte**
  - Verfahren:
    - PSK
    - Zertifikate
    - Kerberos
    - EAP (Siehe Kapitel: 6 EAP)
- **Key Management**
  - Vor Nutzlastübertragung erfolgt Security Assozation (SA Aushandlung über UDP 500, Periodische Schlüsselerneuerung (Problematisch hinter NAT))

14.1.1 IPSec Schutzmethoden

IPSec bietet zwei Schutzmethoden:

- **Transportmodus:**
  - Der Transportmodus wird normalerweise zur Gewährleistung der durchgehenden Sicherheit für die Kommunikation zwischen zwei IPSec-Kommunikationspartner verwendet.
  - Dieser Modus schützt IP-Pakete, indem zwischen dem ursprünglichen IP-Datagramm und dessen Nutzlast ein zusätzlicher Header oder trailer eingefügt wird.
  - Der Transportmodus wird meist innerhalb eines Unternehmens eingesetzt.
- **Tunnelmodus**
  - Der Tunnelmodus wird normalerweise von Netzwerkroutern verwendet, um IP-Datagramme zu schützen, wenn der Datenverkehr über ein nicht geschütztes Verbindungsnetzwerk weiter geleitet wird.
  - Dieser Modus schützt das gesamte IP-Datagramm, indem dieses mit einem IPSec-Header oder Trailer und einem zusätzlichen IP-Header eingekapselt wird.
  - Der Tunnelmodus wird meist ausserhalb eines Unternehmens verwendet, wenn mehrere Standorte über ein öffentliches Netzwerk, beispielsweise das Internet, miteinander verbunden sind.

14.2 Prozesse

- 14.2.1 IPSec Protokoll-Suite verschlüsseltes Tunneling nach RFC 2401
- 14.2.2 Grundidee des Diffie Hellman Verfahrens
- 14.2.3 X.509 Zertifikat und Ausgabestelle
- 14.2.4 X.509 Zertifikats basierte Authentifizierung

14.2.1 IPSec Protokoll-Suite verschlüsseltes Tunneling nach RFC 2401

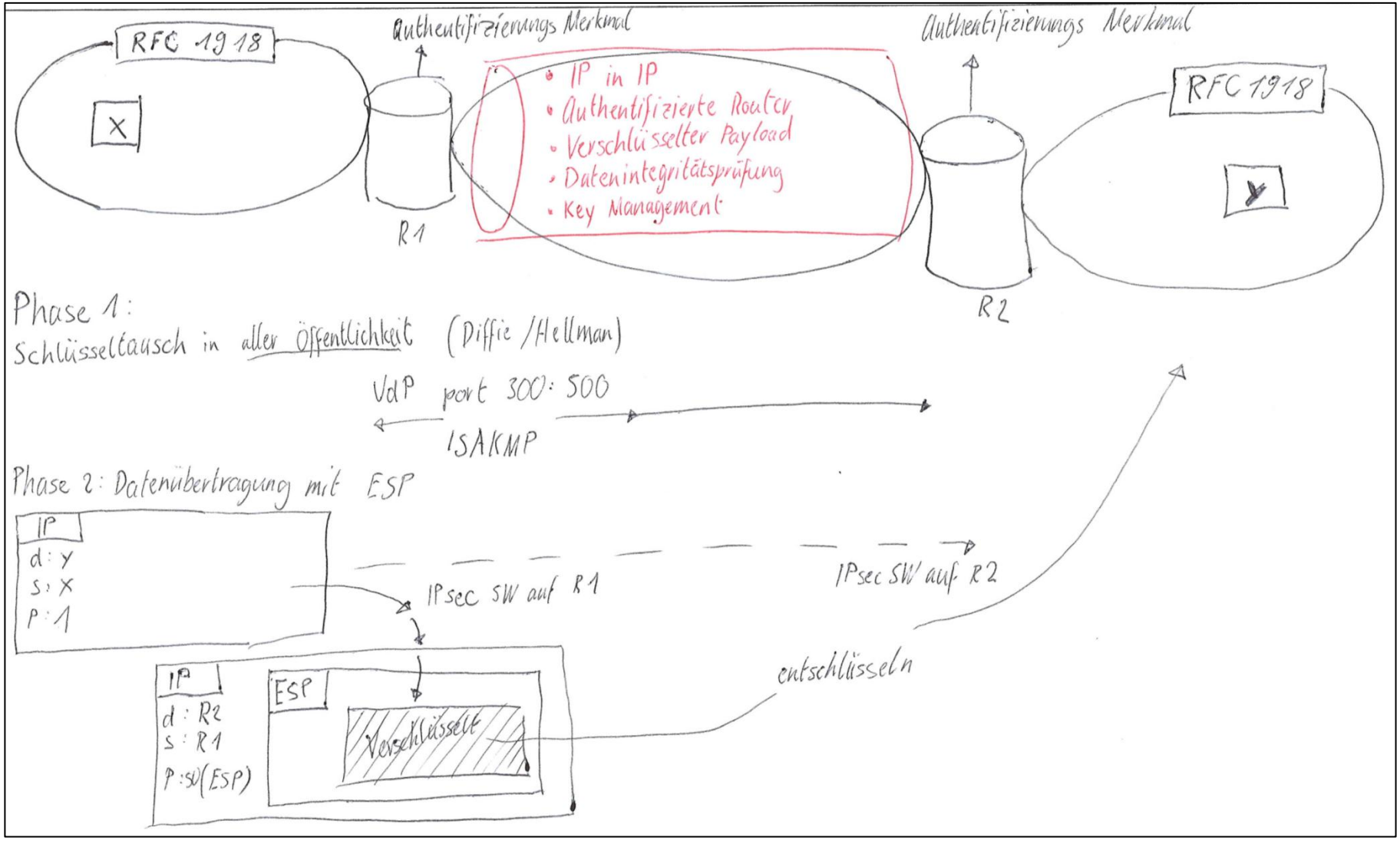


Abbildung 44: IPSec Protokoll-Suite verschlüsseltes Tunneling nach RFC 2401

14.2.2 Grundidee des Diffie Hellman Verfahrens

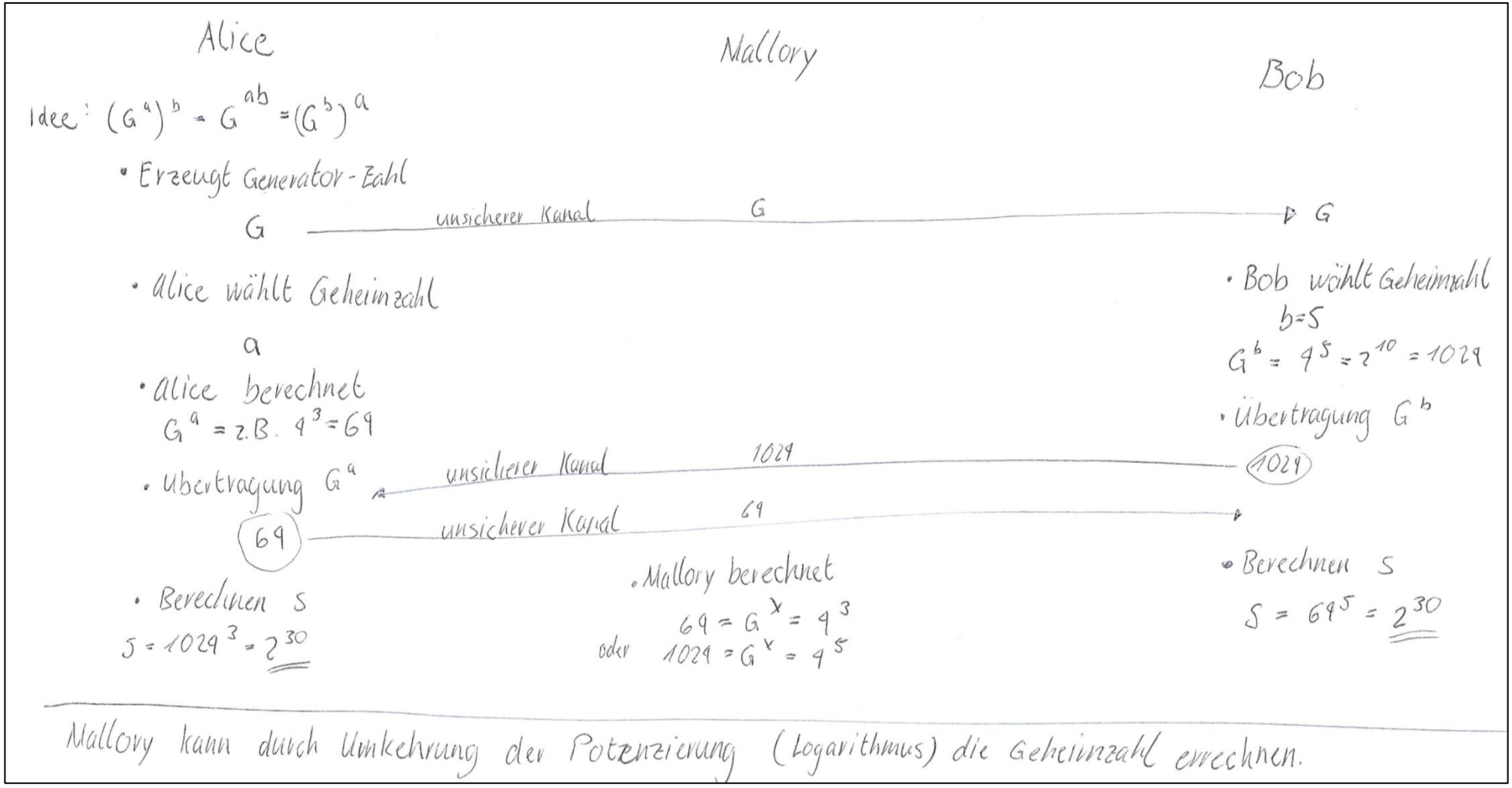


Abbildung 45: Grundidee des DH-Verfahrens

14.2.3 X.509 Zertifikat und Ausgabestelle

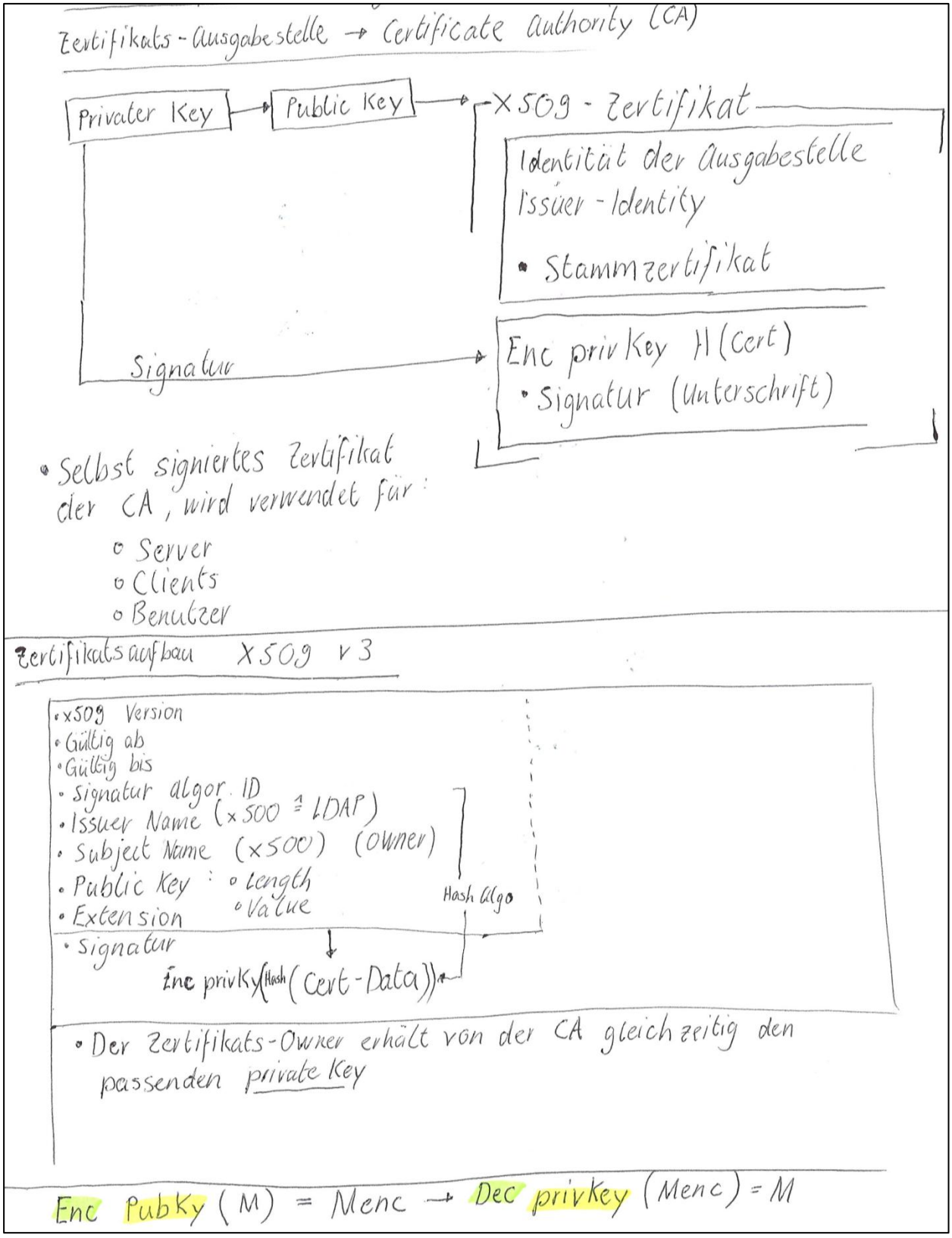


Abbildung 46: X.509 Zertifikat und Ausgabestelle

14.2.4 X.509 Zertifikats basierte Authentifizierung

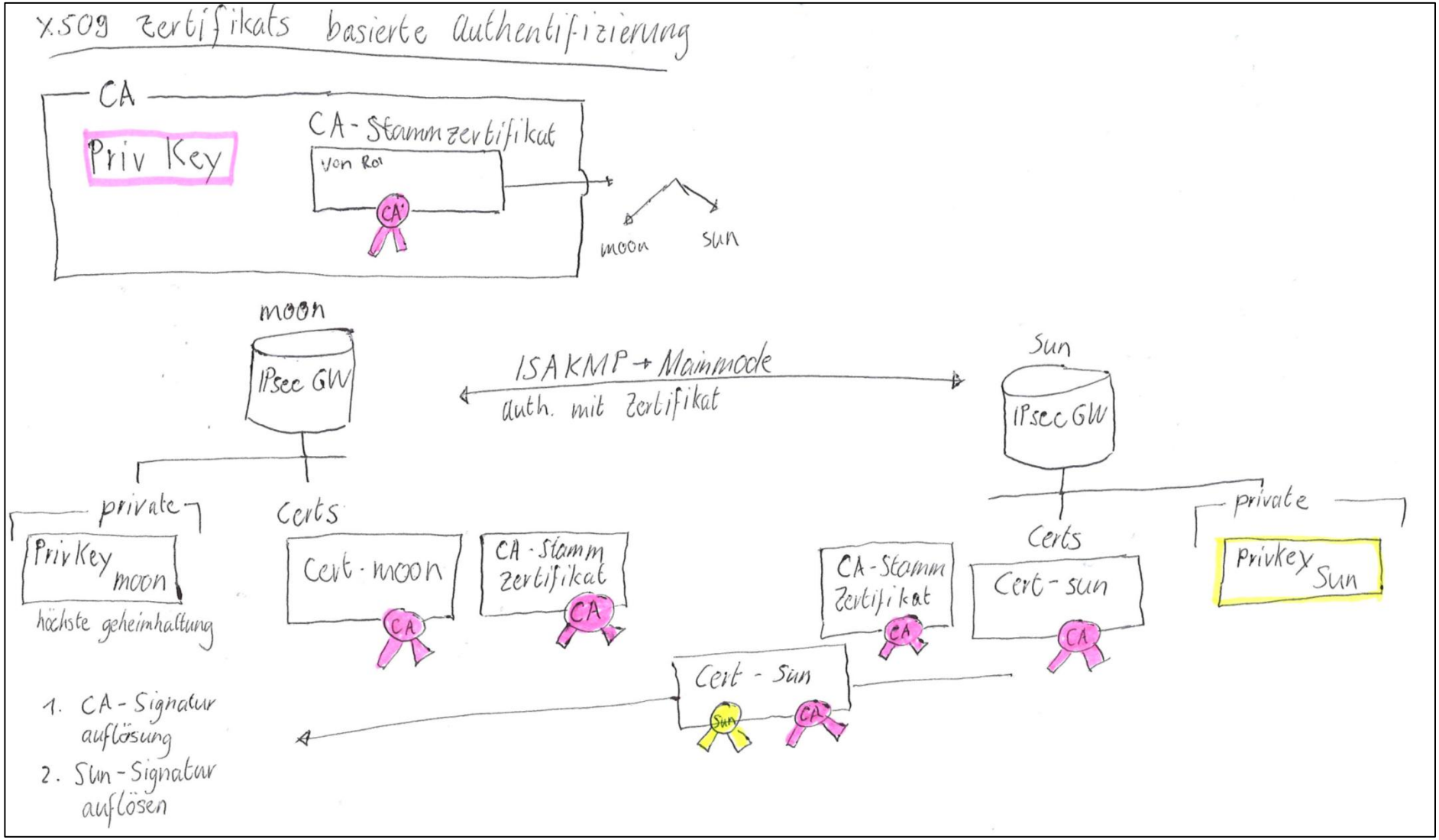


Abbildung 47: X.509 Zertifikats basierte Authentifizierung

14.2.5 Beispiel Tunneling von ICMP Paket

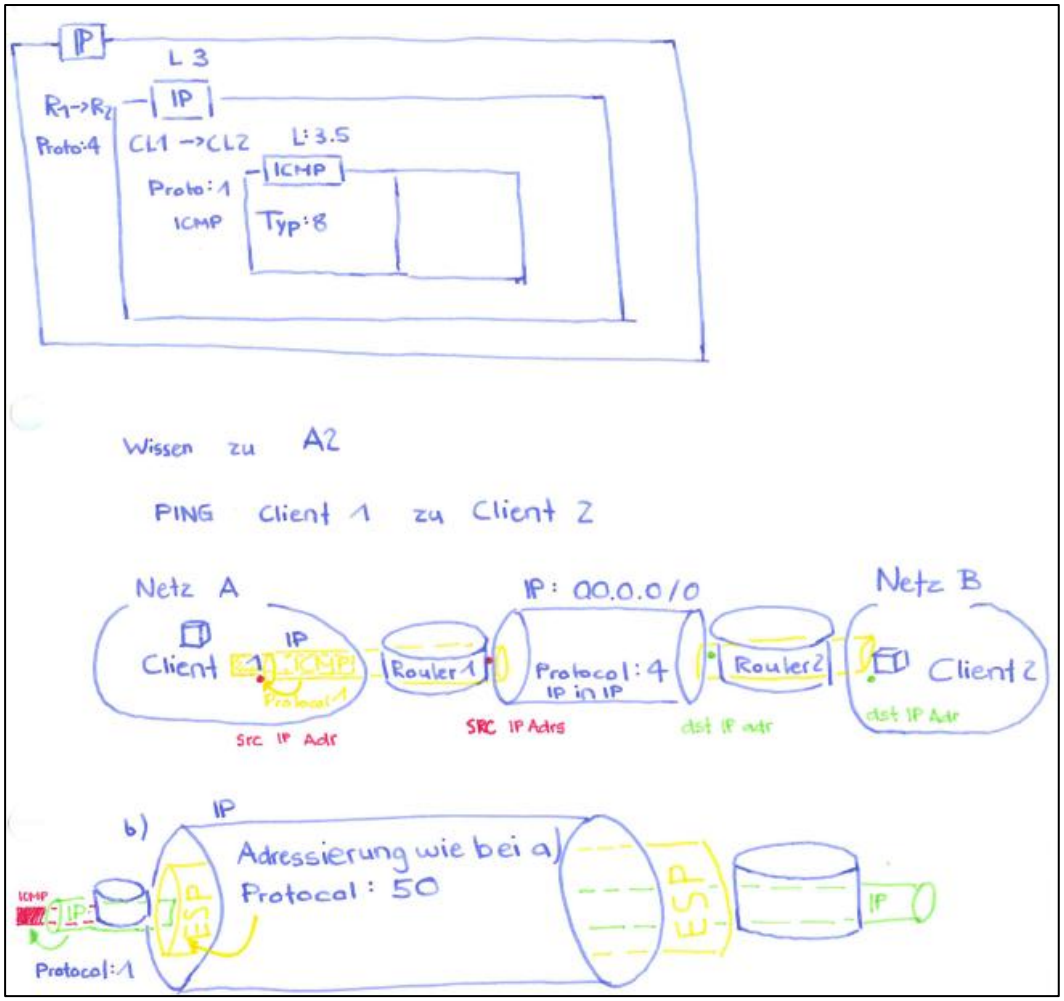


Abbildung 48: Beispiel IPSec Tunneling ICMP Paket

14.3 Summary

IPSec ist eine Standardmethode zum Bereitstellen des kryptographischen Schutzes für IP-Pakete.

Zum Schutz von IP-Paketen werden die beiden Protokolle AH und ESP eingesetzt.

AH stellt die Authentifizierung der Datenquelle, die Datenintegrität und den Wiederholungsschutz für das gesamte IP-Paket bereit.

ESP stellt die Authentifizierung der Datenquelle, die Datenintegrität, die Datenvertraulichkeit und den Wiederholungsschutz für die ESP-eingekapselte Nutzlast bereit.

Zum Aushandeln von Sicherheitszuordnungen für den sicheren Datenverkehr verwendet IPSec IKE, eine Kombination aus ISAKMP und dem Oakley-Schlüsselbestimmungsprotokoll.

Die Hauptmoduls-Aushandlung bestimmt die ISAKMP-Sicherheitszuordnung, mit der alle Schnellmoduls-Aushandlungen geschützt werden.

Die Schnellmodus-Aushandlung bestimmt die IPSec-Sicherheitszuordnungen für den Schutz eingehender und ausgehender Daten.

15 AH

Authentication Header

- Protocol type: Transport layer authentication protocol.
- IP Protocol: 51

15.1 Beschreibung

Der AH-Header stellt die Authentifizierung der Datenquelle, die Datenintegrität und den Wiederholungsschutz für das gesamte IP-Datagramm sicher.

15.2 Header

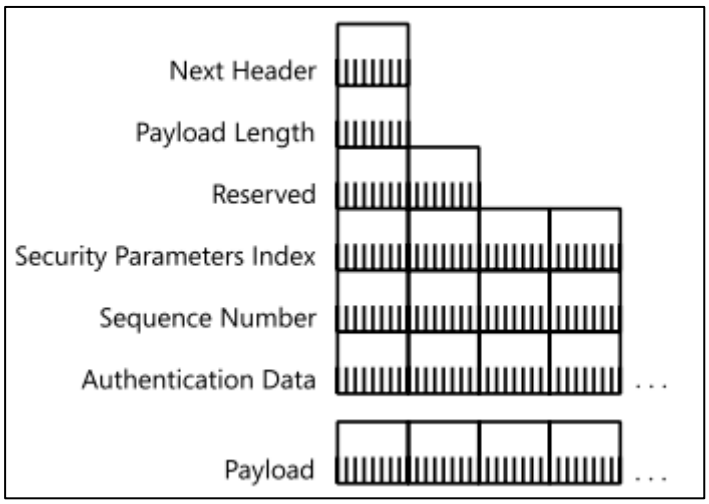


Abbildung 49: IPSec Authentication Header

15.2.1 Header fields

Field	Description
Next Header	Ist gleich dem Wert von Protokoll im IP-Header
Security Parameters Index	gibt die SA an
Authentication Data	Enthält ICV-Berechnung des Absenders

15.3 AH-Transportmodus

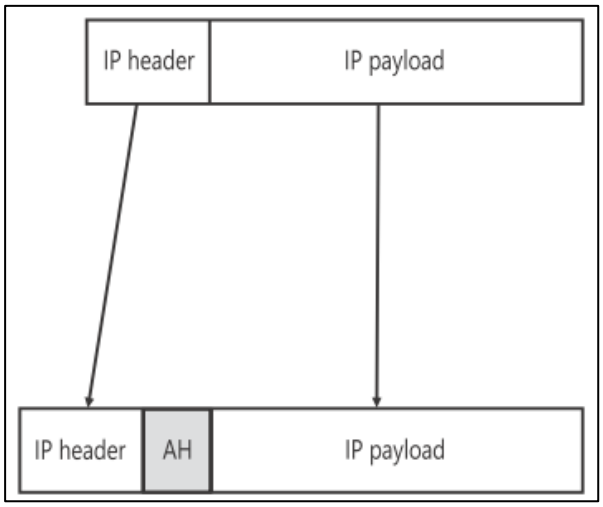


Abbildung 50: AH-Transportmodus

Der AH-Header wird unmittelbar nach dem IP-Header in das IP-Datagramm eingefügt.

15.4 AH-Transportmodus Frame

```
   Frame:
 + Ethernet: Etype = Internet IP (IPv4)
 - Ipv4: Next Protocol = AH, Packet ID = 1807, Total IP Length = 86
   + Versions: IPv4, Internet Protocol; Header Length = 20
   + DifferentiatedServicesField: DSCP: 0, ECN: 0
     TotalLength: 86 (0x56)
     Identification: 1807 (0x70F)
   + FragmentFlags: 0 (0x0)
     TimeToLive: 128 (0x80)
     NextProtocol: AH, 51(0x33)
     Checksum: 11405 (0x2C8D)
     SourceAddress: 131.107.0.2
     DestinationAddress: 131.107.0.1

- Ah: Next Protocol = UDP, SPI = 0x48B7D428, Seq = 0x1
    NextHeader: UDP, 17(0x11)
    PayloadLength: 24 bytes
    Reserved: 0 (0x0)
    SecurityParametersIndex: 1220006952 (0x48B7D428)
    SequenceNumber: 1 (0x1)
    AuthenticationData: 12 UINT8(s)
+ Udp: SrcPort = 50286, DstPort = DNS(53), Length = 42
+ Dns: QueryId = 0xDE8D, QUERY (Standard query), Query  for  test.contoso.com of type Host A
ddr on class Internet
```

Abbildung 51: AH-Transportmodus Frame

15.5 AH-Tunnelmodus

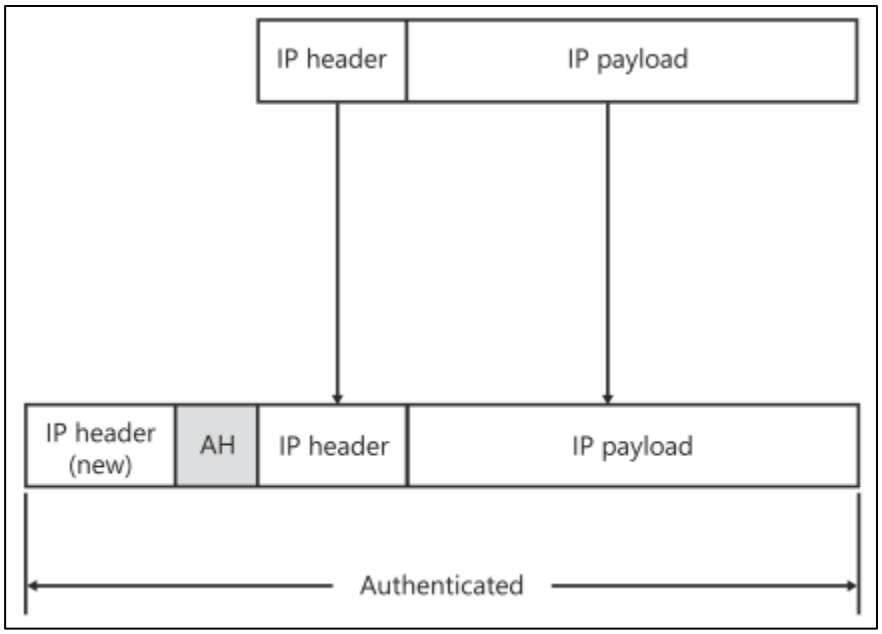


Abbildung 52: AH-Tunnelmodus

Im AH-Tunnelmodus schützt der AH-Header das gesamte ursprüngliche IP-Paket (sowohl den IP-Header wie auch die Nutzlast).

16 ESP

Encapsulating Security Payload

- Protocol type: Transport layer protocol.
- IP Protocol: 50

16.1 Beschreibung

ESP besteht aus einem Header und einem Trailer, die die Authentifizierung der Datenquelle, die Datenintegrität, den Wiederholungsschutz und die Vertraulichkeit der Daten für den ESP-eingekapselten Abschnitt des Pakets sicherstellen.

16.2 Header

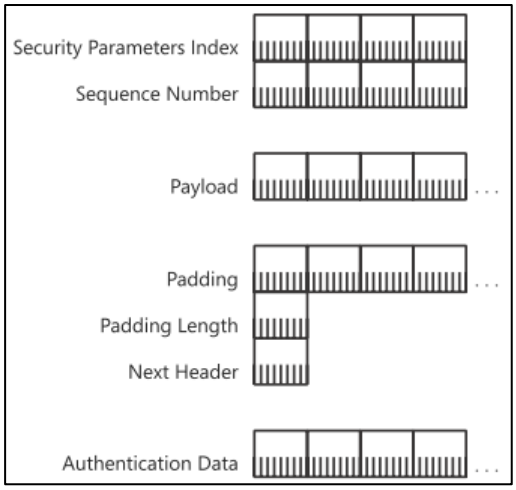


Abbildung 53:ESP Header

16.2.1 Header fields

Field	Description
Security Parameters Index	Gibt die SA an
Padding	Füllt die Nutzlast auf eine passende Länge aus
Next Header	Analog IP-Feld Protocol
Authentication Data	ICV-Berechnung des Absenders

16.3 ES-Frame

```
  Frame:
+ Ethernet: Etype = Internet IP (IPv4)
- Ipv4: Next Protocol = ESP, Packet ID = 1542, Total IP Length = 88
  + Versions: IPv4, Internet Protocol; Header Length = 20
  + DifferentiatedServicesField: DSCP: 0, ECN: 0
    TotalLength: 88 (0x58)
    Identification: 1542 (0x606)
  + FragmentFlags: 0 (0x0)
    TimeToLive: 128 (0x80)
    NextProtocol: ESP, 50(0x32)
    Checksum: 11669 (0x2D95)
    SourceAddress: 131.107.0.2
    DestinationAddress: 131.107.0.1
- Esp: Next Protocol = UDP, SPI = 0x469021eb, Seq = 0x1
    SecurityParameterIndex: 1183850987 (0x469021EB)
    SequenceNumber: 1 (0x1)
  - Trailer:
     PaddingData: Binary Large Object (2 Bytes)
     PaddingLength: 2 (0x2)
     NextProtocol: UDP, 17(0x11)
     AuthenticationData: Binary Large Object (12 Bytes)
+ Udp: SrcPort = 50202, DstPort = DNS(53), Length = 44
+ Dns: QueryId = 0xF341, QUERY (Standard query), Query for test99.contoso.com of type Host A
ddr on class Internet
```

Abbildung 54: ESP-Frame

16.4 ESP-Transportmodus

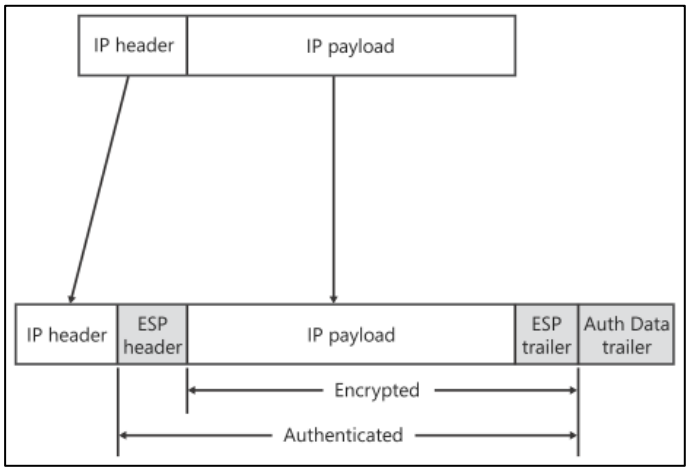


Abbildung 55: ESP-Transportmodus

Im ESP-Transportmodus wird der ESP-Header nach dem IP-Header und der ESP-Trailer nach der Nutzlast eingefügt. Die Nutzlast wird nicht geändert.

16.5 AH und ESP Kombination

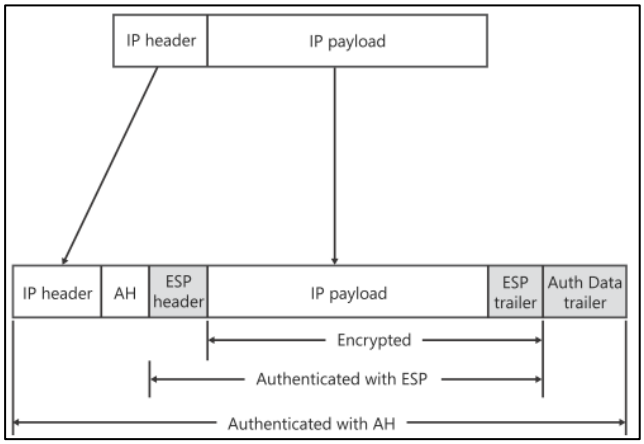


Abbildung 56: AH und ESP Kombination

16.6 AH und ESP Kombination Frame

```
  Frame:
+ Ethernet: Etype = Internet IP (IPv4)
- Ipv4: Next Protocol = AH, Packet ID = 1555, Total IP Length = 120
  + Versions: IPv4, Internet Protocol; Header Length = 20
  + DifferentiatedServicesField: DSCP: 0, ECN: 0
    TotalLength: 120 (0x78)
    Identification: 1555 (0x613)
  + FragmentFlags: 0 (0x0)
    TimeToLive: 128 (0x80)
    NextProtocol: AH, 51(0x33)
    Checksum: 11623 (0x2D67)
    SourceAddress: 131.107.0.2
    DestinationAddress: 131.107.0.1
- Ah: Next Protocol = ESP, SPI = 0x43E235D7, Seq = 0x1
    NextHeader: ESP, 50(0x32)
    PayloadLength: 24 bytes
    Reserved: 0 (0x0)
    SecurityParametersIndex: 1138898391 (0x43E235D7)
    SequenceNumber: 1 (0x1)
    AuthenticationData: 12 UINT8(s)
- Esp: SPI = 0x1ef5e304, Seq = 0x1
    SecurityParameterIndex: 519430916 (0x1EF5E304)
    SequenceNumber: 1 (0x1)
    EncryptedPayload: Binary Large Object (68 Bytes)
```

Abbildung 57: AH und ESP Kombination Frame

16.7 ESP-Tunnelmodus

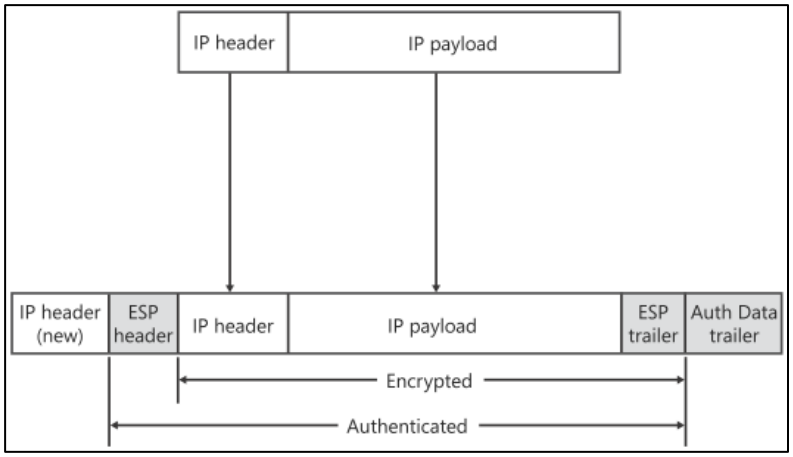


Abbildung 58: ESP-Tunnelmodus

Im ESP-Tunnelmodus wird das gesamte ursprüngliche IP-Datagramm mit einem neuen (äusseren) IP-Header sowie einem ESP-Header und Trailer eingekapselt.

17 ISAKMP, IKE

Internet Security Association and Key Management Protocol, Internet Key Exchange

- Protocol type: Application layer key exchange protocol.
- Port: 500 (UDP)

17.1 Beschreibung SA

Eine SA entspricht der Kombination von Sicherheitsdiensten, Schutzmethoden und kryptografischen schlüsseln, di von den kommunizierenden Partnern ausgehandelt werden.

Es gibt zwei Typen von Sicherheitszuordnungen:

- **ISAKMP-Sicherheitszuordnung**
  - Diese Sicherheitszuordnung wird auch als Hauptmodus-SA bezeichnet, sie schützt die IPSec-Sicherheitsaushandlung.
  - Es werden nicht nur die Daten geschützt, sondern auch dich von den IPSec-Kommunikationspartner ausgehandelten Schutzalgorithmen.
- **IPSec-Sicherheitszuordnung**
  - Dieser SA wird auch als Schnellmodus bezeichnet
  - Es werden zwei Sicherheitszuordnungen getroffen, eine für den eingehenden Datenverkehr und eine für den ausgehenden Datenverkehr.

Die IPSec-Kommunikationspartner müssen für jede IPSec-Sitzung drei SA verwalten:

- ISAKMP-SA
- Eingehende IPSec-SA
- Ausgehende IPSec-SA

17.2 Main-Mode (Hauptmodus)

Die Aushandlung im Hauptmodus bestimmt die Verschlüsselungsschlüssel und die Schutzmethode, die in der nachfolgenden Hauptmodus- oder Schnell-Modus-Kommunikation eingesetzt werden.

Die Aushandlung im Hauptmodus umfasst folgende Schritte:

1. Aushandlung der Schutzkombinationen
2. Einen Diffie-Hellman-Austausch
3. Authentifizierung

17.3 Quick-Mode (Schnellmodus)

Bevor sichere Daten gesendet werden, muss in einer Schnellmodus-Aushandlung festgelegt werden, welchen Typ der Datenverkehr hat und wie dieser gesichert werden soll.

Das Ergebnis einer Schnellmodus-Aushandlung sind zwei IPSec-Sicherheitszuordnungen (eingehender und ausgehender Datenverkehr).

17.4 Beschreibung ISAKMP

ISAKMP kann Kommunikationspartner identifizieren und authentifizieren, SAs verwalten und Schlüsselinformationen austauschen.

ISAKMP ist ein System zum Aushandeln der sicheren Kommunikation, unabhängig von den Schlüsselaustauschprotokollen, Verschlüsselungs- und Integritätsalgorithmen und Authentifizierungsmethoden.

17.4.1 ISAKMP Message Structure

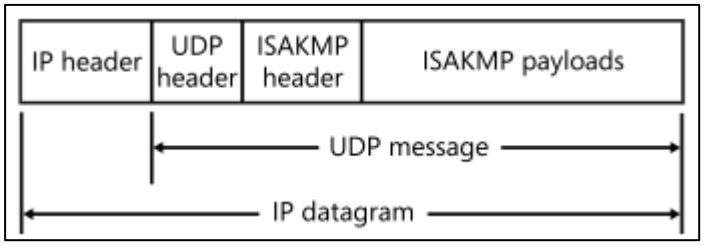


Abbildung 59: ISAKMP Message Structure

17.4.2 ISAKMP-Header

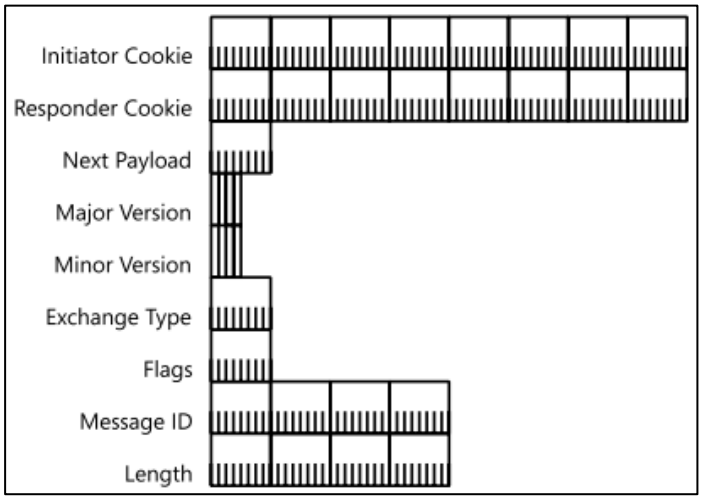


Abbildung 60: ISAKMP-Header

17.4.3 Beschreibung IKE

IKE ist ein Standard zum Erstellen von Sicherheitszuordnungen.

Es kombiniert ISAKMP mit dem Oakley-Schlüsselbestimmungsprotokoll.

17.5 Prozesse

- 17.5.1 Erstellen von IPSec SA mit IKE

17.5.1 Erstellen von IPSec SA mit IKE

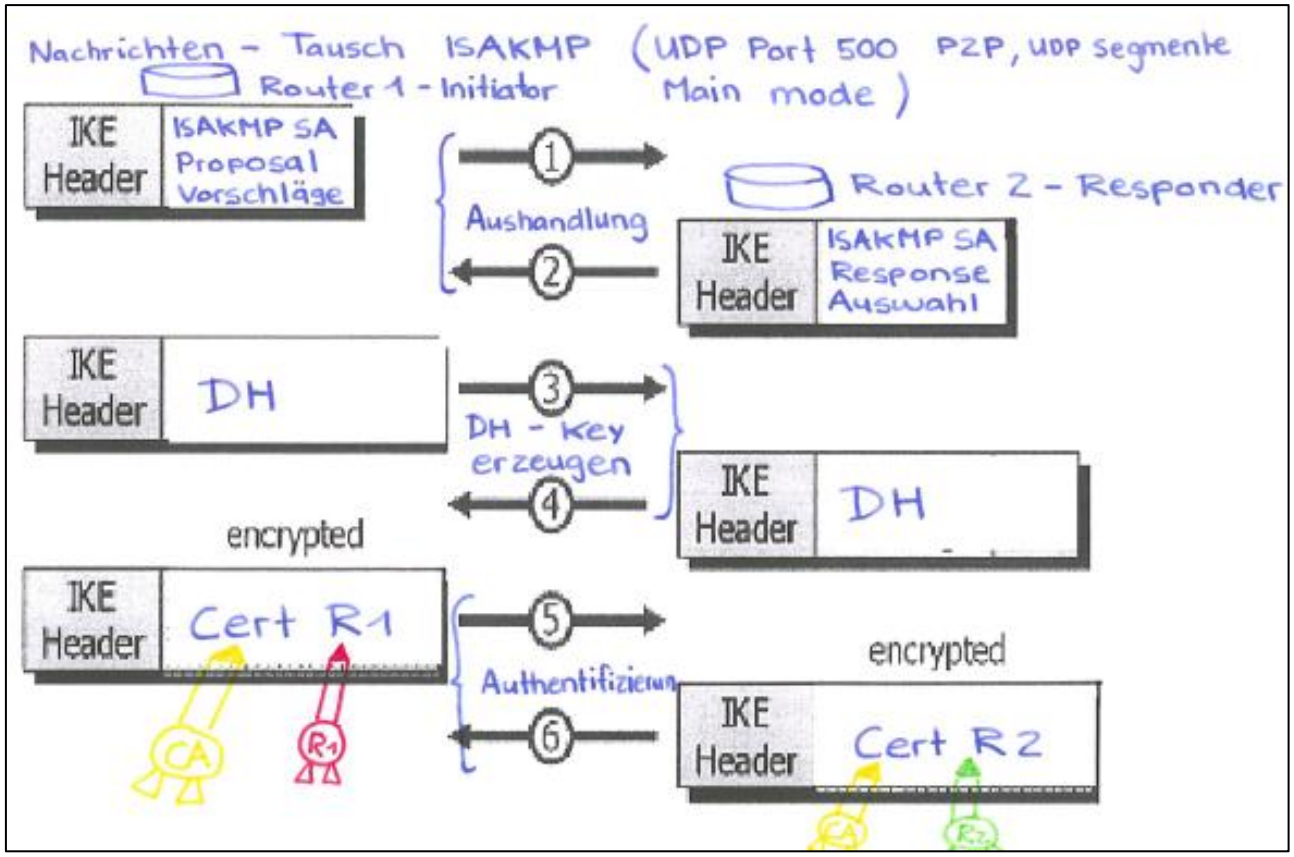


Abbildung 61: Erstellen von IPSec SA mit IKE

18 IPv6

Internet Protocol Version 6

18.1 Beschreibung

IPv6 Adressen haben eine Länge von 128 bit. Um eine IPv6 Adresse möglichst kurz, aber dennoch genügend lesbar zu halten hat man für die Notation ein akzeptierbar „schweres“ Stellenwert-System ausgewählt. Daher werden die IPv6-Adressen im Hexadezimal-System dargestellt.

Ein Beispiel:

2001:470:26:4cd:2c84:41be:4208:4a82

- Eine vollständig ausgeschriebene IPv6 Adresse besteht aus 8 Blöcken
- Ein Block enthält maximal 4 Hex-Ziffern
- Die 4 Hex-Ziffern stehen für 4 Nibbles (Halb-Bytes), oder einfacher gesagt für 2 Bytes
- Die Doppelbyte Blöcke werden durch einen :: getrennt.

18.1.1 Auslassung von 0000 DoppelbyteBlöcken

Durch Auslassung einer zusammenhängenden Folge von Doppelbyte-Blöcken (ein oder mehrere Blöcke) kann eine informationserhaltende Kompression der Notation einer IPv6 Adresse erreicht werden. Die Auslassungsstelle wird durch zwei Doppelpunkte :: eingetragen.

Beispiel:

Verkürzte Form	Ausgeschriebene Form
fe02::cafe:baba	fe02:0000:0000:0000:0000:0000:cafe:baba
fe02::cafe::baba	Das ist keine gültige Verkürzung, da nicht mehr klar ist, wie viele 0000 Doppelbyte-Blöcke an Stelle des :: stehen müssen!

Beispiele für IPv6 Adressen mit besonders kurzer Notation:

ff02::1	Alle Hosts im lokalen Subnet (local link Subnet <-> L2-MC-Domäne)
ff02::2	Alle Router im lokalen Subnet

Bei beiden Adressen handelt es sich um IPv6 Multicast-Adressen, die auf L2 gemäss einem RFC auf Ethernet Multicast-Adressen „gemapt“ werden. Auf den Begriff „IPv6 Multicast-Adresse“ und deren Verwendung wird weiter unten eingegangen.

18.1.2 Adressarten

Unicast	Adresse, genau für einen Host
Multicast	Adressierung einer bestimmten Gruppe von Host im link lokalen Bereich, z.B. Ff02::1 für all Hosts im link lokalen Gebiet ff02:2 für all Routers im link lokalen Gebiet Wenn Wireshark mit Capture Filter „ip6“ eine gewisse Zeit Datagramme auffängt, sind Datagramme mit weiteren Multicast-Adressen sichtbar, z.B. für Microsoft Namensauflösungsprotokolle als Ersatz für NetBIOS Name Service.
Anycast	Adresse ist auf mehreren Hosts eingetragen. Bei der Zustellung wird nur der nächst liegende Host mit dem Datagramm bedient

18.2 Prozesse

- 18.2.1IPv6 Adressierungsbereich
- 18.2.2IPv6 Adressaufbau im Vergleich zu IPv4

18.2.1 IPv6 Adressierungsbereich

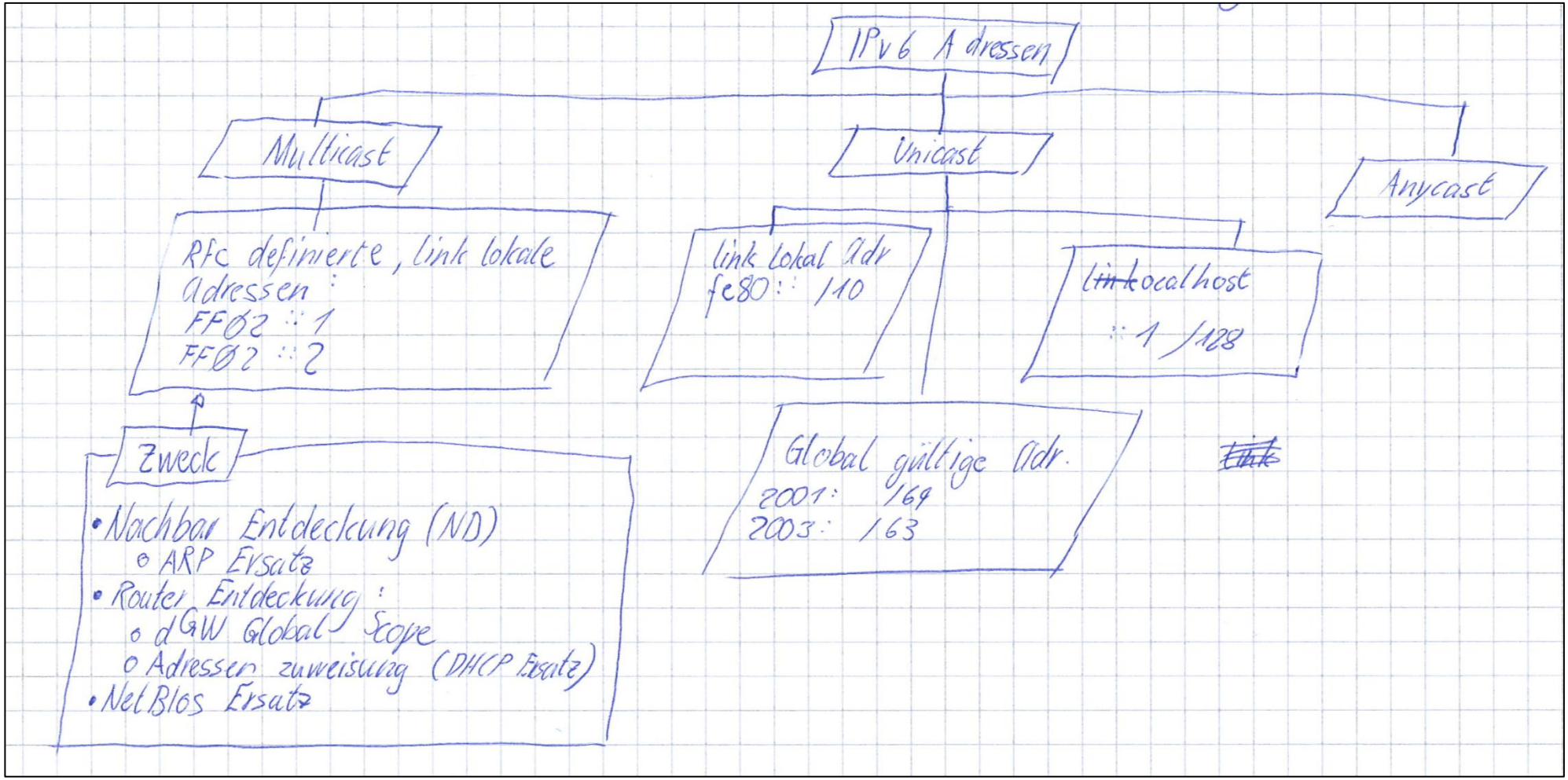


Abbildung 62: IPv6 Adressierungsbereich

18.2.2 IPv6 Adressaufbau im Vergleich zu IPv4

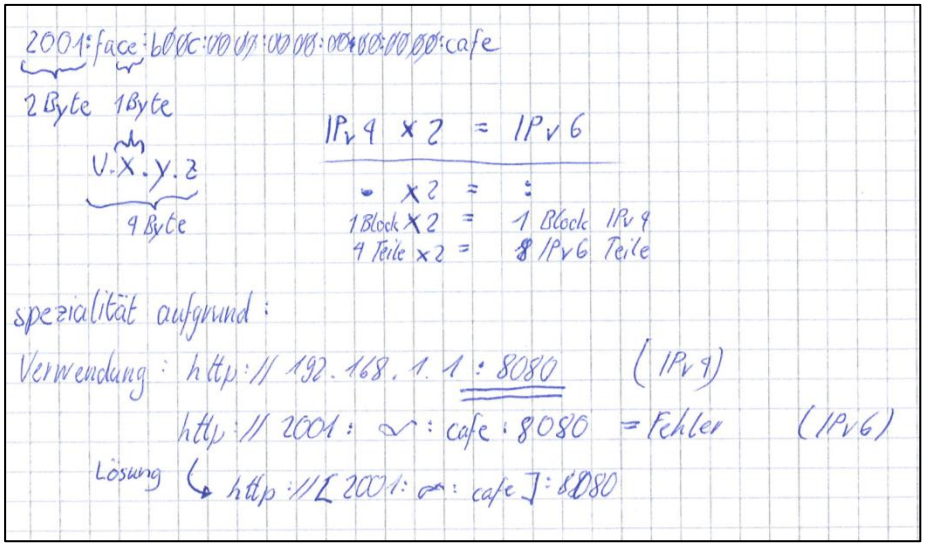


Abbildung 63: IPv4 Adressen im Vergleich zu IPv6

18.3 Summary

Die IPv6-Protokollsuite stellt eine Überarbeitung der aktuellen TCP/IP-Protokollfamilie insbesondere auf der Ebene der Internetschicht dar und ersetzt:

- IP
- ICMP
- IGMP
- ARP

Dabei versucht IPv6, die Probleme von IPv4 mit Hilfe eines effizienten und grossen Adressraums, eines geschwindigkeitsoptimierten Internetschichtheaders, den Router einfacher erarbeiten können, und einer effizienteren Interaktion benachbarter Knoten zu beheben.

19 LCP

Link Control Protocol

Siehe Kapitel: 22 Quellen Verweis: LCP

20 NCP

Network Control Protocol

Siehe Kapitel: 22 Quellen Verweis: NCP

21 ATM

Asynchronus Transport Mode

Asynchronous Transfer Mode (ATM) ist eine Technik der Datenübertragung, bei der der Datenverkehr in kleine Pakete – Zellen oder Slots genannt – mit fester Länge (53 Byte, davon 48 Byte Daten, 5 Byte Zellkopf) codiert und über asynchrones Zeitmultiplexing übertragen wird.

21.1 RIPv2

Routing Information Protocol

Das Routing Information Protocol (RIP) ist ein Routing-Protokoll auf Basis des Distanzvektoralgorithmus, das innerhalb eines autonomen Systems (z. B. LAN) eingesetzt wird, um die Routingtabellen von Routern automatisch zu erstellen. Es gehört zur Klasse der Interior Gateway Protocols (IGP).

21.2 OSPF

Open Shortest Path First

OSPF ist ein dynamisches Routing-Protokoll innerhalb eines autonomen Systems. Es hat das Routing Information Protocol (RIP) als Standard-Interior Gateway Protocol (IGP) abgelöst, insbesondere bei großen Netzen. OSPF verwendet die Kosten eines Pfades als Metrik und kann bei gleichen Kosten lastverteilt arbeiten. Der Standard definiert nicht, wie die Kosten zu berechnen sind. Einige Implementierungen (zum Beispiel Router des Herstellers Cisco Systems) greifen auf die Interface-Übertragungsrate zurück, wenn kein anderer Wert vorgegeben wird. Ein großer Vorteil gegenüber RIP ist, dass jeder Router die vollständige Netztopologie kennt.

22 Quellen

22.1 Windows Server 2008 TCP/IP-Protokolle und –Dienste

ISBN: 978-3-86645-5-640-2

Verweis	Seite
CHAP	103-104
ESP	436
ICMP-Echo und Echoantwort	164-166
ICMP-Nachricht „Ziel nicht erreichbar“	166-169
ICMP-Nachrichten	164
ICMP-Nachrichtenstruktur	162-163
IPCP	113-114
IPSec und Sicherheitszuordnung	411
ISAKMP	442-444
ISAKMP Aushandlung Hauptmodus und Schnellmodus	458-460
LCP	95
LCP-Aushandlungsprozess	99-100
NCP	95
PPPoE	117-119
PPP-Verbindungsprozess	94-95
TCP	239 ff

23 Glossar

Bezeichnung	Beschreibung
DH	Diffie Hellman
PADI	PPPoE Active Discovery Initiation
PADO	PPPoE Active Discovery Offer
PADR	PPPoE Active Discovery Request
PADS	PPPoE Active Discovery Session-confirmation
PSK	Pre-Shared Key
SA	Security Assocation

24 Abbildungsverzeichnis

25 Kontakt

Name	Janik von Rotz
E-Mail	contact@janikvonrotz.ch
Website	http://www.janikvonrotz.ch