

Vorlesung Kommunikationstechnik

Point-to-Point Protocol (PPP)

Harald Orlamünder

SS 2014

Inhalt

- High Level Data Link Control (HDLC)
- Frame Relay (FR)
- Point-to-Point Protocol (PPP)
 - Grundform
 - Sonderformen von PPP
 - Tunneling-Protokolle
 - Breitbandiger Anschluss
 - Unterstützende Funktionen

HDLC – Einleitung (1)

Basis für eine Reihe von Protokollen wie:

- X.25 (LAPB)
- Frame Relay (FR, LAPF),
- ISDN D-Kanal (LAPD)
- Point-to-Point Protocol (PPP),
- Link Access Procedure SDH (LAPS)

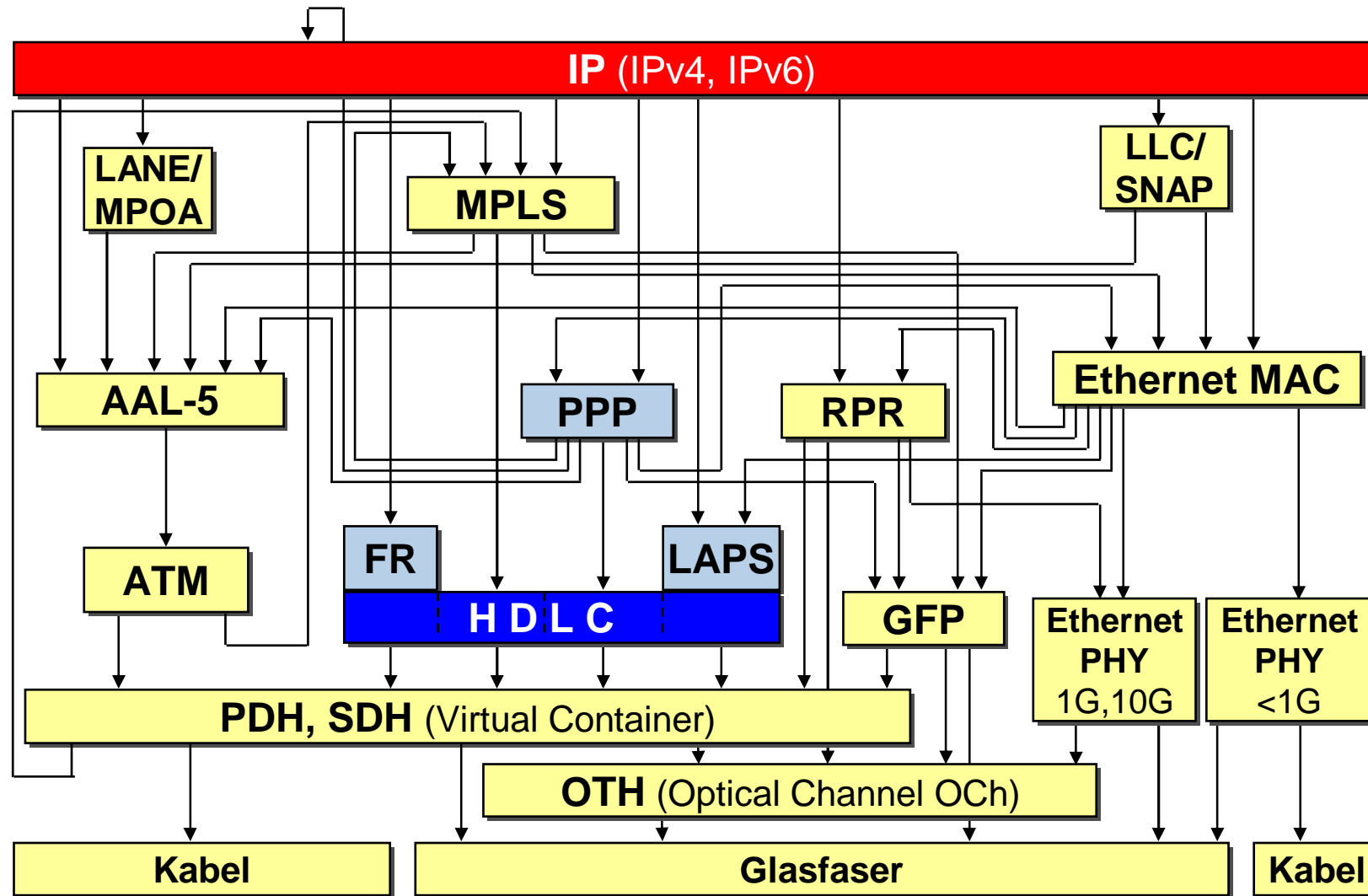
ist ein Rahmenformat gemäß dem Standard

High Level Data Link Control (HDLC)

gemäß dem Standard

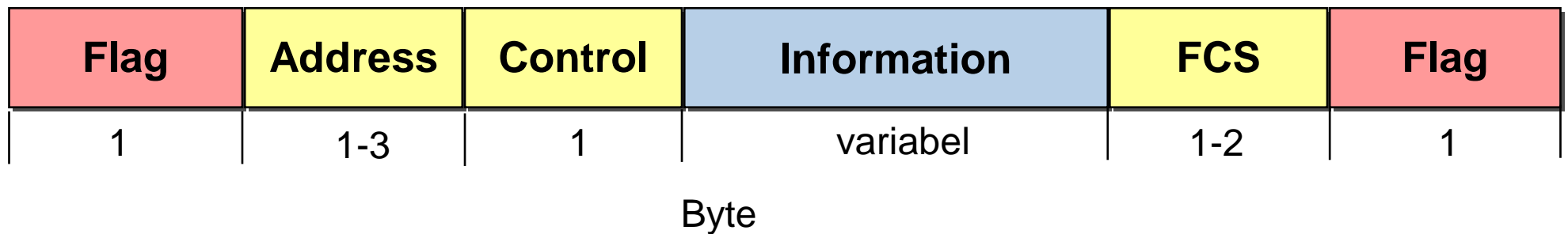
ISO 3309

HDLC – Einleitung (2)



HDLC – Rahmenstruktur

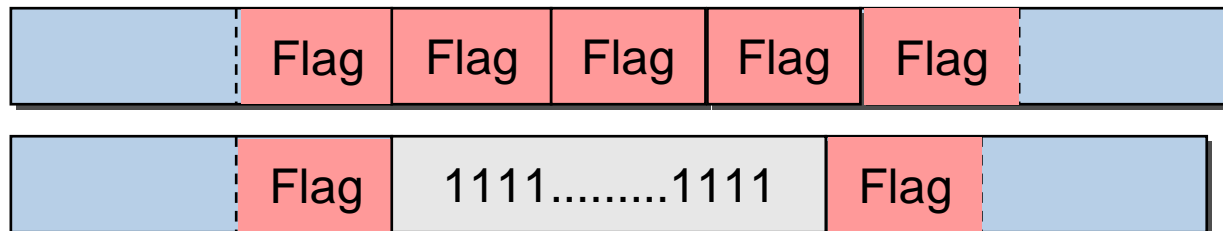
- Rahmenerkennung durch „Flags“ (Wert: 01111110)
- Unterscheidung zwischen Nutz- und Steuerinformation durch ein „Control“-Feld
- Multiplexen mehrere Verbindungen möglich, Unterscheidung durch ein „Address“-Feld
- Fehlerschutz durch eine „Frame Check Sequence“ (FCS) (Realisiert durch einen CRC-16 der Form $x^{16} + x^{12} + x^5 + 1$)



HDLC – Flag und Rahmenerkennung



- Zwischen zwei Datenrahmen darf eine Lücke bestehen.
- Diese Lücke ist entweder mit **Flags** zu füllen oder mit „**1**“-**Bits** zwischen dem schließenden und dem nächsten öffnenden Flag.

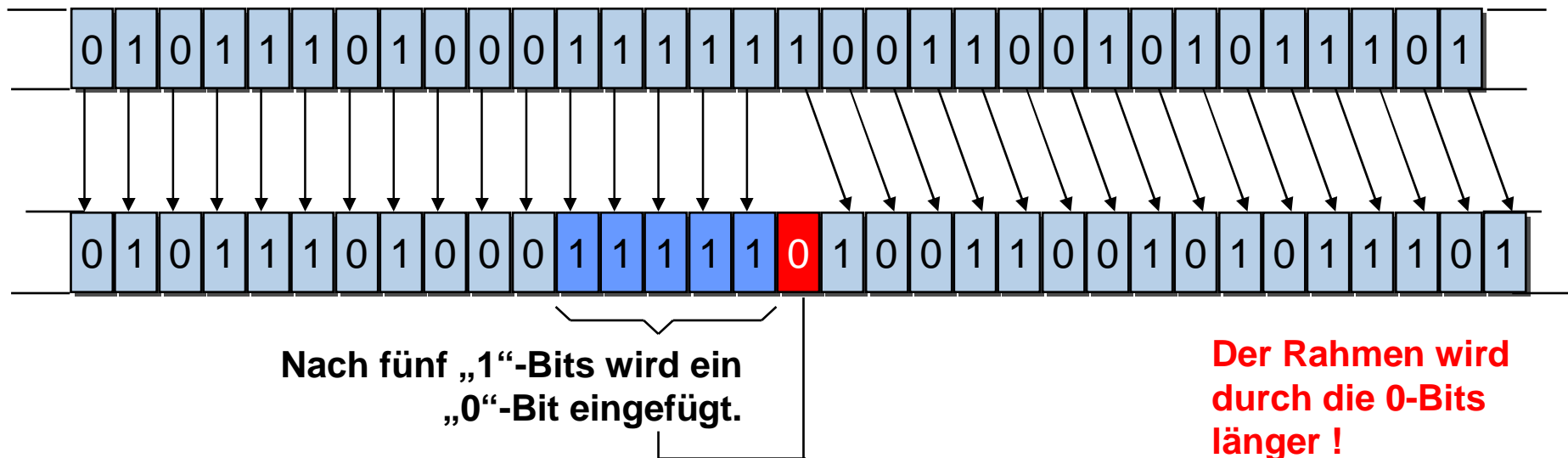


- Bei direkt hintereinander folgenden Datenrahmen dürfen das schließende und das öffnende Flag durch ein **einziges Flag** dargestellt werden.



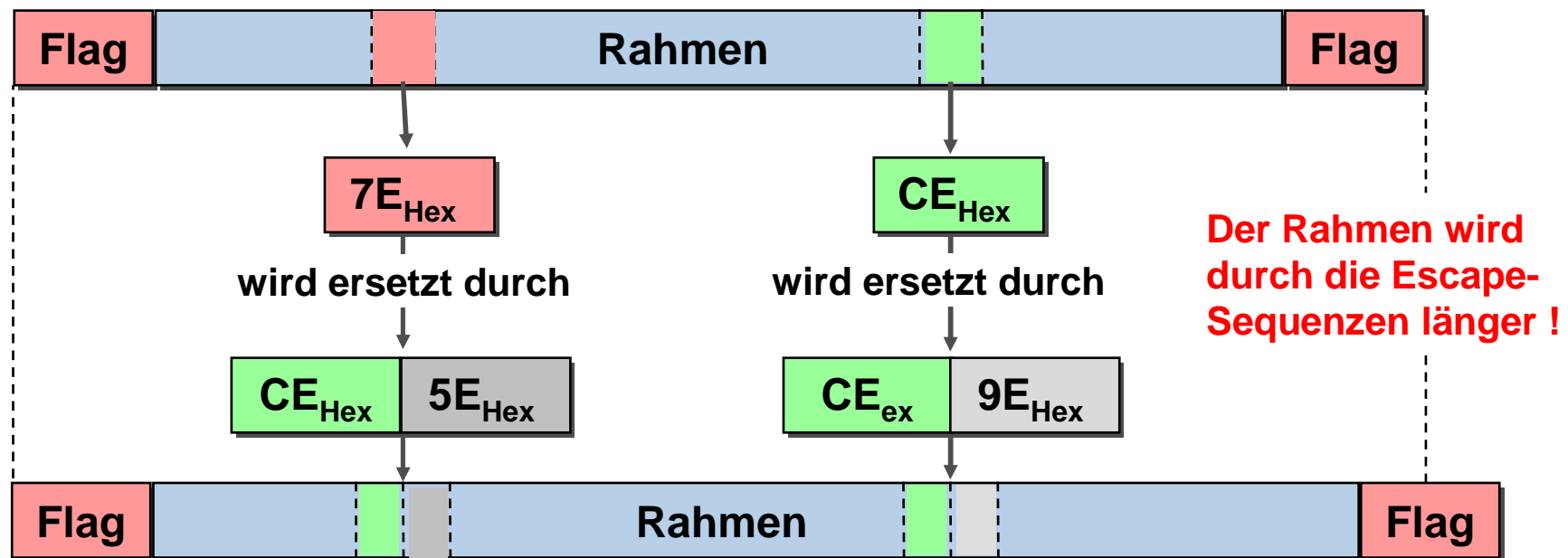
HDLC – Bit-Stuffing

- Das Flag (**01111110**) darf im Datenrahmen nicht auftreten. Eine Methode ist **Bit-Stuffing**:
- Auf der Sendeseite wird nach fünf „1“-Bits ein „0“-Bit eingefügt, dieses wird auf der Empfangsseite wieder entfernt.

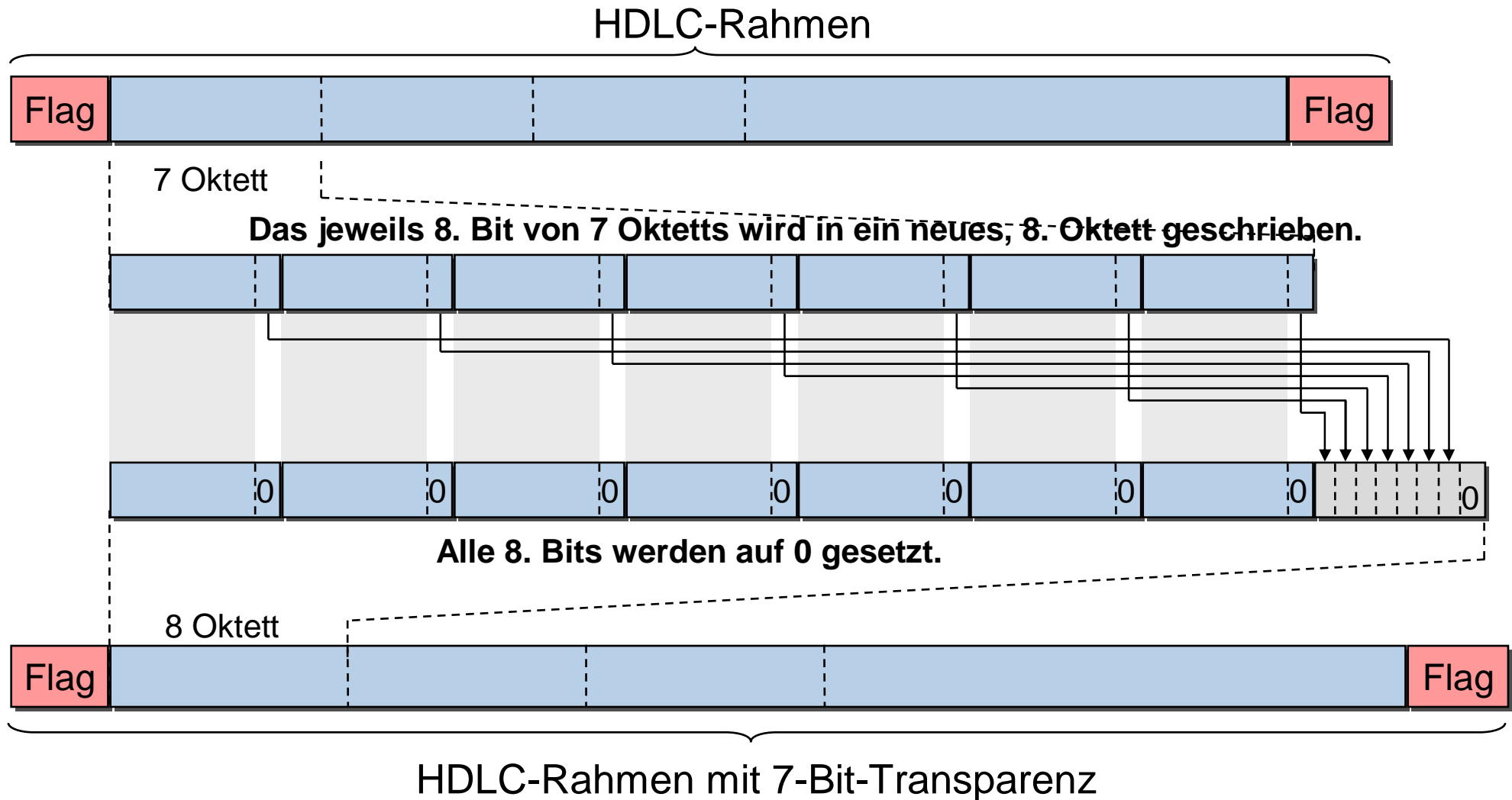


HDLC – Oktett-Stuffing

- Das Flag (**01111110** = **7E_{Hex}**) darf im Datenrahmen nicht auftreten. Eine andere Methode ist **Oktett-Stuffing**:
- Auf der Sendeseite werden Zeichen, die dem Flag entsprechen durch eine Escape-Sequenz ersetzt.



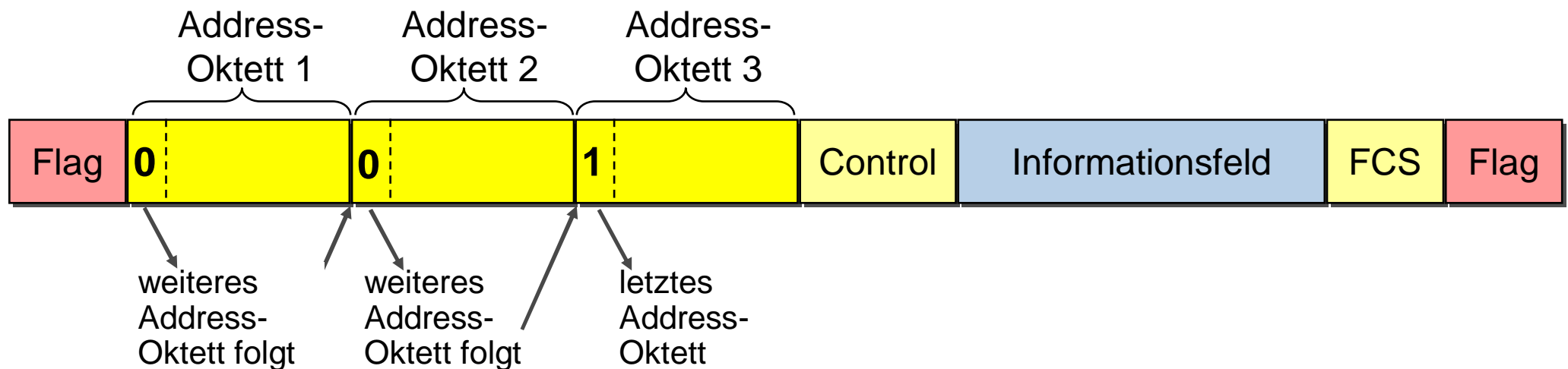
HDLC – 7-Bit-Transparenz beim Oktett-Stuffing (opt.)



HDLC – Adressfeld



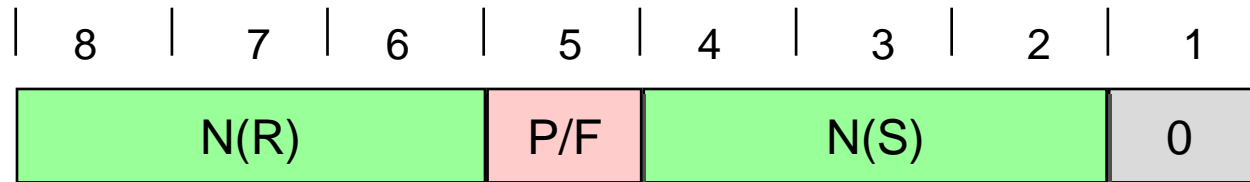
- Im Normalfall 1 Oktett.
- **Spezielle Adressen:**
„All Stations“ (**FF_{Hex}**) und „No Stations“ (**00_{Hex}**)
- **Extended Address** kann vereinbart werden (2 oder 3 Oktett), dabei ist das niederwertigste Bit des vorherigen Adress-Oktetts „0“.



HDLC – Control Feld (1)



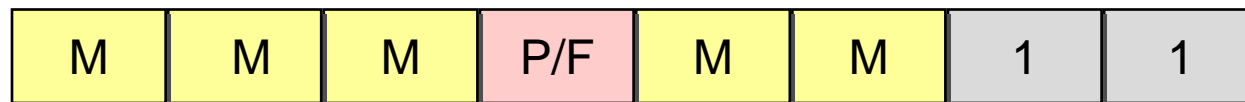
I-Format = Numbered Information Transfer



S-Format = Supervisory Functions

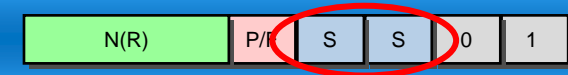


U-Format = Control Functions (Unnumbered Information)



- N(S) = fortlaufende Nummer der eigenen Rahmen, Folgenummer , (0...7, mod 8)
- N(R) = nächster erwarteter Rahmen und Quittung für alle Rahmen bis N-1 , (0...7, mod 8)
- P/F = Poll/Final: Rahmen mit gesetztem P-Bit erzwingt sofortige Antwort mit einem Rahmen mit gesetztem F-Bit
- S = Supervisory: Spezifikation der S-Rahmen (Steuerung)
- M = Modifier: Spezifikation der U-Rahmen

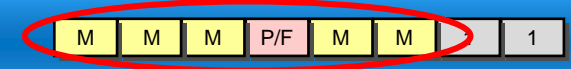
HDLC – Control Feld (2)



■ Bedeutung der Supervisory-Bits (S-Bits)

4	3		
S	S	Name	Bedeutung
0	0	Receiver Ready (RR)	Quittung für alle Rahmen bis N(R)-1, Bereitschaft zum Empfang weiterer I-Rahmen
0	1	Receiver not Ready (RNR)	Keine Bereitschaft I-Rahmen zu empfangen, Quittung bis N(R)-1
1	0	Reject (REJ)	Zurückweisung und Wiederholungs-Anforderung ab Rahmen N(R)
1	1	Selective Reject (SREJ)	Explizite Wiederholungs-Anforderung für Rahmen N(R)

HDLC – Control Field (3)



- Bedeutung der Felder im U-Rahmen (M-Bits und P/F-Bit)
(Auszug, es gibt eine Reihe weiterer Befehle und Meldungen)

| 8 | 7 | 6 | 5 | 4 | 3 |

M	M	M	P/F	M	M	Bedeutung	Befehl	Meldung
						Mode/Verbindungsaufbau:		
1	0	0	P	0	0	Set Normal Response Mode (SNRM)	X	-
0	0	0	P	1	1	Set Asynchronous Response Mode (SARM)	X	-
0	0	1	P	1	1	Set Asynchronous Balanced Mode (SABM)	X	-
0	1	1	F	0	0	Bestätigung: Unnumbered Acknowledge (UA)	-	X
0	1	0	P	0	0	Verbindungsabbau: Disconnect (DISC)	X	-
0	0	0	F	1	1	Bestätigung: Disconnect Mode (DM)	-	X
1	0	0	F	0	1	Fehlermeldung: Frame Reject (FRMR)	-	X
0	0	0	P	0	0	Daten: Unnumbered Information (UI)	-	-

- **Normal Response Mode (NRM)**, Anforderungsbetrieb
 - Zentralisierte Steuerung: Ein zentrales Leitsystem („primary“) sendet an untergeordnete Folgesysteme („secondaries“)
 - Die Folgesysteme dürfen nur nach entsprechender Erlaubnis senden (Leitsystem hat Poll-Bit gesetzt).
 - Folgesysteme kennzeichnen das Ende ihrer Sendung durch ein gesetztes Final-Bit.
- **Asynchronous Response Mode (ARM)**, Spontanbetrieb
 - Folgestationen dürfen ohne Erlaubnis der Leitstation senden.
 - Betriebsweise für unsymmetrische Konfigurationen.
- **Asynchronous Balanced Mode (ABM)**, gleichberechtigter Spontanbetrieb
 - Punk-zu-Punkt-Verbindungen
 - Beide Seiten können Befehle und Meldungen senden.
 - Betriebsweise für symmetrische Konfigurationen.

Inhalt

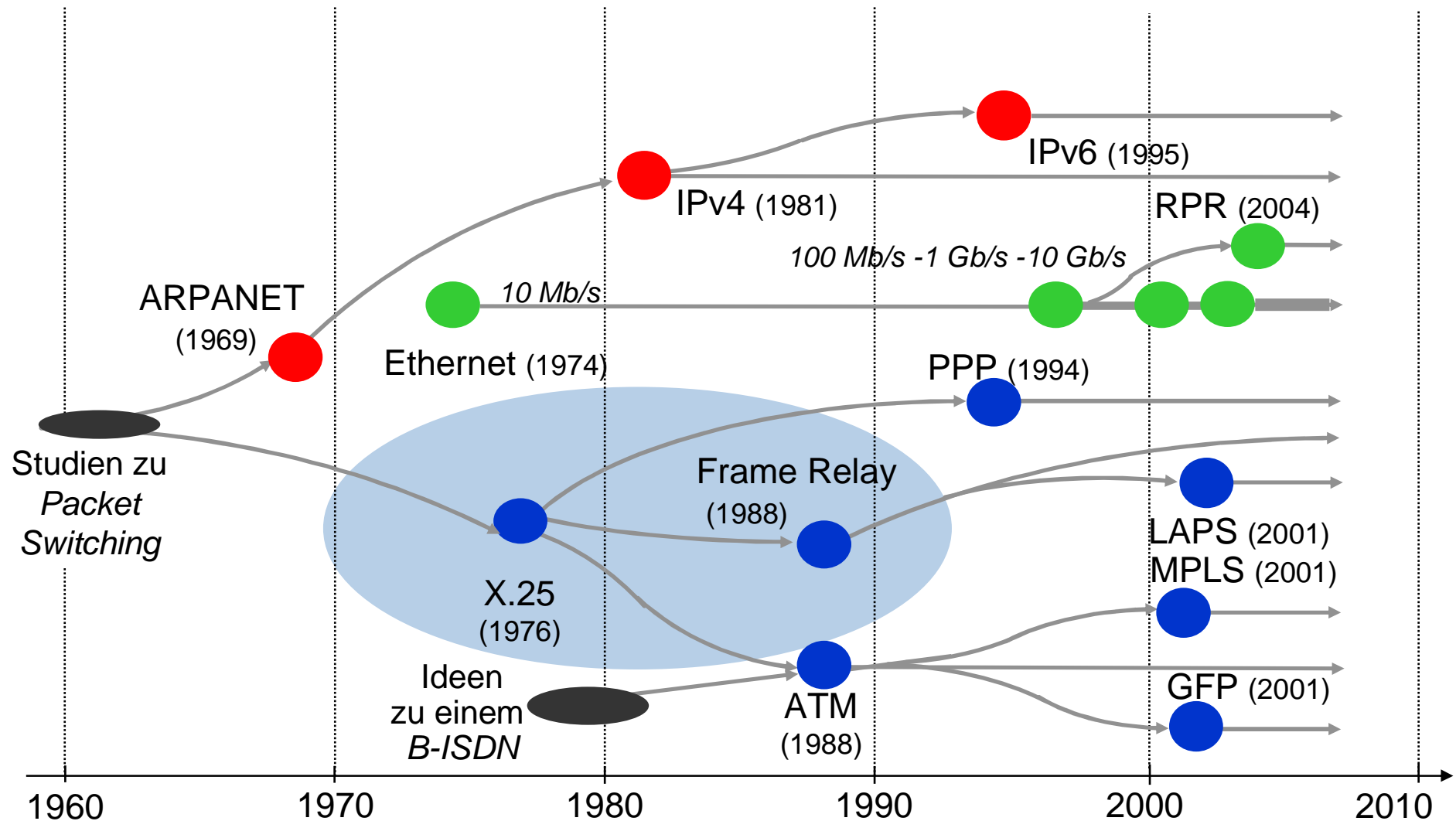
- High Level Data Link Control (HDLC)
- Frame Relay (FR)
- Point-to-Point Protocol (PPP)
 - Grundform
 - Sonderformen von PPP
 - Tunneling-Protokolle
 - Breitbandiger Anschluss
 - Unterstützende Funktionen

Frame Relay – Einleitung

- Frame Relay ist eine **Paketvermittlung**, die in den USA sehr erfolgreich war, in Europa aber eher ein Nischendasein führte.
- Basis ist ein Rahmenformat gemäß dem **HDLC**-Standard (High Level Data Link Control).
- Öffentliche Datennetze basierten in Deutschland lange auf dem Datenpaket-Vermittlungsprotokoll **X.25** (DATEX-P).
- Eine einfachere Möglichkeit ergab sich durch folgende Änderungen gegenüber dem X.25-Protokoll:
 - Beibehalten des HDLC-Rahmens, aber Sicherung nicht mehr Linkweise, sondern nur noch auf Ende-zu-Ende Basis;
 - Entfernen der Flusskontrolle;
 - Vereinfachen der Verbindungssteuerung.

Das Ergebnis führte dann zu **Frame Relay**.

Die Entwicklung der Paket-Protokolle – bis heute



Inhalt

- High Level Data Link Control (HDLC)
- Frame Relay (FR)
- Point-to-Point Protocol (PPP)
 - Grundform
 - Sonderformen von PPP
 - Tunneling-Protokolle
 - Breitbandiger Anschluss
 - Unterstützende Funktionen

Point-to-Point Protocol (PPP) – Allgemeines

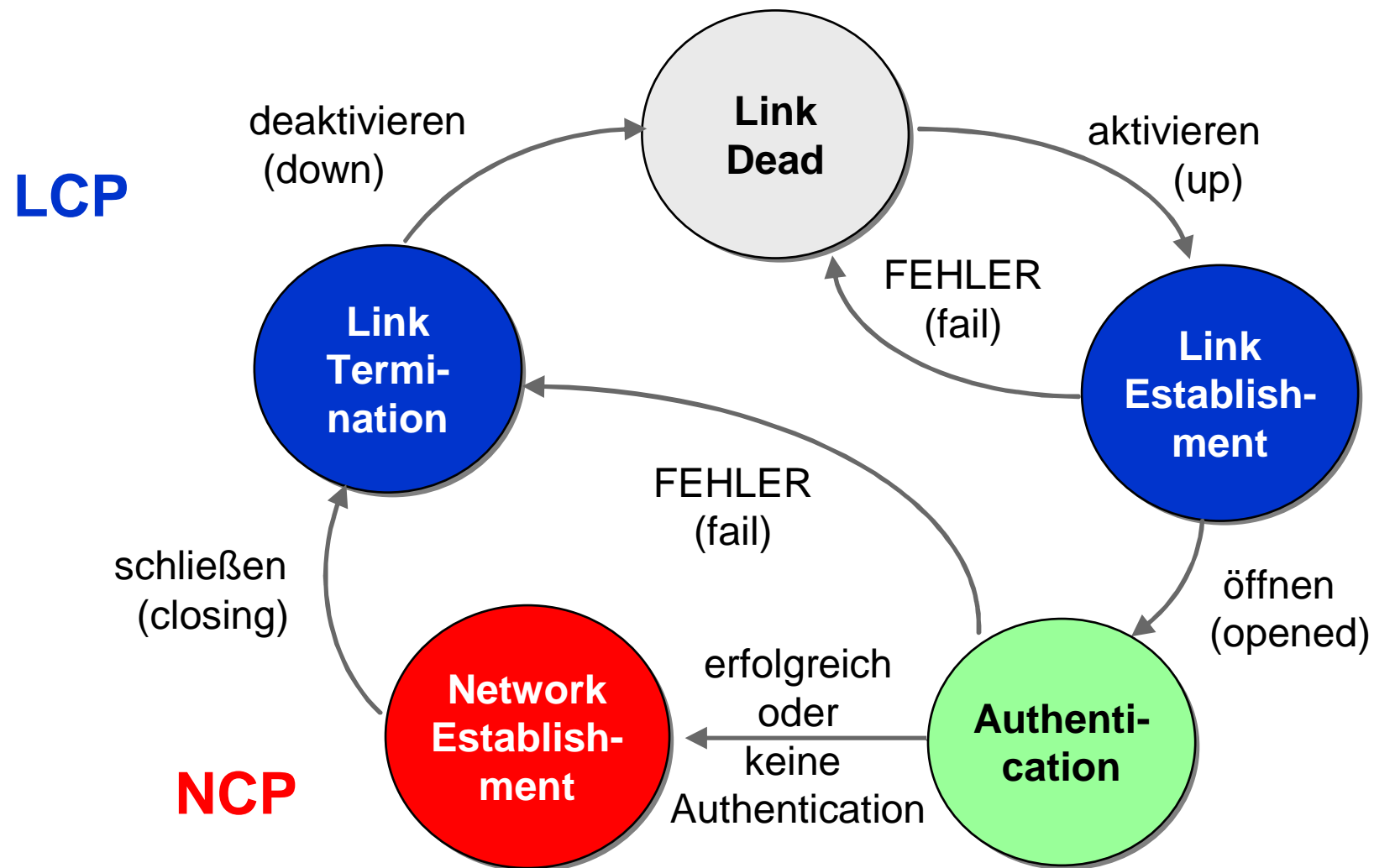
- Das Protokoll wird allgemein zur **Einwahl** in das Internet benutzt, klassisch über **Wählleitungen** (Modem, ISDN als Schicht 1)
- Durch seinen einfachen Aufbau wird es auch als Schicht 2 für den Transport von IP-Verkehr über die klassische **Übertragungstechnik** (SDH) eingesetzt.
- Aufgrund seiner Verbreitung fand es schließlich auch Einzug in die **Breitband-Zugangsnetze** (DSL), obwohl dort andere Verfahren möglich wären.
- Basis von PPP ist das **HDLC**, das dem Anwendungsfall (Punkt-zu-Punkt-Verbindung) angepasst wurde.
- Die Basis-Spezifikation ist der **RFC 1661**.

Point-to-Point Protocol (PPP) – Prinzip

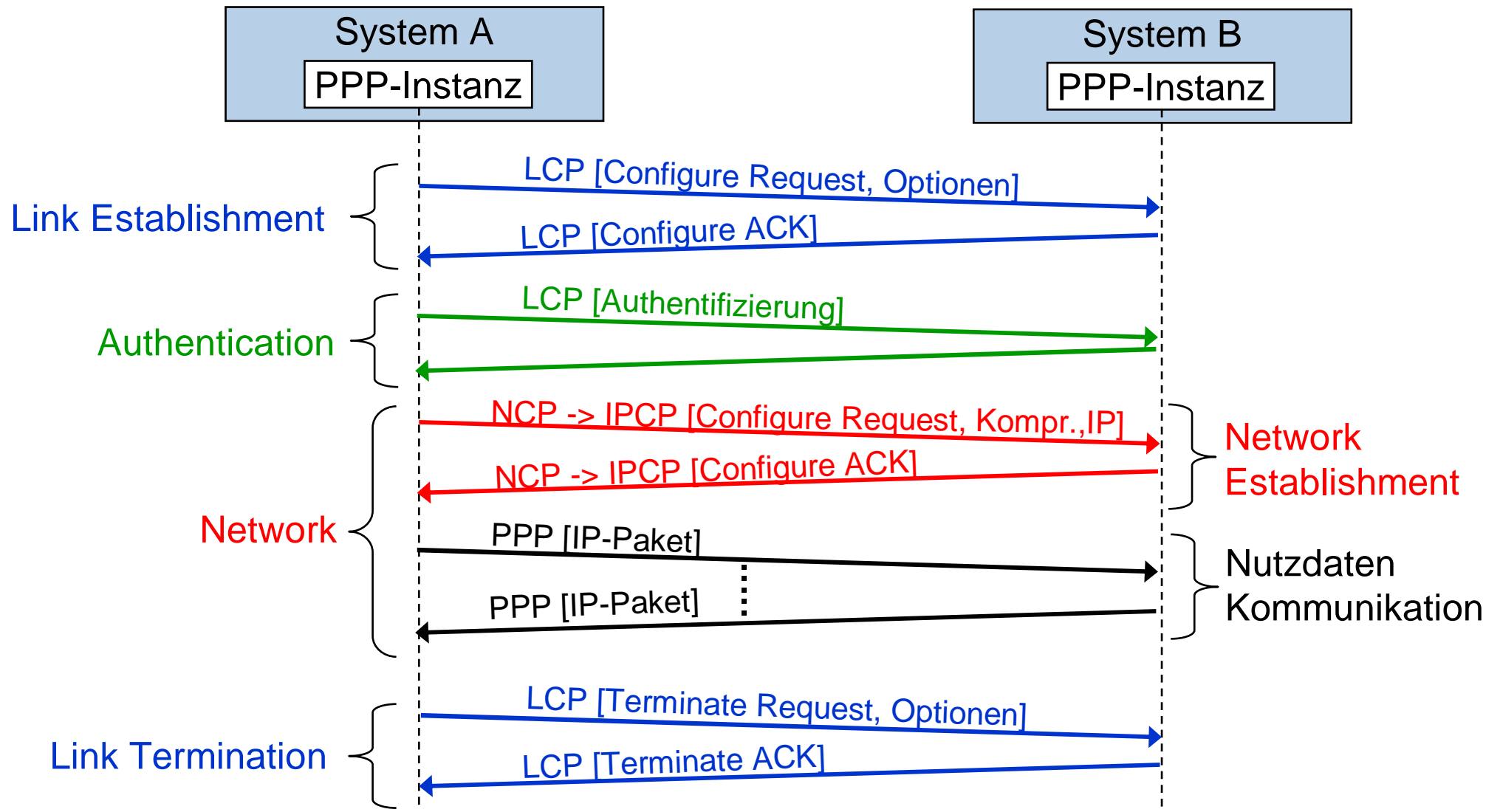
Das PPP besteht aus drei Komponenten:

- Eine Methode um Paket-Daten entsprechend verpackt zu übertragen - **PPP Encapsulation**.
Dabei wird von einer bidirektionalen Vollduplex-Übertragung ausgegangen.
- Ein Protokoll um die Übertragungsstrecke auf- und abzubauen, zu konfigurieren und zu testen, das **Link Control Protocol (LCP)**.
- Ein entsprechendes Steuerprotokoll, um verschiedene Schicht-3-Protokolle auf- und abzubauen und zu konfigurieren, das **Network Control Protocol (NCP)**.

PPP – State-Diagram



PPP – Verbindungsphasen



PPP – Prinzip

Das PPP besteht aus drei Komponenten:

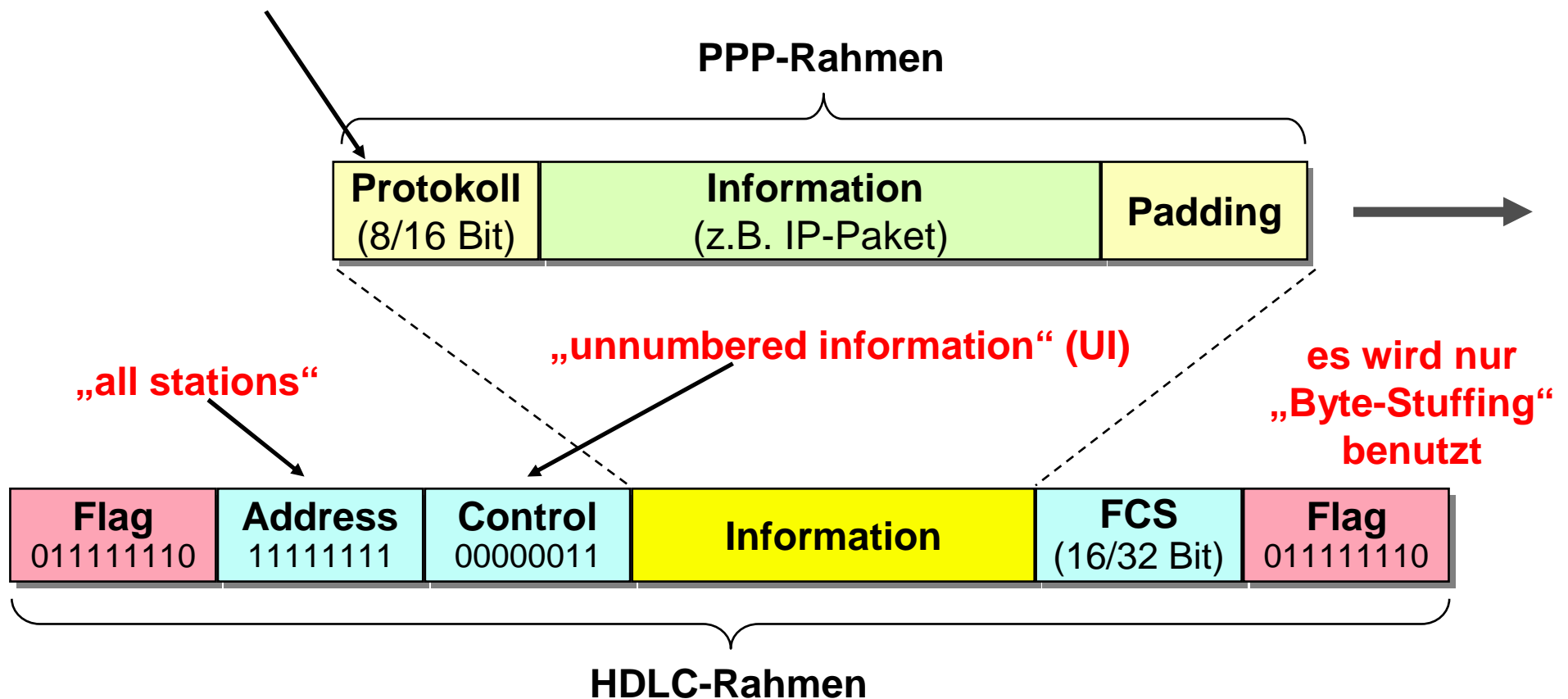
- Eine Methode um Paket-Daten entsprechend verpackt zu übertragen - **PPP Encapsulation**.
Dabei wird von einer bidirektionalen Vollduplex-Übertragung ausgegangen.
- Ein Protokoll um die Übertragungsstrecke auf- und abzubauen, zu konfigurieren und zu testen, das **Link Control Protocol (LCP)**.
- Ein entsprechendes Steuerprotokoll, um verschiedene Schicht-3-Protokolle auf- und abzubauen und zu konfigurieren, das **Network Control Protocol (NCP)**.

PPP über


- **X.25 / FR** - Dabei wird X.25 oder FR nur als Framing-Mechanismus benutzt, die übrigen Leistungsmerkmale bleiben unbenutzt.
- **ISDN** - Dabei wird der ISDN B-Kanal als Bit-synchroner Link betrachtet. Als Rahmenstruktur wird HDLC vorgesehen.
- **PDH /SDH** - Dabei wird die Übertragungsstrecke als Oktett-strukturierter, synchroner Link betrachtet. Als Rahmenstruktur wird HDLC vorgesehen.
- **ATM** Adaptation Layer Type 5 - Anstatt des Framings über HDLC wird ein Framing über AAL Type 2 oder Type 5 eingesetzt.
- **Ethernet** - Hierbei wird eine Punkt-zu-Punkt-Verbindung im Ethernet emuliert.
- **IP** - durch das PPTP
-

PPP – Rahmenstruktur

Kennzeichnet das entsprechende, transportierte Protokoll
(Network Layer Protocol, Link Control Protocol, Network Control Protocol, ...)



PPP – Felder im Rahmen

- Protokoll (1 oder 2 Oktett) 
 - Identifiziert die Information im Paket.
 - Werte von der IANA verwaltet.
- Informationsfeld
 - Enthält das zu übertragende Datenpaket (also z.B. ein IP-Paket).
 - Die minimale Länge ist null, die maximale Länge richtet sich nach den Fähigkeiten des Empfängers.
- Padding-Feld
 - kann zum Auffüllen bis zur maximalen Größe des Paketes benutzt werden.

IANA Internet Assigned Number Authority (www.iana.org)

PPP – Protocol-Feld – Wertebereiche

Wert	Protokoll
0000 _{Hex} ... 3FFF _{Hex}	Network Layer Protocol
4000 _{Hex} ... 7FFF _{Hex}	„ langsame “ Protokolle (ohne zugehöriges Network Control Protocol)
8000 _{Hex} ... BFFF _{Hex}	Network Control Protocol (NCP) (zu den entsprechenden Network Layer Protocols)
C000 _{Hex} ... FFFF _{Hex}	Link Control Protocol (LCP)



PPP – Protocol-Feld – Network Layer Protocols

0001 _{Hex}	Padding Protokoll
0003 _{Hex} - 001F _{Hex}	reserviert
0021 _{Hex}	Internet Protocol (IP)
0031 _{Hex}	Remote Bridging
003D _{Hex}	Multilink PPP
0041 _{Hex}	LAN Extension
0053 _{Hex}	verschlüsselte Daten (Datagramm)
0055 _{Hex}	verschlüsselte Daten (Link)
0057 _{Hex}	IPv6 [RFC2472]
005B _{Hex}	Vendor-specific Network Protocol
007D _{Hex}	reserviert
00CF _{Hex}	reserviert
00FB _{Hex}	komprimierte Daten (Link)
00FD _{Hex}	komprimierte Daten (Datagramm)
00FF _{Hex}	reserviert
0201 _{Hex}	Bridging Protocol Data Unit (BPDU)

PPP – Prinzip

Das PPP besteht aus drei Komponenten:

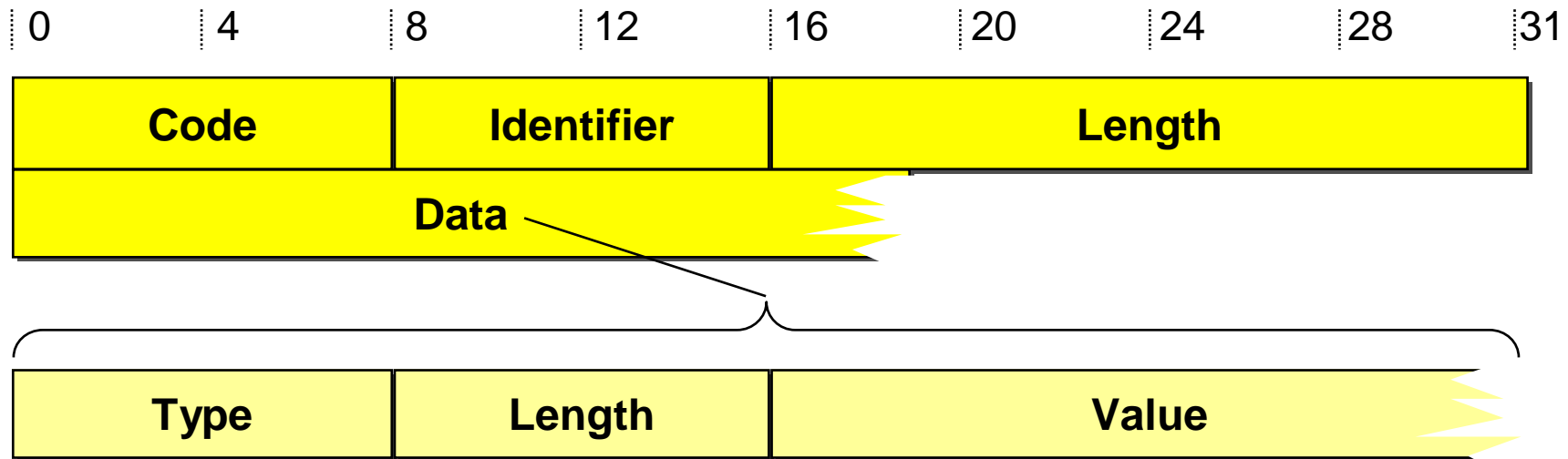
- Eine Methode um Paket-Daten entsprechend verpackt zu übertragen - **PPP Encapsulation**.
Dabei wird von einer bidirektionalen Vollduplex-Übertragung ausgegangen.
- Ein Protokoll um die Übertragungsstrecke auf- und abzubauen, zu konfigurieren und zu testen, das **Link Control Protocol (LCP)**.
- Ein entsprechendes Steuerprotokoll, um verschiedene Schicht-3-Protokolle auf- und abzubauen und zu konfigurieren, das **Network Control Protocol (NCP)**.

PPP – Protocol-Werte für das Link-Control Protocol (LCP)

- Im Protocol-Feld des PPP-Rahmens sind die Werte $C000_{\text{Hex}} \dots FFFF_{\text{Hex}}$ für das LCP reserviert.

$C021_{\text{Hex}}$	Link Control Protocol
$C023_{\text{Hex}}$	Password Authentication Protocol
$C025_{\text{Hex}}$	Link Quality Report
$C02B_{\text{Hex}}$	Bandwidth Allocation Control Protocol
$C02D_{\text{Hex}}$	Bandwidth Allocation Protocol
$C05B_{\text{Hex}}$	Vendor-specific Authentication Protocol
$C223_{\text{Hex}}$	Challenge Handshake Authentication Protocol
$C227_{\text{Hex}}$	Extensible Authentication Protocol

PPP – Link-Control Protocol (LCP) Format



- **Code:** Typ der LCP-Nachricht
 - **Identifier:** Korrelation von Anfragen und Antworten.
 - **Length:** Gesamtlänge der LCP-Nachricht
-
- **Type:** Typ der Konfigurationsoption
 - **Length:** Gesamtlänge des Datenfeldes
 - **Value:** Wert gemäss den Konfigurationsoptionen.

TLV-Format

- Type
- Length
- Value

PPP – Link-Control Protocol Nachrichten – „Code“

Code	Typ	Bedeutung
1	Configure-Request	Öffnen einer Verbindung
2	Configure-Ack	Bestätigung des Configure-Request
3	Configure-Nak	Der Configure-Request und die gewünschten Optionen wurden zwar vollständig erkannt, einige Optionen werden aber nicht akzeptiert.
4	Configure-Reject	Der Configure-Request bzw. einige Optionen wurden nicht erkannt.
5	Terminate-Request	Schließen der Verbindung
6	Terminate-Ack	Bestätigung des Terminate-Request
7	Code-Reject	Eine LCP-Nachricht mit unbekanntem Code wurde empfangen.
8	Protocol-Reject	Es wurde versucht, ein Protokoll zu initiieren, das nicht unterstützt wird.
9	Echo-Request	Erlaubt Schleifen-Prüfungen in beide Übertragungsrichtungen für Test und Performance Messungen.
10	Echo-Reply	
11	Discard-Request	
12	Identification	dient der eigenen Identifizierung, z. B. zur Fehlersuche oder bei Lizenz-Prüfungen.
13	Time-Remaining	die Netz-Seite informiert über die Dauer der Session
14	Reset-Request	Für Datenkompression
15	Reset-Ack	

PPP – Link-Control Protocol Nachrichten – „Type“

Type	Typ	Bedeutung
1	Maximum-Receive-Unit	Maximale Datenpaket-Länge, die der Empfänger verarbeiten kann (Def.: 1500 Oktett).
2	Async-Control-Character-Map	bestimmt, wie Steuerzeichen in einer asynchronen Kommunikation behandelt werden
3	Authentication-Protocol	Typ des verwendeten Authentisierungs-Protokolls (zwei Optionen: „Password Authentication Protocol“ oder „Challenge Handshake Authentication Protocol“)
4	Quality-Protocol	Typ des verwendeten Quality Protokolls (derzeit nur der „Link Quality Report“)
5	Magic-Number	Eine Zufallszahl, die z.B. vom Quality-Protokol benötigt wird.
7	Protocol-Field-Compression	Fordert die Kompression des PPP-Protokoll-Elements auf 1 Oktett an.
8	Address-and-Control-Field-Compression	Fordert die Kompression der Data-Link-Layer-Address und des -Control-Fields an.
13	Callback	Anforderung eines Rückrufes
14	Connect-Time	
15	Compund-Frames	erlaubt mehrere Datenpakete in einem PPP-Rahmen
17	Multilink-MRU	Für Multilink PPP
18	Multilink-Short-Sequence-Number-Header-Format	
19	Multilink-Endpoint-DIsriminator	
23	Link-Discriminator-Option	Für Bandwidth Allocation Protocol
25	DCE Identifier	Data Circuit-Terminating Equipment (DCE) versucht seriellen Link aufzubauen
26	Prefix-Elision-Option	Für Multiclass Extension und Suspend & Resume
27	Multilink-Header-Format-Option	
28	Internationalization	Aushandeln von Zeichensatz und Sprache

PPP – Prinzip

Das PPP besteht aus drei Komponenten:

- Eine Methode um Paket-Daten entsprechend verpackt zu übertragen - **PPP Encapsulation**.
Dabei wird von einer bidirektionalen Vollduplex-Übertragung ausgegangen.
- Ein Protokoll um die Übertragungsstrecke auf- und abzubauen, zu konfigurieren und zu testen, das **Link Control Protocol (LCP)**.
- Ein entsprechendes Steuerprotokoll, um verschiedene Schicht-3-Protokolle auf- und abzubauen und zu konfigurieren, das **Network Control Protocol (NCP)**.

PPP – Network Control Protocol (NCP)

- Nachdem der Link mit dem LCP konfiguriert und aufgebaut wurde, muss mit dem NCP eines oder mehrerer Network Layer Protokolle ausgewählt und konfiguriert werden.
- Der Aufbau des NCP entspricht dem des LCP. Einziger Unterschied ist, dass sich jetzt die Funktionen auf die Netz-Schicht beziehen und nicht mehr auf die Link-Schicht.
- Für viele Network-Protokolle wurden Network Control Protocols definiert.

PPP – Network Control Protocol (NCP) – Typen

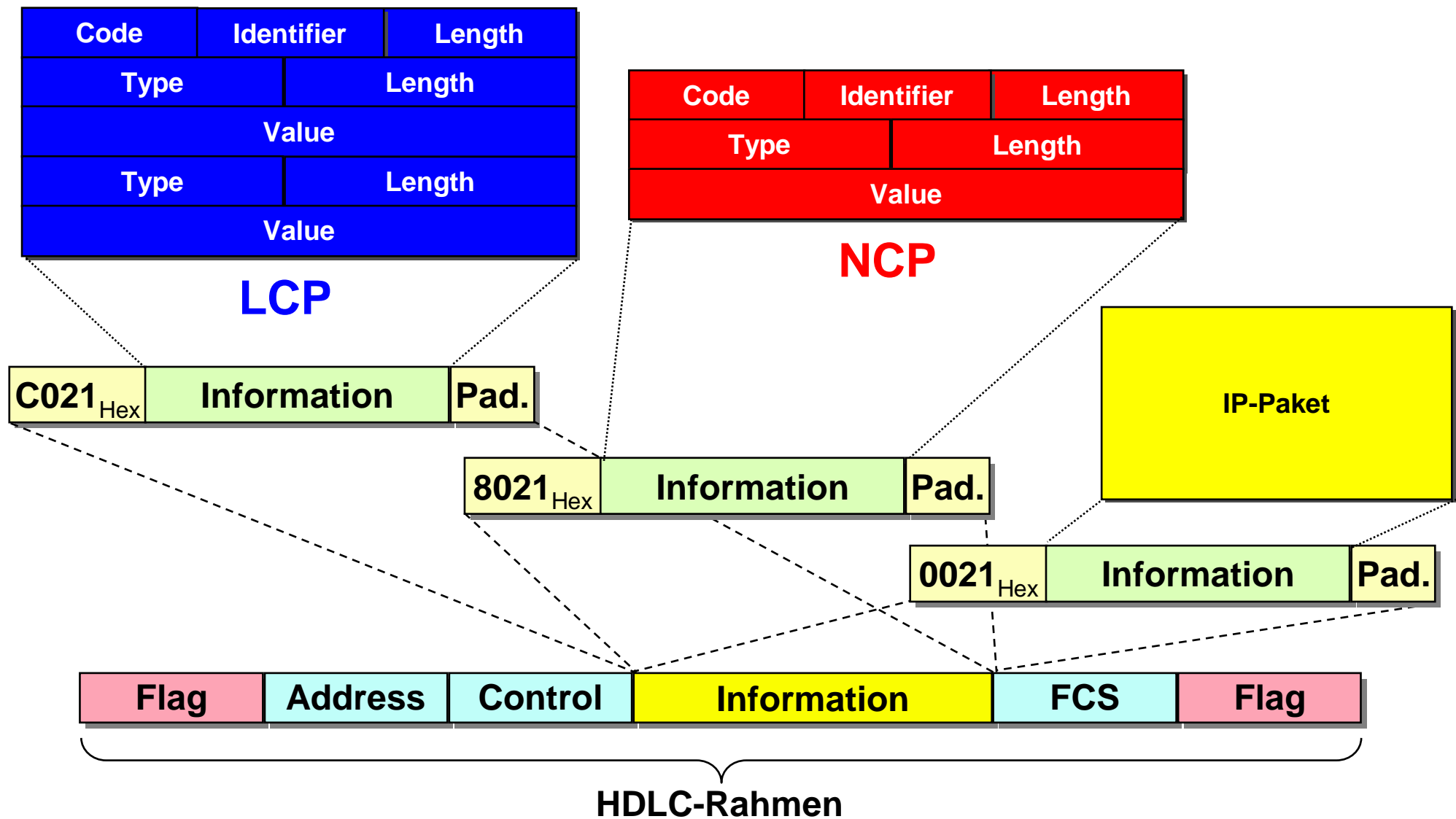
NCP	Network Protocol
IPCP	Internet Protocol Version 4
IPV6CP	Internet Protocol Version 6
OSINLCP	OSI Network Layer (CLNP, ES-IS, IS-IS, IDPR, ..)
ATCP	Apple Talk
IPXCP	IPX (Internetwork Packet Exchange, Novell)
DNCP	DECnet Phase IV (Digital Equipment Corporation)
BVCP	Banyan Vines
XNSCP	XNS IDP (Xerox Network Systems Internet Datagram Protocol)
SNACP	SNA (Systems Network Architecture, IBM)
NBFCP	NetBIOS (NetBIOS Frame, IBM)
PPMuxCP	PPP Multiplexing Control Protocol
BCP	Remote Bridging nach IEEE 802.1D

PPP – Protocol-Werte für das Network-Control Protocol (NCP)

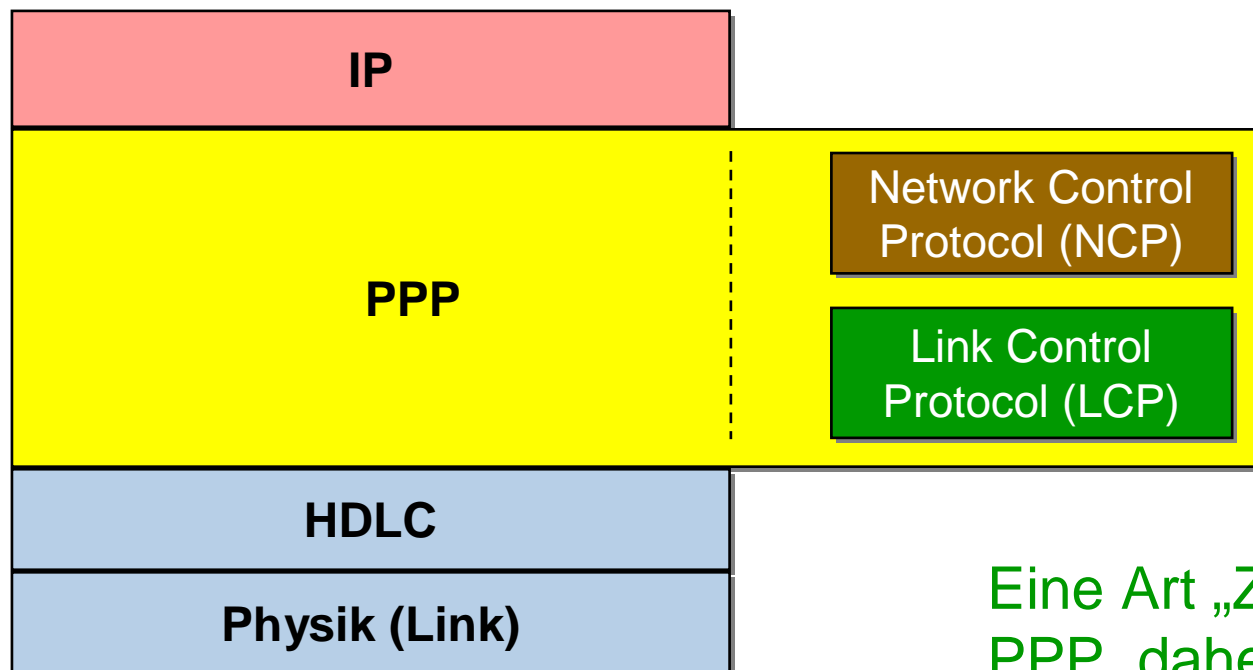
- Im Protocol-Feld des PPP-Rahmens sind die Werte 8000_{Hex} ... BFFF_{Hex} für das NCP reserviert.

8001 _{Hex} - 801F _{Hex}	nicht benutzt
8021 _{Hex}	für IP = IPCP
8041 _{Hex}	für LAN Extension
8057 _{Hex}	für IPv6 = IPV6CP [RFC2472]
8059 _{Hex}	für PPMuxCP
805B _{Hex}	Vendor Specific NCP
807D _{Hex}	nicht benutzt
80CF _{Hex}	nicht benutzt
80FB _{Hex}	komprimierte Daten (Link)
80FD _{Hex}	komprimierte Daten (Datagramm)
80FF _{Hex}	nicht benutzt

PPP – Rahmentypen



PPP – Protokollmodell



Eine Art „Zeichengabe“ für PPP, daher separat gezeichnet

PPP – Qualitätsüberwachung

- Übertragungsstrecken sind selten ideal - Paketfehler oder Paketverluste können auftreten. Eine Überwachung der Qualität ist daher sinnvoll.
- PPP stellt dafür einen „**Link Quality Report**“ (LQR) bereit, mit dem einem Sender die Anzahl fehlerfrei empfangener Oktetts zurückgemeldet wird. Der Sender kann dann diese Information mit seinen eigenen Zählerständen vergleichen.
- Drei Zähler müssen für die Qualitätsüberwachung vorgesehen werden:
 - **OutLQRs**: ein 32-Bit-Zähler für die gesendeten Link Quality Reports, startend mit dem 1. LQR.
 - **InLQRs**: ein 32-Bit-Zähler für die Empfangenen Link Quality Reports, ebenfalls startend mit dem 1. LQR.
 - **InGood_Octetts**: ein 32-Bit-Zähler, der die fehlerfrei empfangenen Oktetts zählt.

PPP – Was PPP nicht leistet

Folgende Funktionen sind in PPP nicht beinhaltet:

- Flusskontrolle
- Fehlerkorrektur
- Paketreihenfolge

Diese Funktionalitäten müssen bei Bedarf von höheren Schichten geleistet werden.

Inhalt

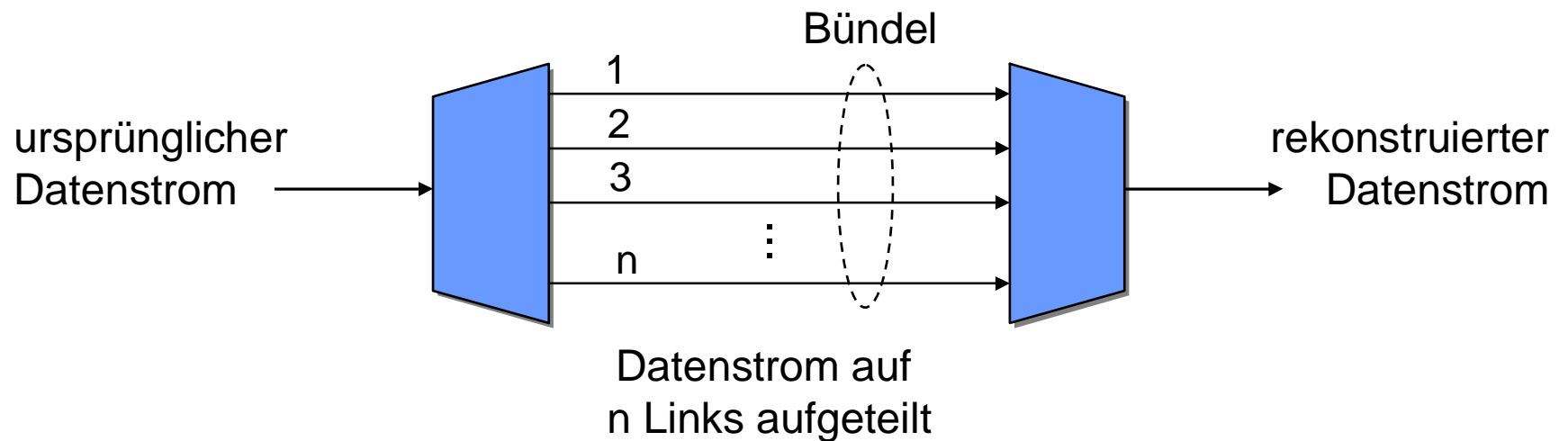
- High Level Data Link Control (HDLC)
- Frame Relay (FR)
- Point-to-Point Protocol (PPP)
 - Grundform
 - Sonderformen von PPP
 - Tunneling-Protokolle
 - Breitbandiger Anschluss
 - Unterstützende Funktionen

Sonderformen von PPP

- Multilink-PPP
- Multinode-Unterstützung
- Dynamische Bandbreitensteuerung
- Always-On / Dynamic ISDN (AO/DI)
- Unterstützung von links geringer Bitrate
 - Multiclass Extension
 - Suspend & Resume
 - PPP Multiplexing

Multi-Link PPP – Konfiguration

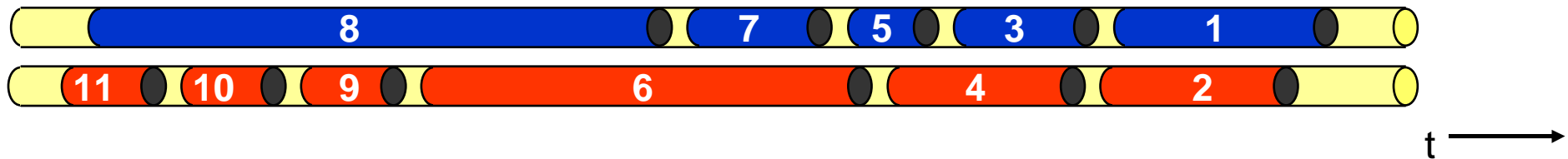
- **Warum?** Mit dem Aufkommen von ISDN und dem Transport von IP-Daten über ISDN wuchs auch der Wunsch, nicht nur einen, sondern mehrere B-Kanäle zu benutzen.
- **Wie?** Inverses Multiplexing



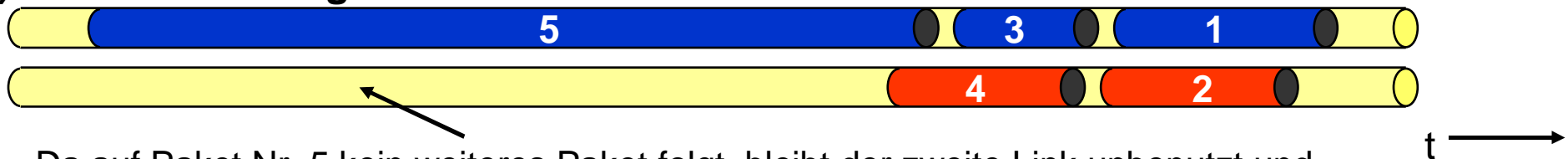
- **Problem?** Effizientes Multiplexen unterschiedlich langer Pakete
- **Lösung:** Fragmentieren langer Pakete

Multi-Link PPP – Fragmentierung

a) Paketweises Multiplexen, nächstes Paket auf nächsten freien Link

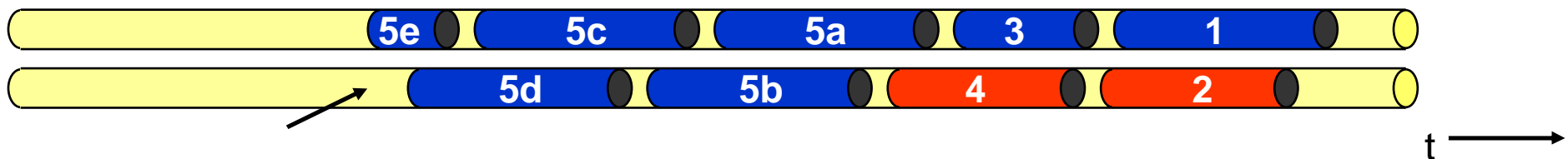


b) Problem der langen Pakete



Da auf Paket Nr. 5 kein weiteres Paket folgt, bleibt der zweite Link unbenutzt und Paket Nr. 5 wird nur mit der Bitrate eines Links ausgesendet.

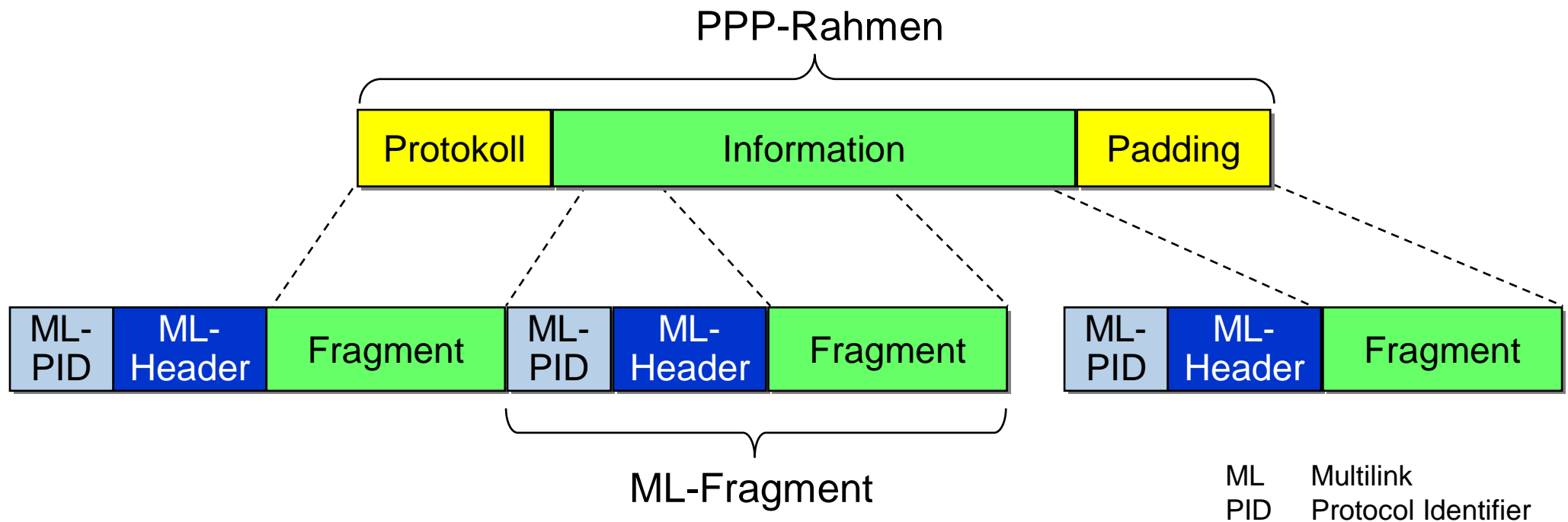
c) Fragmentieren großer Pakete, nächstes Fragment auf nächsten freien Link



Paket Nr. 5 wird fragmentiert in die Fragmente 5a bis 5e. Diese werden auf die beiden Links gemultiplext. Die Übertragung ist früher beendet wie oben.

Multi-Link PPP – Datenrahmen der Fragmente

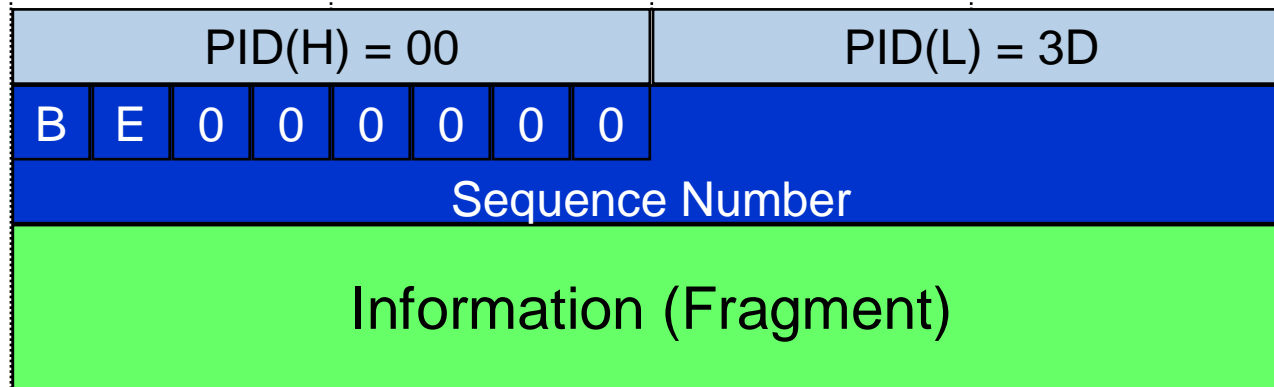
- Fragmente benötigen eigene Protokoll-Elemente (Konfigurationsoptionen).
- Fragmente und PPP-Rahmen müssen unterscheidbar sein.
- Neue Konfigurationsoptionen im LCP notwendig.



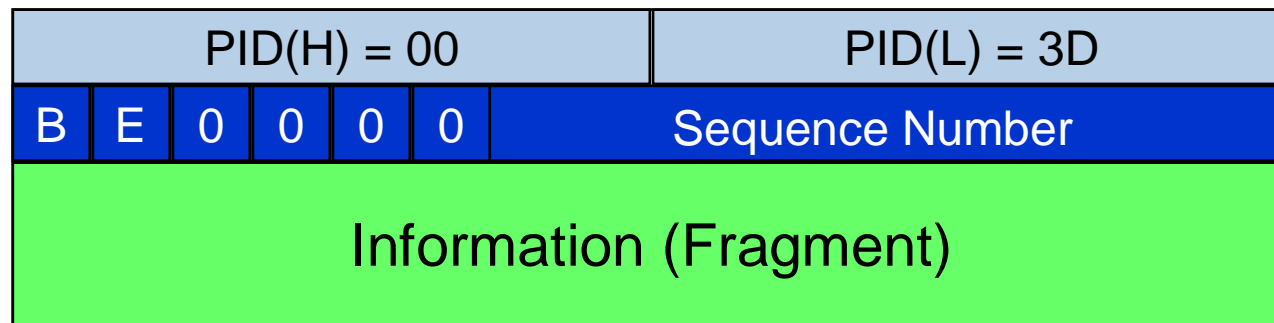
Multi-Link PPP – Fragment-Formate

0 4 8 12 16 20 24 28 31

ML-Fragment mit langer Sequence Number



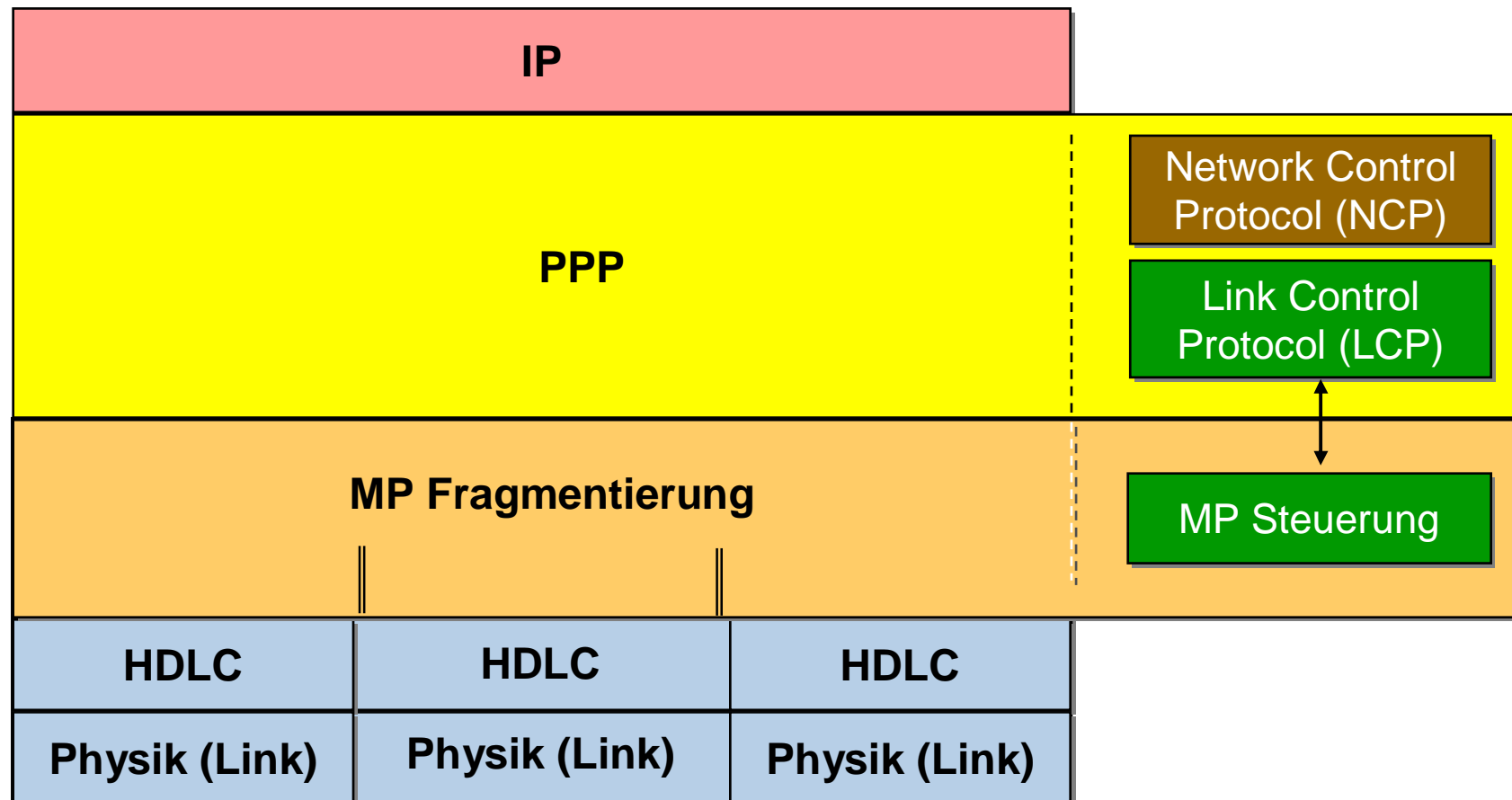
ML-Fragment mit kurzer Sequence Number



Zwei Fragment-Formate
mit unterschiedlich
langer Sequenz-
Nummer.

B Begin = erstes Fragment
E End = letztes Fragment

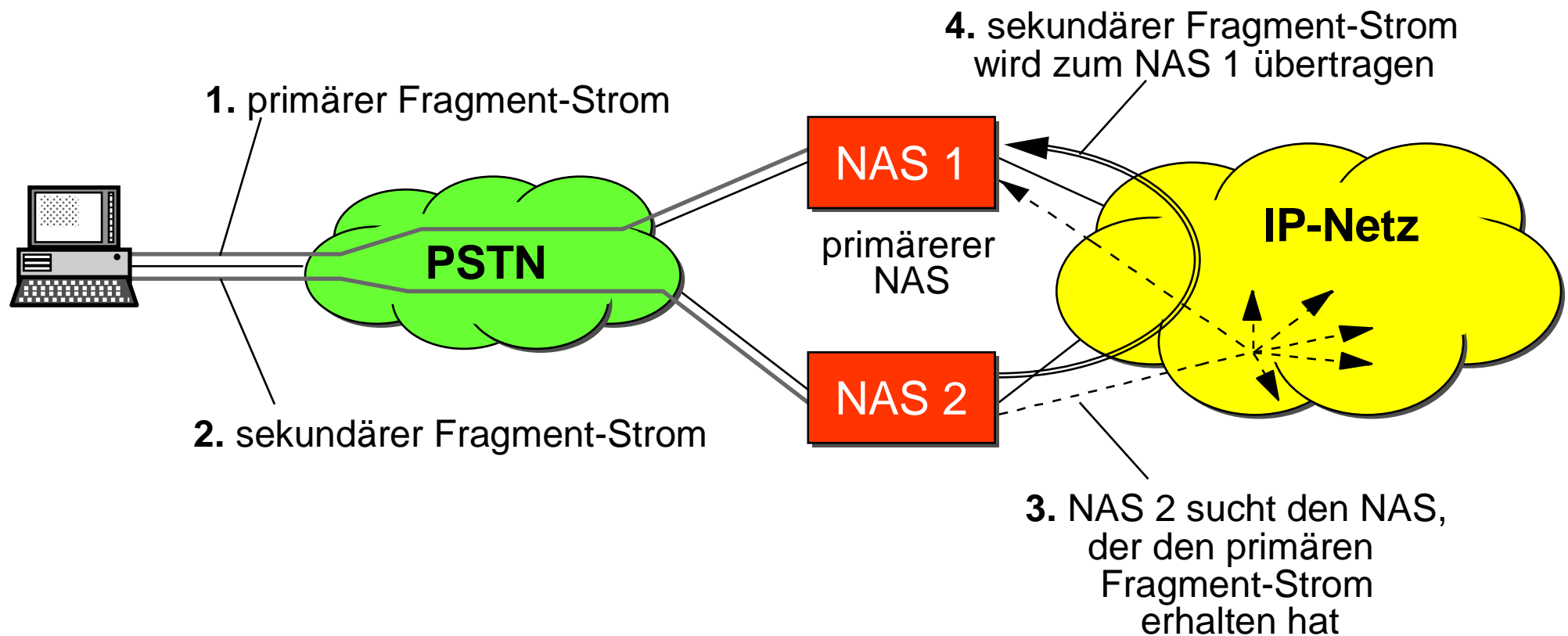
Multi-Link PPP – Protokollmodell



Multi-Node-Unterstützung (1)

- Fragmentströme werden in einem Knoten (**Network Access Server**, NAS) wieder zusammengefasst.
- Aufgrund einer Überlastung des NAS, könnten Fragmentströme an andere NAS des gleichen Internet Service Providers (ISP) geleitet werden.
- Problem: wie finden sich die **Fragmentströme** wieder zusammen?
- Lösung: zwei Komponenten sind notwendig
 - Ein Protokoll mit dem der NAS ermittelt werden kann, der den primären Fragmentstrom erhält
 - einfaches **Discovery-Protocol**, Anfrage per Multicast
 - Ein Transportprotokoll, mit dem sekundäre Fragmente an den primären NAS übertragen werden.
 - **Layer-2 Tunneling Protocol**

Multi-Node-Unterstützung (2)



NAS Network Access Server
PSTN Public Switched Telephone Network

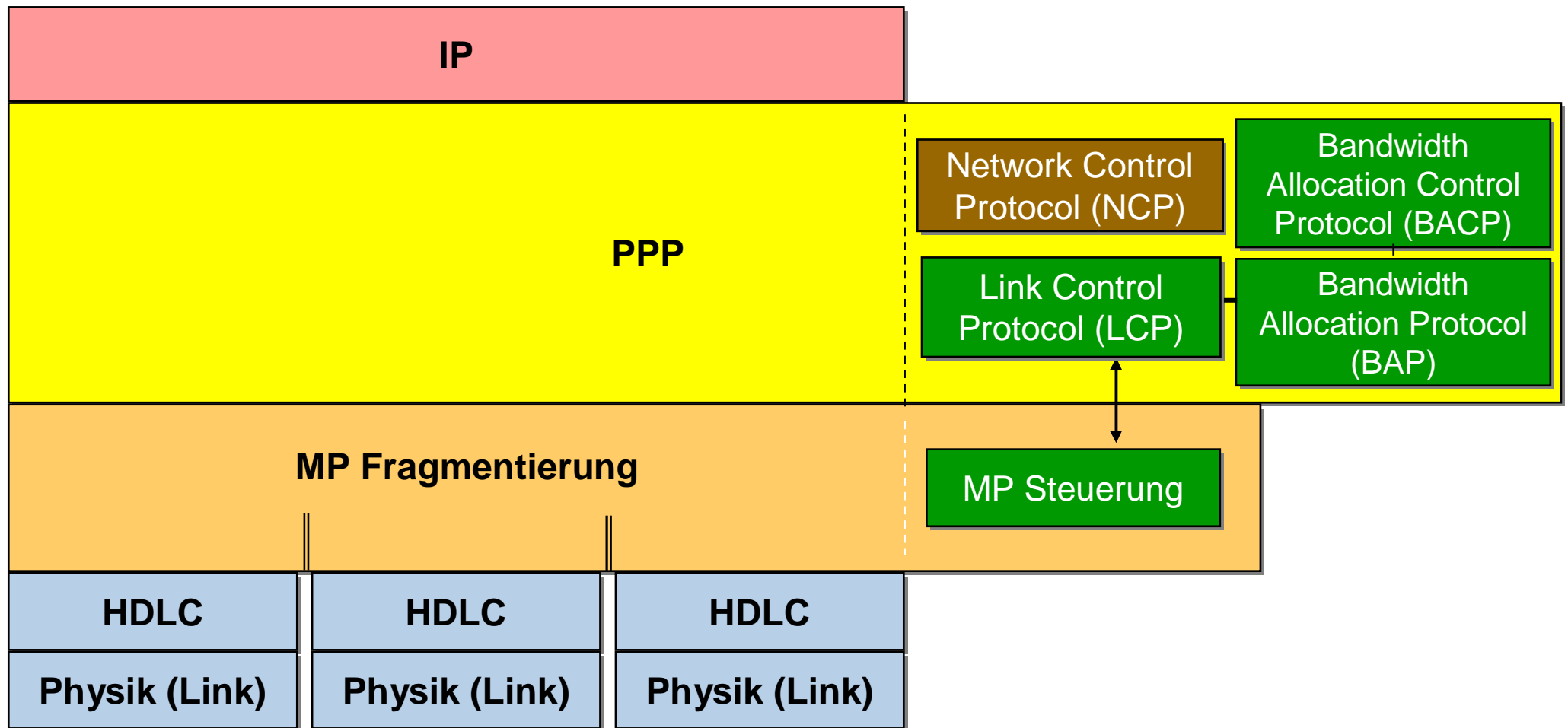
Dynamische Bandbreitensteuerung (1)

- **Problem:** jede Leitung, jeder Kanal kostet Geld
- **Lösung:** ein dynamischer Prozess, der bei Bedarf weitere Leitungen/Kanäle zur Verbindung addiert und wenn dieser Bedarf nicht mehr besteht, diese zusätzliche Kapazität wieder freigibt.
- Dazu wurden zwei Protokolle entwickelt:
 - **Bandwidth Allocation Protocol (BAP)**
und das zugehörige Steuerprotokoll
 - **Bandwidth Allocation Control Protocol (BACP).**
- Eindeutige Kennzeichnung für die Links notwendig („Link Discriminator“)
- Neue Konfigurationsoptionen im LCP notwendig.

Dynamische Bandbreitensteuerung (2)

- **Bandwidth Allocation Control Protocol (BACP)**
 - eigenes Link-Layer Control Protocol, vergleichbar dem LCP;
 - zuständig für das ganze ML/PPP-Bündel;
 - spezifisch: um den Falle einer Kollision (wenn die zwei Seiten gleichzeitig eine Anforderung für einen Link senden) auflösen zu können, wird eine Seite zum „Chef“ erklärt.
- **Bandwidth Allocation Protocol (BAP)**
 - Funktionen für jeden einzelnen Link in einem Bündel
 - Nachrichten und Prozeduren, mit denen:
 - ein zusätzlicher Link hinzugefügt werden kann;
 - die andere Seite aufgefordert werden kann, einen zusätzlichen Link hinzuzufügen („callback“);
 - ein Link wieder freigegeben werden kann.

Dynamische Bandbreitensteuerung (3)



Always-On / Dynamic ISDN (1)

- Mit der Entwicklung
 - von PPP
 - zu MultiLink PPP und dann
 - mit BAP/BACP

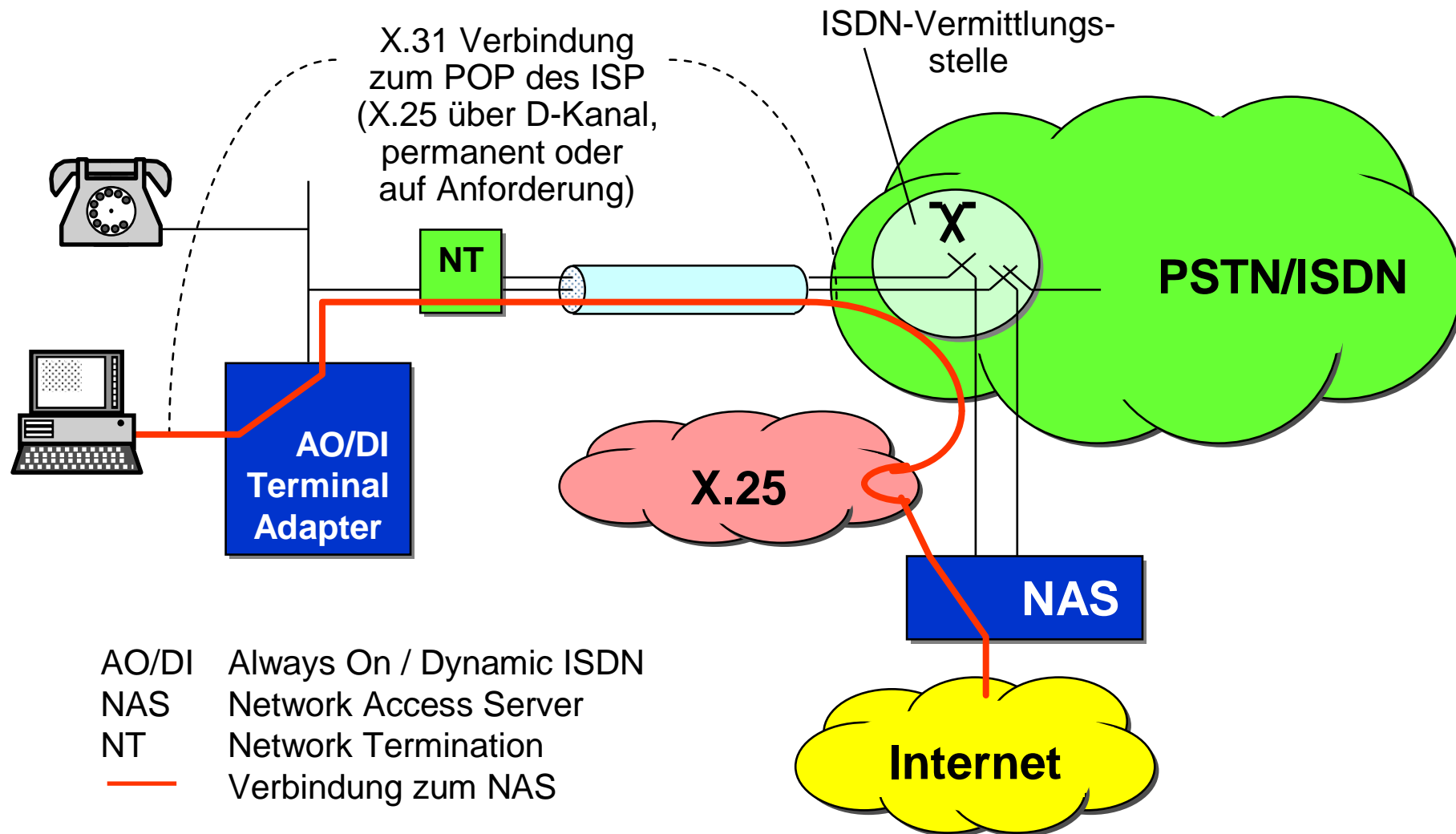
fehlt nur noch ein kleiner Teil, um eine sehr elegante ISDN-Lösung zu erzielen, die unter dem Namen
Always On / Dynamic ISDN (AO/DI)
bekannt wurde.

- Einzige Erweiterung: der Zugang zu einem paketvermittelten Netz (X.25) über den D-Kanal, auch als X.31-Paket-Transport bezeichnet.

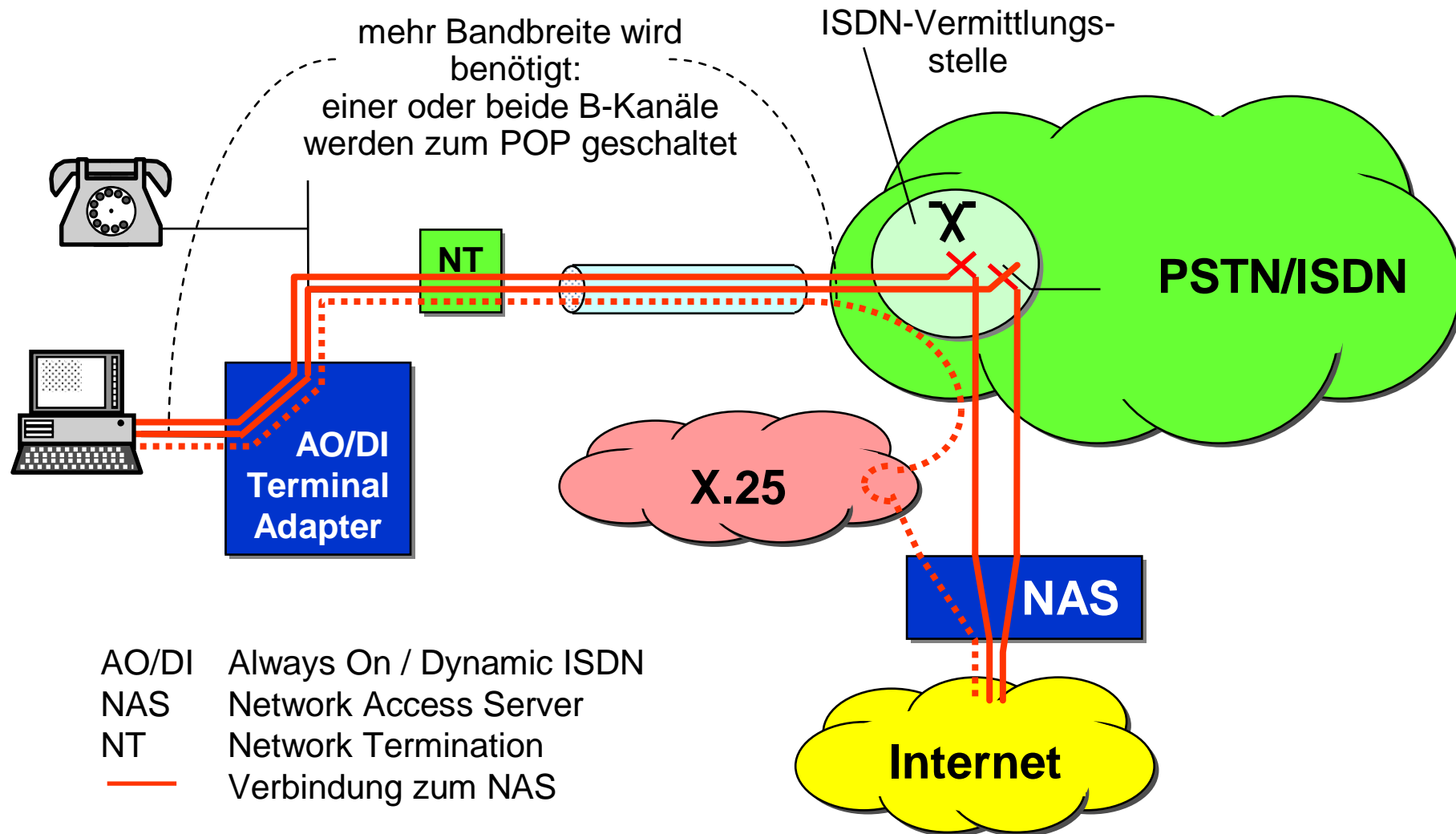
ISDN: Always On / Dynamic ISDN

- Vorschlag der amerikanischen “Vendors ISDN Association” (VIA).
- Benutzung des D-Kanals eines ISDN Basic Access um direkt und mit dem Internet verbunden zu sein.
- Der D-Kanal transportiert TCP/IP über X.25 / LAPD und dient als “low speed access”.
- B-Kanäle werden nach Bedarf zu- und abgeschaltet und damit besser genutzt als heute.

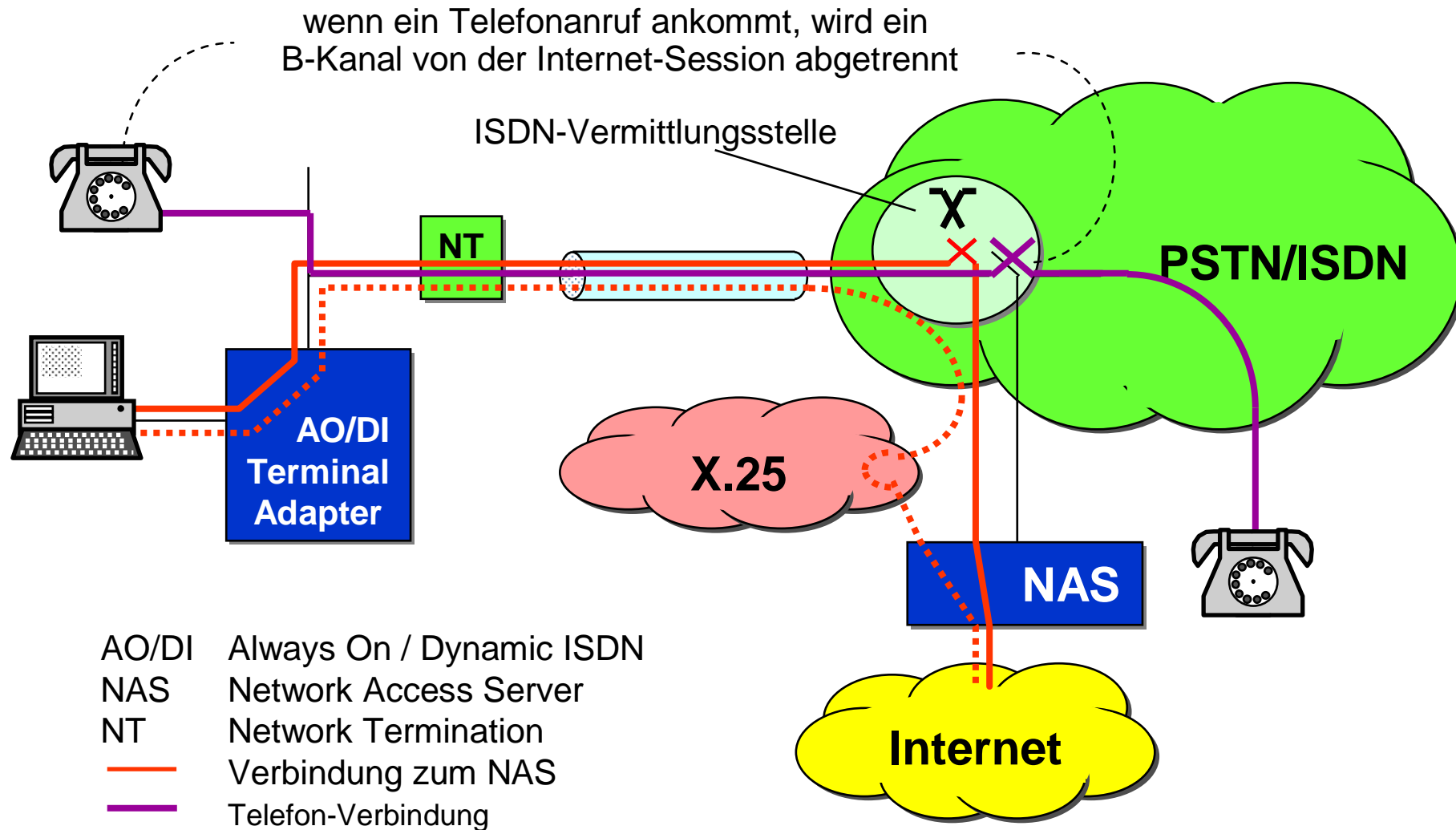
Always-On / Dynamic ISDN (2)



Always-On / Dynamic ISDN (3)



Always-On / Dynamic ISDN (4)



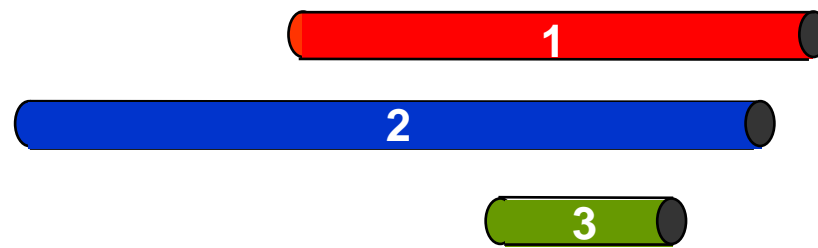
Erweiterungen für Links mit geringer Bitrate

- **Problem:** Für die Übertragung von multimedialer Information sind Links mit geringer Bitrate wie z. B. Modemstrecken, ISDN, X.25 nur eingeschränkt geeignet. Grund: solche multimediale Information bestehen normalerweise aus mehr oder weniger parallel zu übertragenden Informationsströmen unterschiedlichster Art. Beispiel ist eine Videokonferenz mit Bild, Ton, Zusatzdaten und begleitenden Steuerinformationen. Lange Pakete belegen dabei den Link und blockieren damit u.U. kurze Echtzeit Pakete.
- **Lösungsmöglichkeiten:**
 - Fragmentierung auf der IP-Schicht
 - Benutzen einer Schicht 2 mit kleinen, konstanten Datenpaketen
 - Benutzen des Multiplex-Schemas nach H.223
 - Einsatz einer Fragmentierung auf dem Link mit Prioritätensteuerung

Multiclass Extension

Erste Lösung: Fragmentieren wie bei Multilink-PPP aber mit Qualitätsklassen

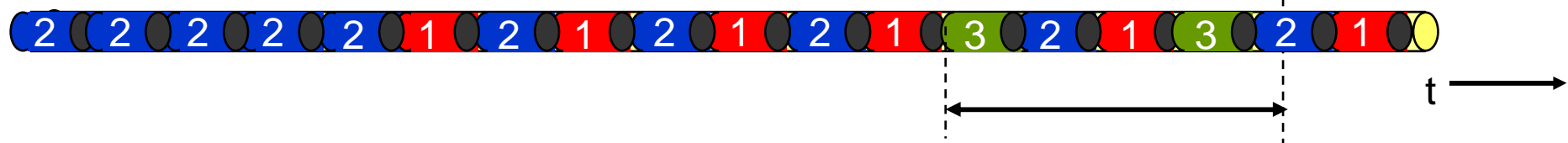
a) 3 Pakete stehen zur Übertragung an



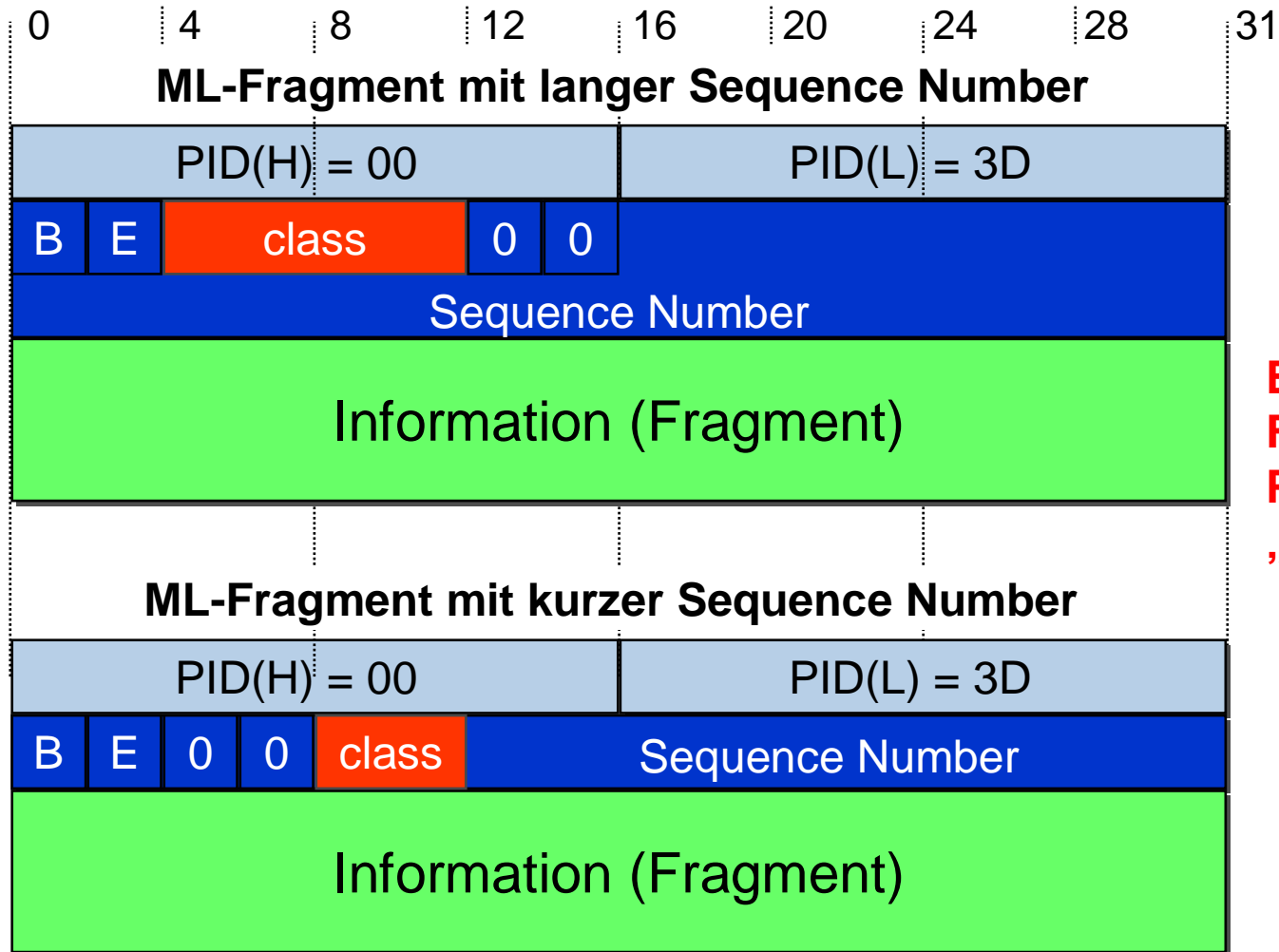
b) Normales Multiplexen: Paket 3 muss sehr lange warten



c) Fragmentieren: „Schnellere“ Übertragung für Paket 3



Fragment-Formate mit Multiclass Extension



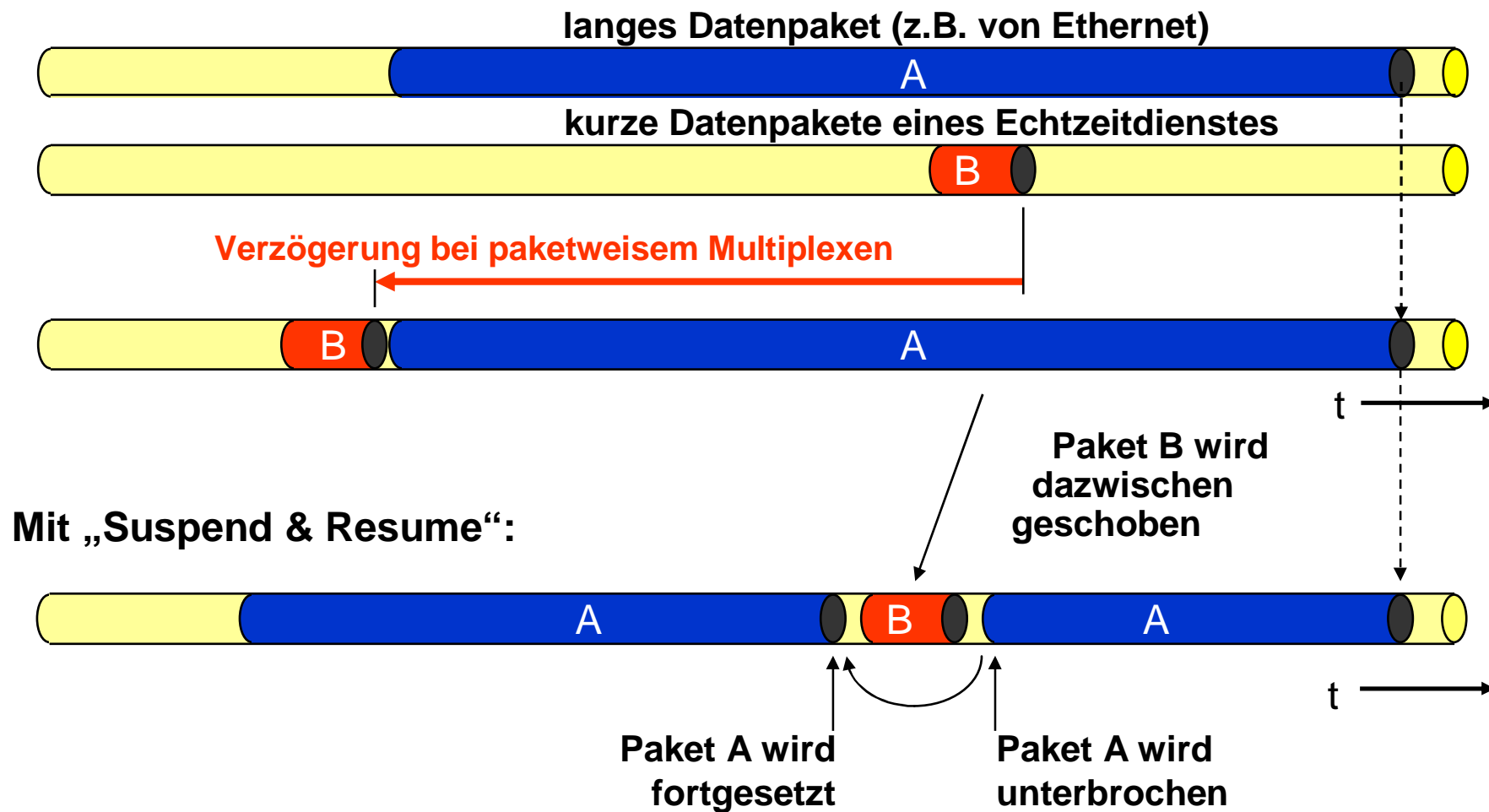
Erweiterung der
Fragmente um eine
Prioritätsangabe, hier
„class“ genannt.

B Begin = erstes Fragment
E End = letztes Fragment

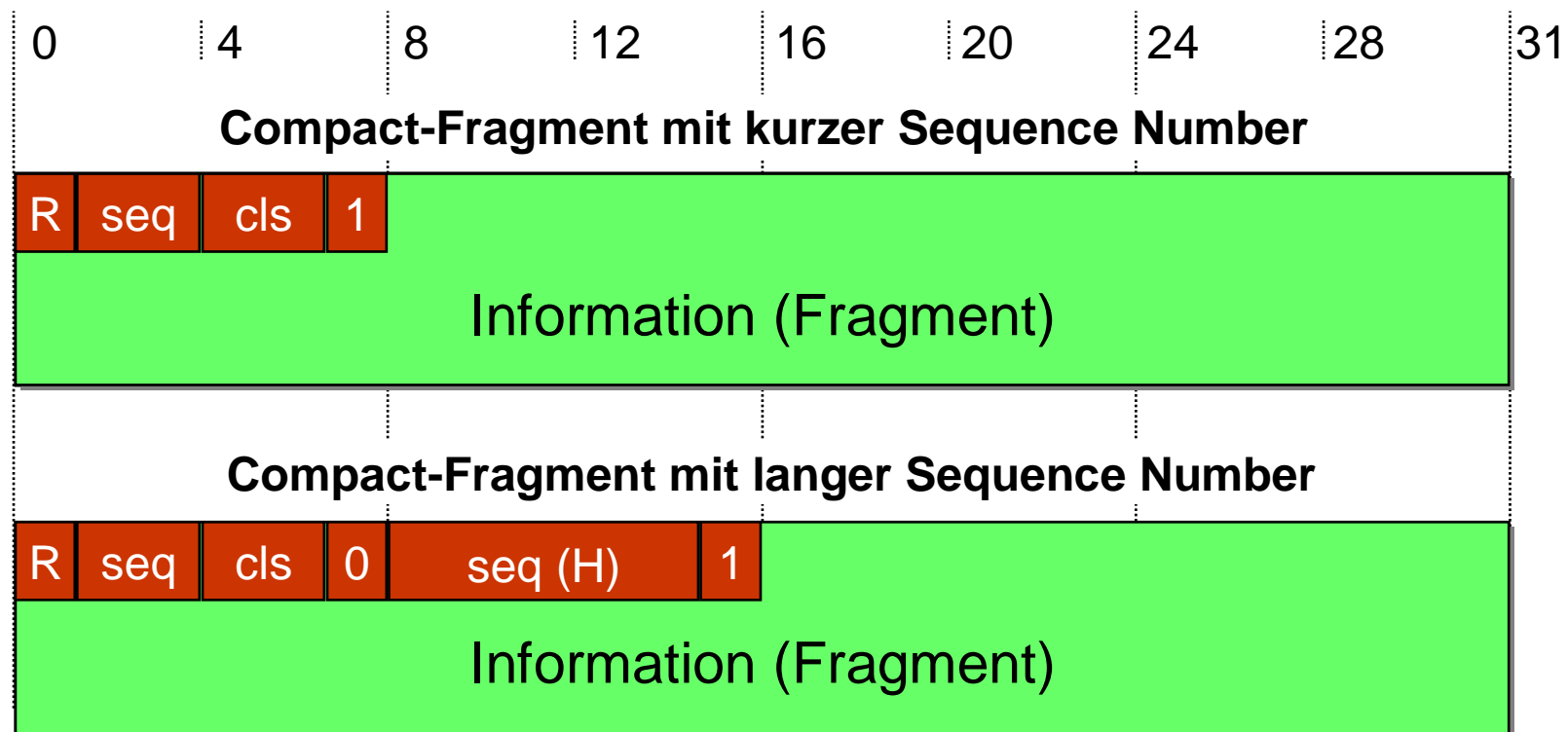
Suspend & Resume – Allgemeines

- **Zweite Lösung:** Bei Sendern, die auf Oktett-Ebene die Kontrolle über die Sendung haben, wird versucht, ein langes Paket ohne Fragmentierung zu senden. Erst wenn ein Echtzeit-Dienst versucht, ebenfalls ein Paket abzusenden, dann wird das lange Paket unterbrochen, das kurze Echtzeit-Paket gesendet und danach das lange Paket fortgesetzt.
- **Vorteil:** es wird nur fragmentiert, wenn es auch notwendig ist.
- Da hierzu größere Änderungen am Multiplik-PPP-Fragment notwendig wären, wird ein anderes, kompakteres Fragment-Format vorgeschlagen.

Suspend & Resume – Funktionsweise



Suspend & Resume – Fragment-Formate



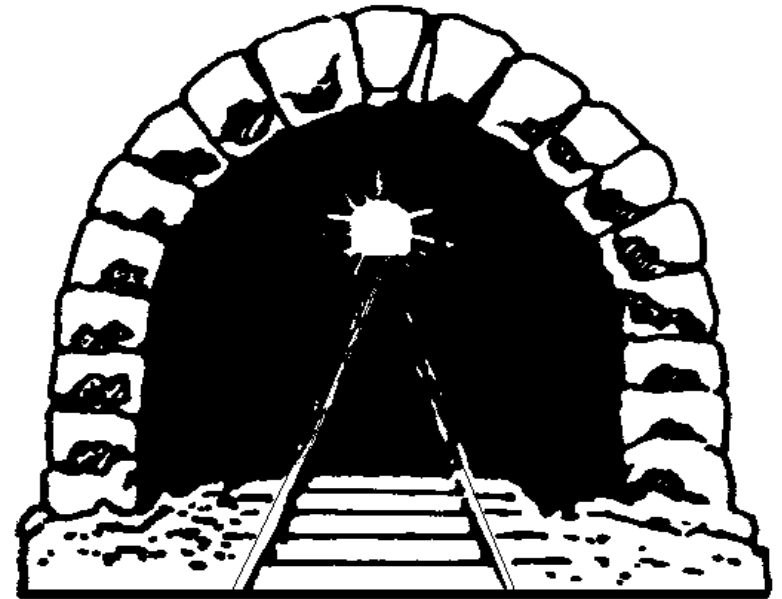
R Resume (1 Bit)
seq Sequence-Number (3 oder 10 Bit)
cls Class (Prioritätsklasse, 3 Bit, erweiterbar)

Inhalt

- High Level Data Link Control (HDLC)
- Frame Relay (FR)
- Point-to-Point Protocol (PPP)
 - Grundform
 - Sonderformen von PPP
 - Tunneling-Protokolle
 - Breitbandiger Anschluss
 - Unterstützende Funktionen

Tunneling

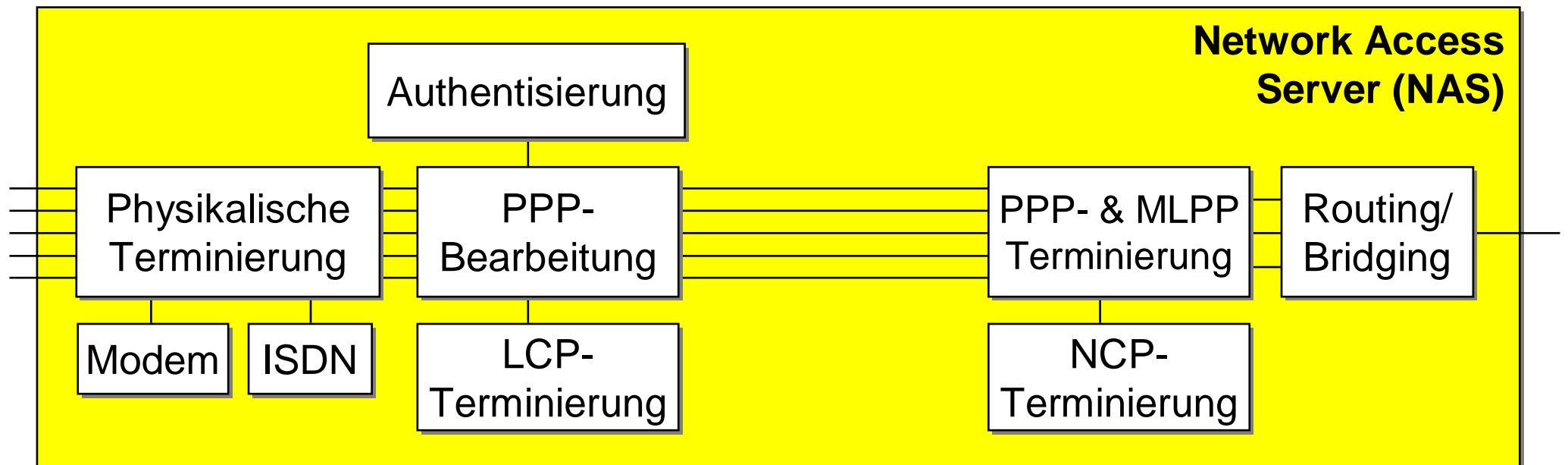
- Wenn Protokolle einer Schicht den Dienst anderer Protokolle der gleichen Schicht oder gar einer höheren Schichten nutzen, dann spricht man von **Tunneling**.
- Der Begriff ist umgangssprachlich, denn weder ITU noch ETSI verwenden ihn in offiziellen Dokumenten.
- Im Zusammenhang mit PPP wurden eine Reihe von **Tunneling-Protokollen** entwickelt.



Point-to-Point Tunneling Protocol (PPTP)

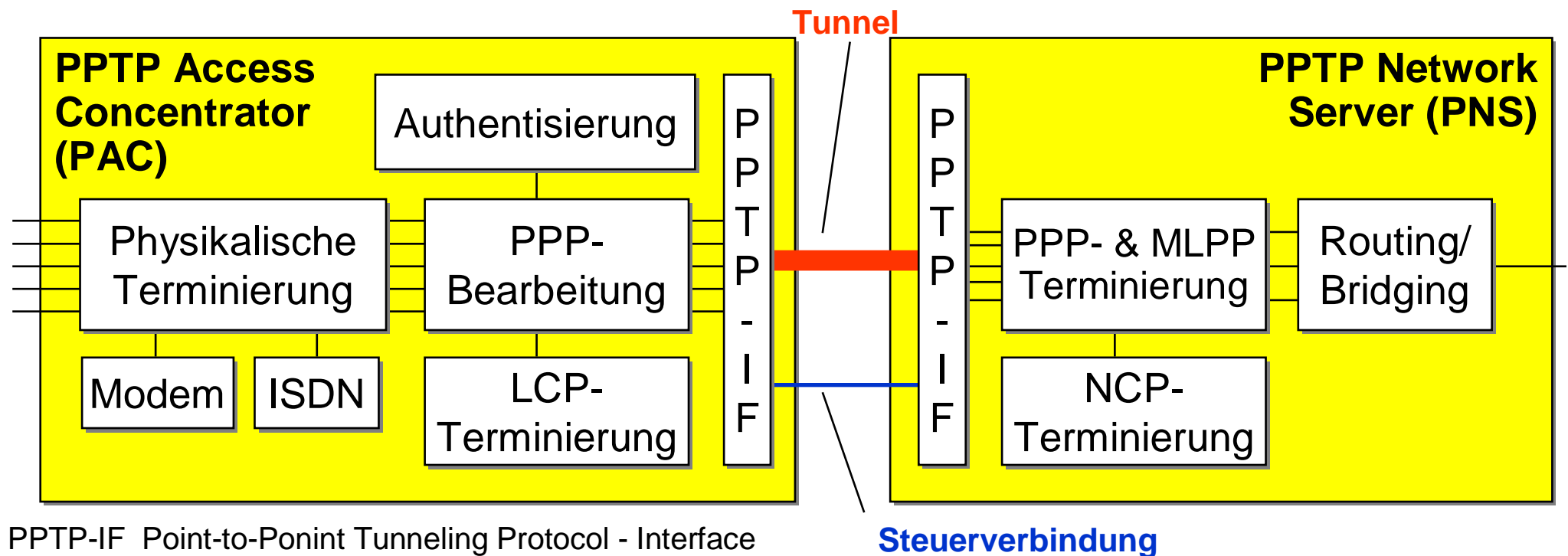
- Beim Point-to-Point Tunneling Protocol (PPTP) wird PPP über ein IP-Netz zu transportiert.
- Die Anwendung liegt in der Idee, den Zugangspunkt zum Internet, den Network Access Server (NAS), aufzuteilen.
- Die typischen Funktionen des NAS sind:
 - Terminierung der physikalischen Schnittstelle zur PSTN/ISDN-Welt mit Modem-Pool bzw. ISDN-Abschluss,
 - Terminierung des Link Control Protokolls (LCP),
 - Authentisierung,
 - Terminierung des PPP und, wenn vorhanden, auch des Multilink-PPP,
 - Terminierung der Network Control Protokolle (NCP) und schließlich
 - Bridging oder Routing zum IP-Netz.

PPTP – Network Access Server (NAS)

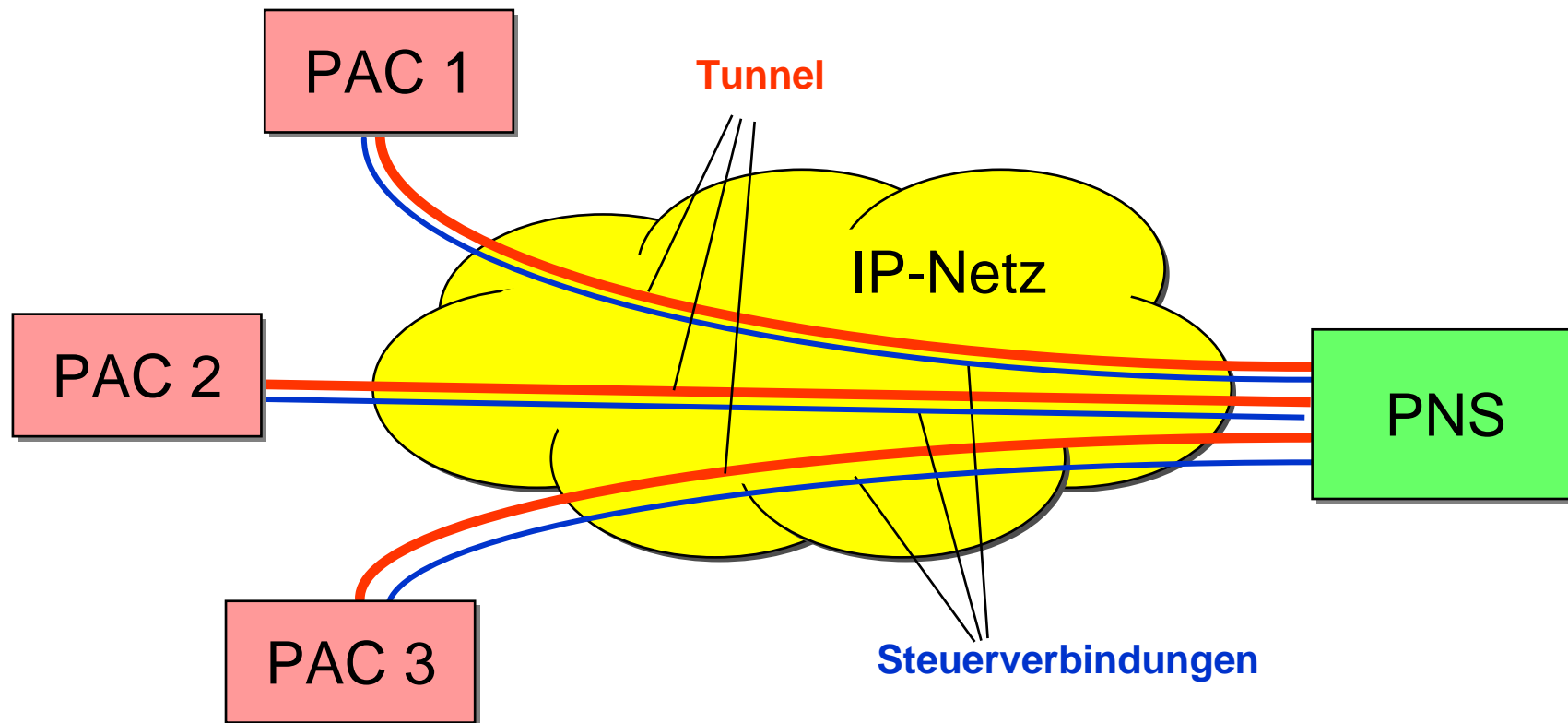


PPTP – Aufteilung des NAS

- Aufteilung des NAS in zwei neue Netzelemente
 - **PPTP Access Concentrator (PAC)**
 - **PPTP Network Server (PNS)**
- verbunden mit dem Point to Point Tunneling Protocol (PPTP)



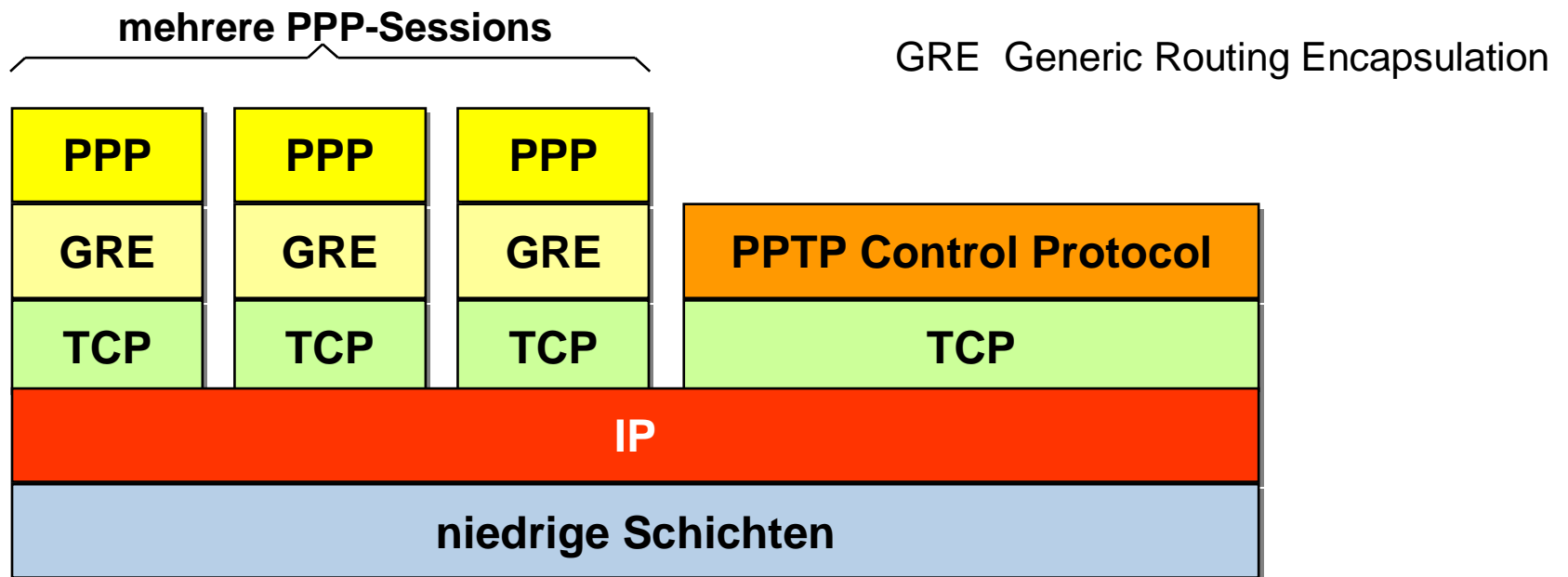
PPTP – Konfiguration mit mehreren PACs



PAC PPTP Access Concentrator
PNS PPTP Network Server

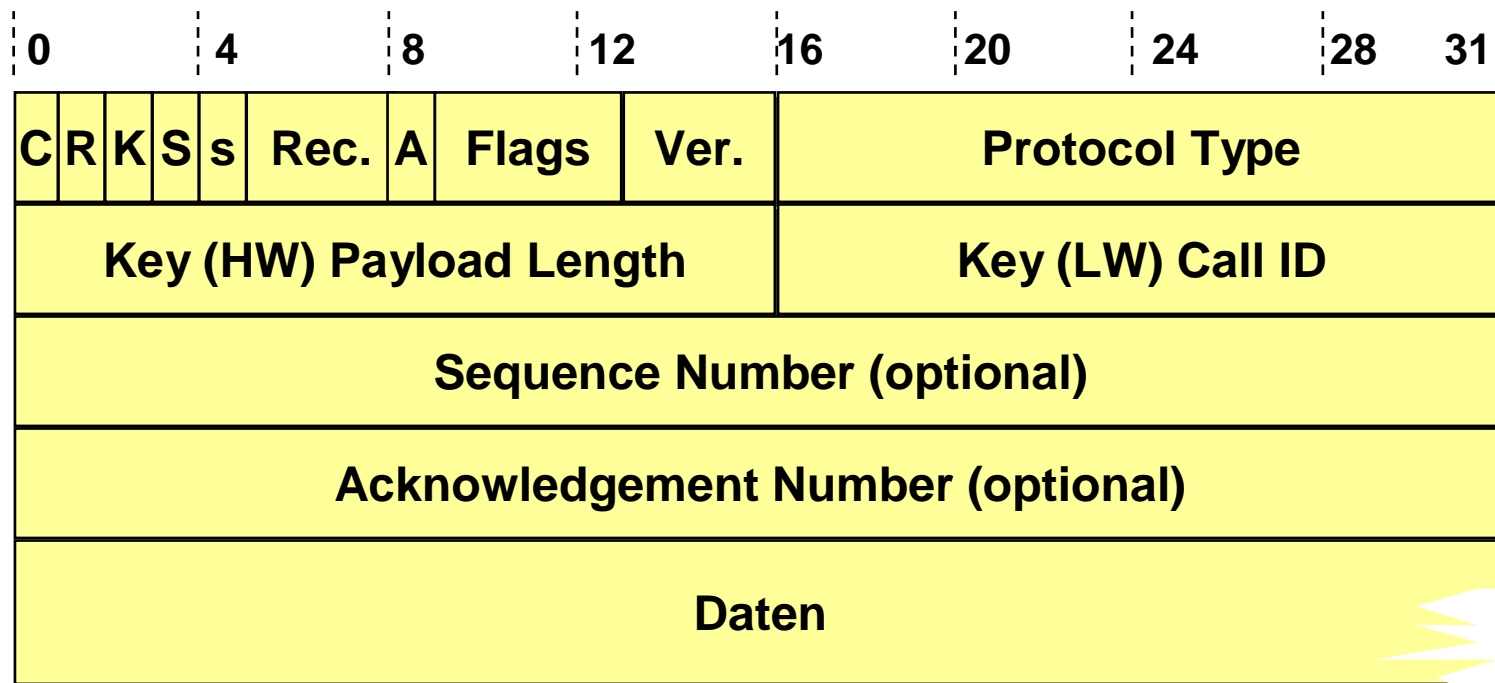
PPTP – Protokolle

- Ein Tunnel verbindet ein PAC-PNS-Paar und transportiert PPP-Rahmen. Mehrere Sessions werden gemultiplext und teilen sich einen Tunnel.
- Eine Steuerverbindung dient dem Auf- und Abbau sowie der Modifikationen des Tunnels.



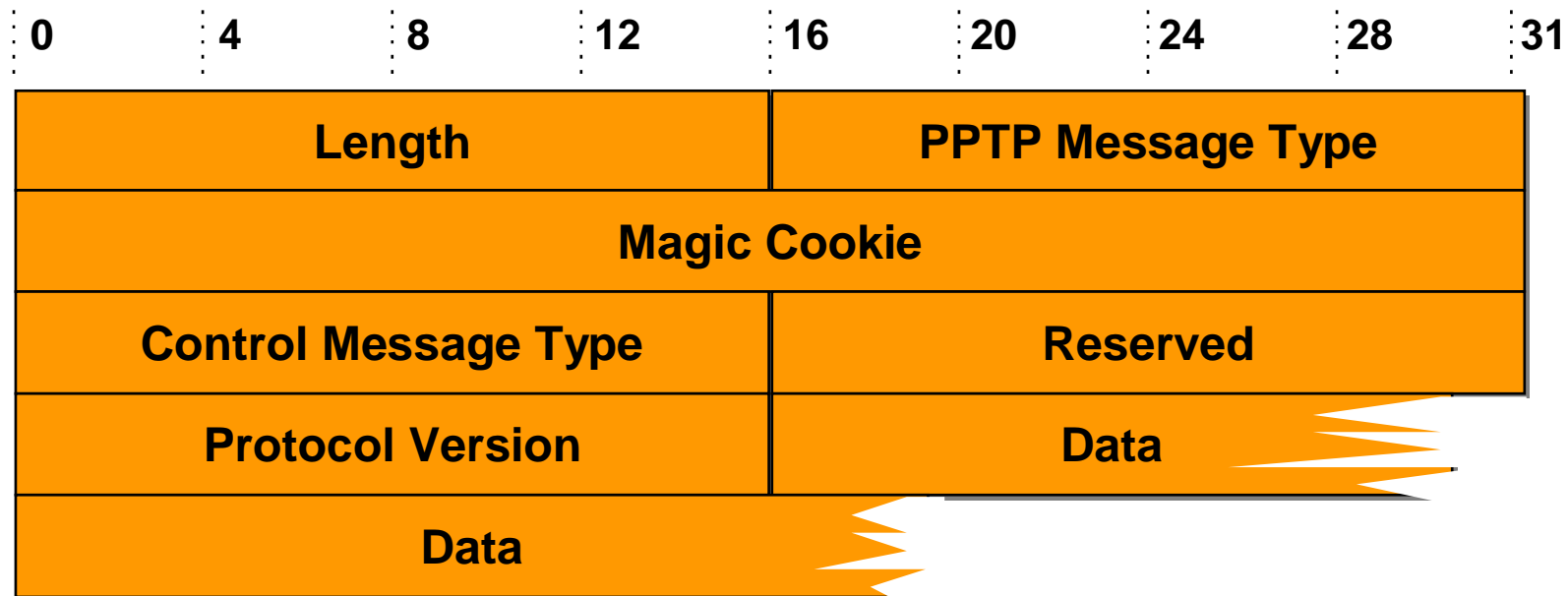
PPTP – Transport der Daten

- Die PPP-Information wird ohne Flags, Stuffing und Fehlerkorrektur in eine modifizierte Datenstruktur der **Generic Routing Encapsulation** (GRE) eingepackt.



PPTP – Steuerung

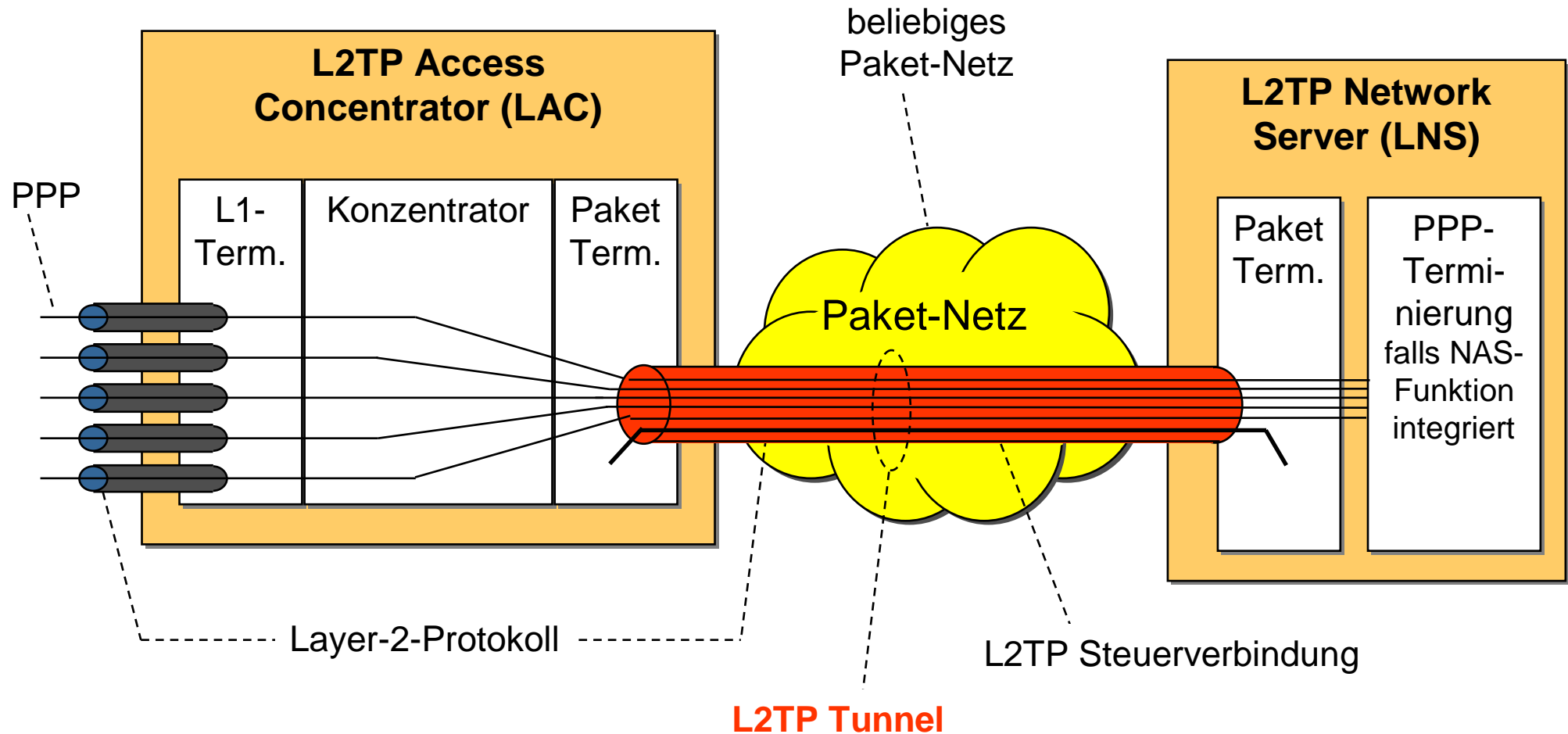
- Man unterscheidet
 - Steuernachrichten (PPTP Message Type 1) und
 - Management-Nachrichten (PPTP Message Type 2).



Layer-2 Tunneling Protocol (L2TP)

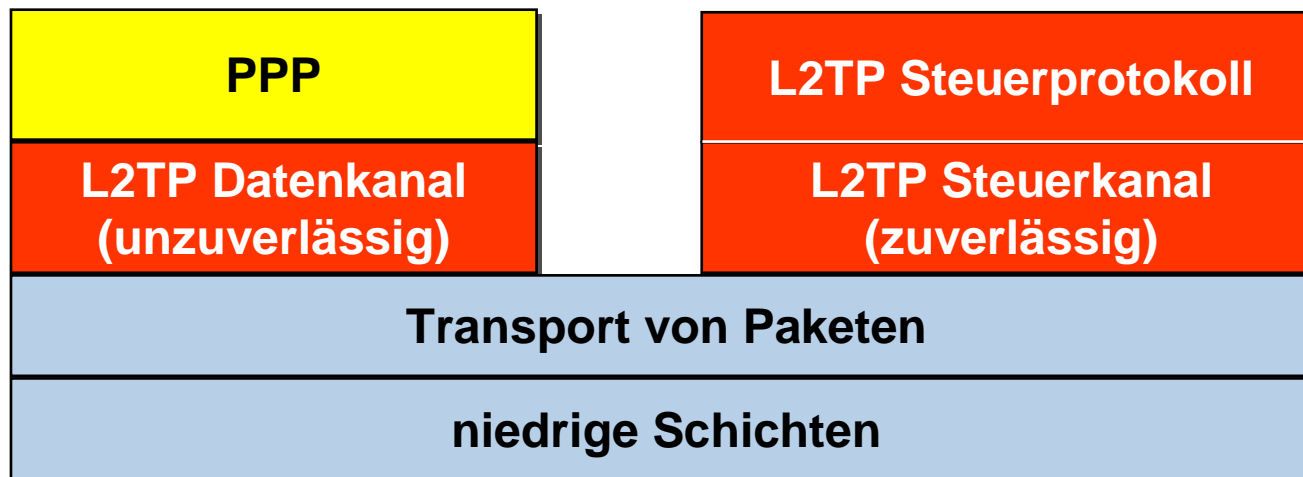
- Das PPTP dient dem transparenten Transport von **PPP-Rahmen über ein IP-Netz**.
- Das Layer-2 Tunneling Protocol (L2TP) verallgemeinert dieses Prinzip und beschreibt den transparenten Transport von **PPP-Rahmen über ein beliebiges Paketnetz**.
- Der Grund für dieses Vorgehen ist, dass jetzt die Terminierung der transportierenden Schicht und des PPP nicht mehr in einem Gerät vereinigt sein müssen. Die beteiligten Funktionsblöcke sind:
 - **L2TP Access Concentrator (LAC)**, der die Schicht-1 von den Teilnehmern terminiert, die PPP-Sessions zusammenfasst und über eine neue Paket-Schicht weiterleitet.
 - **L2TP Network Server (LNS)**, der die neue Paket-Schicht terminiert. Der LNS kann die Funktion des Network Access Servers (NAS) gleich mit übernehmen, dann muss er auch PPP terminieren, Authentisierung durchführen usw.

L2TP – Konfiguration



L2TP – Protokolle

- Im Vorfeld kann eine Konzentration durchgeführt werden
- Zwischen LAC und LNS sind mehrere Tunnels möglich.
- Mehrere LACs können an einen LNS angeschlossen sein .
- Ein spezielles Steuerprotokoll dient dem Auf- und Abbau der Tunnels.

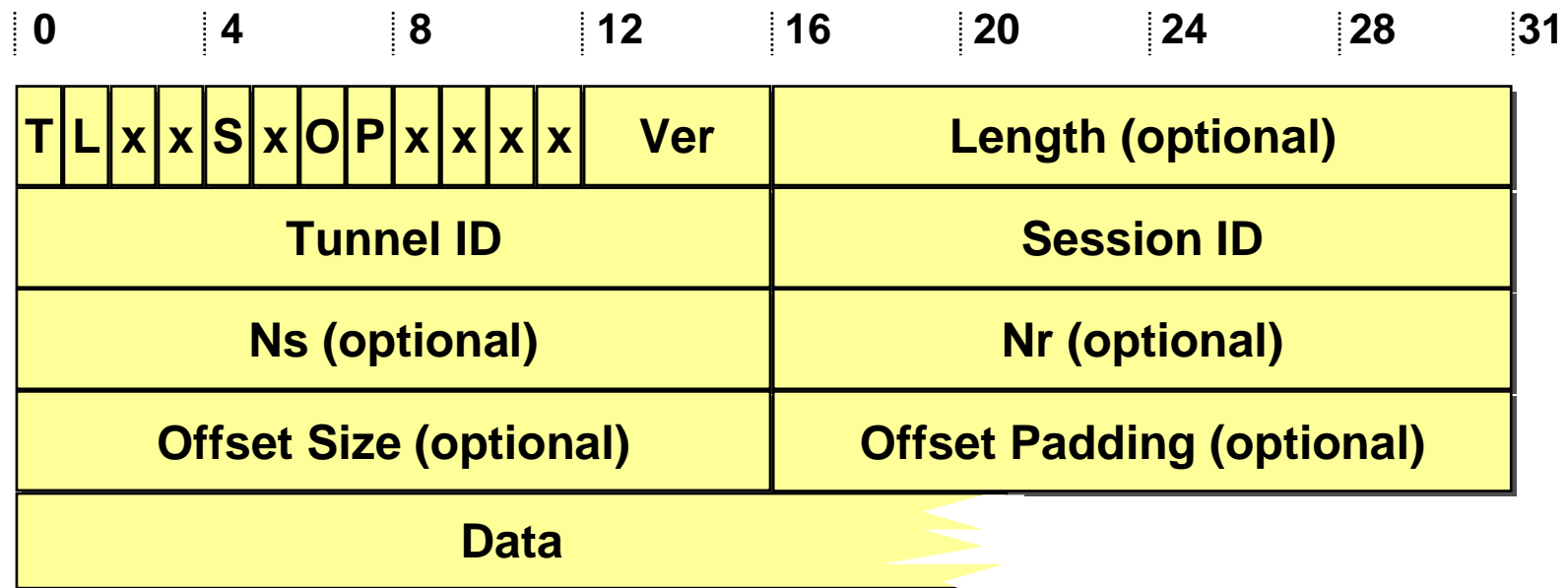


L2TP – Ablauf

- Aufbau der L2TP Steuerverbindung für einen Tunnel.
 - Dabei werden grundsätzliche **Parameter ausgehandelt**
 - Optional eine **Authentisierung** für den Tunnel durchgeführt.
 - Sowohl der LAC als auch der LNS können eine **Steuerverbindung anfordern**.
- Aufbau einer L2TP-Session.
 - Für jede PPP-Session ist eine eigene L2TP-Session notwendig.
 - Je nachdem ob ein eingehender Ruf oder ein abgehender Ruf behandelt werden müssen, wird die L2TP-Session vom LAC oder vom LNS aus initiiert.
- Übertragen von PPP-Rahmen.
 - Dabei werden im LAC alle nicht benötigten Anteile des PPP-Paketes entfernt.
 - Ein L2TP-Kopf wird angefügt

L2TP – Protokollkopf

- Sowohl die Steuernachrichten als auch die PPP-Rahmen werden mit einem einheitlichen L2TP-Kopf versehen.
- Je nach Anwendung werden unterschiedliche Elemente benutzt bzw. frei gelassen

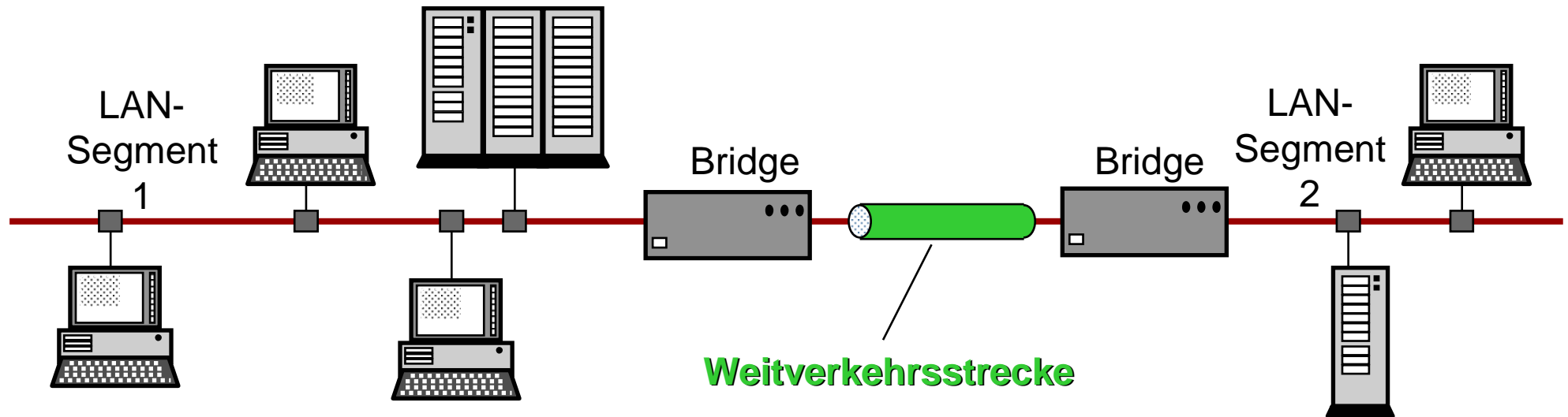


Verbindungen zu abgesetzten Standorten

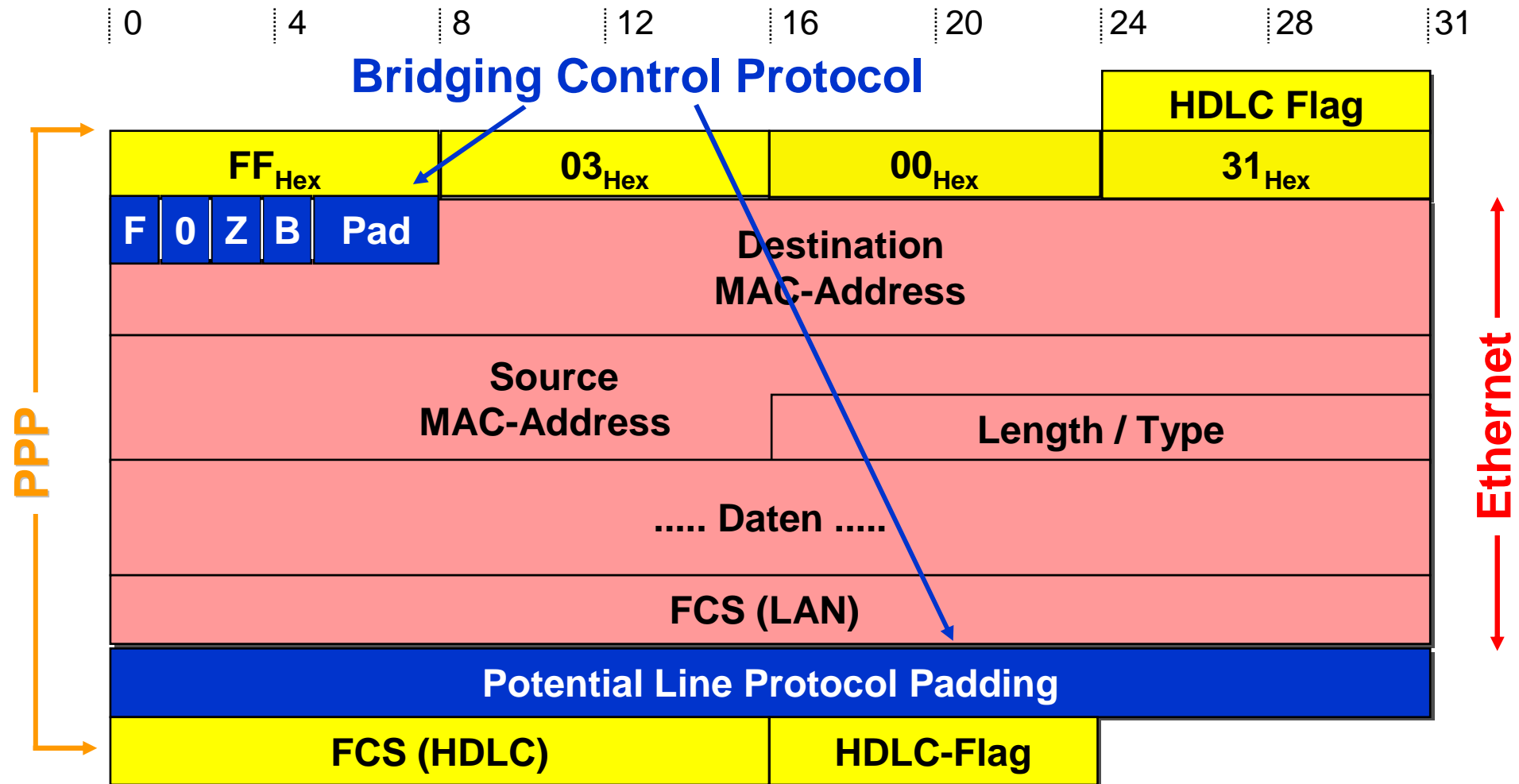
- Das PPP dient zur Verbindung zwischen zwei Standorten über ein beliebiges Transportnetz, wobei in der Regel auf beiden Seiten jeweils ein Router die Verbindung herstellt.
- Drei Sonderfälle sind zu unterscheiden:
 - **Remote Bridging**
 - **LAN Extension**
 - **PPP over Ethernet (PPPoE)** →
wird heute beim breitbandigen Anschluss benutzt

Remote Bridging – Konfiguration

- Eine der Möglichkeiten der Verbindung von LAN-Segmenten ist die Benutzung einer Bridge.
- Dieses Verfahren lässt sich dahingehend erweitern, dass eine Weitverkehrsstrecke zwischen zwei Bridges eingefügt wird.
- Für die Übertragung zwischen den beiden Bridges (oder Halb-Bridges) kann das Point-to-Point Protokoll verwendet werden.
- Dazu wird der Ethernet-Rahmen mit einigen Protokoll-Elementen versehen und gemäss PPP in einen HDLC-Rahmen eingepackt.

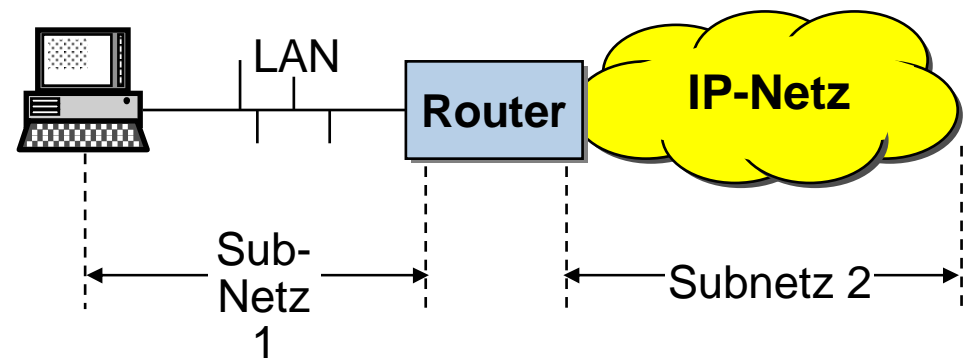


Remote Bridging – Datenrahmen



LAN-Extension (1)

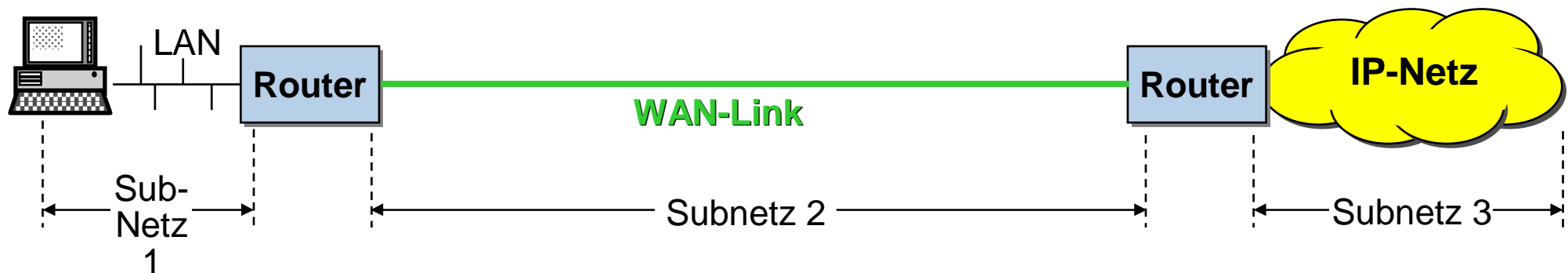
Direkte Verbindung



- Klassische Konfiguration einer direkt an ein LAN angeschlossenen Station.

LAN-Extension (2)

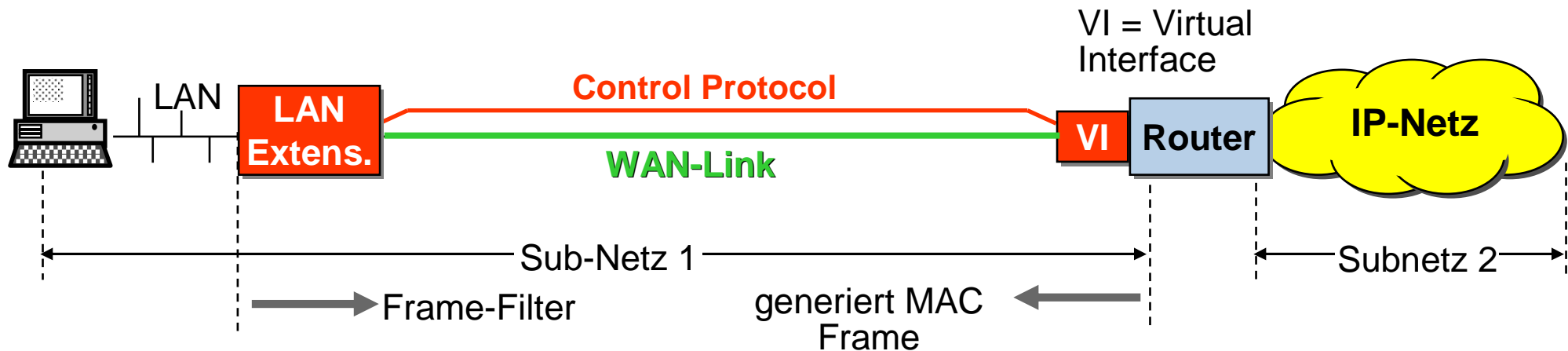
Anschluss eines abgesetzten Standortes



- Traditionelle Konfiguration eines angesetzten Standortes, wobei an dem abgesetzten Standort ein Router eingesetzt wird.
- Nun ist am abgesetzten Standort aber normalerweise kein System-Administrator für das Rechnernetz (... den Router) präsent.
- Zudem wäre es ideal, wenn das IP-Netz nur ein Sub-Netz sehen würde, keine zwei hintereinander geschalteten.

LAN-Extension (3)

Abgesetzter Standort über LAN-Extension angeschlossen



- Zwei Funktionsblöcke begrenzen die Weitverkehrs-Strecke:
 - *LAN Extension* am abgesetzten Standort und
 - *Virtual Interface* (VI) am Router des IP-Netzes.
- Der abgesetzte Standort bildet jetzt zusammen mit der Weitverkehrs-Strecke ein Sub-Netz. Es ist kein Router am abgesetzten Standort zu verwalten.
- Für den Transport der Daten wird das PPP benutzt. Ein eigenes Steuerprotokoll zwischen LAN-Extension und VI sorgt für die Konfiguration.

Inhalt

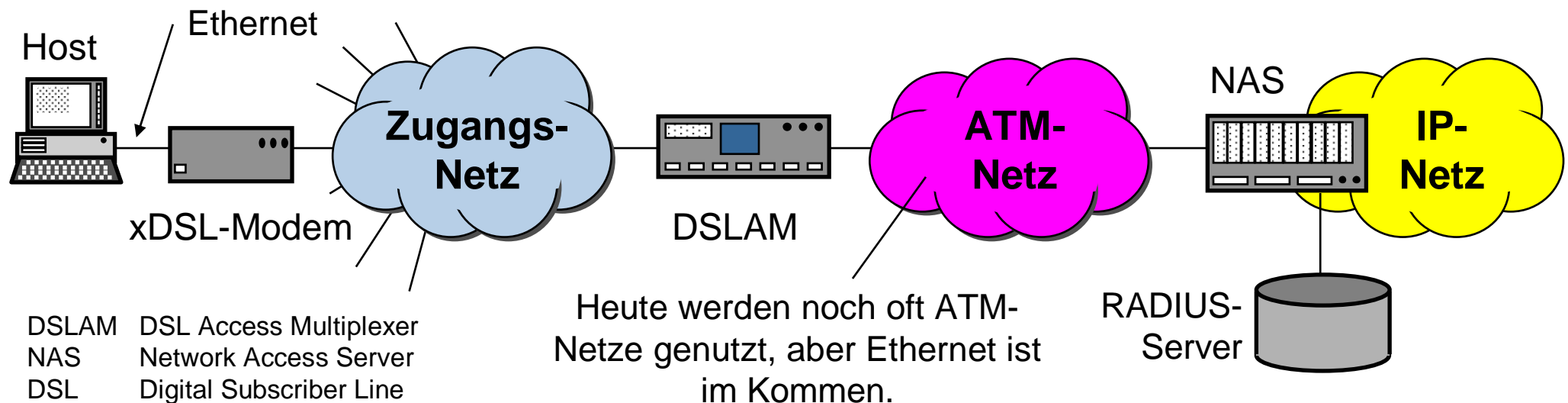
- High Level Data Link Control (HDLC)
- Frame Relay (FR)
- Point-to-Point Protocol (PPP)
 - Grundform
 - Sonderformen von PPP
 - Tunneling-Protokolle
 - Breitbandiger Anschluss
 - Unterstützende Funktionen

Breitbandiger Internet-Zugang (1)

- Mit der Einführung breitbandiger Teilnehmerzugänge (über xDSL, HFC, LMDS,...) wurden neue Protokolle notwendig.
- Der Teilnehmer, braucht eine neue, breitbandigere Schnittstelle. Durch seine weite Verbreitung war das **Ethernet** die billigste Schnittstelle im Bereich einiger Mbit/s (USB war noch nicht eingeführt).
- Nicht vergleichbar mit einer Büroumgebung: es ist ein Zugang zu einem (öffentlichen) Netz. Muss Betriebssystem-unabhängig sein und eine Entgelderfassung bieten.
- Mit dem **PPP** und dem zugehörigen **RADIUS-Protokoll** wurden diese Leistungsmerkmale für Einwahl-Kunden verwirklicht. Daher auch nutzbar für breitbandigen Kunden.
- Führt zum Vorschlag **PPP over Ethernet** (PPPoE).

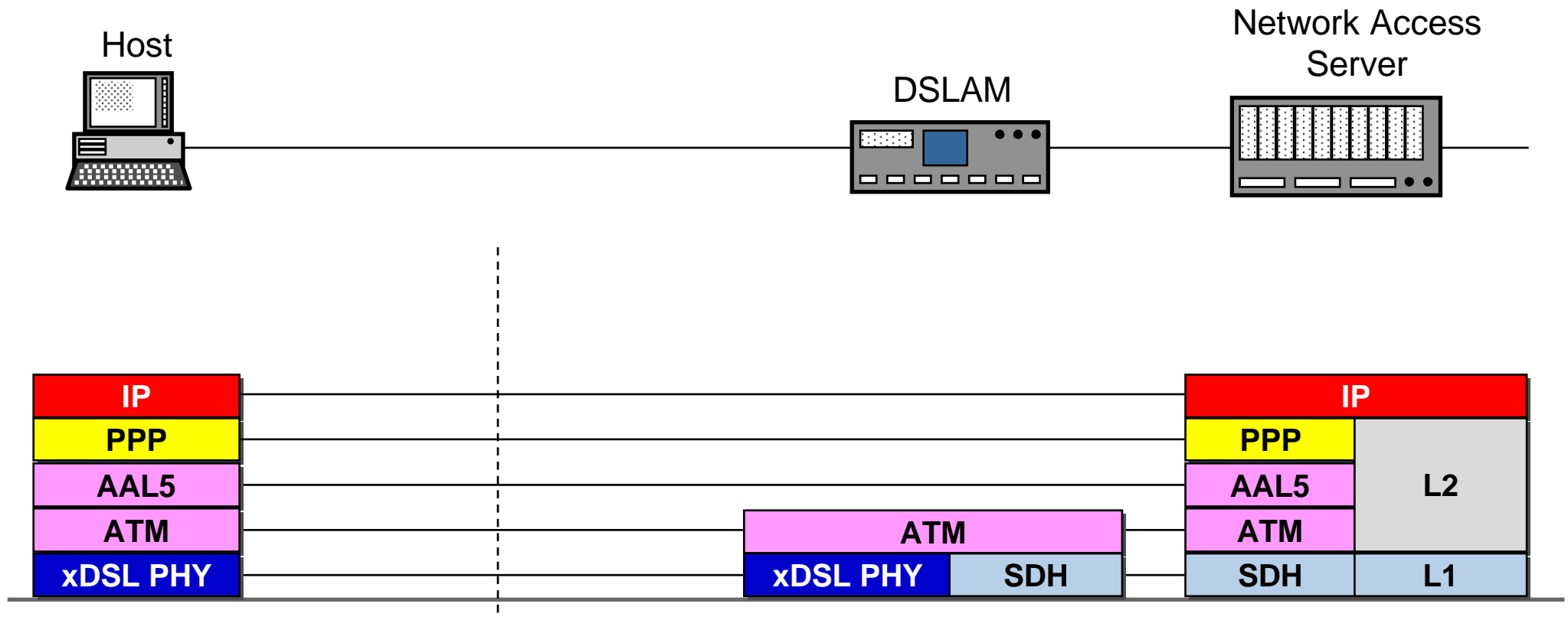
Breitbandiger Internet-Zugang (2)

- Der PC des Teilnehmers (Host) wird an ein xDSL-Modem angeschlossen.
- Die Datenströme vieler Teilnehmer werden in einem Gerät, dem **DSL Access Multiplexer** (DSLAM) konzentriert.
- Von dort gelangen die Daten zum breitbandigen **Network Access Server** (NAS), dem ersten Knoten, der auf der IP-Ebene arbeitet und üblicherweise zusammen mit einem Management-Server (RADIUS-Server) Aufgaben der Authentisierung, Entgelderfassung usw. erledigt.



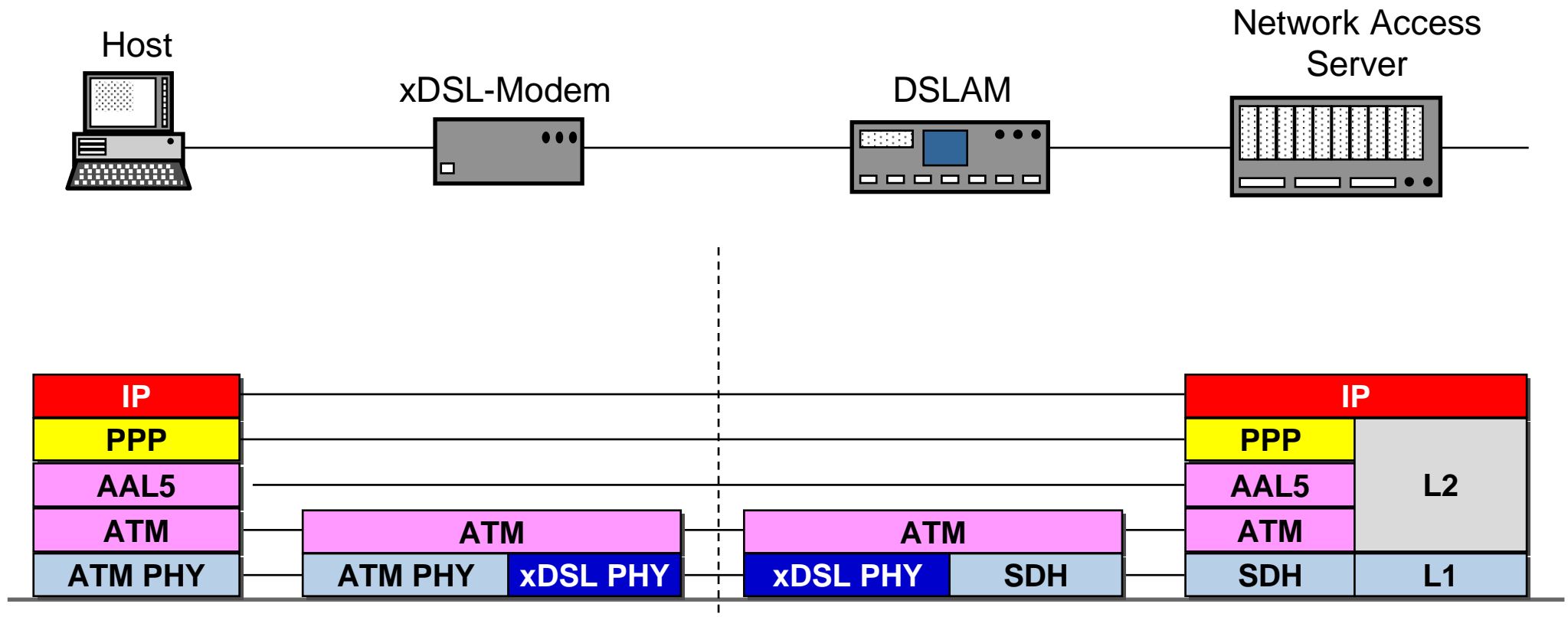
Optionen (1)

- xDSL-Karte direkt im PC



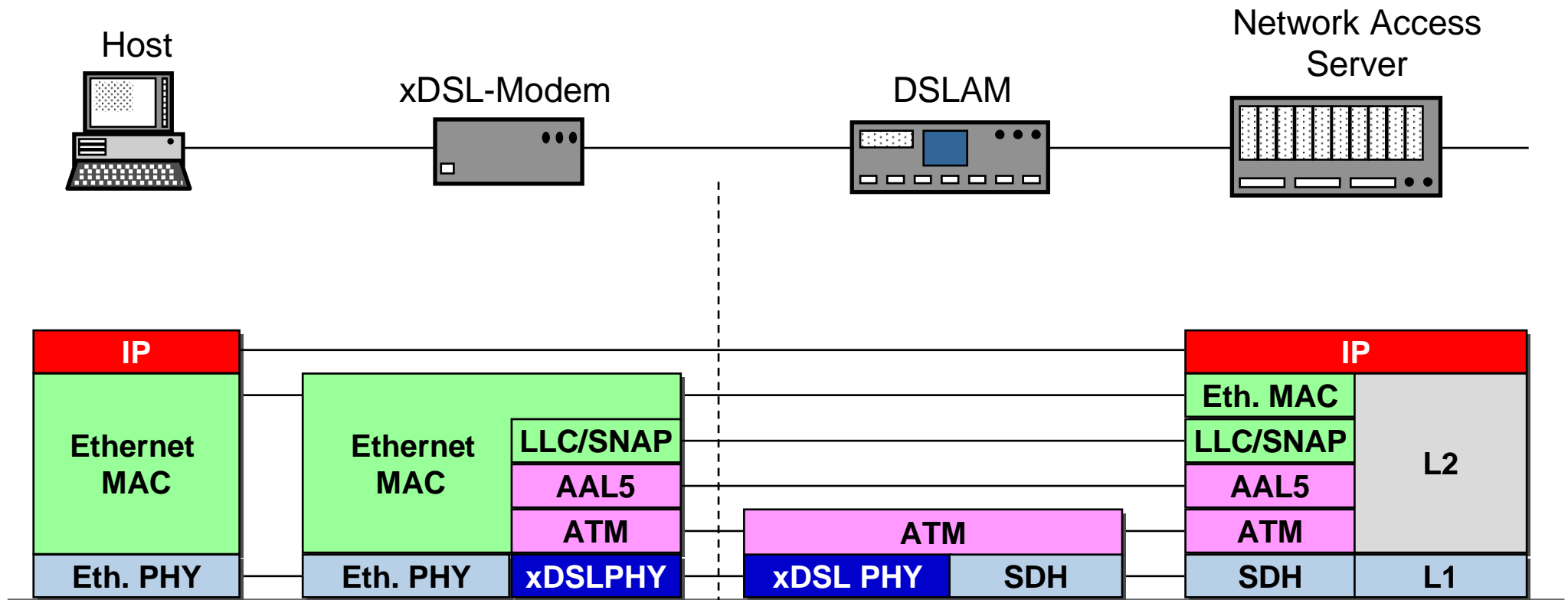
Optionen (2)

- ATM-Schnittstellenkarte direkt im PC



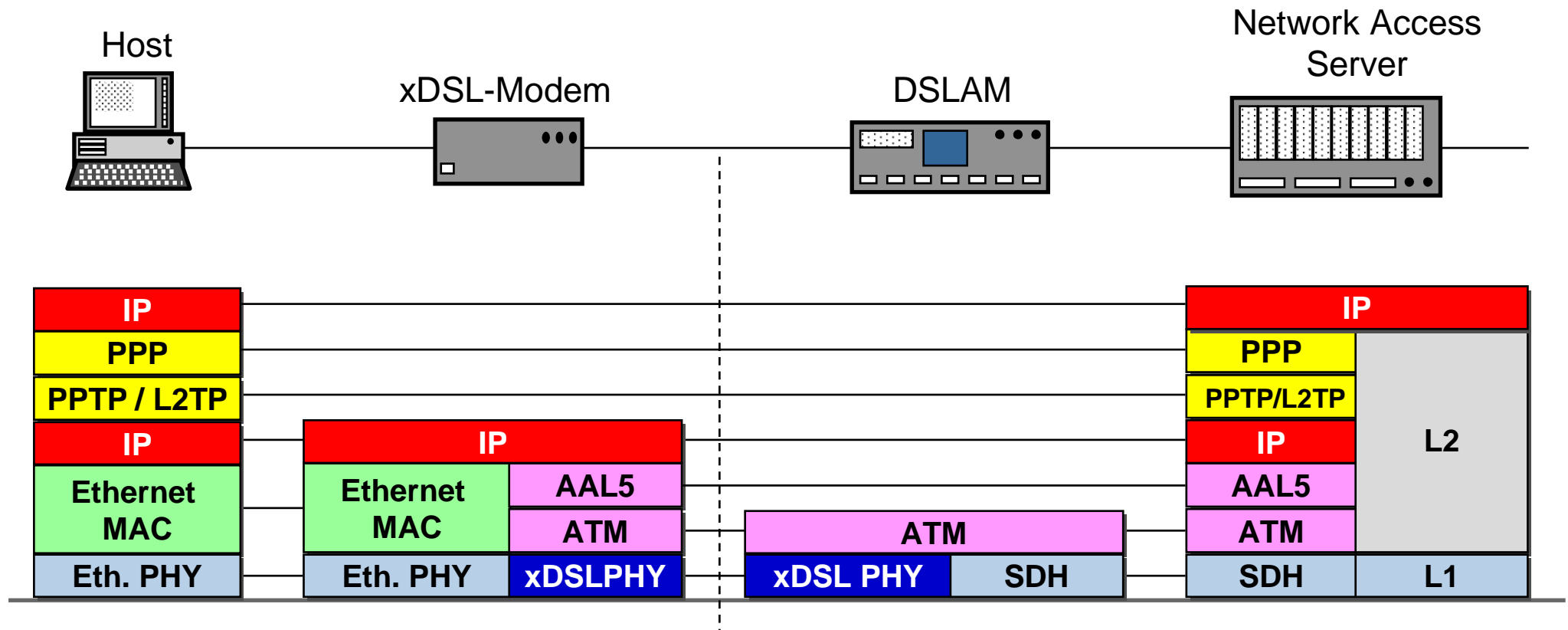
Optionen (3)

- Ethernet-Karte im PC - Remote Bridging



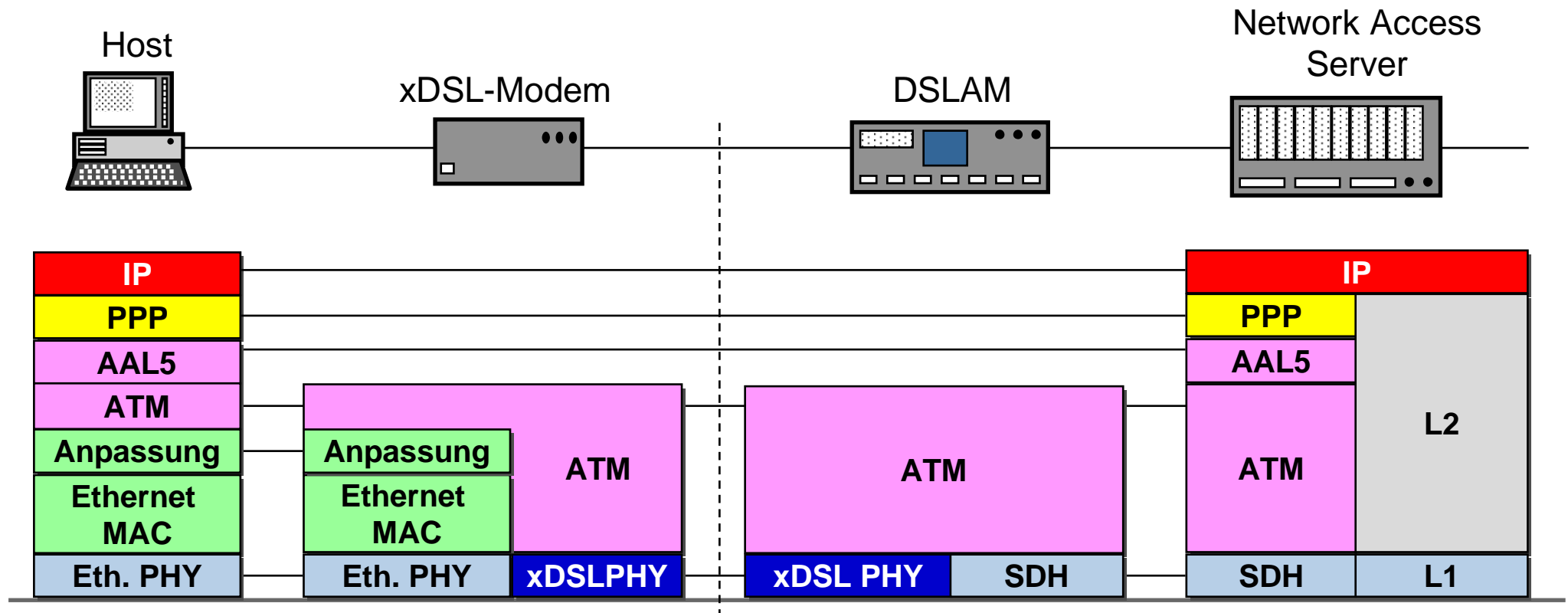
Optionen (4)

- Ethernet-Karte im PC - mit Tunneling-Protokoll



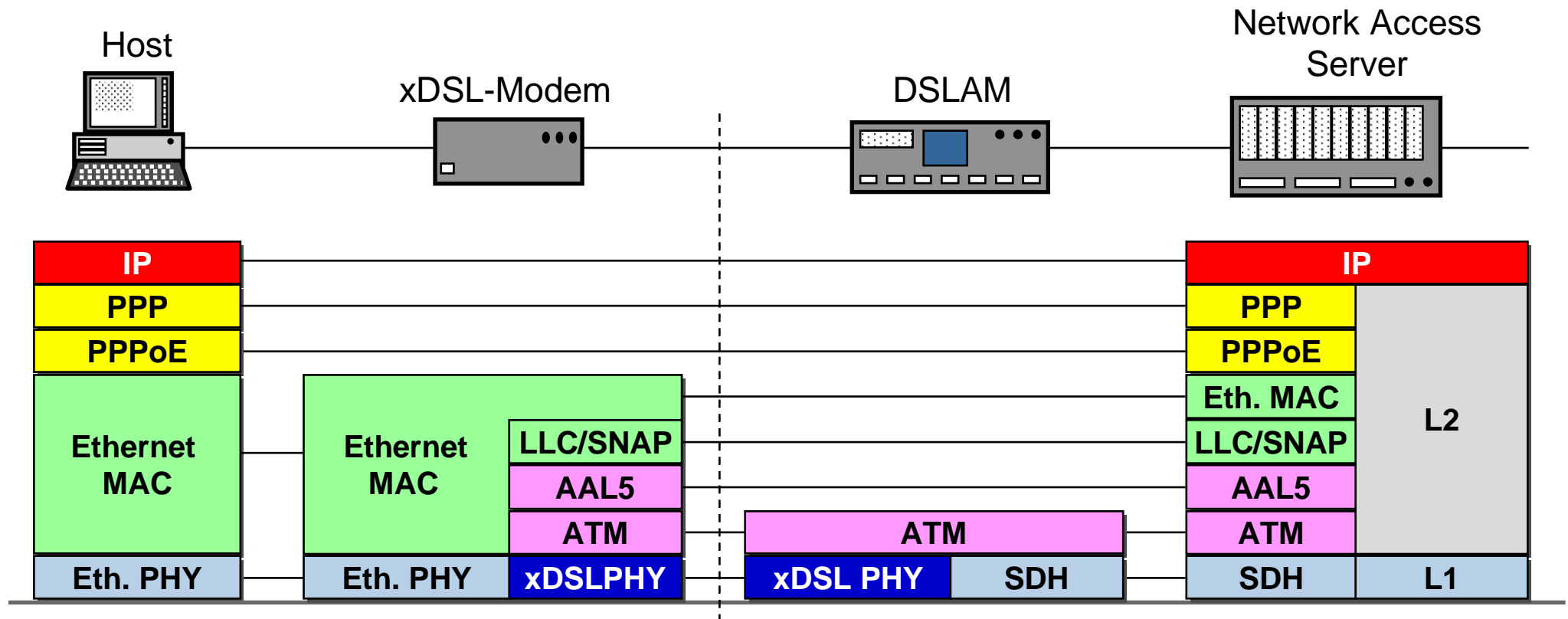
Optionen (5)

- Ethernet-Karte im PC - Nutzung einer Anpassungsschicht zwischen ATM und Ethernet



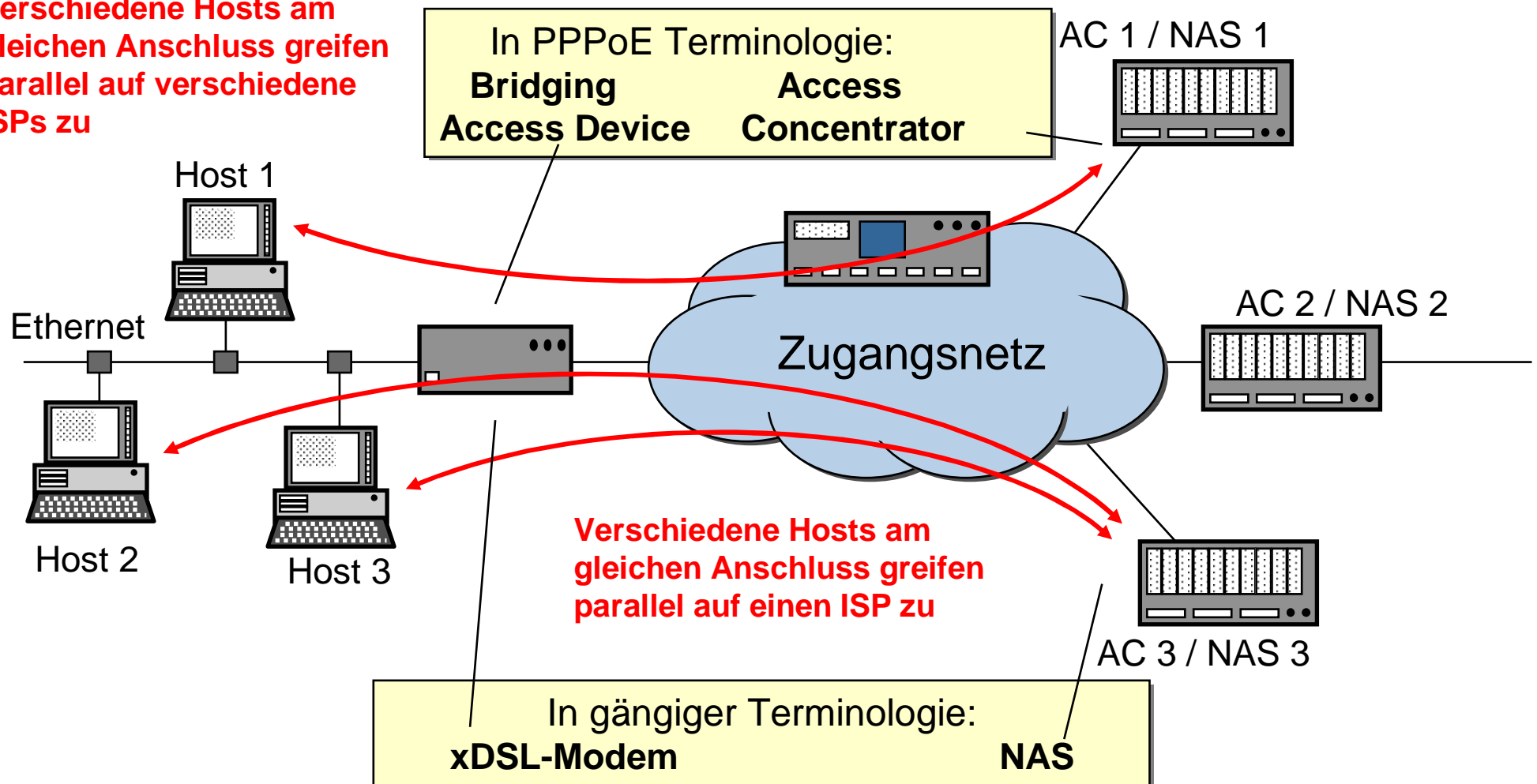
Optionen (6)

- PPPoE – eine neue Anpassungsschicht



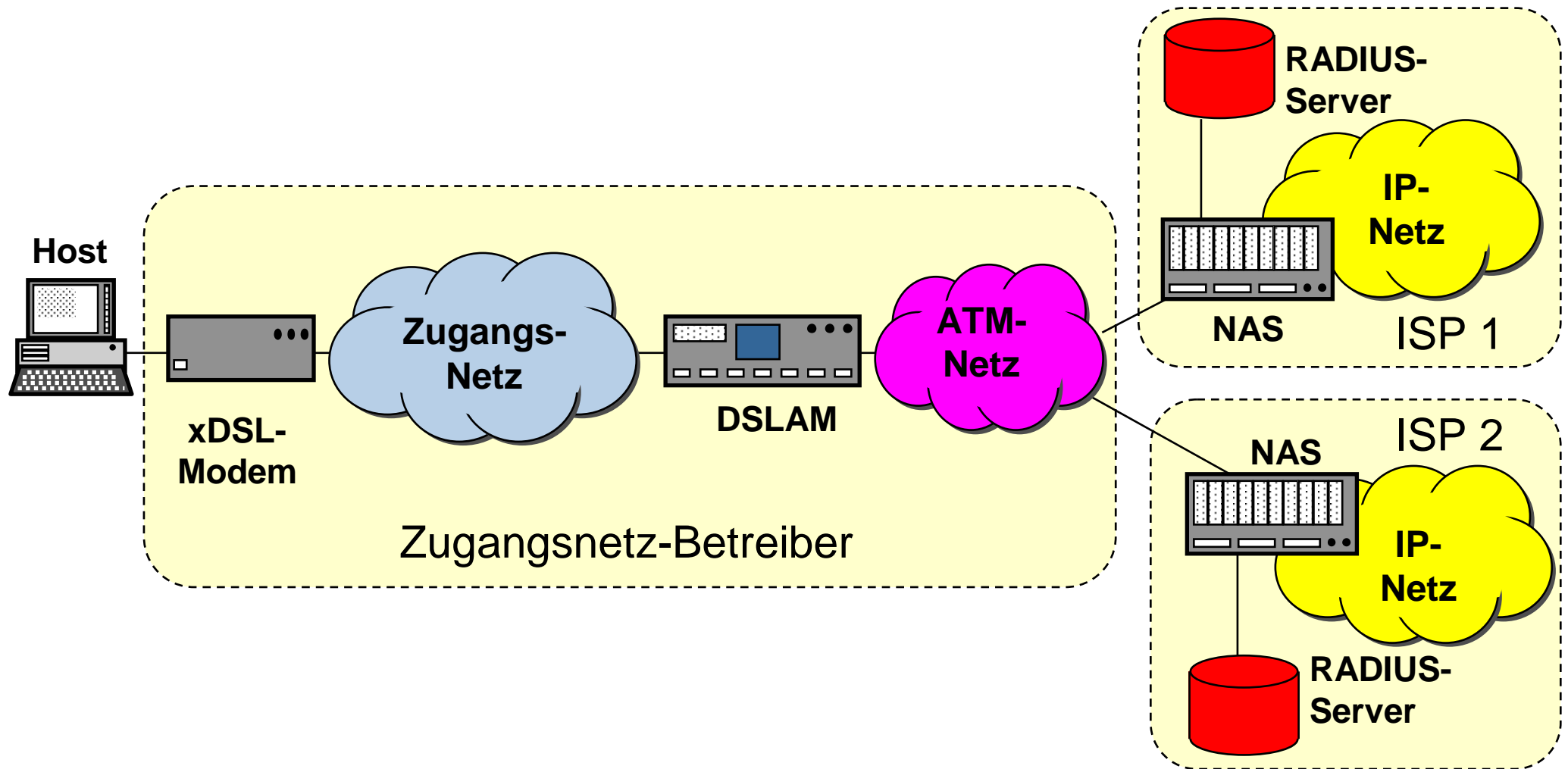
PPPoE Grundkonfiguration

Verschiedene Hosts am gleichen Anschluss greifen parallel auf verschiedene ISPs zu



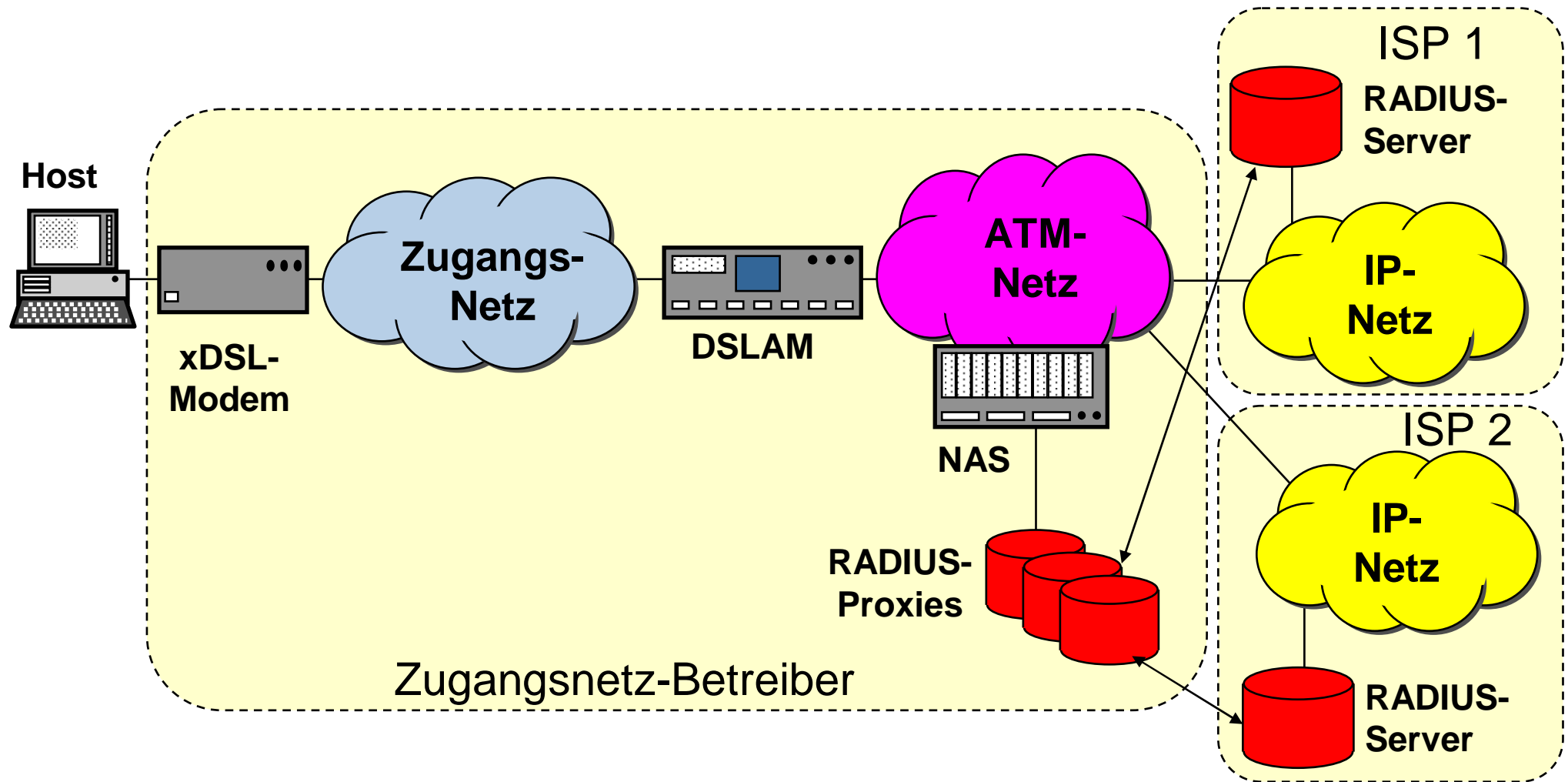
PPPoE – NAS beim ISP

Backup

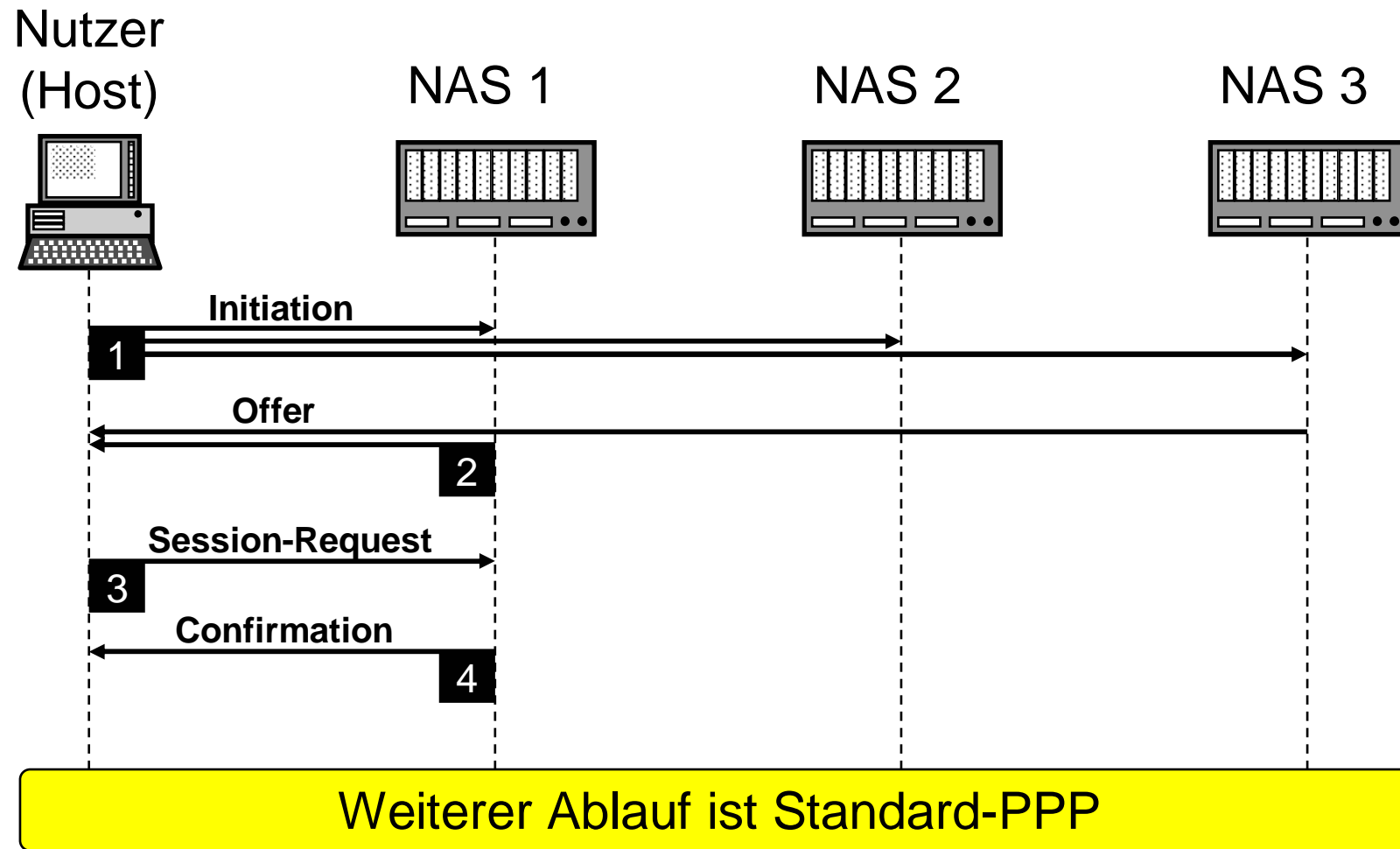


PPPoE – NAS beim Zugangsnetz-Betreiber

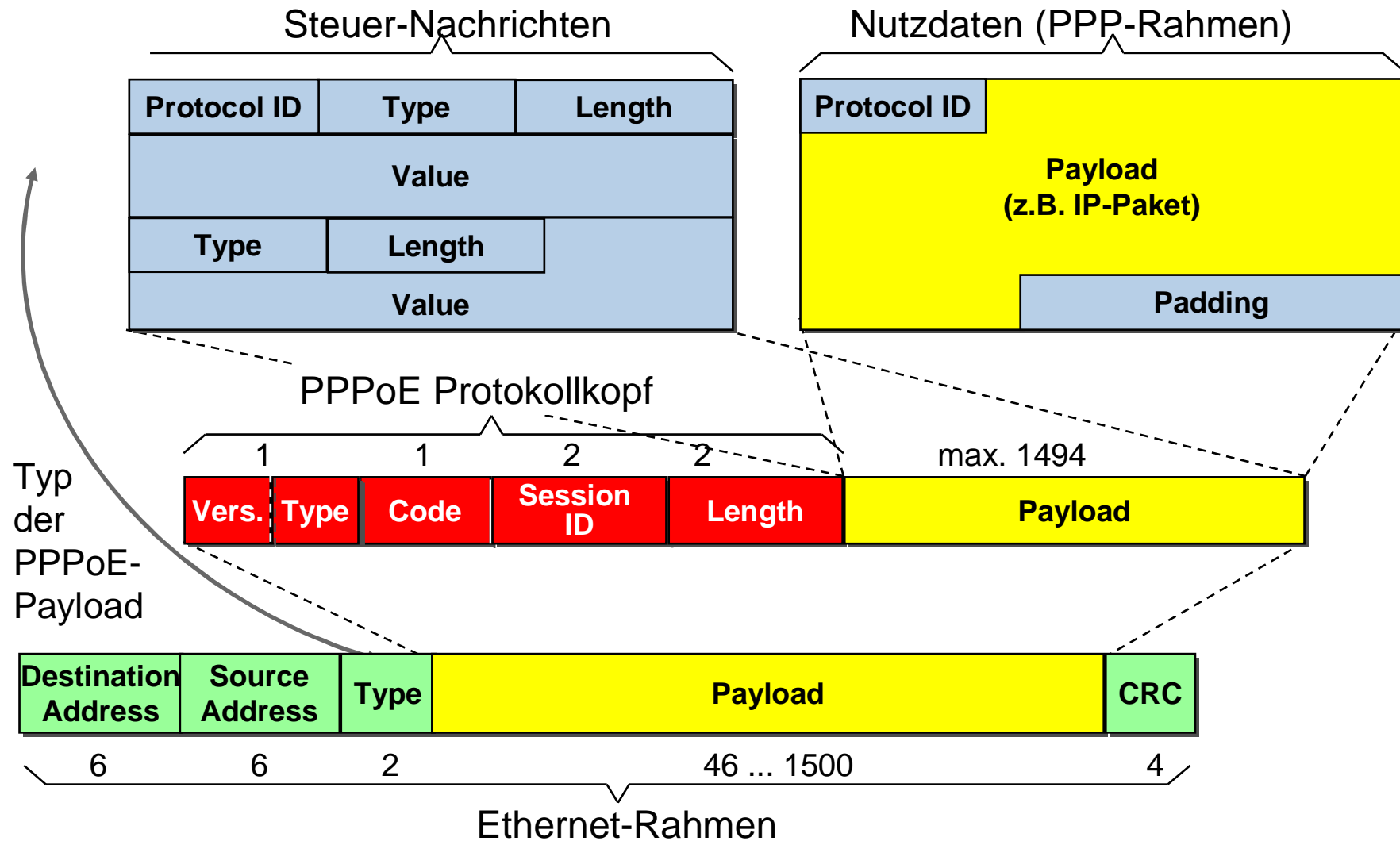
Backup



PPPoE – Discovery Stage



PPPoE - Datenformate



PPPoE - Protokollelemente

Feld	Länge	Beschreibung		
Ver.	4 Bit	Version des Protokolls, hier „1“		
Type	4 Bit	Typ der Nachricht, derzeit nur Type „1“ spezifiziert		
Code	8 Bit	Dient der Kennzeichnung des Inhalts der Payload. Folgende Werte sind möglich:		
		00 _{Hex}	Encapsulierte PPP-Rahmen	Nutzdaten
		09 _{Hex}	PPPoE-Active-Discovery-Initiation	Steuer-Nachrichten
		07 _{Hex}	PPPoE-Active-Discovery-Offer	
		19 _{Hex}	PPPoE-Active-Discovery-Request	
		65 _{Hex}	PPPoE-Active-Session-Confirmation	
		A7 _{Hex}	PPPoE-Active-Discovery-Terminate	
		B9 _{Hex}	PPPoE-Active-Service-Change	
Session ID	16 Bit	Wert, mit dem die PPP-Session gekennzeichnet wird und der sich während der Session nicht ändert. (Der Wert FFFF _{Hex} ist für zukünftige Erweiterungen reserviert.)		
Length	16 Bit	Länge der PPPoE Payload (also ohne Ethernet- und PPPoE-Protokollköpfe)		

Inhalt

- High Level Data Link Control (HDLC)
- Frame Relay (FR)
- Point-to-Point Protocol (PPP)
 - Grundform
 - Sonderformen von PPP
 - Tunneling-Protokolle
 - Breitbandiger Anschluss
 - Unterstützende Funktionen

Unterstützende Funktionen

Einige Funktionen sind nicht spezifisch für PPP, werden aber besonders dort verwendet

- **Kompression**

- Header-Kompression
- Daten-Kompression

- **Authentisierung**

- Password Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP)

- **Verschlüsselung**

- **Verwaltung des Teilnehmers**

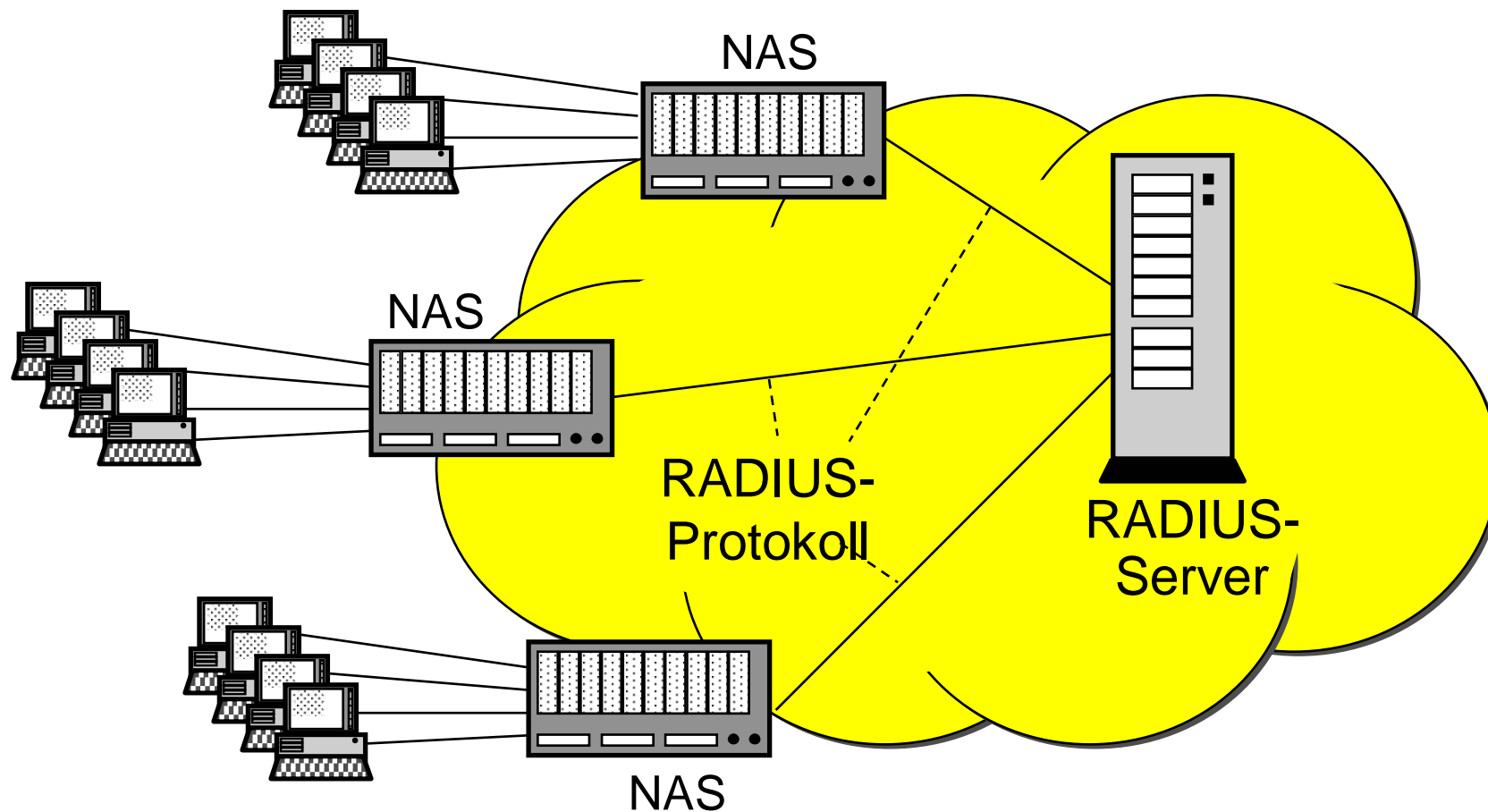
- Remote Authentication Dial-In User Service (RADIUS)

Remote Authentication Dial In User Service (RADIUS)

- Für Authentisierung/Autorisierung muss der **Network Access Server** (NAS) Kenntnis über den Teilnehmer haben, der sich Authentisieren will.
- Anstatt jedem NAS lokal diese Information zu geben, wird ein Server vorgesehen. Viele NAS teilen sich einen solchen Server, das erlaubt die Portabilität der Teilnehmer.
- **Remote Authentication Dial In User Service** (RADIUS) ist ein Protokoll, mit dem ein NAS mit einem Authentication Server Informationen über die Authentisierung, Autorisierung und Konfigurierung austauscht
- Der Server kann auch andere Aufgaben wahrnehmen, z. B. im Rahmen der Entgelterfassung.

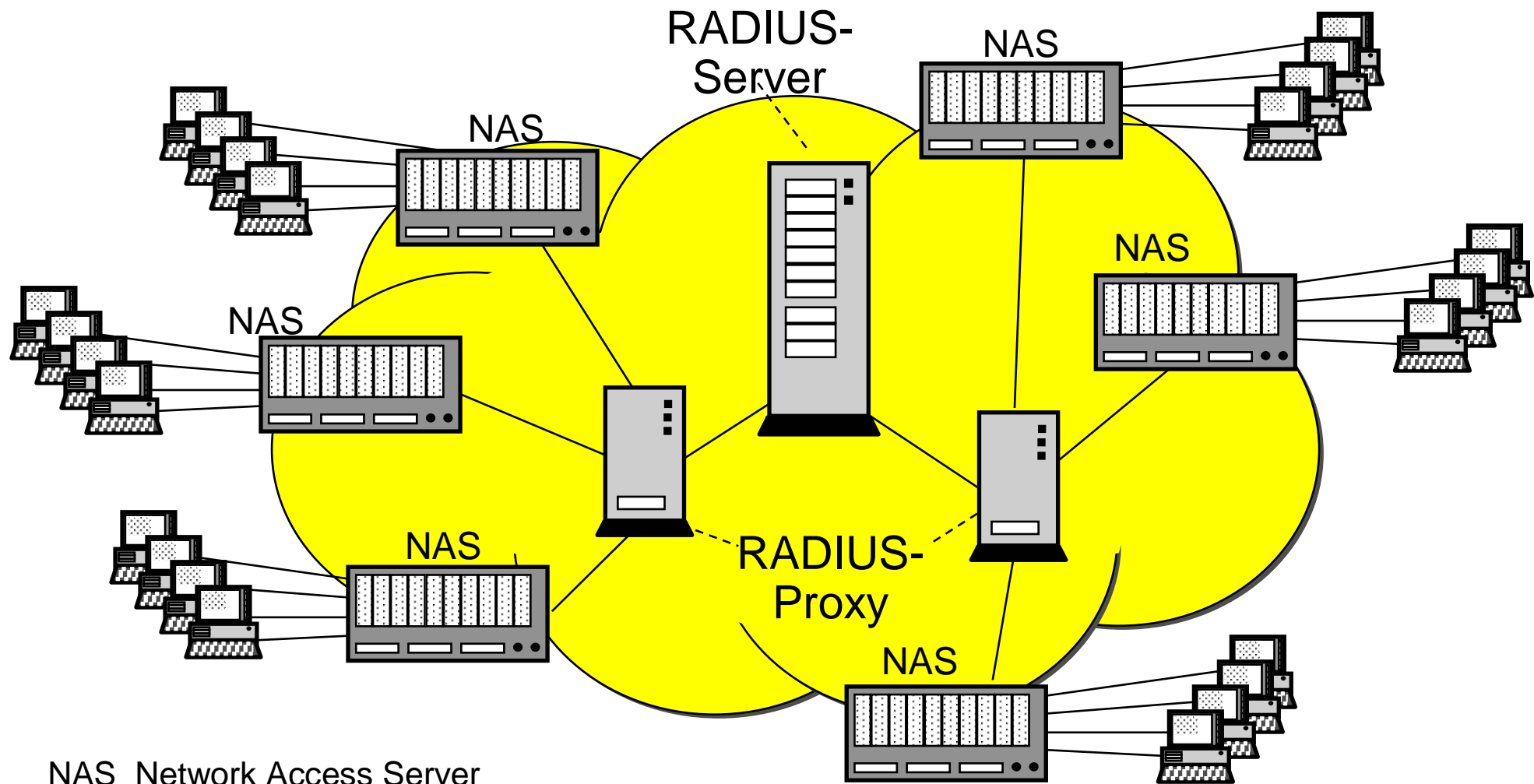
RFC 2138 , RFC 2139

RADIUS – Konfiguration



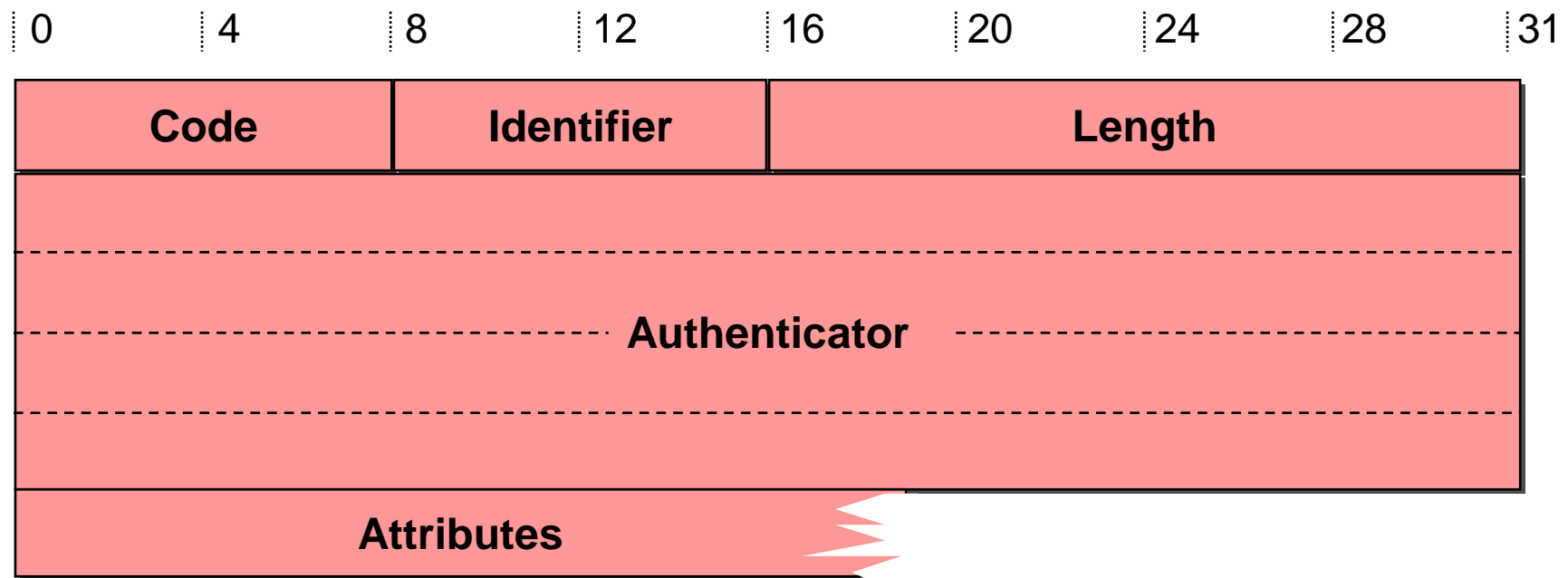
NAS Network Access Server

RADIUS-Proxy



NAS Network Access Server

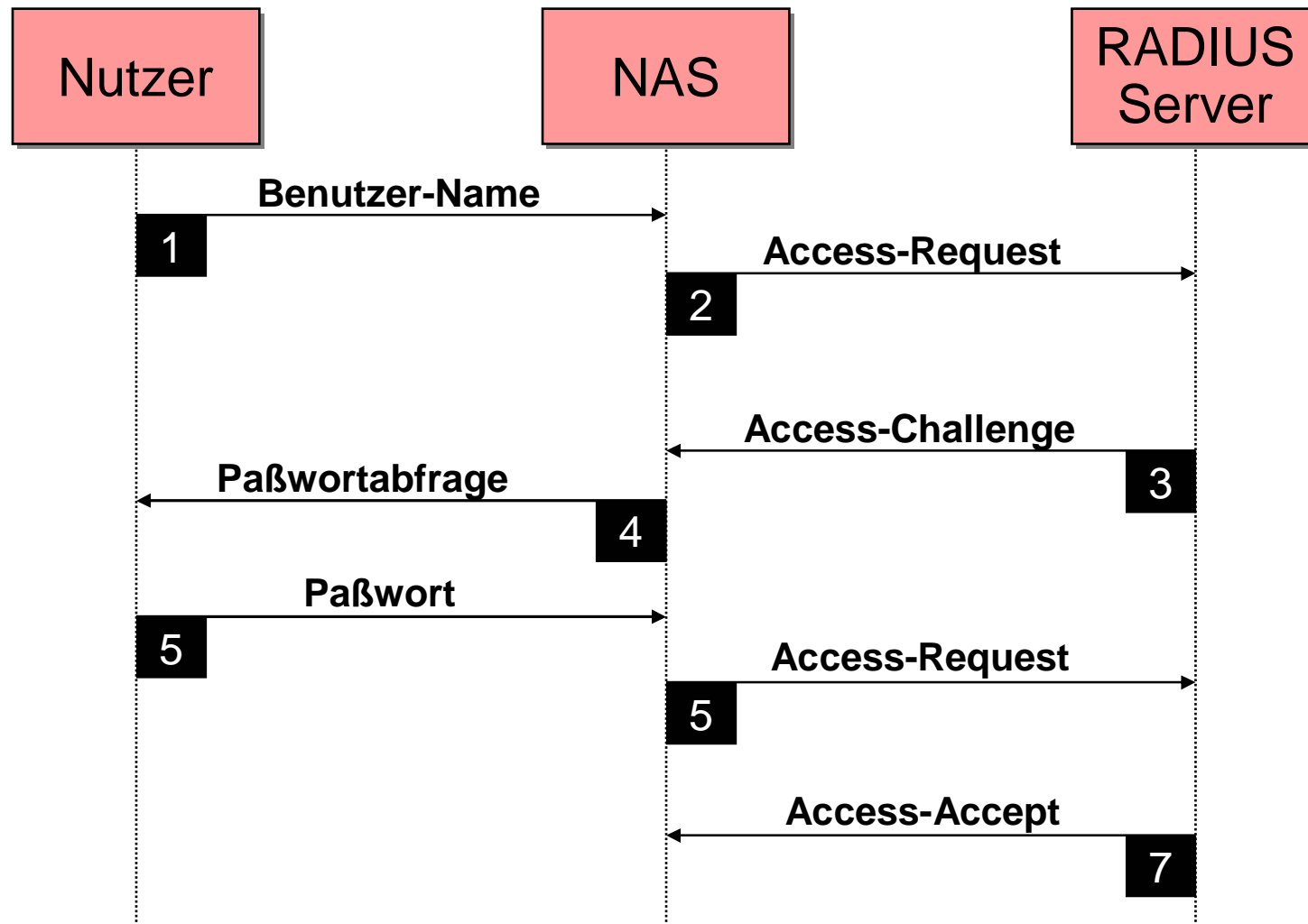
RADIUS-Nachricht



RADIUS – Nachrichten-Elemente

Feld	Bedeutung		
Code	Identifiziert den Typ der RADIUS-Nachricht. Mögliche Typen sind:		
	1	Access-Request	Anfrage, ob ein Teilnehmer Zugang erhalten darf oder nicht
	2	Access-Accept	positive Antwort des RADIUS-Servers
	3	Access-Reject	negative Antwort des RADIUS-Servers
	4	Accounting-Request	Anforderung an den Server bezüglich Entgelterfassung
	5	Accounting-Response	Antwort des Servers
	11	Access-Challenge	Abfrage des Paßwortes
	12	Status-Server	experimentell
	13	Status-Client	experimentell
	255	reserved	reserviert
Identifizier	Dient dazu, Anfragen und Antworten zu korrelieren		
Legth	Gibt die Gesamtlänge des RADIUS-Paketes an		
Authenticator	Wird zur Authentisierung und für die versteckte Übertragung von Paßwörtern benutzt.		
Attributes	Je nach Nachrichtentyp werden unterschiedliche Attribute benötigt (ca. 60 definiert).		

RADIUS – Ablauf



PPP – Ausblick

- Das Point-to-Point Protokoll hat einschließlich seiner Varianten eine große Verbreitung erfahren.
- Ständige Anpassungen haben dafür gesorgt, dass es nicht „veraltete“. Daher empfiehlt es sich bei der Suche an einer speziellen Anwendung zuerst zu prüfen, ob nicht das PPP schon die notwendigen Prozeduren bietet oder evtl. leicht anpassbar ist.
- Trotzdem gibt es natürlich auch Kritik und neuere Protokolle wie LAPS und GFP werden sicher dem PPP einige Anwendungsfelder, besonders im Weitverkehr, abnehmen.



ENDE

Vielen Dank für Ihre Aufmerksamkeit!

Dipl.-Ing. Harald Orlamünder
harald.orlamuender@t-online.de