Vorlesung Kommunikationstechnik

Multi-Protocol Label Switching (MPLS), Virtual Private Networks (VPN) und die Generic Framing Procedure (GFC)

Harald Orlamünder

SS 2014

Inhalt

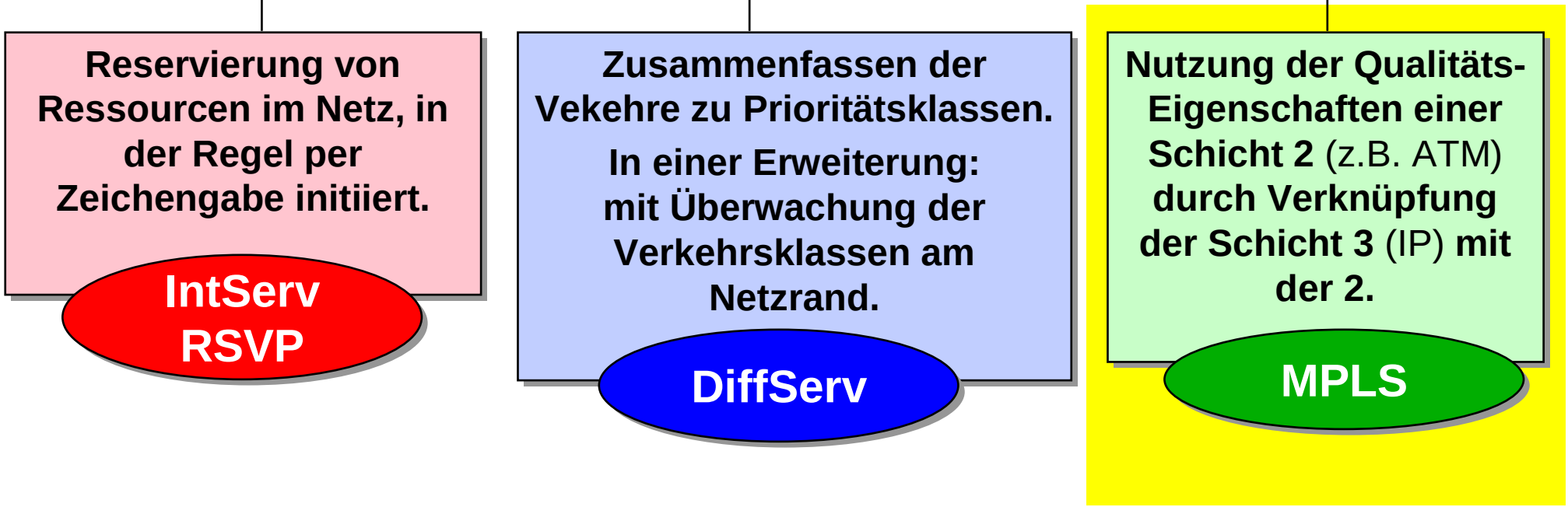
- Qualität in IP-Netzen
- Multi-Protocol Label Switching (MPLS)
  - MPLS - Prinzipen
  - MPLS - Label
  - MPLS - Steuerprotokolle
  - Einsatz vom MPLS
  - Weiterentwicklungen
- Virtual Private Networks (VPN)
- Generic Framing Procedure (GFP)

Qualität und Echtzeit im Internet – Kernnetz

- **Integrated Services** (IntServ-Ansatz mit dem Protokoll RSVP) als Lösung für die Reservierung von Ressourcen wird nur in begrenzen Netzbereichen eingesetzt werden,
  z.B. Bereich eines Betreibers oder in Intranets.
  → Qualität wird pro Verbindung garantiert = Quality of Service (QoS).
- **Differentiated Services** (DiffServ-Ansatz) ist eine interessante Lösung, allerdings nur dort, wo wirklich aggregierter Verkehr vorkommt, also z.B. in Kernnetzen.
  → Qualität wird pro Verkehrsklasse garantiert = Class of Service (CoS).
- **Multi-Protocol Label Switching** (MPLS) findet einen weiten Einsatz. Extrem starkes, weltweites Interesse, besonders bei „traditionellen“ Netzbetreibern!
  ATM geeignet als Schicht 2, aber heute Einsatz mit eigener Schicht 2.
  → Qualität pro „Verbindung“, wobei eine Verbindung mehrer Verkehrsströme tragen kann.

Qualität und Echtzeit im Internet – Methoden

- Prinzipielle Lösungen für Qualität :
  - „genügend“ Kapazität im Netz
  - Methoden der Verkehrssteuerung
  - geeignete Anpassungs-Schicht



Inhalt

- Qualität in IP-Netzen
- Multi-Protocol Label Switching (MPLS)
  - MPLS - Prinzipen
  - MPLS - Label
  - MPLS - Steuerprotokolle
  - Einsatz vom MPLS
  - Weiterentwicklungen
- Virtual Private Networks (VPN)
- Generic Framing Procedure (GFP)

MPLS – Prinzip

- Den Layer 2 PDUs werden kurze Kennzeichnungen – sogenannte „**Lables**“ – zugewiesen werden, die im MPLS-Netz umgewertet werden (so wie es ein ATM-Knoten mit VPIs/VCIs macht).
- Normale Schicht-3-Routingprotokolle (wie OSPF und BGP) werden verwendet, um die Routing-Informationen zu erhalten. Diese werden verwendet um die Labels zuzuweisen. Dann wird eine direkte Schicht-2-Verbindung für die Kommunikation benutzt, als „**Shortcut**“ bezeichnet.
- Multiprotocol Label Switching (MPLS) wurde zwar im Kontext von „IP over ATM“ entwickelt, ist aber nicht auf ATM als Schicht 2 und IP als Schicht 3 festgelegt.
- Im Falle von ATM können direkt VPI/VCI-Werte als Label eingesetzt werden.

RFC 3031

MPLS – Zu lösende Problemfelder

- **Skalierbarkeit** - hier besonders die Frage der Zusammenfassung (Aggregierung) von Informationsströmen;
- **QoS/CoS** - die Benutzung der Labels, um eine Qualitätsklasse zu kennzeichnen;
- **Verkehrssteuerung** - die Benutzung der Labels, um einen expliziten Pfad aufzubauen, der sich vom klassischen, auf Basis der Zieladresse konstruierten Pfad unterscheidet;
- **Performance** - Erhöhung;
- **Integration** von Routern mit Zell-Vermittlungen (z.B. ATM) dadurch, daß
  - die Zell-Vermittlungen sich aus Router-Sicht wie Peers benehmen,
  - die physikalische Topologie dem Network Layer Routing bekannt gemacht wird, und
  - gemeinsames Adressieren, Routing und Management vorhanden ist.

MPLS – Shortcut

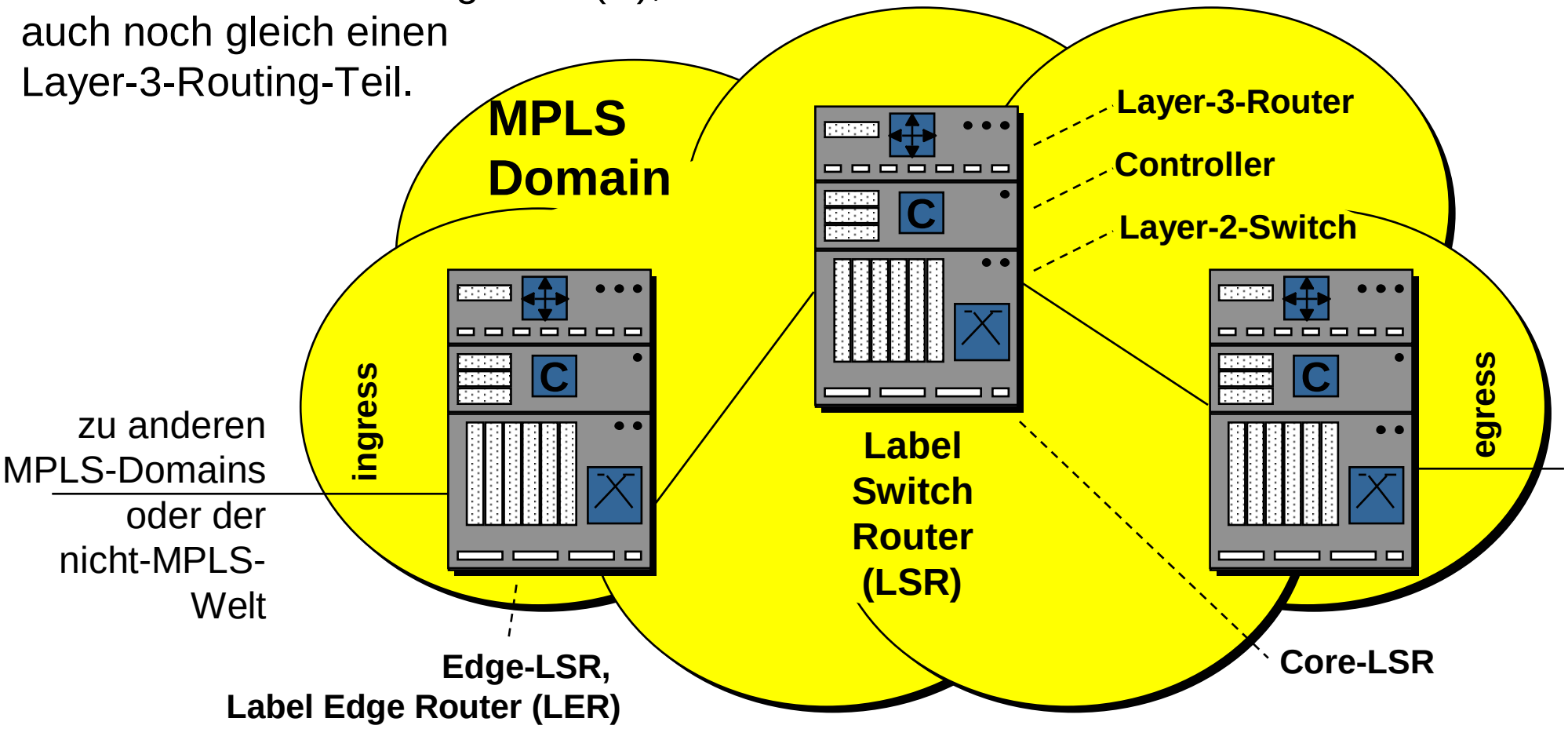
- Intelligente Integration der Routingfunktionalität der Schicht 3 mit der Switching-Funktionalität der Schicht 2.
- Dadurch aufwändiger Prozess der Bearbeitung jedes einzelnen Datenpaketes minimiert.
- Der besondere Vorteil ist jetzt, daß die Information auf kurzem Wege durch das Schicht-2-Netz durchgeschaltet werden kann - man spricht hier von einem „**Shortcut**“ bzw. von „**Shortcut-Routing**“.
- Im MPLS wird der Shortcut als „**Label Switched Path**“ (LSP) bezeichnet.
  - Er ist durch das Label gekennzeichnet
  - Er führt durch Switches (= Schicht-2-Weiterleitung)
- Der Label Switched Path ist **unidirektional**.

MPLS – Auslöser für Shortcuts

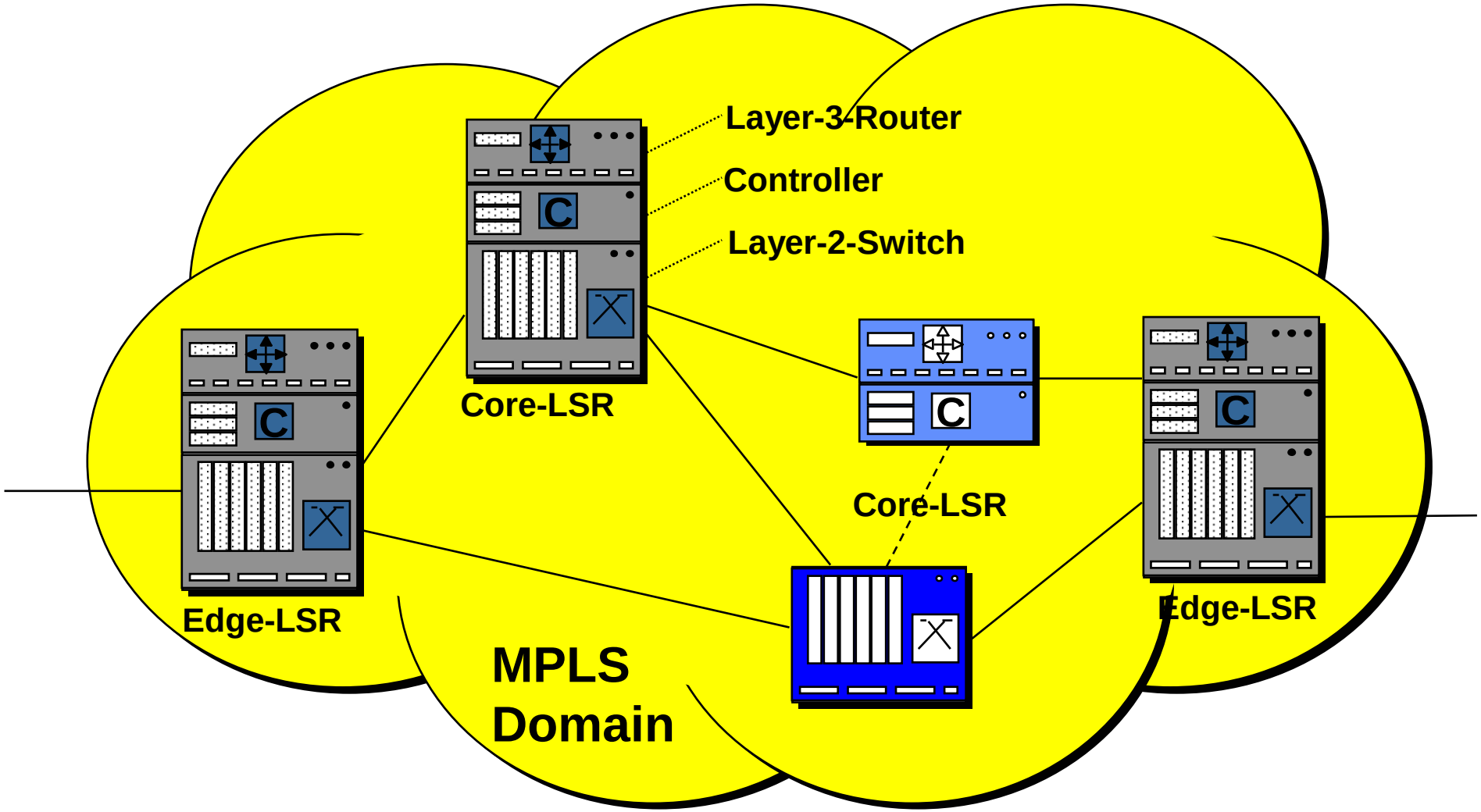
- Durch den **Datenverkehr** selbst ausgelöst („Data driven“, „Traffic driven“ oder „Flow driven“);
  - Analyse des aktuellen Verkehrs, Verbindungen in der Schicht 2 werden erst bei tatsächlichem Bedarf eingerichtet.
- Durch die **Topologie** bestimmt (übliche Bezeichnung dazu ist „Topology driven“);
  - Durch IP-Routing-Protokolle wird Topologie-Informationen gewonnen und aufgrund dieser wiederum in der Schicht 2 Verbindungen fest eingerichtet, unabhängig vom Verkehr.
- Durch ein spezielles Anforderungs-**Signal** bzw. -**Protokoll** ausgelöst
  - Derzeit gibt es in der Internet-Welt nur ein Protokoll, das dieses leisten kann: das Resource Reservation Protocol (RSVP).

MPLS – Konfiguration (1)

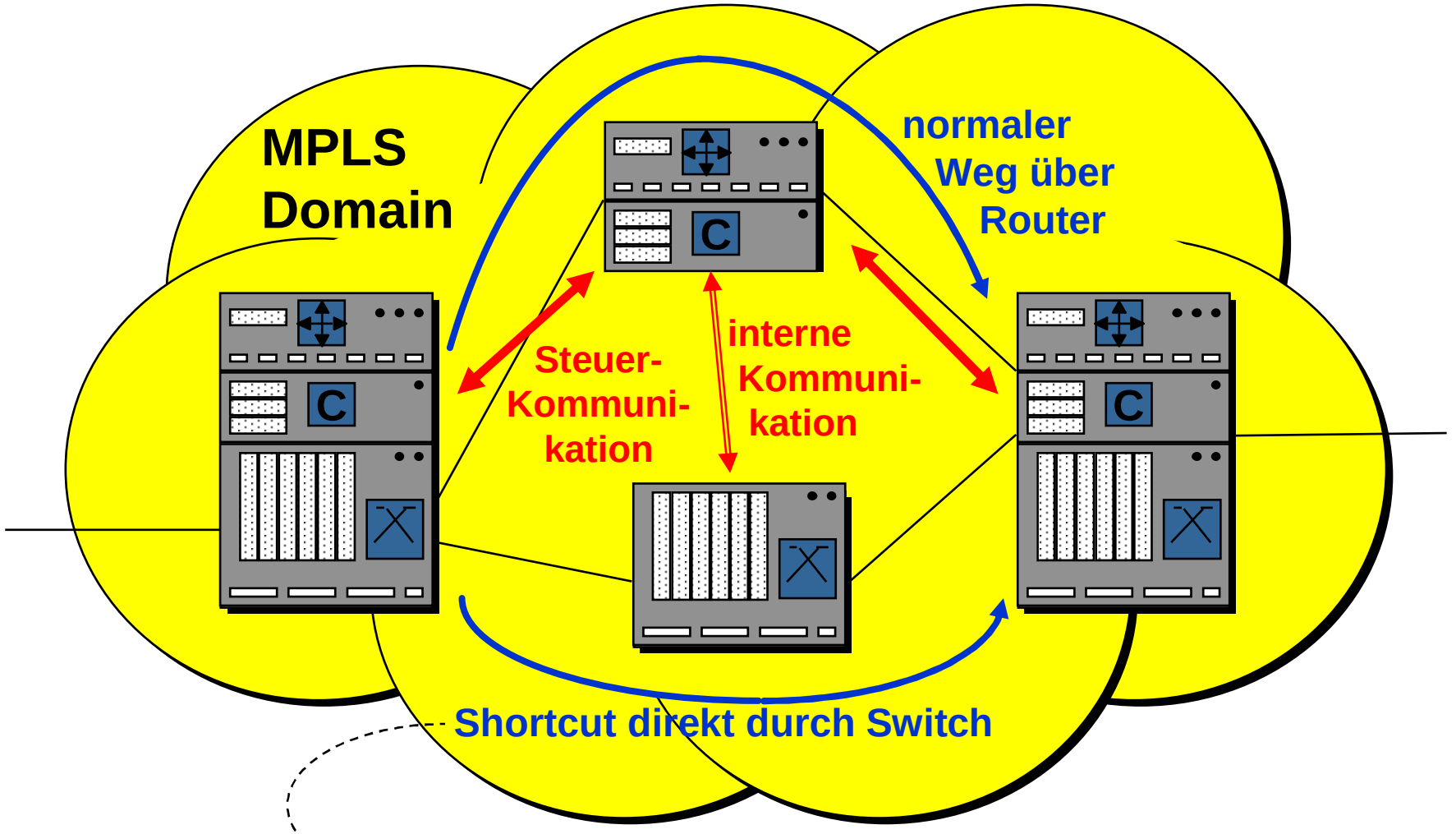
Die MPLS-Knoten bestehen aus einem Layer-2-Switching-Teil und einer Steuerung dazu (C), evtl. enthalten sie auch noch gleich einen Layer-3-Routing-Teil.



MPLS – Konfiguration (2)



MPLS – Konfiguration (3)



Der Shortcut wird „Label Switched Path“ (LSP) genannt!

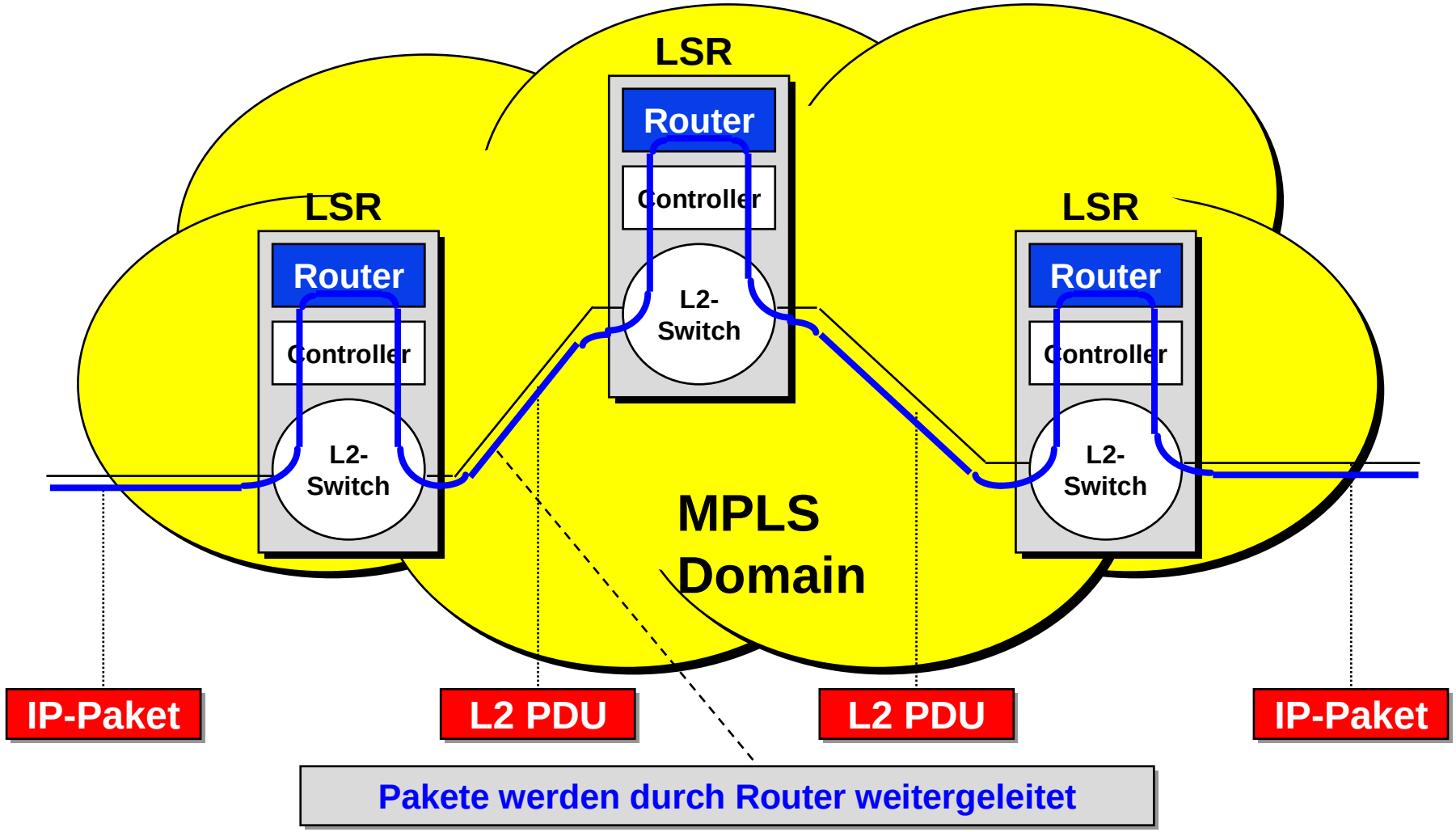
MPLS – Terminologie

- Label
  - definiert eindeutig einen Fluss (flow) pro Router bzw. LSR (Analogie Autobahn: Gibt an der Kreuzung die richtige Spur vor)
  - Label haben nur lokale Bedeutung pro Link (zwischen zwei LSRs)
- Label Switched Path (LSP)
  - werden oft auch als „Tunnel“ durch das Netz bezeichnet,
  - sind immer unidirektional, d.h. müssen für beide Richtungen getrennt aufgebaut werden,
  - LSP für dieselbe „**Forward Equivalent Class**“ (FEC) werden in einem LSR zusammengefasst, unabhängig davon, von welchem Upstream Router Pakete gesendet werden (MPLS skaliert), **LSP Merging**.
- Label Switched Router (LSR)
  - Router, der der MPLS-Funktion beinhaltet (... auf dem MPLS Software läuft).

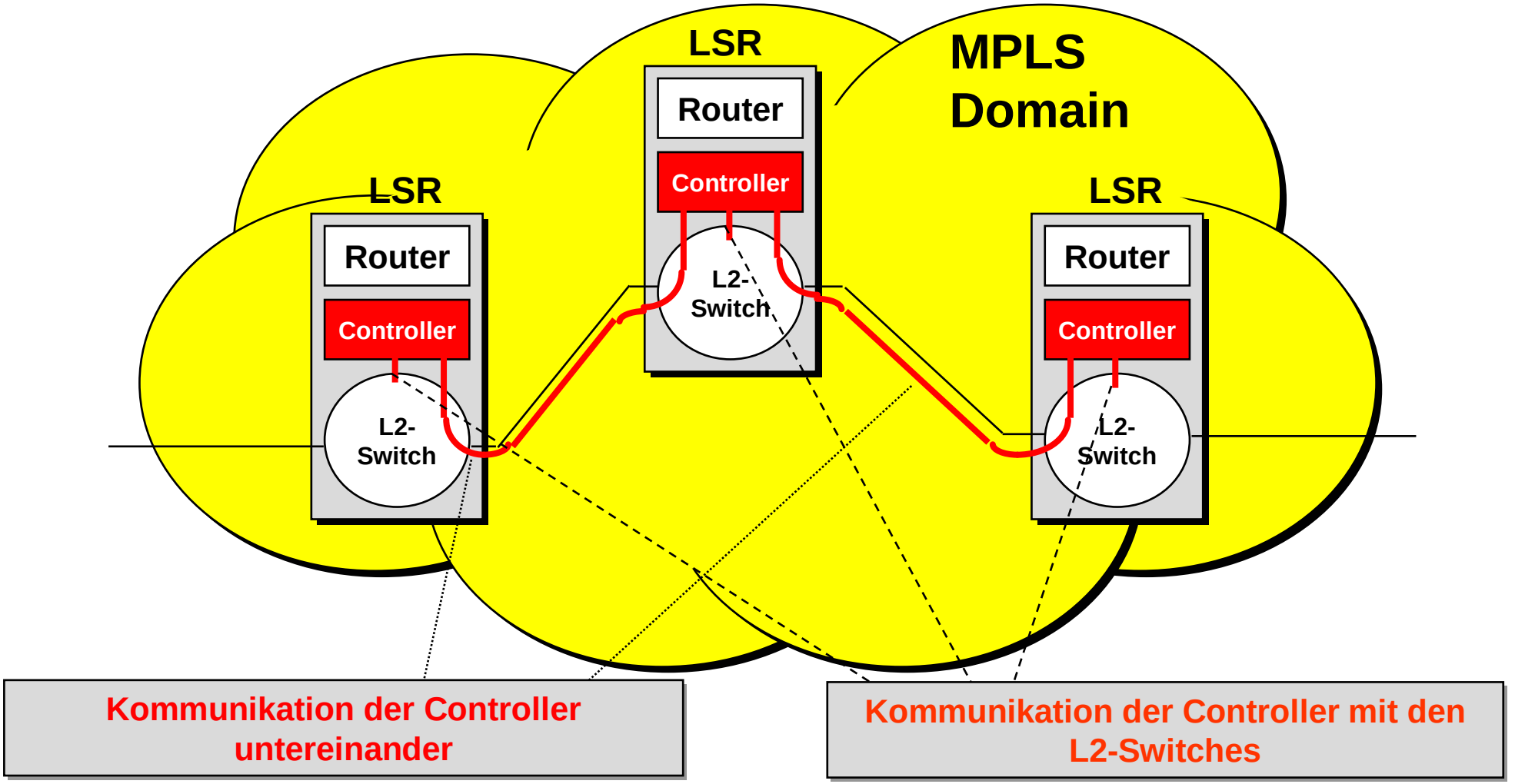
MPLS – Forward Equivalent Class (FEC)

- Unter einer „Forward Equivalent Class“ (FEC) wird eine Gruppe von Paketen verstanden, die weiter geleitet werden:
  - in gleicher Art und Weise,
  - über den gleichen Pfad und
  - mit gleicher Behandelung.
- Eine FEC kann durch die Zieladresse gekennzeichnet sein oder durch ein anderes Merkmal, das der Edge-LSR anerkennt. Das können z.B. sein:
  - definierte IP Precedence-Werte (im ToS-Feld), oder
  - spezielle Schicht-4-Protokolle (im Protocol-Feld).

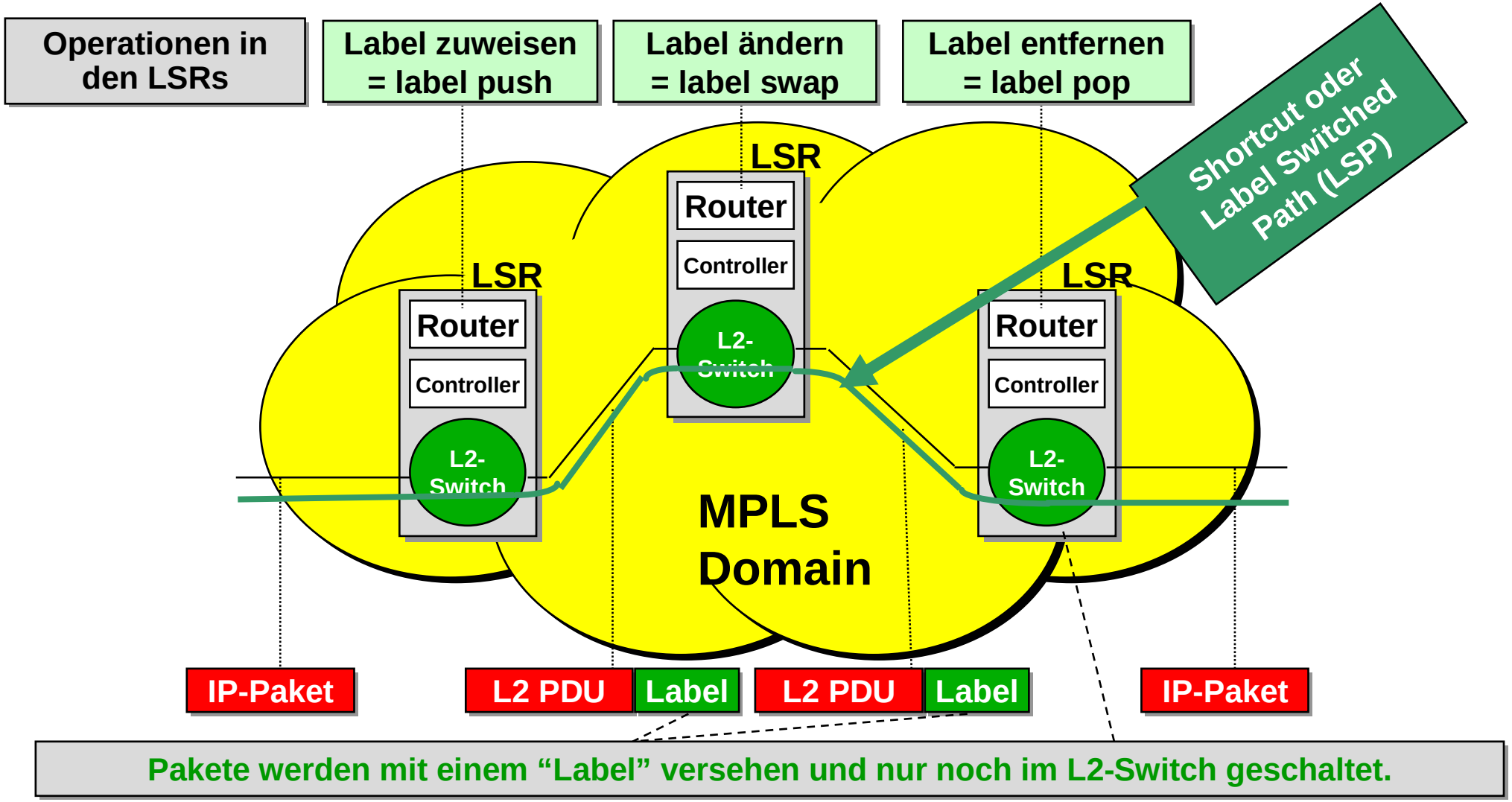
MPLS – Ablauf 1



MPLS – Ablauf 2



MPLS – Ablauf 3



MPLS – Label-Umwertung - Beispiel

Forwarding-Tabelle (Umwertetabelle)

Eingang 1

Label. ein	Aus-gang	Label aus
04	3	17
11	1	23
25	2	11

Eingang 2

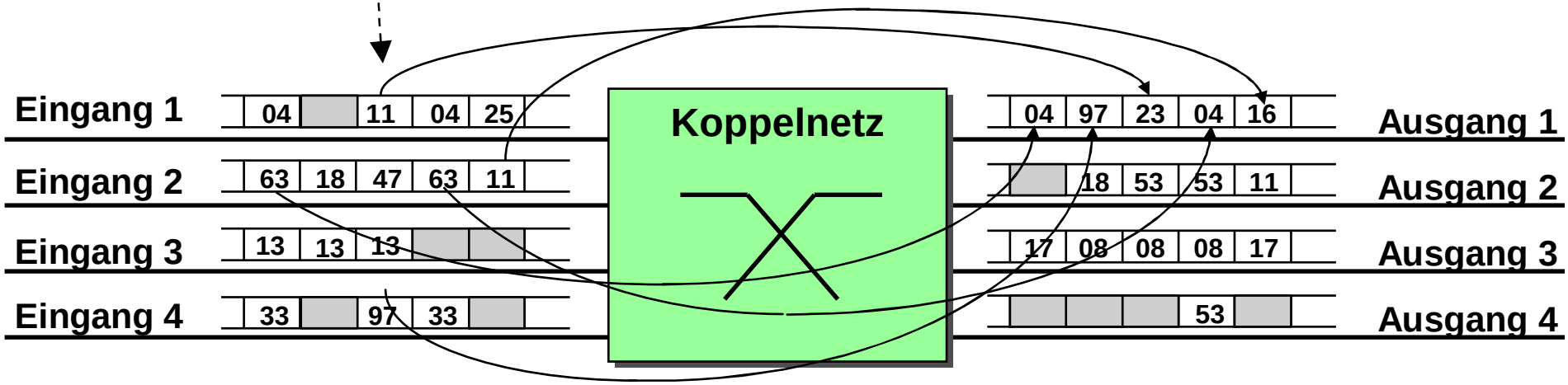
Label ein	Aus-gang	Label aus
11	1	16
18	2	18
47	4	53
63	1	04

Eingang 3

Label ein	Aus-gang	Label aus
13	3	08

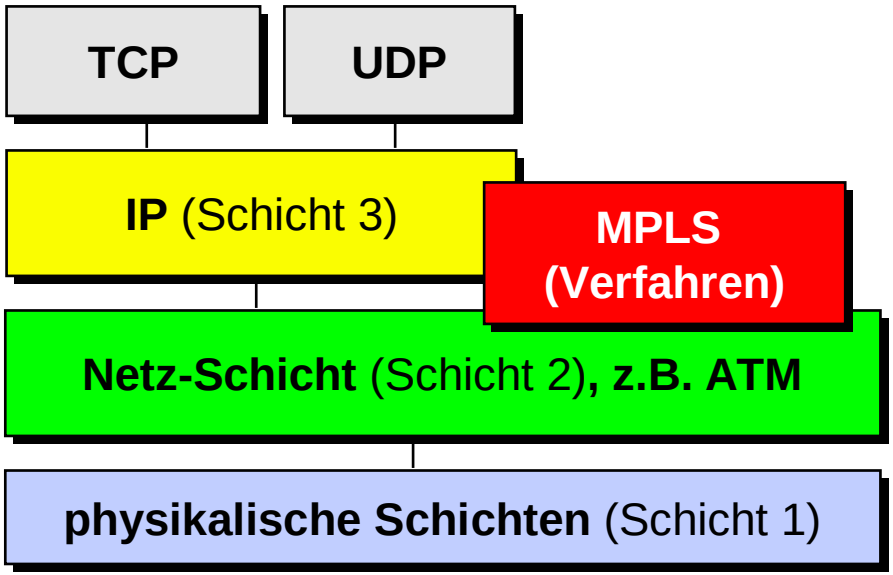
Eingang 4

Label ein	Aus-gang	label aus
33	2	53
97	1	97



MPLS – Protokoll-Stacks

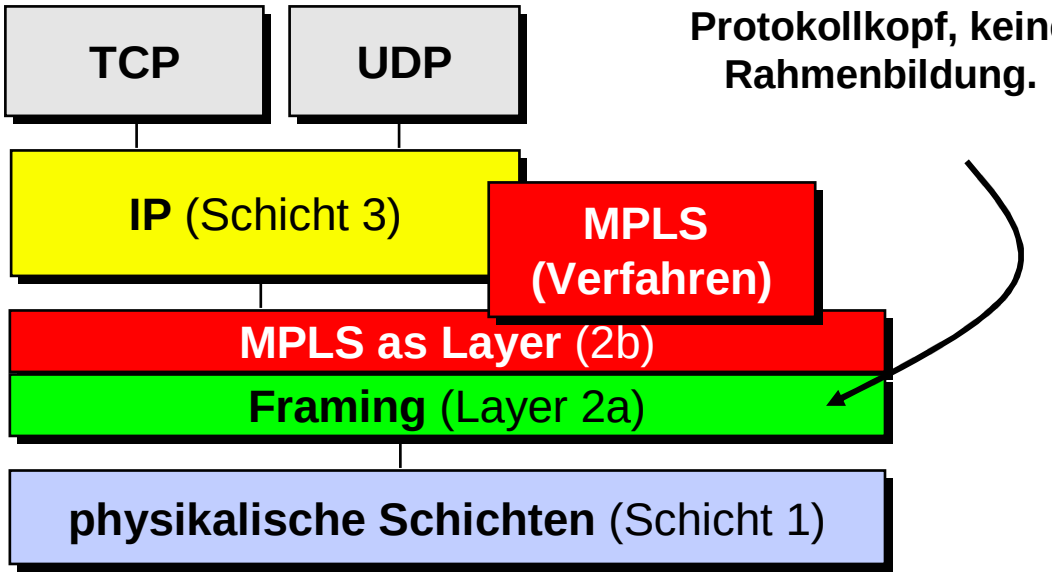
a) MPLS mit ATM



MPLS als Klammer zwischen Schicht 3 und Schicht 2

b) MPLS als Schicht

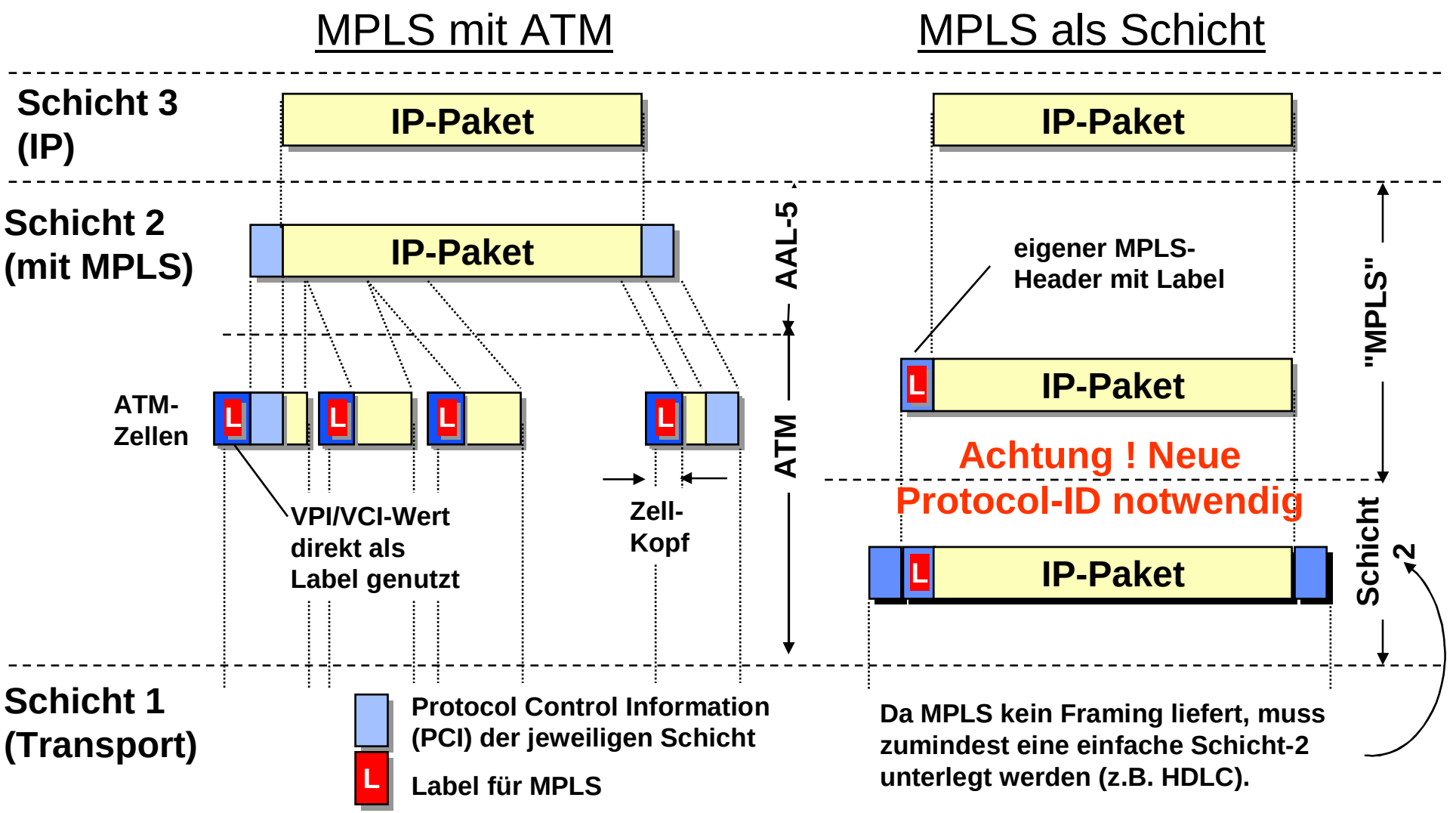
Die MPLS-Schicht bietet nur einen Protokollkopf, keine Rahmenbildung.



MPLS als eigenständige Schicht 2

- Label Switch Router auf ATM-Basis: „ATM-LSR“
- Label Switch Router, der ganze Pakete schaltet: „Frame-based LSR“

MPLS – Das Label im Protokoll-Modell



Inhalt

- Qualität in IP-Netzen
- Multi-Protocol Label Switching (MPLS)
  - MPLS - Prinzipen
  - MPLS - Label
  - MPLS - Steuerprotokolle
  - Einsatz vom MPLS
  - Weiterentwicklungen
- Virtual Private Networks (VPN)
- Generic Framing Procedure (GFP)

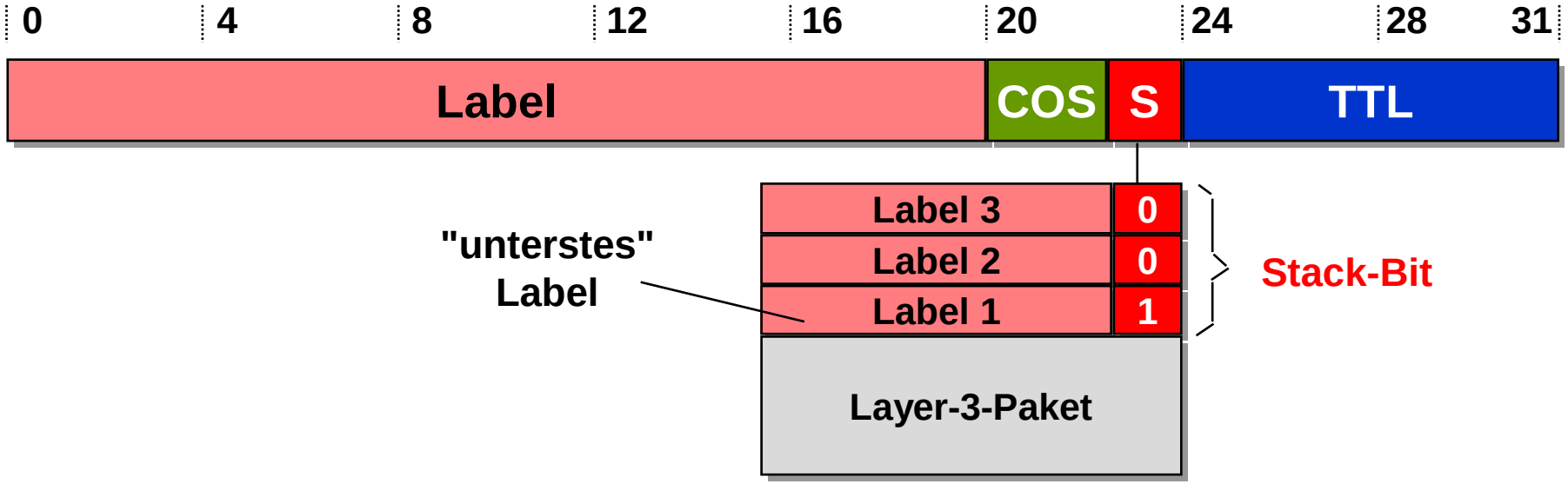
MPLS – Möglichkeiten für das Label

- Als Label wird verwendet:
  - im Falle von ATM das VPI/VCI-Feld,
  - in Falle eines eigenen MPLS-Headers ein 20-Bit-Label.
- Felder des speziellen MPLS-Headers:
  - Label (20 Bit)
  - Lebensdauer - TTL (8 Bit)
  - Stack-Bit (1 Bit)
  - Class of Service (3 Bit)
    (wurde lange als „experimentelle Bits“ bezeichnet)

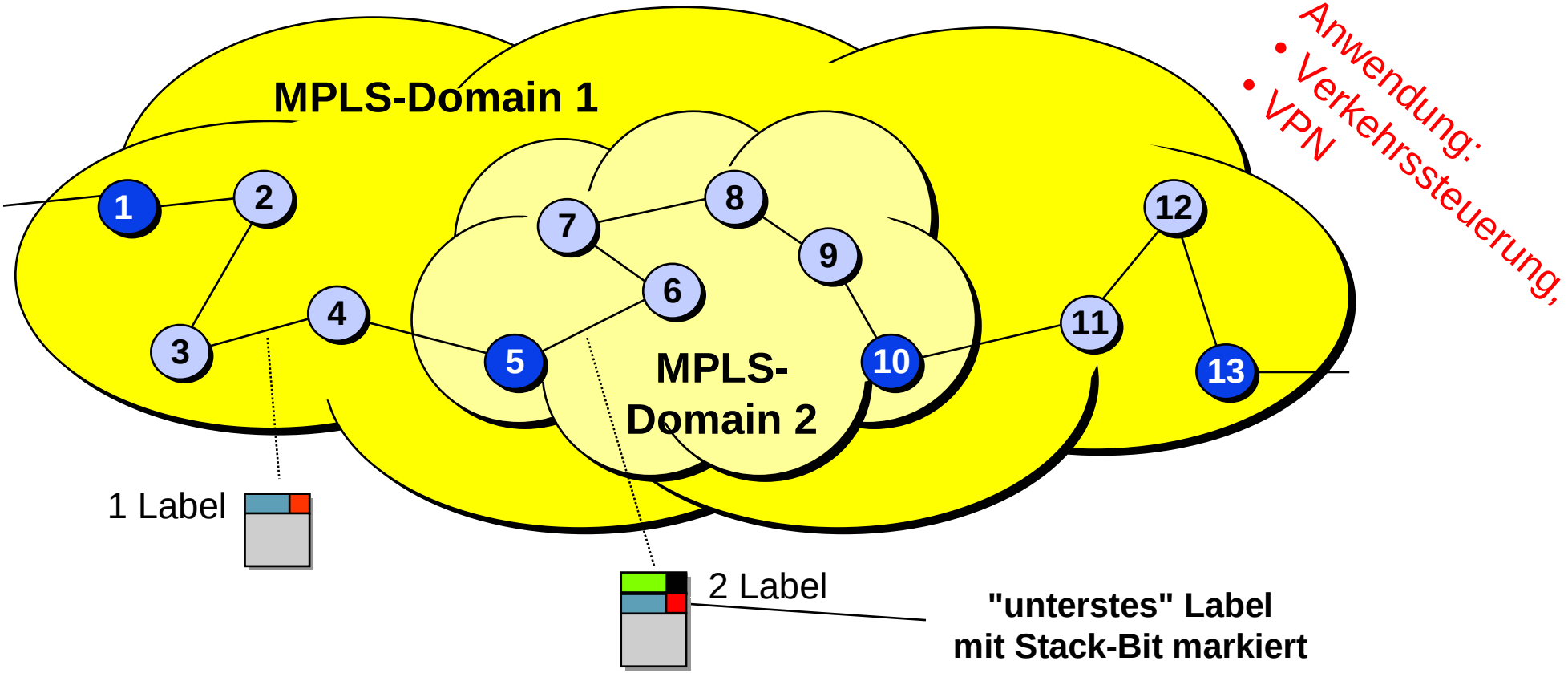
  weitere Ideen (nicht realisiert) waren:
  - next Header-Type
  - Prüfsumme

MPLS – eigenes MPLS-Label

Label	Paket-Typ	Aktion
0	IPv4 NULL	Label entfernen und IPv4 Paket routen
1	Router Alert	Paket zur lokalen SW-Instanz routen
2	IPv6 NULL	Label entfernen und IPv6 Paket routen
3	General NULL	Label entfernen und Paket routen
4...13	reserved	reserved
14	OAM	Operation and Maintenance
15	reserved	reserved



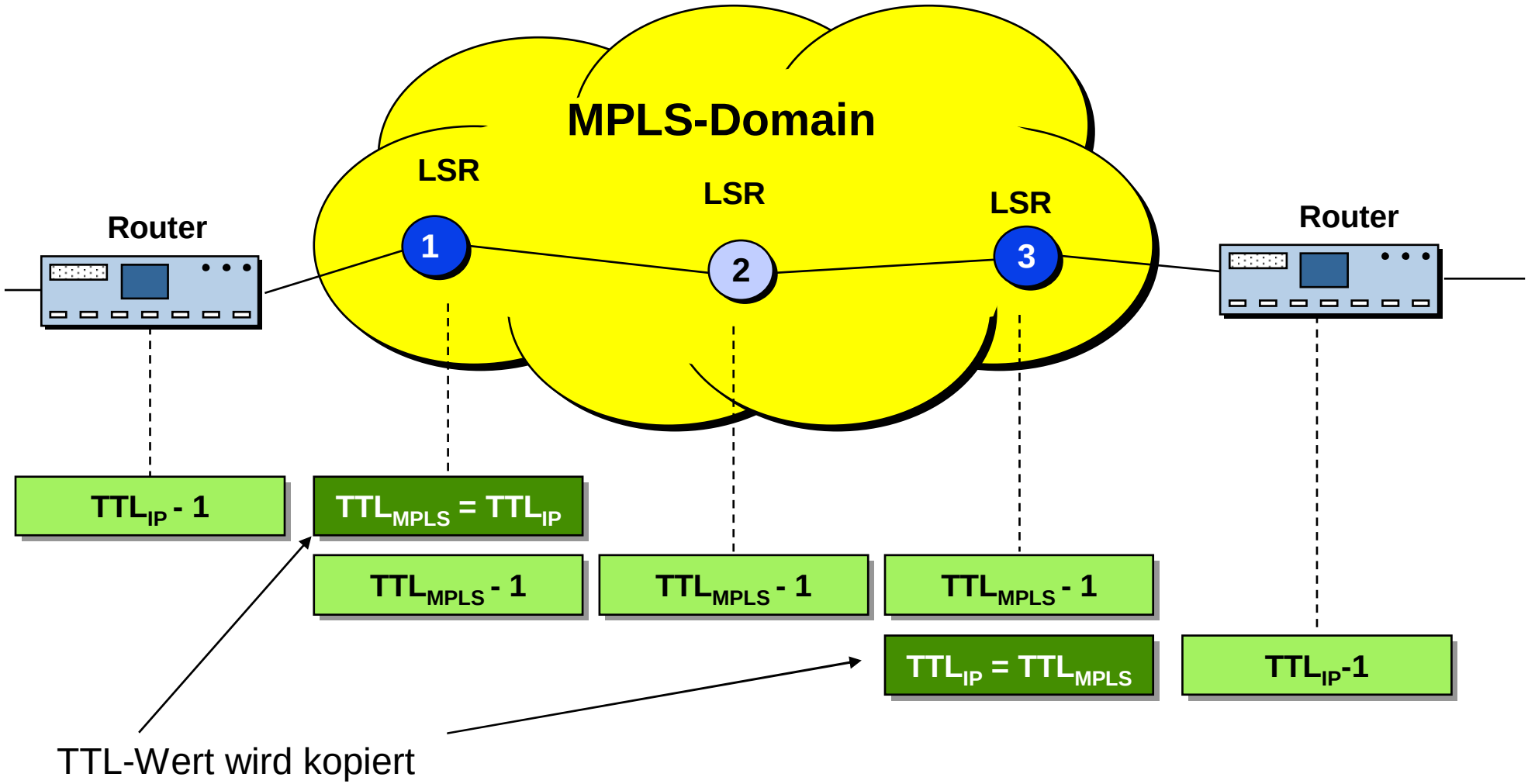
MPLS – MPLS-Domain und Label-Stack



1 **Edge-LSR** (arbeitet intern im Interior Routing Protokoll, z.B. OSPF, nach extern mit Exterior Routing Protokoll, z.B. BGP)

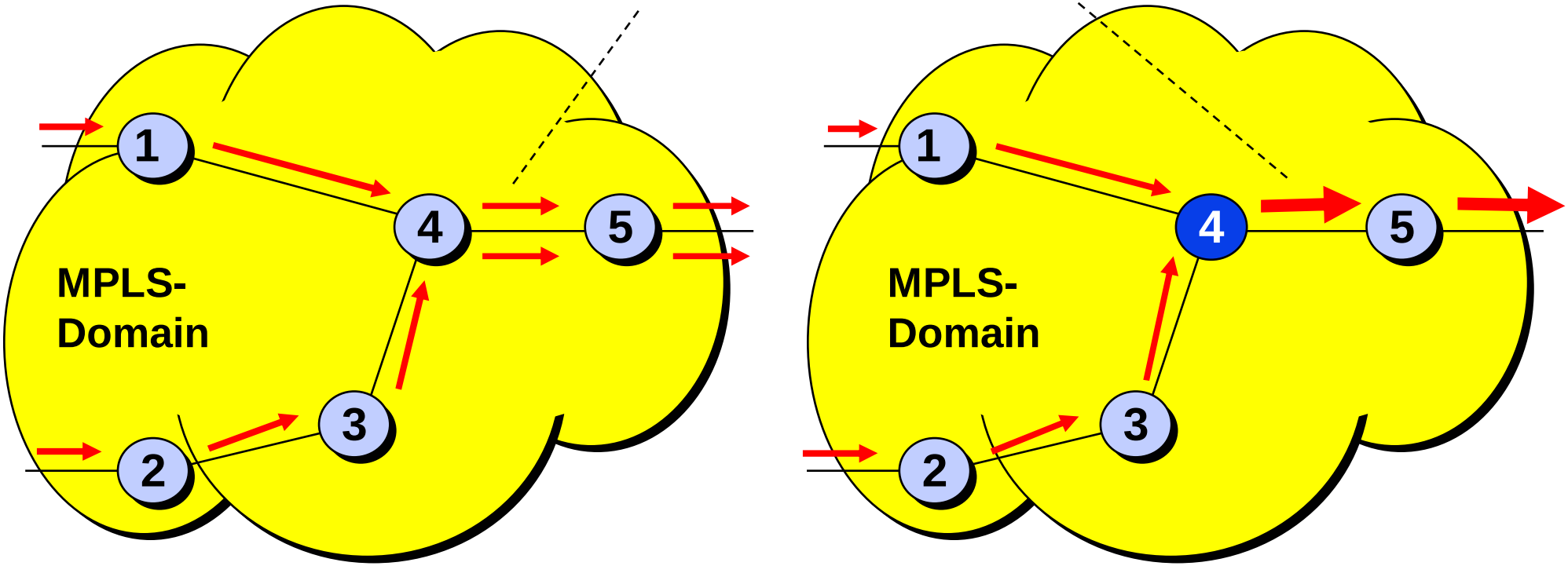
6 **Core-LSR** (arbeitet im Interior Routing Protokoll, z.B. OSPF)

MPLS – TTL-Behandlung



MPLS – "Merging"

Bessere statistische Ausnutzung
des Summenverkehrs gegenüber
den zwei Einzel-Verkehren.



ohne Merging

mit Merging

Inhalt

- Qualität in IP-Netzen
- Multi-Protocol Label Switching (MPLS)
  - MPLS - Prinzipen
  - MPLS - Label
  - MPLS - Steuerprotokolle
  - Einsatz vom MPLS
  - Weiterentwicklungen
- Virtual Private Networks (VPN)
- Generic Framing Procedure (GFP)

MPLS – Steuerprotokolle

- Zum Austausch von Informationen über Bedeutung und Benutzung der Labels zwischen den beteiligten Netzelementen wird ein eigenes Protokoll eingesetzt. Dafür gibt es zwei Möglichkeiten:
  - ein spezielles Protokoll, z.B. das **Label Distribution Protocol** (LDP), oder
  - Huckepack auf einem anderen Protokoll, z.B. **RSVP**.
- Entsprechend der Methode, wie der Weg bestimmt wird, unterschiedet man zwei LSPs:
  - Hop-by-hop LSP (oder Control-driven LSP);
  - Constraint-based routed LSP (oder explicitely routed LSP).
- Die Zuordnung (label binding) wird in einer Tabelle gespeichert, der **Label Information Base** (LIB)

Label Distribution Protocol (LDP)

- Nach Generierung der LIB wird jeder FEC ein Label zugewiesen
- Label Verteilung und Management
  - Neighbour Discovery
  - Austausch von Label Informationen
- Es existieren unterschiedliche Möglichkeiten
  - Label zu propagieren (Label Distribution Mode)
    - downstream on demand distribution (Verteilung auf Anforderung)
    - unsolicited downstream distribution (Verteilung ohne explizite Anforderung)
  - Label zuzuweisen (Label Control Mode)
    - independent control allocation mode
    - ordered control allocation mode
  - Label zu speichern (Label Retention Mode)
    - liberal retention mode
    - conservative retention mode

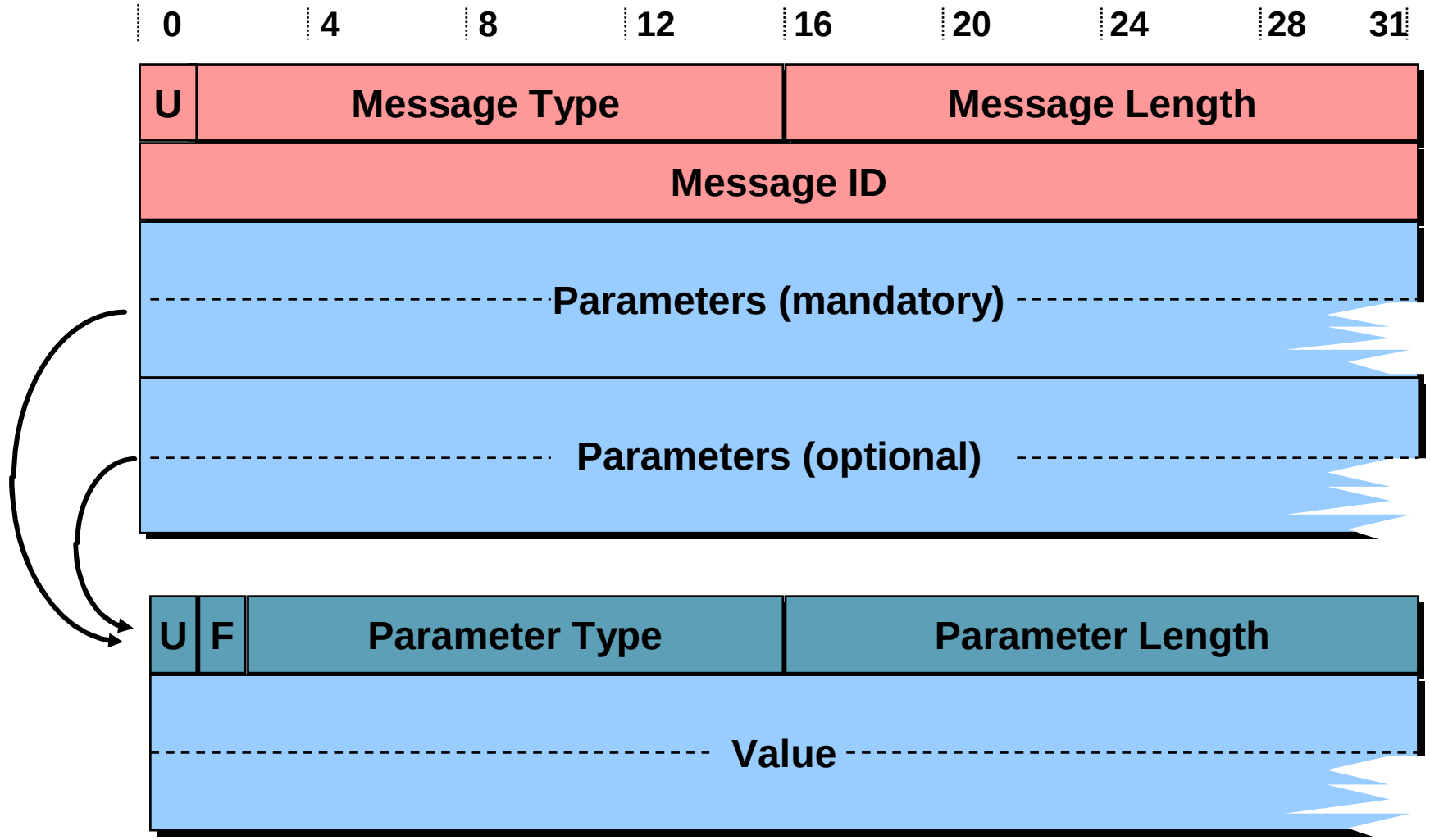
RFC 5036

LDP – Nachrichtenklassen

- Discovery-Nachrichten
  - Kündigen bestehende LSPs an, dazu gehört auch, dass sich LSRs periodisch melden und sich bekannt machen (Hello-Pakete);
  - Nutzt Multicast im Subnetz, über UDP, Port-Nr. 646.
- Session-Nachrichten
  - Aufbauen, generieren und unterhalten von LDP-Sessions zwischen LDP-Peers;
- Advertisements-Nachrichten
  - Generieren, ändern und löschen von Label-Zuordnungen zu Verkehrsklassen (FECs) („Binding”);
- Notification-Nachrichten
  - tragen Fehlermeldungen und sonstige Informationen.

über TCP Port 646

LDP – Nachricht



LDP – Nachrichtenelemente

Feld	Beschreibung	
Unknown Message	Kennzeichnet, daß der Empfänger, so er die Nachricht nicht versteht, den Sender informieren soll	
Message Type	Typ der Nachricht, folgende Typen sind definiert:	
	Hello	für LDP-Discovery
	Initialization	Aufbau der LDP-Session
	Keep Alive	hält eine LDP-Session aktiv, auch wenn kein Nachrichtenaustausch stattfindet
	Address	teilt Schnittstellen-Adressen zu
	Address Withdraw	löscht Schnittstellen-Adressen wieder
	Label Mapping	teilt eine Label-Zuordnung mit
	Label Request	fordert für eine FEC eine Label-Zuordnung an
	Label Withdraw	fordert die Löschung eine Label-Zuordnung
	Label Release	löscht eine Label-Zuordnung
	Notification	Fehler- und sonstige Meldungen
Message Length	Gesamtlänge der Nachricht in Oktett	
Message ID	Eindeutige Identifizierung, dient zur Korrelation von Anfragen und Antworten, bzw. Fehlermeldungen	
Parameters	Parameter für die Nachricht	

CR-LDP – „Constraints“

- Explicit Route:
  - eine Liste der zu durchlaufenden Knoten wird angegeben.
- Traffic Characteristics:
  - Verkehrs-Parameter werden mitgegeben die in den Knoten dann die Wege-Auswahl beeinflussen (z.B. Spitzenbitrate).
- Preemption:
  - Angaben über die benötigten Ressourcen auf dem Pfad, sowie eine Angabe über die Priorität werden mitgegeben. Sind diese Ressourcen nicht verfügbar, dann versuchen die Knoten bestehende Pfade umzukonfigurieren.
- Route Pinning:
  - hier wird der Pfad (oder Teile des Pfades) absolut festgelegt, d.h. auch wenn ein „besserer” Pfad verfügbar wird, bleibt es beim festgelegten.

RFC 3212

RSVP-TE – Prinzipen

- In Netzen, die RSVP und MPLS, unterstützen, kann eine Beziehung zwischen den „Label Switched Pathes“ (LSPs) von MPLS und den „Flows“ von RSVP hergestellt werden .
- Die Nachrichten für den Aufbau eines Flows in RSVP (PATH und RESV) lassen sich so auch für den Aufbau eines LSPs nutzen.
- Dazu wird ein neues Element eingeführt, das Label-Request-Objekt. (Für hart definierte Routen das Explict-Route-Object.)
- Dem LSP können so direkt Ressourcen zugewiesen werden (... die ureigene Funktion von RSVP).
- Das Ergebnis: RSVP-TE (Resource Reservation Protocol – Traffic Engineering)

RFC 3209

RSVP-TE – neue Objekte

Element (Name des Objects)	in PATH-Nachricht	in RESV-Nachricht	Bedeutung
LABEL_REQUEST	X		fordert eine Label-Zuweisung an wobei ein Wertebereich angegeben werden kann (wichtig z. B. bei ATM und Frame Relay)
LABEL		X	Label-Zuordnung
EXPLICIT_ROUTE	X		Legt den kompletten Pfad fest, unter Angabe einer Kette von Knoten
RECORD_ROUTE	X	X	fragt Informationen über den LSP, bzw. dessen Weg durchs Netz ab.
SESSION_ATTRIBUTE	X		dient der Steuerung und Überwachung

CR-LDP oder RSVP-TE?

- RSVP-TE steht in Konkurrenz zu CR-LDP.
- Beide Protokolle sind geeignet und es gibt heute keine Erkenntnis, welches „besser“ oder besser für einen bestimmten Anwendungsfall ist.
- Als Unterschiede werden gesehen:
  - CR-LDP wird (als Abkömmling von LDP) über TCP transportiert und ist ein Hard-State-Protokoll.
  - RSVP-TE (als Abkömmling von RSVP) wird direkt über IP transportiert, steht also auf der gleichen Stufe wie ein Transportprotokoll und arbeitet mit Soft-States, muss also laufend den Status auffrischen. Vielleicht ist dies ein Grund, weshalb oft RSVP-TE bevorzugt wird.

OAM im MPLS

- OAM für MPLS
  - vergleichbar den OAM-Funktionen im ATM
- OAM-Funktionen
  - Connectivity Verification
  - Forward Defect Indicator
  - Backward Defect Indicator
  - Performance Messung (geplant)
  - Loopback (geplant)
  - Ersatzschaltung (Protection Switching)

QoS und MPLS

- MPLS hat vom Prinzip erst einmal nichts mit der Bereitstellung von QoS zu tun.
- QoS kann auch über andere Mechanismen erreicht werden.
- Aus Marketinggründen haben die meisten ISP beschlossen, MPLS mit QoS anzubieten und so diese beiden Begriffe miteinander zu verquicken.
- Andererseits – man macht Traffic Engineering zur Verkehrstrennung. Und kann damit auch Qualitätsklassen unterscheiden.

Inhalt

- Qualität in IP-Netzen
- Multi-Protocol Label Switching (MPLS)
  - MPLS - Prinzipen
  - MPLS - Label
  - MPLS - Steuerprotokolle
  - Einsatz vom MPLS
  - Weiterentwicklungen
- Virtual Private Networks (VPN)
- Generic Framing Procedure (GFP)

Einsatz von MPLS (1)

- Eine Mischung von Routern ohne MPLS und MPLS-Knoten ist begrenzt möglich. Über die Router muss dann ein Tunnel zwischen den MPLS-Knoten aufgebaut werden, z.B. mit dem Layer-2-Tunneling-Protocol (L2TP).
- Auch Schicht-2-Knoten können dazwischen liegen, die dann aber einen transparenten Pfad zwischen MPLS-Knoten schalten müssen.
- Es gibt Fälle, in denen MPLS nicht eingesetzt werden kann:
  - Wenn eine kleinere Granularität benötigt wird, als sie MPLS bieten kann.
  - Aus Sicherheits-Gründen, wenn z.B. ein Paketfilter eingesetzt wird (Firewall).
  - Im ersten Router, wenn der Host kein MPLS kann.

Einsatz von MPLS (2)

- Bereitstellen einer definierten **Qualität**
  Manche sehen aber eine Überdimensionierung und/oder eine Priorisierung wie DIFFSERV als ausreichend an.
- **Verkehrssteuerung** (TE - Traffic Engineering)
  Als Maßnahme des Netzbetreibers erlaubt MPLS eine bessere Verteilung des Verkehrs als IP.
- Transport einer (anderen) Schicht-2-Information (z.B. Frame-Relay, Ethernet, ...) = „**Pseudo Wire**“.
- Realisierung von **VPNs**
  Striktere Trennung der VPNs gegeneinander als mit reinem IP-VPN. Erstes MPLS-Dokument war zu VPN !

VPN = Virtual Private Network

Inhalt

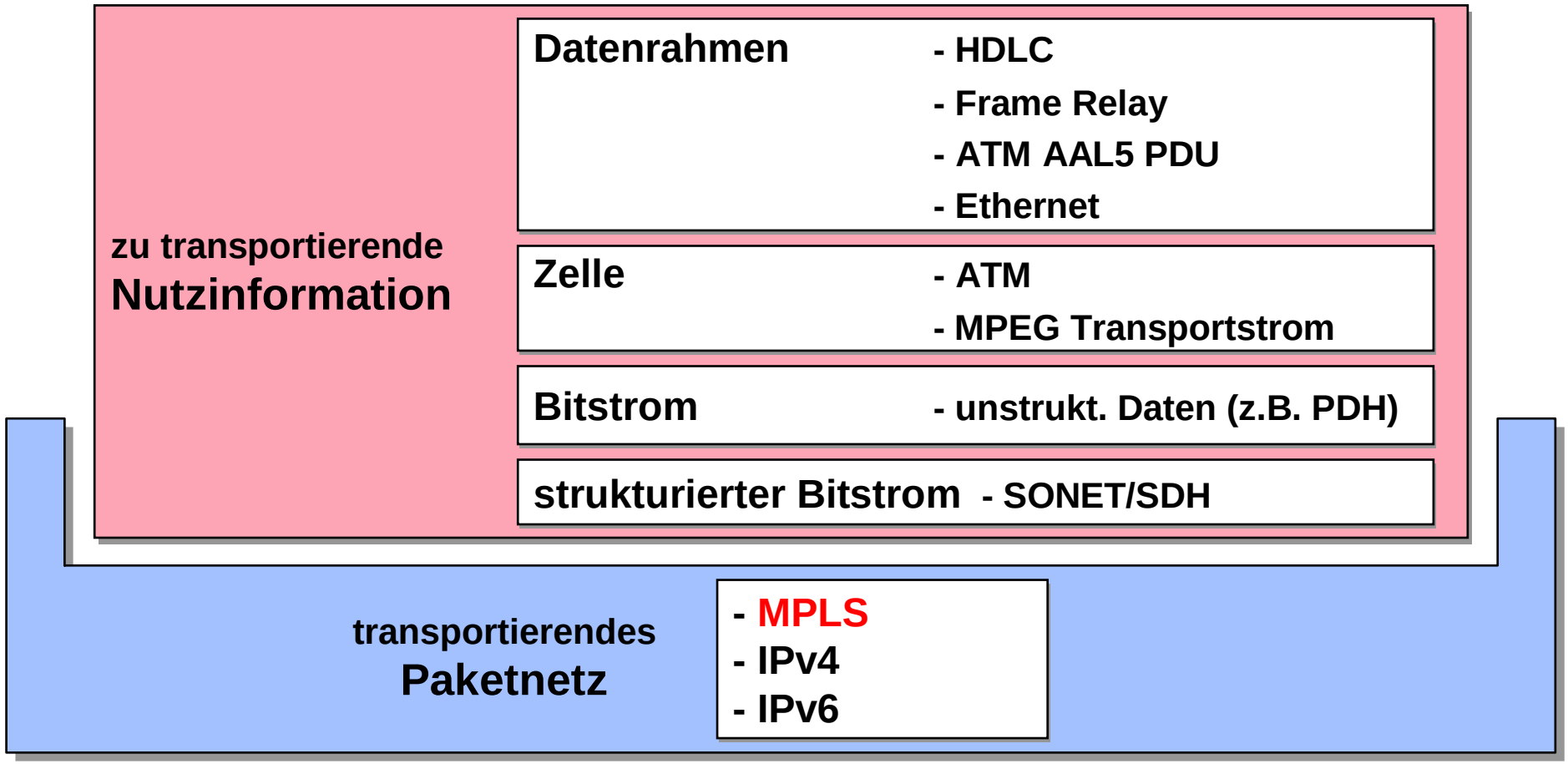
- Qualität in IP-Netzen
- Multi-Protocol Label Switching (MPLS)
  - MPLS - Prinzipen
  - MPLS - Label
  - MPLS - Steuerprotokolle
  - Einsatz vom MPLS
  - Weiterentwicklungen
- Virtual Private Networks (VPN)
- Generic Framing Procedure (GFP)

MPLS-Weiterentwicklungen (1)

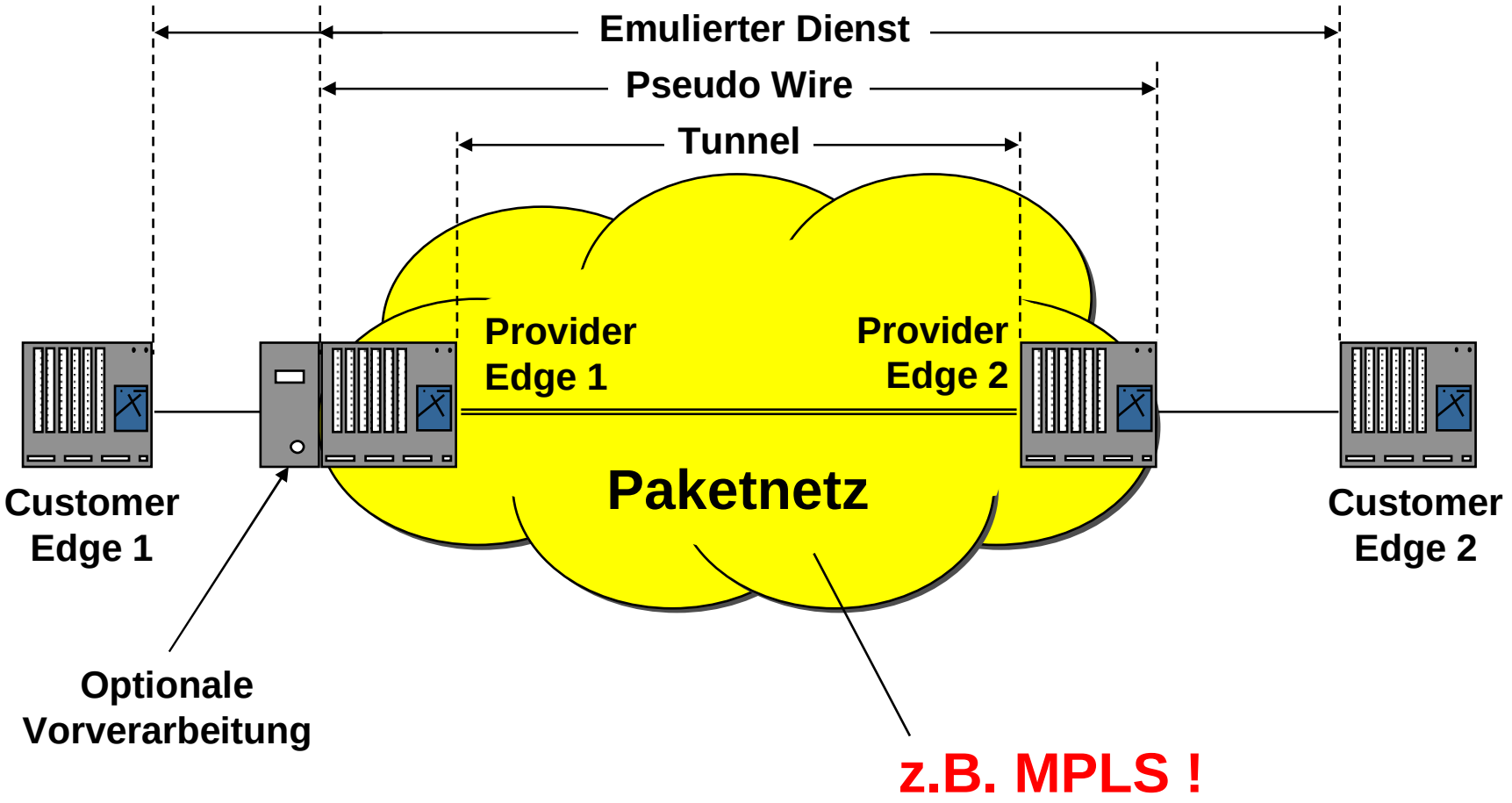
- Es bildet sich hier eine Art Hierarchie heraus:
  - **Paket / Rahmen / Zell-Ebene** (seitheriger Einsatz von MPLS),
  - **Zeitschlitz-Ebene** (TDM), z.B. die Benutzung von MPLS für das Einrichten von Virtual Containers in einem SDH-System,
  - **Wellenlängen-Ebene** (Lambda), z.B. die Benutzung von MPLS für das Einrichten einer Wellenlänge in einem WDM-System („light path“), und
  - **Schnittstellen-Ebene** (räumlich), z.B. die Benutzung von MPLS für das Einrichten von Ports in einem System.
- Diese neue Betrachtungsweise wird unter dem Schlagwort **Generalized MPLS** (GMPLS) gehandelt.

MPLS-Weiterentwicklungen (2a)

MPLS als Generelles Transport-Protokoll = "Pseudo Wire"



MPLS-Weiterentwicklungen (2b)



Ausblick

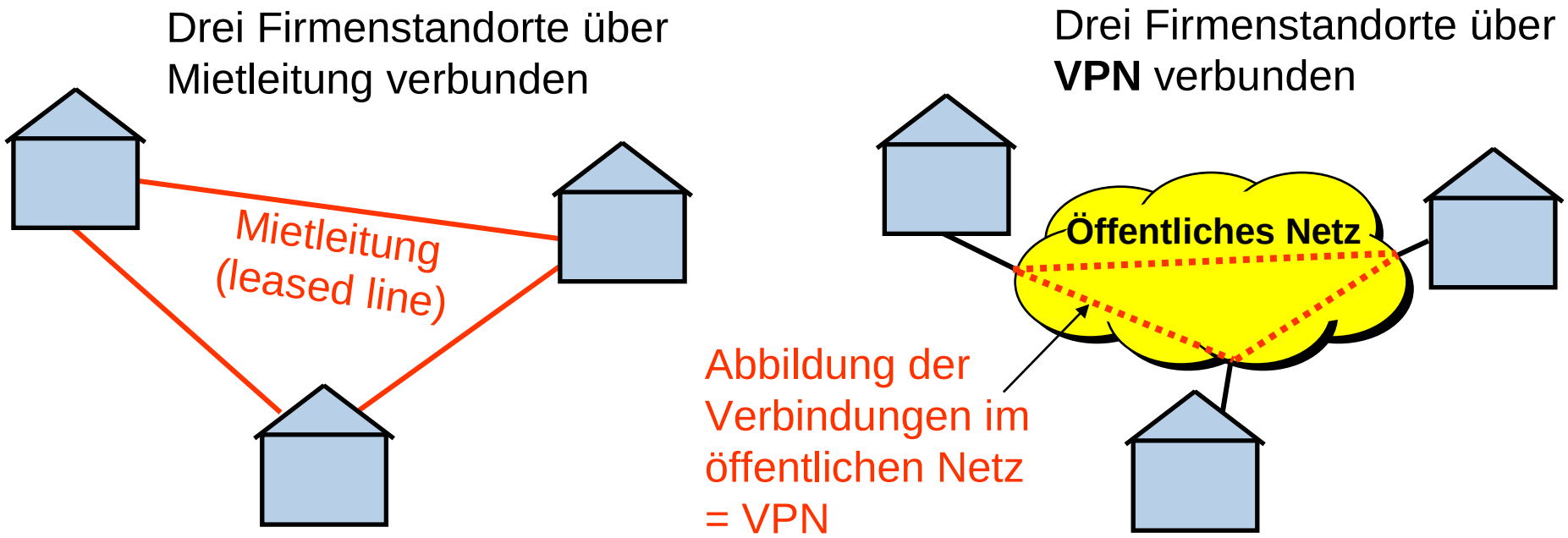
- MPLS gilt als sehr zukunftsträchtige Technik, wenn es darum geht, höhere Geschwindigkeiten und Qualität in IP-Netzen einzuführen.
- Die Vorteile von MPLS werden gesehen in:
  - der Bereitstellung von (Ende-zu-Ende) Qualität,
  - der Skalierbarkeit - MPLS soll auch in großen Netzen funktionieren,
  - der Unabhängigkeit von der Schicht 2-Technologie und
  - der Bereitstellung neuer Dienste, allen voran VPNs.
- Die Technik ist aber komplex und es dauerte lange, bis stabile Standards verfügbar waren.
- MPLS ist in den Netzen vorhanden und ist die bevorzugte Lösung von traditionellen Telekommunikations-Netzbetreibern für ihre Daten-Backbones.

Inhalt

- Qualität in IP-Netzen
- Multi-Protocol Label Switching (MPLS)
  - MPLS - Prinzipen
  - MPLS - Label
  - MPLS - Steuerprotokolle
  - Einsatz vom MPLS
  - Weiterentwicklungen
- Virtual Private Networks (VPN)
- Generic Framing Procedure (GFP)

Virtuelle Private Netze (VPN)

- Ein **Virtual Private Network** (VPN) (Virtuelles Privates Netz) ist ein Netz, das zum Transport privater Daten ein öffentliches Netz (zum Beispiel das Internet) nutzt.
- Teilnehmer eines VPN können Daten wie in einem internen Netz (LAN, Intranet) austauschen.



VPN – Anforderungen (1)

- Sicherheit
  - Mechanismen für Vertraulichkeit, Authentifizierung, Verkehrstrennung
- Skalierbarkeit
  - Unterstützung von kleinen Lösungen (für SOHO) bis hin zu großen Unternehmensnetzen
  - Schnelles Umkonfigurieren (Hinzufügen und Entfernen von Standorten)
- Unterstützung unterschiedlicher Zugangstechnologien und Netztopologien
  - Unterstützung verschiedener Bandbreitenanforderungen für Zentrale und Außenstellen
  - Unterstützung von z.B. Dial-In (Einwahl) Lösungen für Remote Zugriff in das VPN für den Außendienst
- Unterstützung verschiedener VPN Topologien
  (Full Mesh, Hub and Spoke, beliebige Kommunikationsbeziehungen zwischen Standorten)

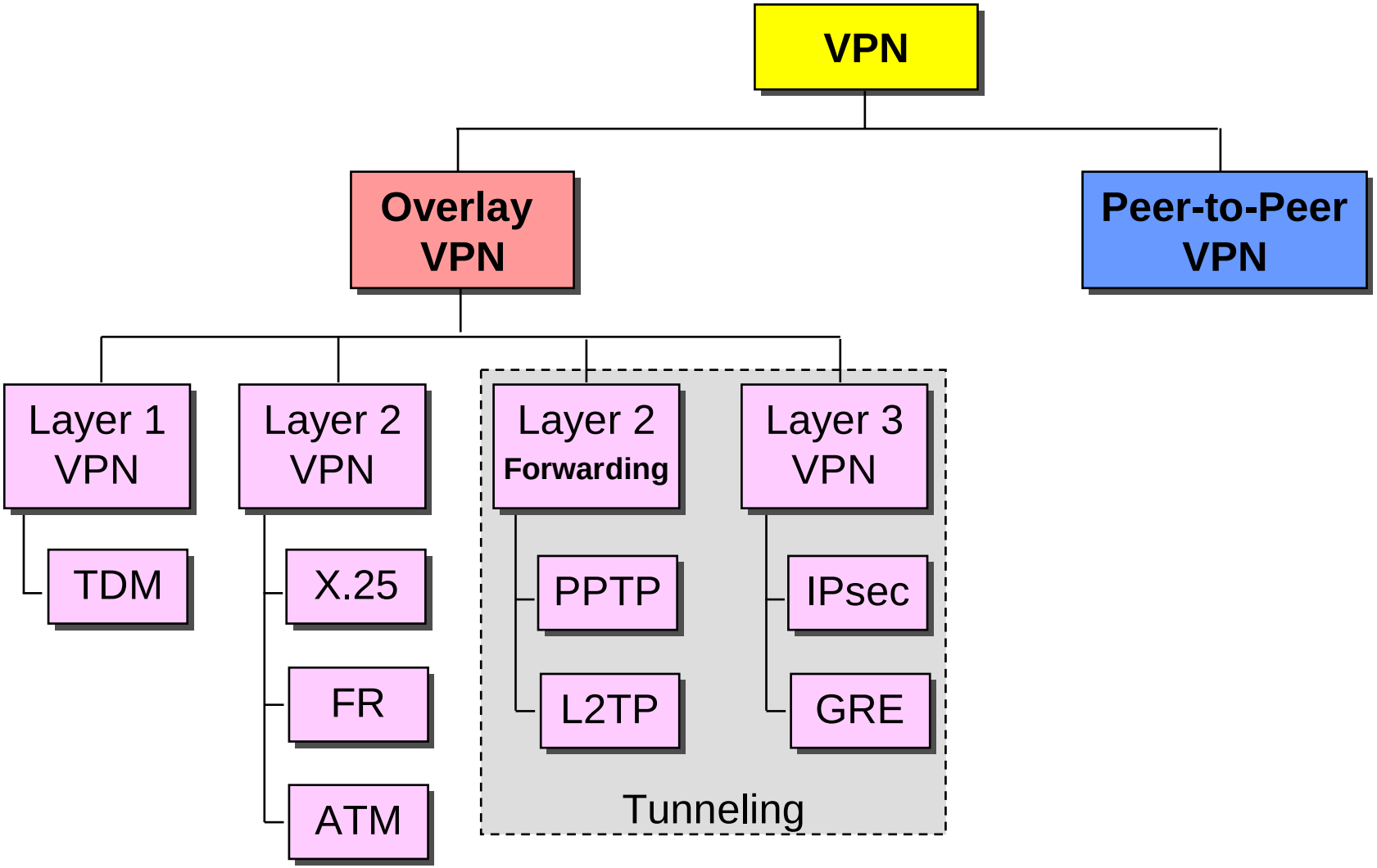
VPN – Anforderungen (2)

- Zuverlässigkeit
  - Einhaltung des vereinbarten Service Level Agreements (SLA)
- Dienstgüte (QoS)
  - Mechanismen zur Priorisierung von geschäftskritischem Verkehr
- Management
  - kosteneffektives Management
  - Management der CPE durch den Provider oder den Kunden
  - Überwachung Verfügbarkeit und Dienstgüte
- Niedrige Kosten
  - zur Einrichtung eines VPN
- Beibehaltung der bestehenden Adressierung

VPN – Netztechnologien

- Klassische Verbindungen zwischen Firmenstandorten benutzten **Mietleitungen** (leased lines) – teuer und unflexibel, aber sehr sicher!
- Mit dem Aufkommen von **Paketnetzen**, die „virtuelle Verbindungen“ unterstützen, konnte man Firmenstandorte auch über solche Netze verbinden – z.B. über Frame Relay, ATM, MPLS, IP.
- Da die Sicherheitsproblematik bei höheren Schichten zunimmt, siedelt man VPNs gerne in der **Schicht 2** an. Heute ist hier **MPLS** der Favorit.
- Durch ihre Flexibilität und breite Verfügbarkeit hat trotzdem das **VPN auf Schicht 3** (.. IP) seine Berechtigung und Bedeutung.

VPN – Konzepte



VPN auf Layer 1

Traditionelle TDM Lösung

- Der Service Provider stellt eine physikalische Verbindung zwischen einzelnen Kunden-Standorten bereit (Standleitung).
- Der Kunde hat die Verantwortung für alle höheren Schichten.
- Probleme:
  - Skalierung: n^2 Verbindungen müssen bei n Standorten geschaltet werden.
  - hohe Fixkosten z.B. für eine E3 (34 Mbit/s) bei konstanter Bandbreite.
- Vorteil:
  - hohe Sicherheit - keine Schaltung im Netz, aber damit auch keine Ersatzschaltung durch den Provider bei Fehlern.
- In der Regel werden eher Layer-2- oder Layer-3-VPNs angeboten.

VPN auf Layer 2

Switched WAN

- Der Service Provider stellt eine Layer-2-Verbindung zwischen einzelnen Kunden-Standorten bereit.
- Statt der Standleitung wird eine „virtuelle Standleitung” über Permanent Virtual Connections (PVCs, ATM oder FR-Verbindungen) fest geschaltet.
- Der Kunde hat die Verantwortung für alle höheren Schichten.
- Probleme:
  - Skalierung: n^2 Verbindungen müssen bei n Standorten geschaltet werden.
  - Beim Hinzufügen von neuen Kunden-Standorten müssen Konfigurations-arbeiten an allen Standorten vorgenommen werden (angenommen Vollvermaschung).
- Meist „sternförmige“ Topologie: Zentrale und n Außenstellen.

VPN auf Layer 3

Tunneling/Forwarding

- VPN wird über IP-in-IP-Tunnel realisiert (Ebene 3 wird in IP eingepackt).
- Tunnel Realisierung mit GRE oder IPSec:
  - GRE ist ein schnelleres und einfacheres Protokoll,
  - IPSec bietet Authentifikation und Sicherheit.
- Problem
  - Skalierung: n^2 Tunnel müssen bei n Standorten geschaltet werden.
  - Problem: Hoher Overhead.

GRE = Generic Routing Encapsulaton

VPN – Layer 2 und Layer 3

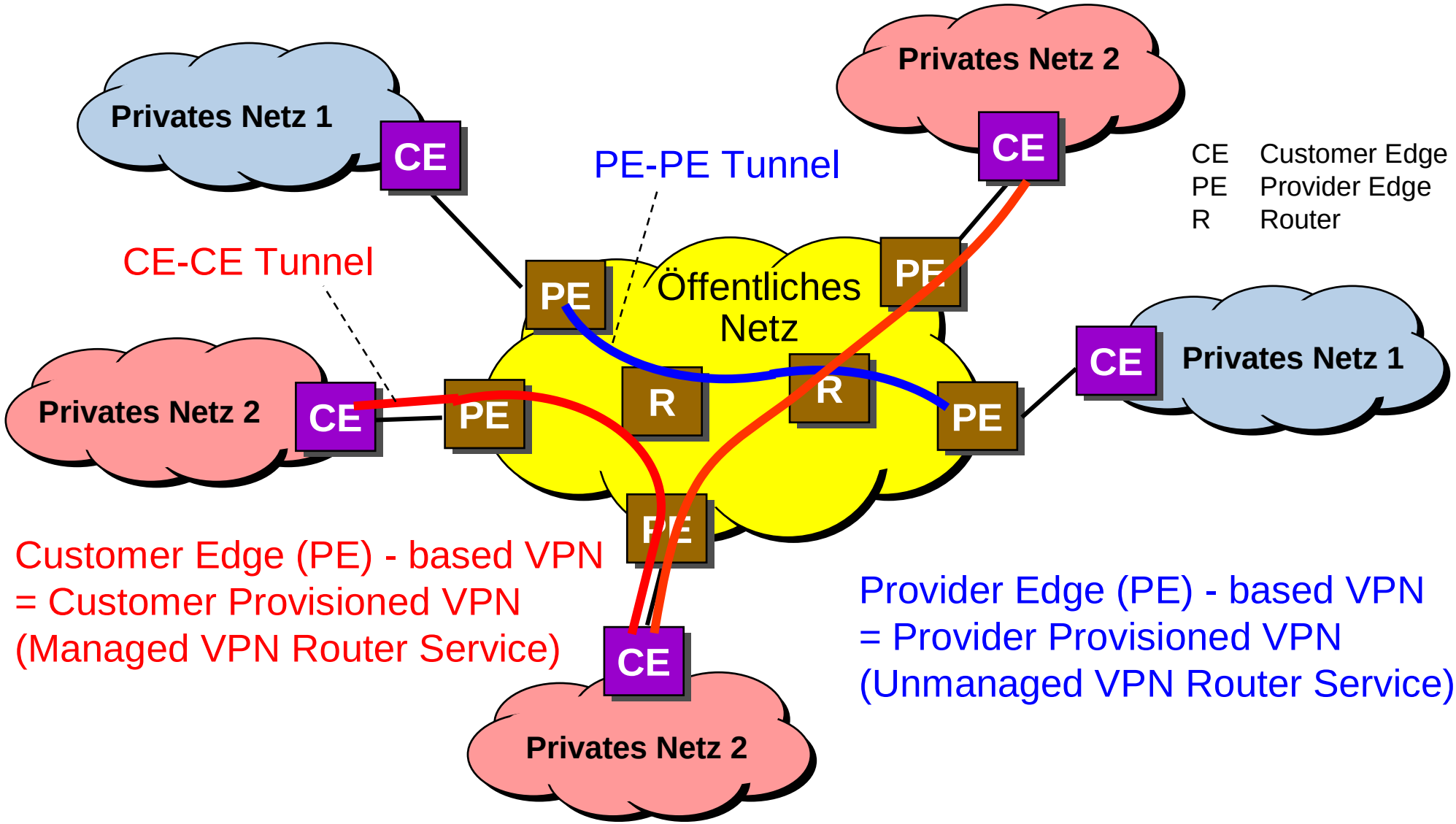
Layer 2 VPNs

- Das Service-Provider-Netz schaltet Layer-2-Rahmen des Kunden aufgrund ihres Layer-2-Headers
- Der Service Provider baut zu jedem Kundenstandort eine Layer-2-Verbindung auf.
- Die Kunden bilden ihr Schicht-3-Routing auf die Schicht-2-Vermaschung ab.
- Das Routing des Kunden ist für den Service Provider transparent.
- Erreichbarkeit muss einzeln durch PVCs zwischen den Standorten geschaffen werden,

Layer 3 VPNs

- Der Service Provider routet die Kunden-Pakete aufgrund der Ziel-IP-Adresse.
- Das Service-Provider-Netz nimmt damit am Routing des Kunden teil
- Das Service-Provider-Netz managt VPN-spezifische Routing-Tabellen und teilt die Routen den Kundenstandorten mit.
- Die Kundenstandorte machen dem Service Provider ihre Routen bekannt.
- Any-to-Any-Erreichbarkeit durch das Prinzip vorgegeben.

VPN – Grundkonfiguration



Einsatz von MPLS für VPNs

- MPLS bietet den erforderlichen Tunneling-Mechanismus.
  - MPLS kann zum Aufbau von „traffic engineered“ PE-PE-Tunnels benutzt werden.
  - Mit einem weiteren MPLS-Label kann die Zuordnung von Paketen zu VPNs markiert werden.
- MPLS kann als Layer-3- oder Layer-2-basiertes VPN konfiguriert werden:
  - Layer 3 MPLS-based VPNs:
    - BGP/MPLS VPNs (RFC 2547bis)
  - Layer 2 MPLS-based VPNs:
    - Virtual Private Wire Service (VPWS)
    - Virtual Private LAN service (VPLS)

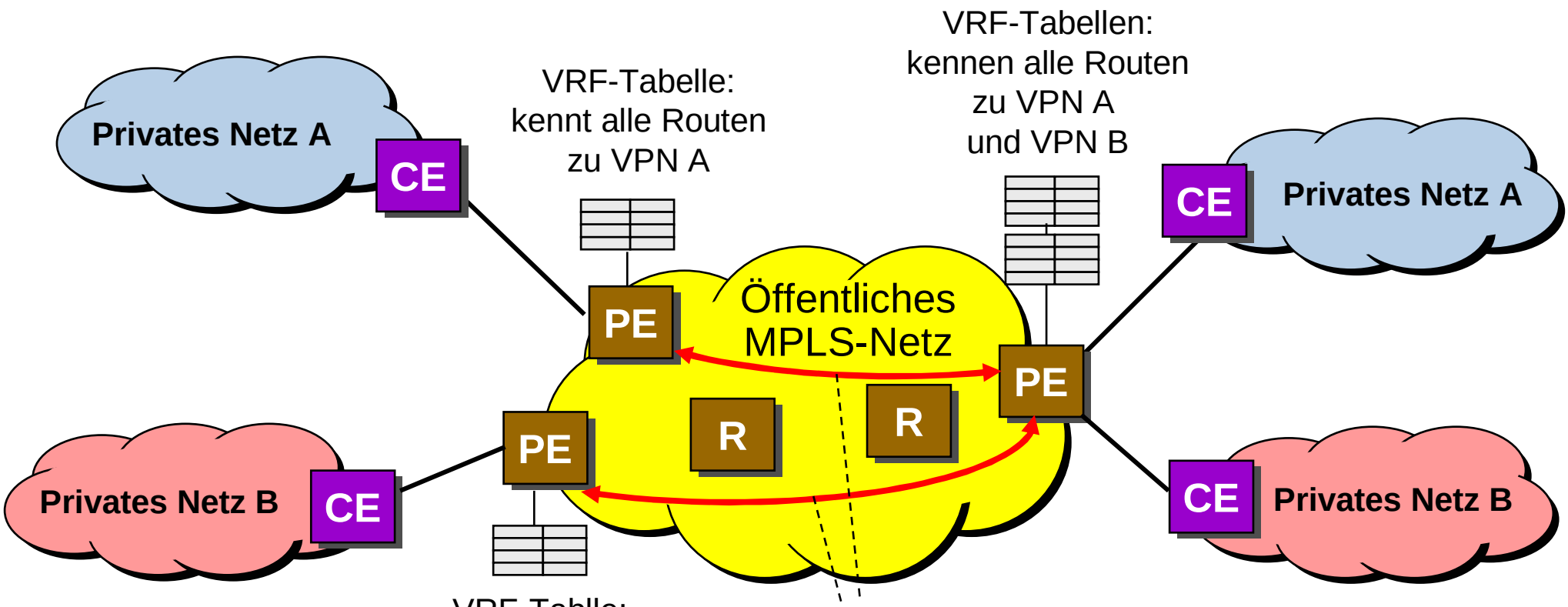
MPLS-VPN – Grundlagen (1)

- Erreichbarkeit der Kunden IP-LANs über statische Routen oder Routing Protokoll (beim letzteren kein Konfigurationsarbeiten beim Provider erforderlich, wenn sich IP Adressrange ändert)
- Für **jedes** VPN wird auf den Provider Edge (PE) Routern eine eigene Routing Tabelle eingerichtet, die nur Informationen zu Zielen in dem VPN enthält -> Virtual Routing and Forwarding Table (VRF-Table).
- Jeder PE-Router „spricht“ mit den anderen PE Routern über das Routing Protokoll „ Multiprotocol Internal BGP“ (MP-IBGP) und tauscht so mit den anderen Edge Routern die Adressinformationen des VPNs (Inhalte der VRF Table) aus. Zusätzliche Informationen werden über BGP Attribute mitgeteilt (Zugehörigkeit zum VPN, Label, …)
- Die Adressen werden mit einem Route Distinguisher (RD) versehen, um sie von Adressen anderer VPN unterscheiden zu können (Möglichkeit überlappender Adressräume).

MPLS-VPN – Grundlagen (2)

- Zusätzlich werden die Adressen mit einem Label versehen (Übertragung über Label Attribute in BGP), damit der Egress LSR bei der Datenübertragung die Adressen dem richtigen VPN zuordnen kann
- Es existieren somit **zwei Label**
  - das äußere Label wird über LDP verteilt und kennzeichnet den Weg zum Egress LSR (PE-Router)
  - das innere Label wird über MP-IBGP zwischen den Edge Routern verteilt und kennzeichnet das richtige Interface, über welches das IP Paket weitergeleitet werden muss
- Community Attribut von BGP beinhaltet Route Target zur Kennzeichnung des VPN. Ein PE Router kann so die Routen in den jeweiligen VRF Routing Table übernehmen
- Auswertung des **äußeren Label** bei der Datenübertragung durch die **Router** im Backbone ohne Berücksichtigung des inneren Labels
- Auswertung des **inneren Label** bei der Datenübertragung durch die **PE Router** zur Identifizierung des richtigen VPN (Router Interface)

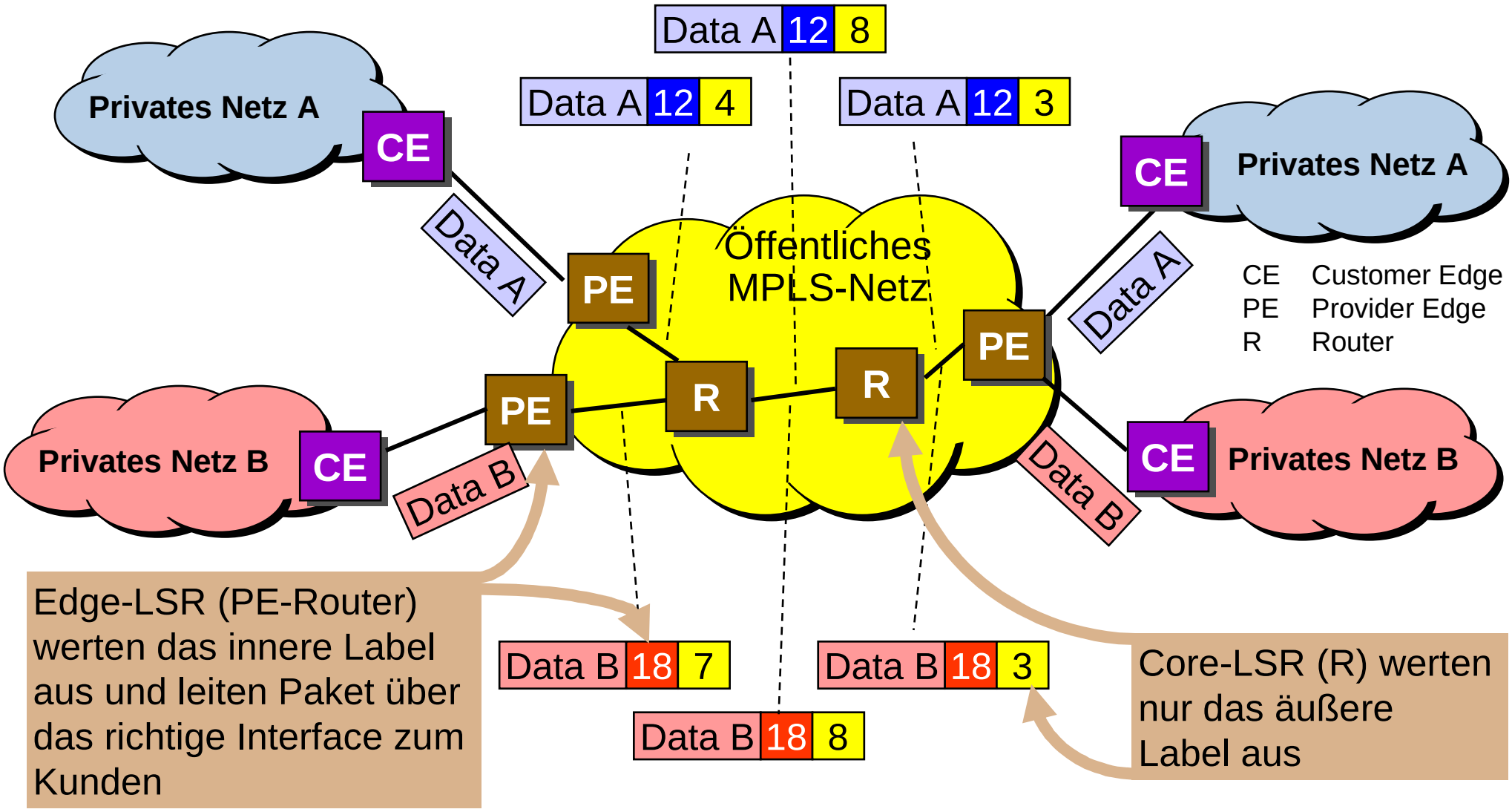
MPLS-VPN – Realisierung (1)



Austausch der Zielinformationen über MP-IBGP Verteilung des inneren Label zur Kennzeichnung des VPN Interface

CE	Customer Edge
PE	Provider Edge
R	Router
VFR	Virtual Routing and Forwarding

MPLS-VPN – Realisierung (2)



Inhalt

- Qualität in IP-Netzen
- Multi-Protocol Label Switching (MPLS)
  - MPLS - Prinzipen
  - MPLS - Label
  - MPLS - Steuerprotokolle
  - ATM und MPLS
  - Einsatz vom MPLS
  - Weiterentwicklungen
- Virtual Private Networks (VPN)
- Generic Framing Procedure (GFP)

Warum eine neue Rahmenstruktur

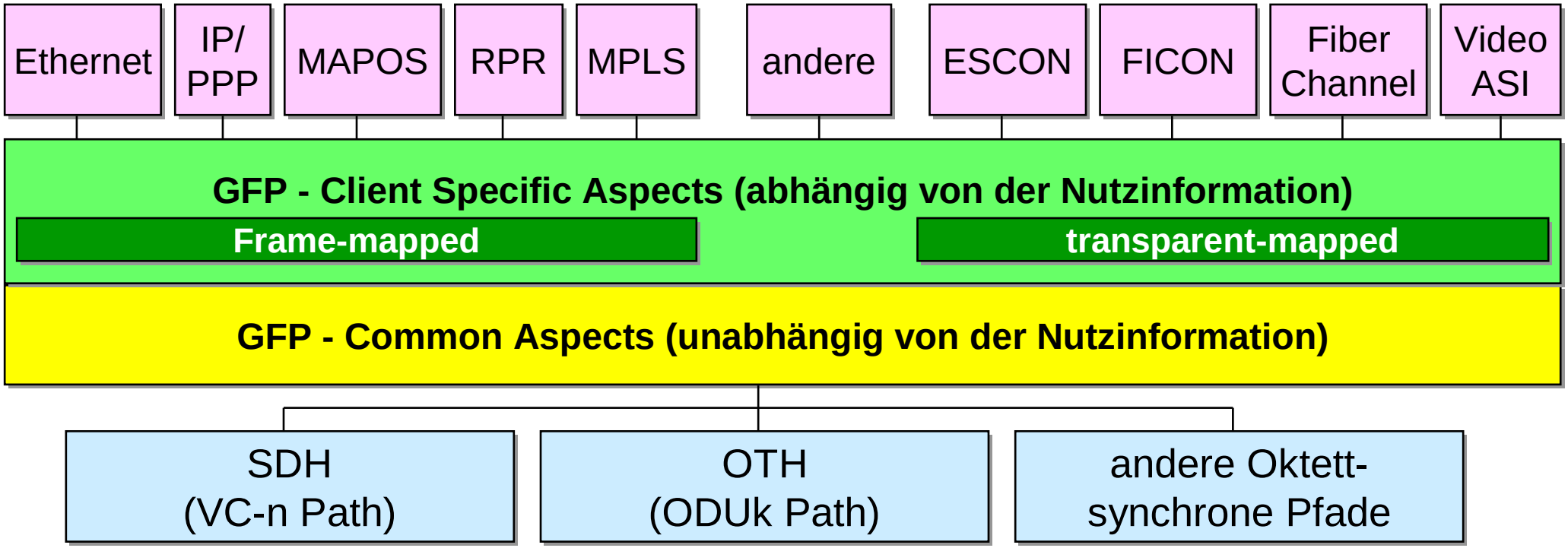
- Traditionell wird **HDLC** als Rahmenstruktur verwendet. Die Probleme sind:
  - unnötiger Overhead („Address“ und „Protocol“ sind unnötige Felder)
  - unvorhersehbare Längenänderung des Rahmens durch Stuffing
- **ATM** stellt eine Alternative dar, aber auch hier Probleme:
  - feste Länge nicht gewünscht (nicht zeitgemäß)
  - unnötige Felder (für reine Rahmenbildung)
- Schließlich bleibt noch der **Ethernet-MAC-Rahmen**. Probleme:
  - im Punkt-zu-Punkt-Betrieb nicht notwendige Adresse (MAC-Adresse).
  - „Präambel“ nicht ideal für den Transport über eine Oktett-strukturierte Übertragungstechnik.

Generic Framing Procedure (GFP) als Alternative

- Als Alternative wurde die **Generic Framing Procedure** (GFP) entwickelt (ITU-T Rec. G.7041):
  - variable Rahmen-Größe
  - Minimaler Basis-Overhead (4 Byte)
  - „Self-Delineating“ (wie bei ATM)
  - kein Stuffing (= keine Änderung der Rahmenlänge)
  - „Leer-Rahmen“ als Lückenfüller (wie bei ATM)

GFP – Architektur

- Aufteilung des Protokolls in:
  - GFP - Common Aspects (generischen Anteil)
  - GFP - Client-specific Aspects (Nutzlast-spezifisch)



GFP – Common Aspects

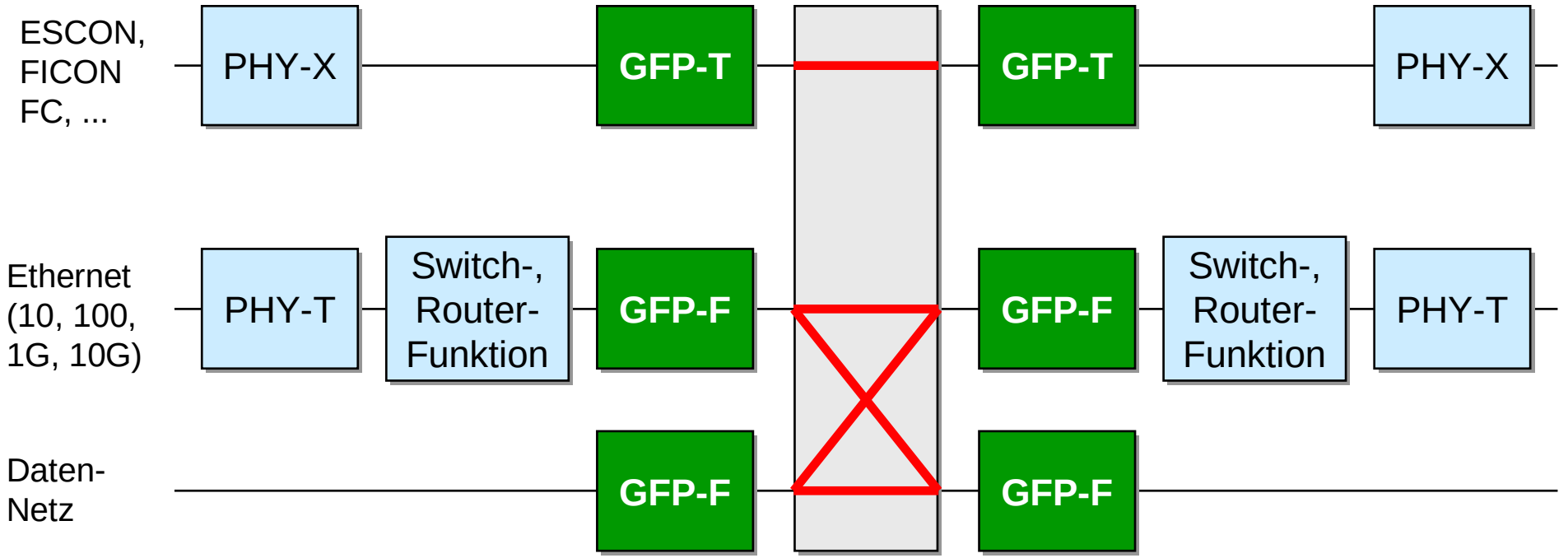
Die GFP Common Aspects gelten für alle GFP-Lösungen und umfassen folgende Funktionen:

- **PDU-Delineation** (Erkennen der Rahmengrenzen),
- **Leer-Rahmen** zum Aufstopfen von Lücken im Datenstrom,
- **Synchronisation**,
- **Scrambling** (Verwürfeln des Signals, sorgt für genügend Signalwechsel und annähernd konstante Leistungsdichte),
- **Multiplexing**.

GFP – Client-specific Aspects (1)

Zwei Typen „Client-specific Aspects“:

- Frame-mapped GFP (GFP-F) für Paket-orientierte Daten
- Transparent-mapped GFP (GFP-T) für Block-codierte Datenströme

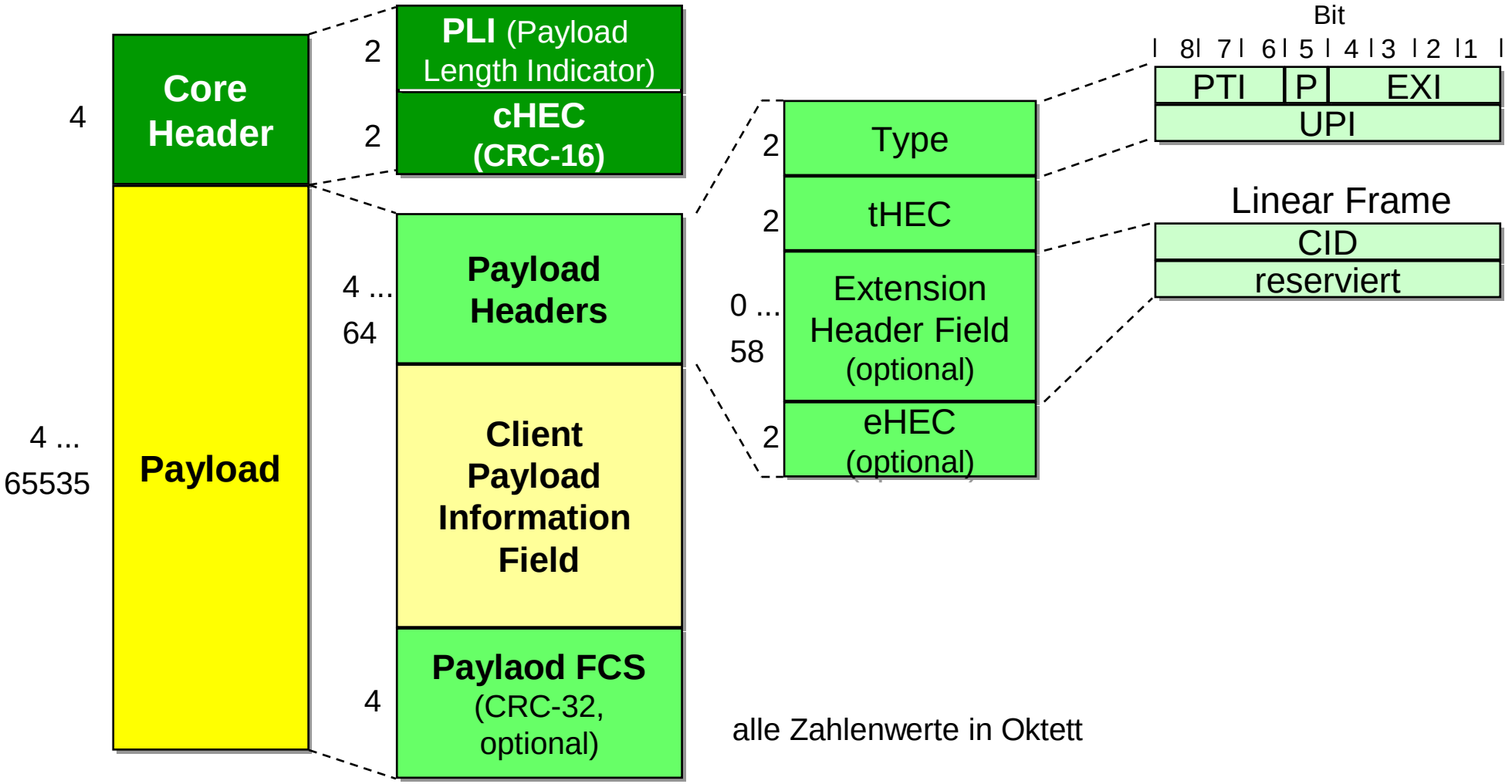


GFP – Client-specific Aspects (2)

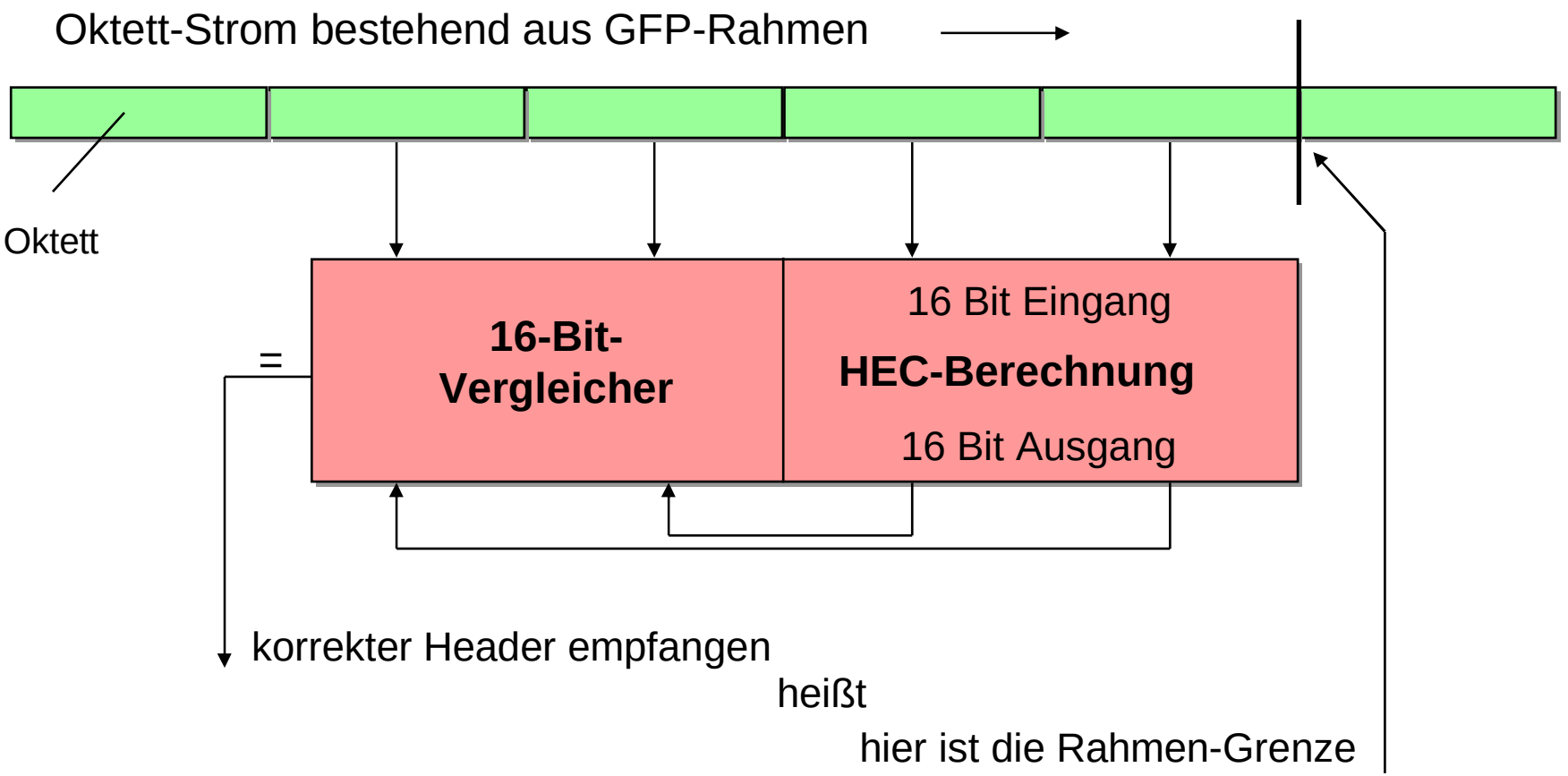
- Frame-mapped GFP:
  - Transport von Datenrahmen der bekannten Schicht-2-Protokolle wie PPP, IP, MPLS, Ethernet usw.
  - Ressource Management auf der Daten-Seite angenommen.
- Transparent GFP:
  - Einsatz unter zeitkritischen Bedingungen
  - Einsatz bei Kanal-codierten Signalen (z.B. bei Storage Area Networks (SAN) und Video-Signale (DVB-ASI).

Parameter	**Frame-mapped GFP**	**Transparent-mapped GFP**
Länge	variabel	fest
Konfiguration	Punkt-zu-Punkt, Multipunkt, Ring	nur Punkt-zuPunkt
Mapping	Paket- oder Rahmenstrukturierte Daten, 1-zu-1 in GFP-Rahmen	kontinuierlicher Datenstrom, 8B/10B-codiert
Höhere Schichten	müssen bekannt sein, um die eigent-lichen Daten zu extrahieren	müssen nicht bekannt sein, Datenstrom wird transparent transportiert

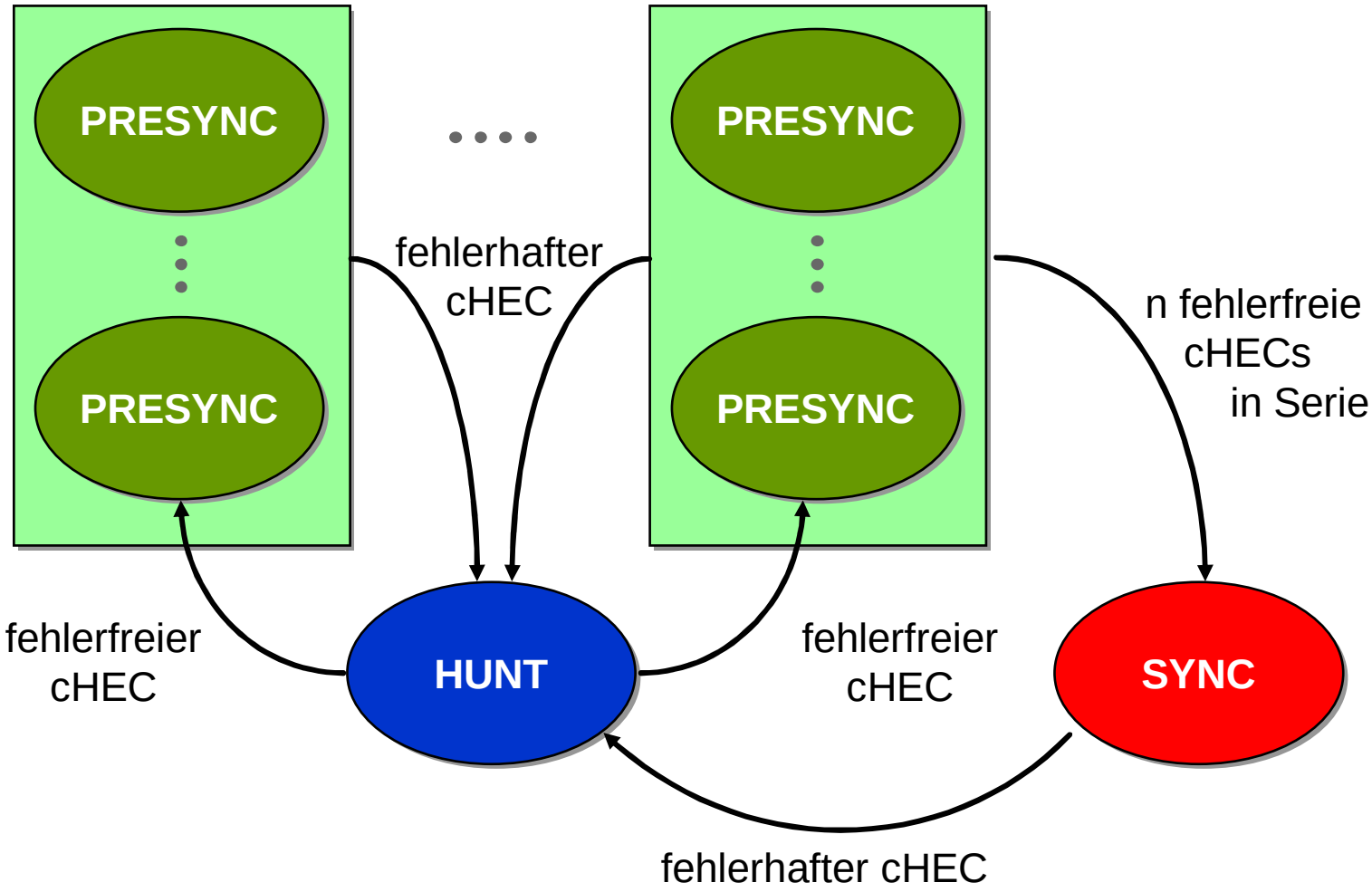
GFP – Rahmenstruktur



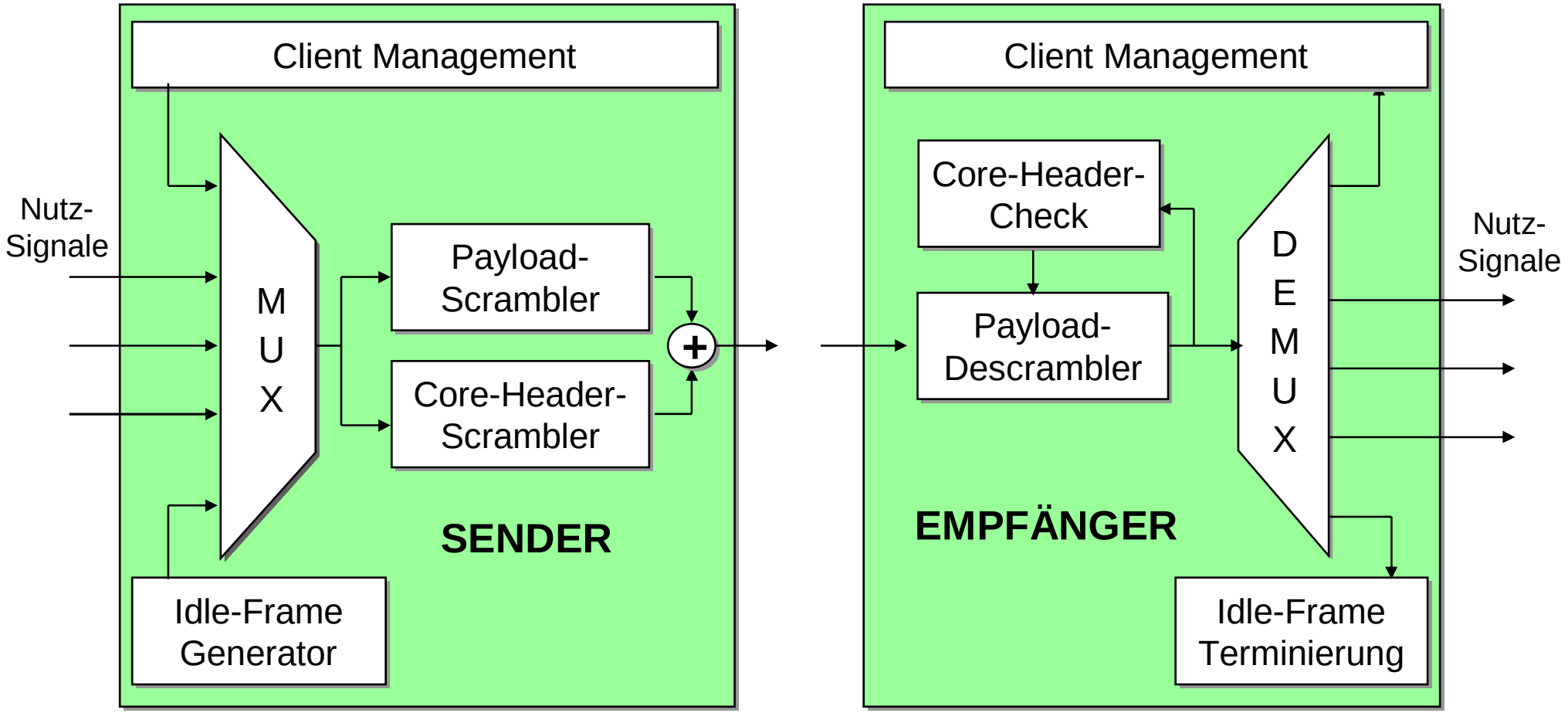
GFP – Prinzip der Rahmenerkennung



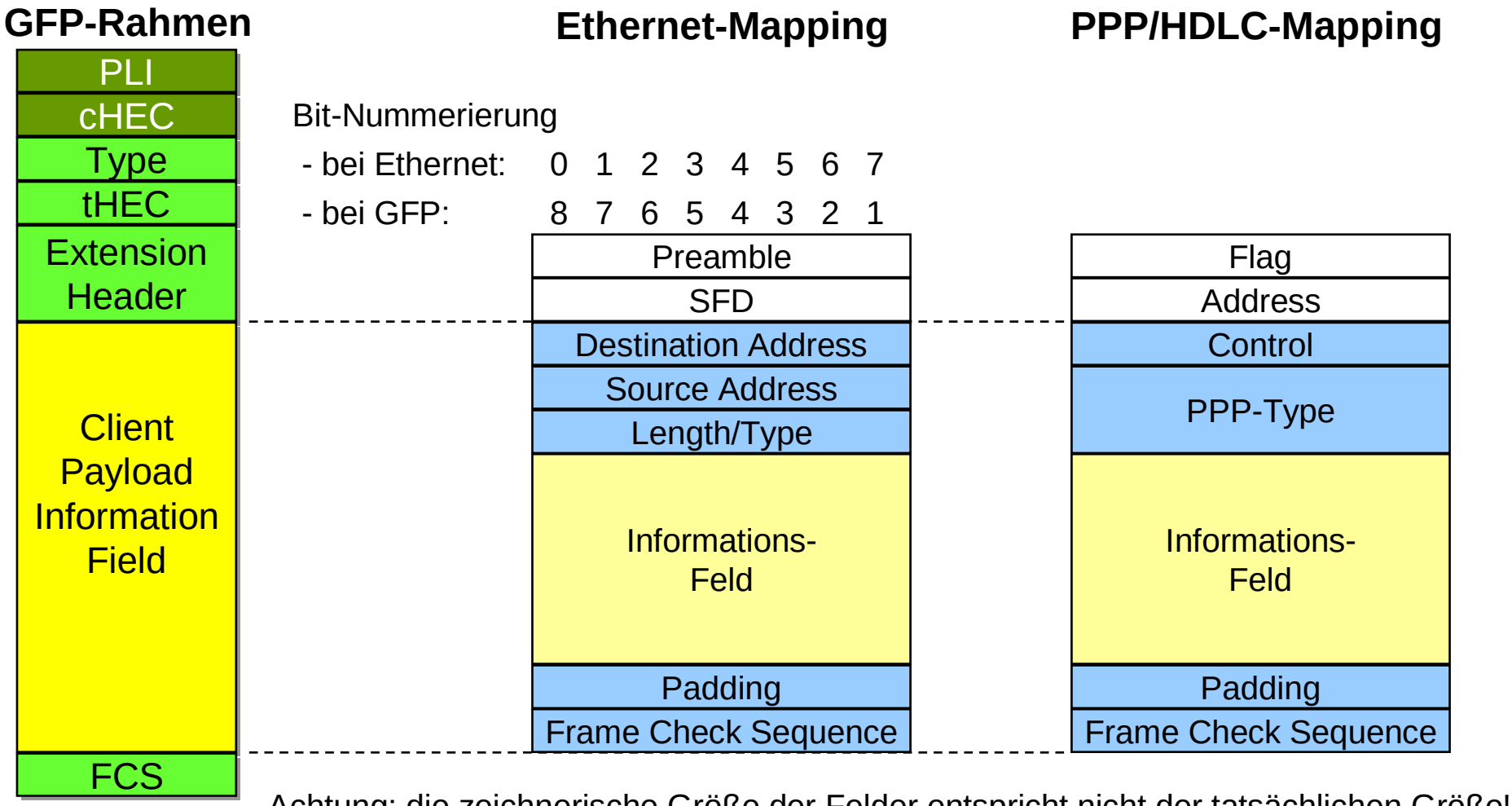
GFP – Status-Diagramm der Rahmenerkennung



GFP – Multiplexing



GFP-Mapping – Frame-mapped



Achtung: die zeichnerische Größe der Felder entspricht nicht der tatsächlichen Größe!

Ausblick

- Die Daten-Welt kritisiert SDH als zu unflexibel.
- Das effiziente GFP zusammen mit dem SDH und seinen Erweiterungen
  - „Virtual Concatenation, die eine feinere Granularität des Containers erlaubt, sowie
  - „Link Control Adjustment Scheme“, das eine Zeichengabe-Steuerung der Virtual Concatenation erlaubt,

  sind die Antwort auf diese Kritik.
- Produkte sind am Markt verfügbar.
- Es ist noch zu früh, um eine Bewertung über die Akzeptanz von GFP abzugeben - aus der Vergangenheit wissen wir, dass nicht alles was technisch sinnvoll ist auch einen Markterfolg hat. GFP wäre es aber zu wünschen.

ENDE

Vielen Dank für Ihre Aufmerksamkeit!

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