Integrierte IT-Service-Management-Lösungen anhand von Fallstudien

„Virtuelle Private Netze“
Teil 2

Dr. Michael Nerb et al.,
Prof. Dr. Heinz-Gerd Hegering
SoSe 2008

Virtuelle Private Netze – Wiederholung
Charakteristika

- Virtual:
  - Eine „logische“ Struktur
  - Statisch oder dynamisch
  - Unterschiedliche Technologien und Techniken zur Virtualisierung
- Private:
  - Beschränkter Zugang und Zugriff, „Closed User Groups“
  - Mandantenfähigkeit
  - Sicherstellung von Authentifizierung, Integrität, Vertraulichkeit
- Network:
  - Strukturen auf Basis einer „gesharten“ Infrastruktur
  - Tunneling oder Tagging
  - Transparent oder „Nicht-Transparent“ für Benutzer

Virtuelle Private Netze

Inhalte dieses Teils (verteilt auf zwei Termine)

- Inhalte des letzten Termins (08.05.08):
  - Virtuelle Private Netze
    - Beispiel, Begriffsdefinition eines VPN‘s
    - Charakteristika, Anforderungen und Klassifikation von VPN‘s
  - Layer-2, Layer-3 und Layer-4-7 Technologien für VPN‘s
- Inhalte dieses Termins: VPN‘s in Weitverkehrnetzen
  - Motivation und Konzepte zu MPLS
  - Packet Forwarding und Label Distribution
  - MPLS basierende VPN‘s:
    - Beispiele und Routing
    - Packet Forwarding
  - QoS in MPLS-Netzen:
    - IntServ
    - Diffserv

VPN‘s in Weitverkehrsnetzen
Historie

- Beispiel ATM (nur *sehr* kurz skizziert):
  - „Leitungs/Zellvermittlung“ mit reservierten Ressourcen (QoS)
  - „Routingentscheidung“ einmal pro Verbindung („verbindungsorientiert“)
  - „Virtuelle Pfade“ und „Virtuelle Kanäle“, Switching von Zellen
  - Eines (von vielen) ATM-Problemen: Als Layer 2 für IP zu komplex
- IP Netze (ebenfalls nur *sehr* kurz skizziert):
  - „Paketvermittlung“ mit „Best Effort“, keine QoS
  - Routingentscheidung für jedes Datenpaket („verbindungslos“)
  - Zwei (von vielen) Problemen:
    - Routing problematisch bei hohen Datenraten (> 2.5 Gbit/s)
    - QoS-Garantien für IP schwierig ohne „Verbindungskonzept“
- Idee: Nutze Vorteile beider Ansätze!
  - Umgehe das zeitaufwändige IP Routing wo immer möglich
  - „Switch what you can, route what you must“

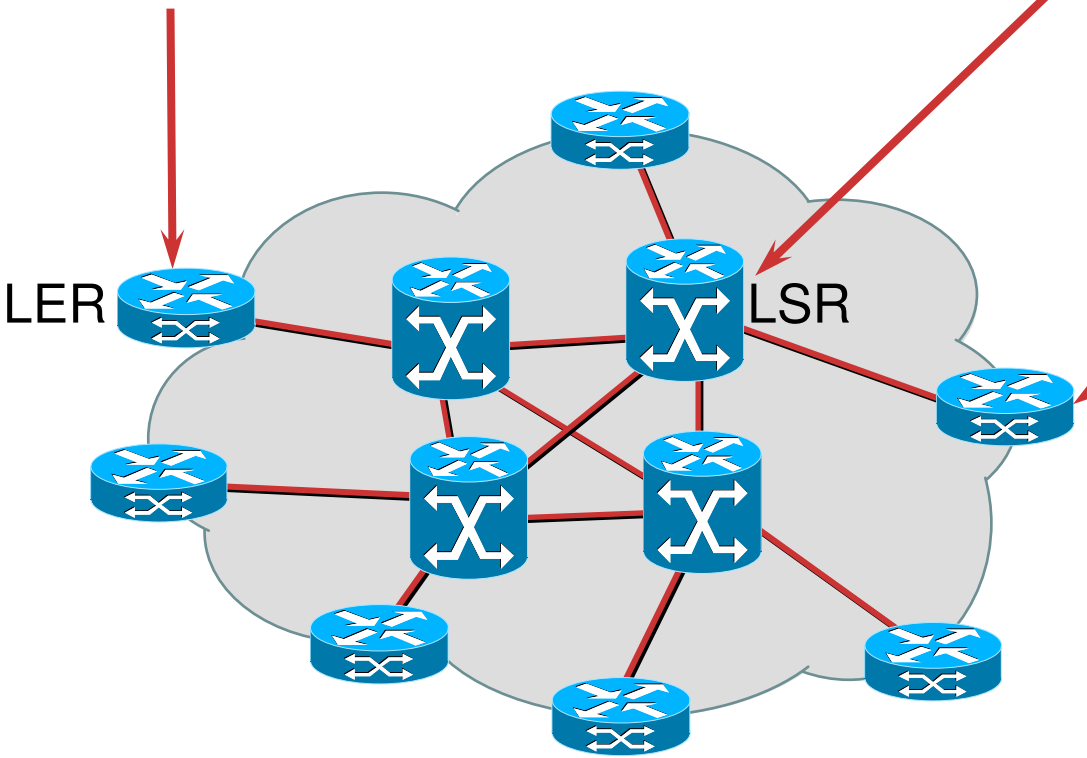
VPN‘s in Weitverkehrsnetzen
MPLS Motivation

- Entstanden aus mehreren „Switching-Technologien“, u.a.
  - MPOA (Multi Protocol over ATM): ATM Forum
  - IP Switching (datenstromorientiertes IP-Switching): U.a. Ipsilon
  - Tag Switching (topologieorientiertes IP-Switching): U.a. Cisco
- Bündelung und Harmonisierung dieser Ansätze durch die IETF
  - MPLS: „Multi-Protocol Label Switching“ (RFC 3031ff)
  - MPLS basiert auf verbindungsorientiertem „Schicht-2-Protokoll“ ähnlich ATM VCs
  - Besser angepasst auf IP als z.B. ATM
  - Nutzung vorhandener ATM-Hardware für Switching
  - Gängige Routingmechanismen (d.h. IP-Routing-Protokolle) bleiben erhalten (bzw. werden weiterhin benötigt)

- Gute Eignung für VPN‘s und QoS

MPLS
Konzept – Überblick

1) Am Netzzugang (d.h. am “LER”):
- Pakete klassifizieren in FEC (“einer virt. Verbindung zuordnen”)
- Label anfügen

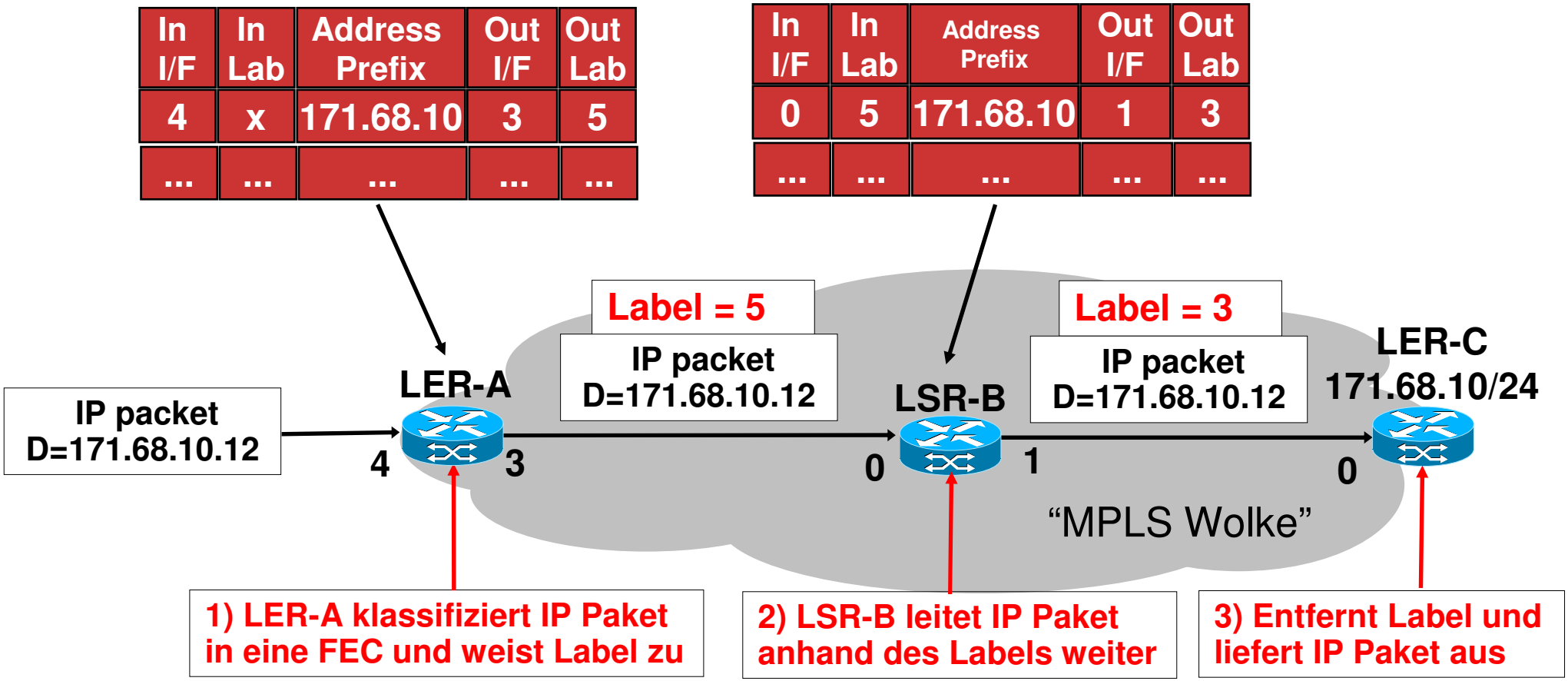


2) Im MPLS Netz (d.h. beim “LSR”):
- Keine Analyse der IP Pakete
- Weiterleiten anhand des Labels, nicht anhand der IP-Adresse
- Statt dessen: “Label Swapping” d.h. Austausch des Labels

3) Am Netzausgang (beim LER):
- Label entfernen
- Ausliefern an den Empfänger anhand IP Routingtabelle

FEC: Forwarding Equivalence Class (“haben das gleiche Label”)
LER: Label Edge Router
LSR: Label Switch Router

MPLS
Konzept – Paket Forwarding (vereinfacht)



MPLS
Konzept – Label Distribution Protocol (LDP)

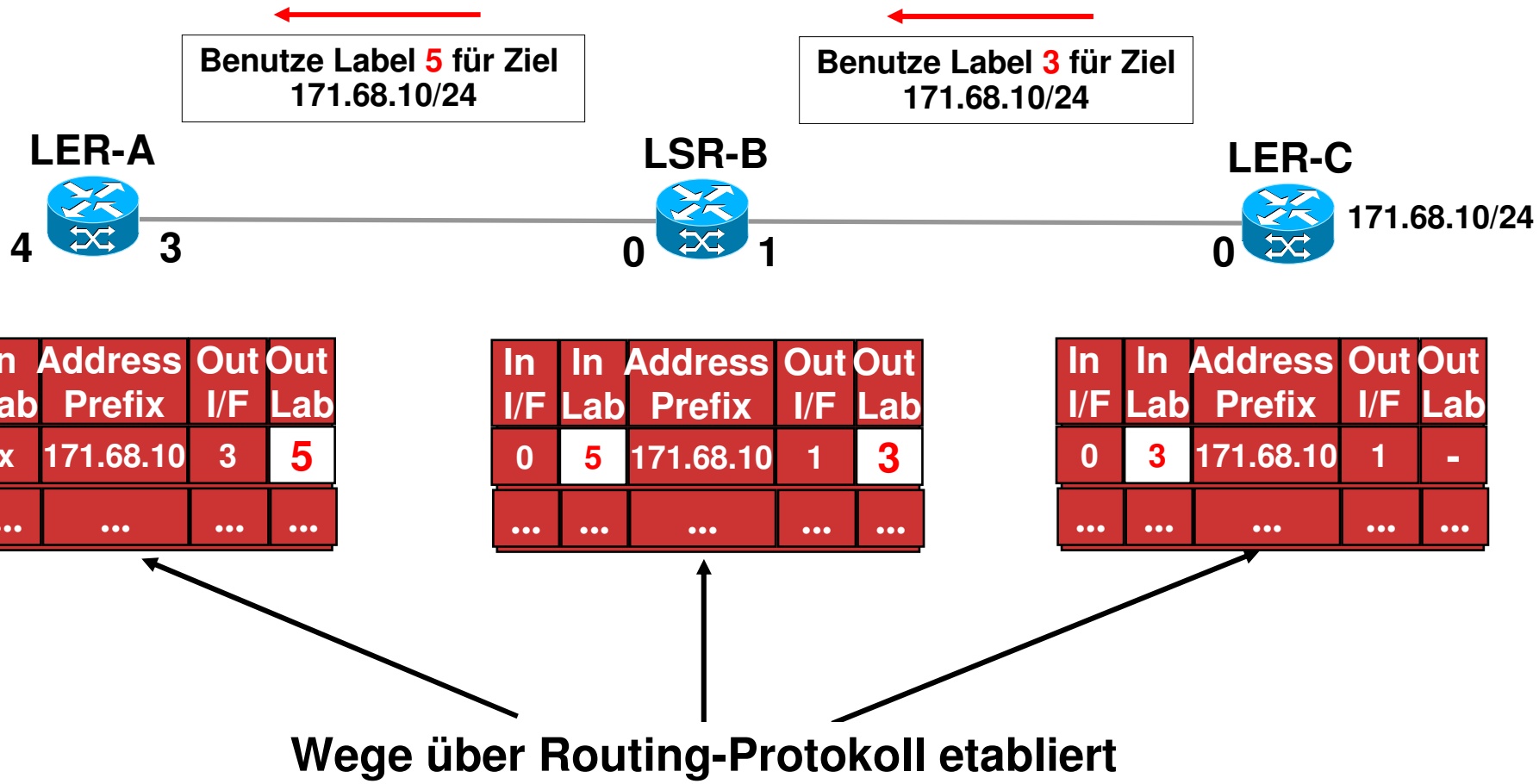
- Woher weiß der LER/LSR, welches Out-I/F und welches Out-Label er verwenden soll?

- Out-I/F: MPLS Router kennen ihre Nachbarn durch Routing-Protokolle:
  - Erreichbarkeit von IP-Netzen über Routing Protokolle
  - Kenntnis, welche IP-Netze über welche Out-I/F geroutet werden

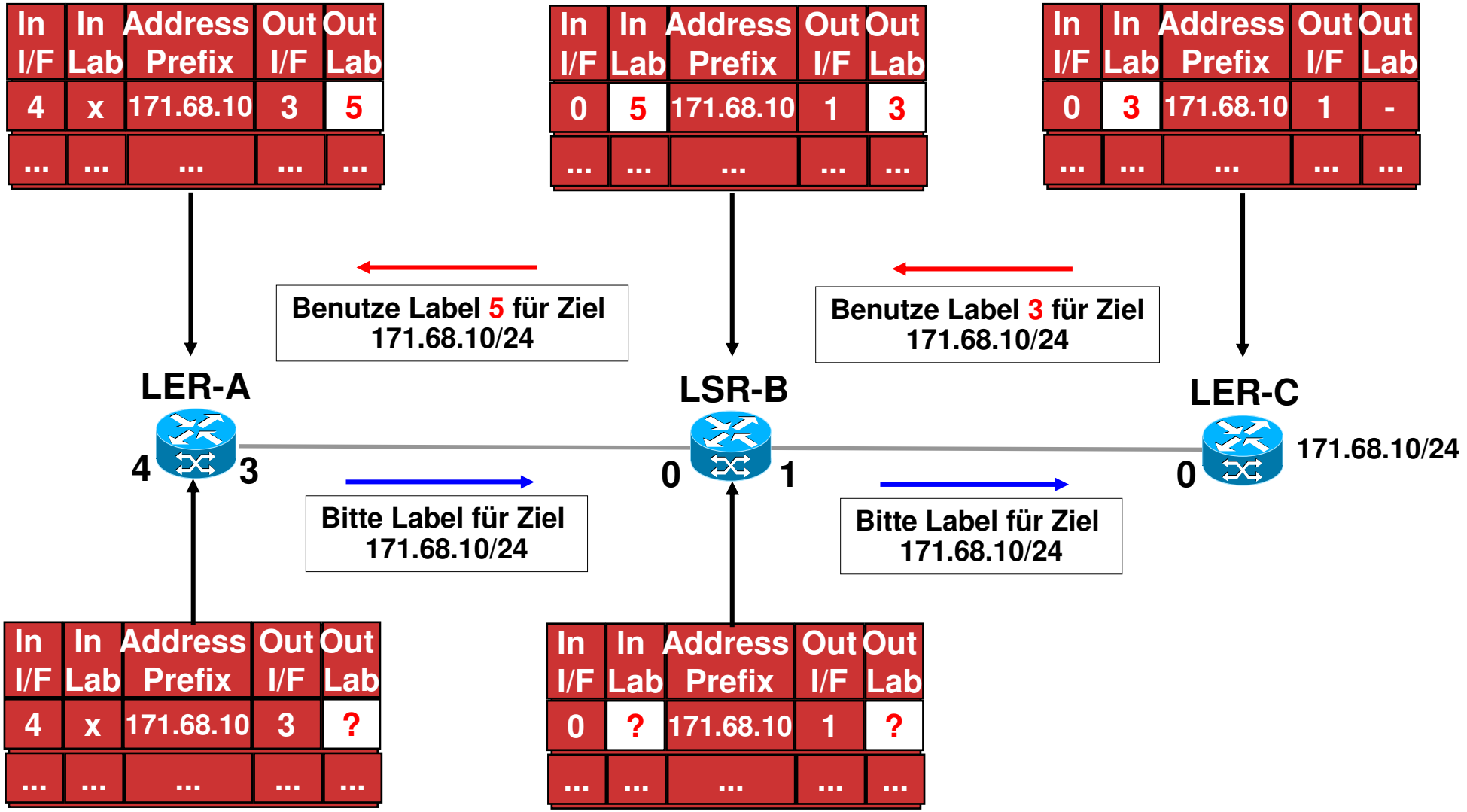
- Out-Label: MPLS Router erfragen dies vom „Downstream LSR“ via LDP:
  - Verteilung der Labels also ausgehend von Senke des IP-Stroms
  - Labels sind nur für „Teilstrecken“ gültig (d.h. nicht eindeutig im Netz)
  - 2 Varianten: „Unsolicited Downstream” oder “Downstream on demand”

In I/F	In Lab	Address Prefix	Out I/F	Out Lab
4	x	171.68.10	3	5
...	...	...	...	...

MPLS
Details – Unsolicited Downstream

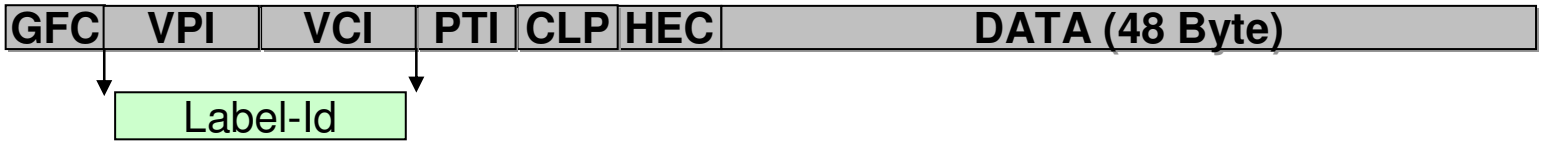


MPLS
Details – Downstream on Demand

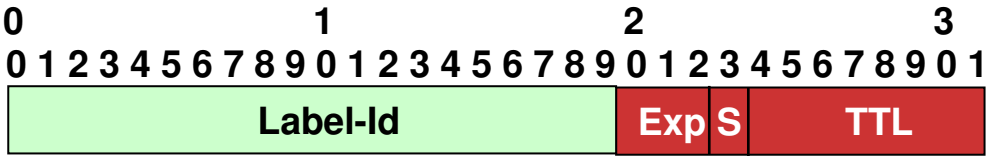


MPLS
Struktur und Einbettung der MPLS Labels

- Grundlage: (Format von) ATM-Zellen (5 Byte Header, 48 Byte Data)

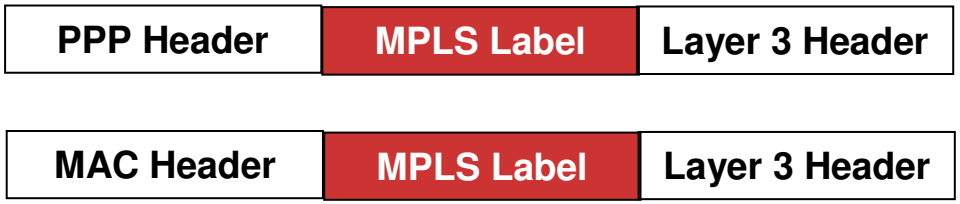


- Ergänzung um zusätzliche Informationen (insg. 4 Byte, 32 bit):



Label-Id:	20 bits
Exp:	Experimental, 3 bits
S:	Bottom of stack, 1bit
TTL:	Time to live, 8 bits

- Einbettung des MPLS Labels „zwischen Schicht 2 und 3“, z.B.:

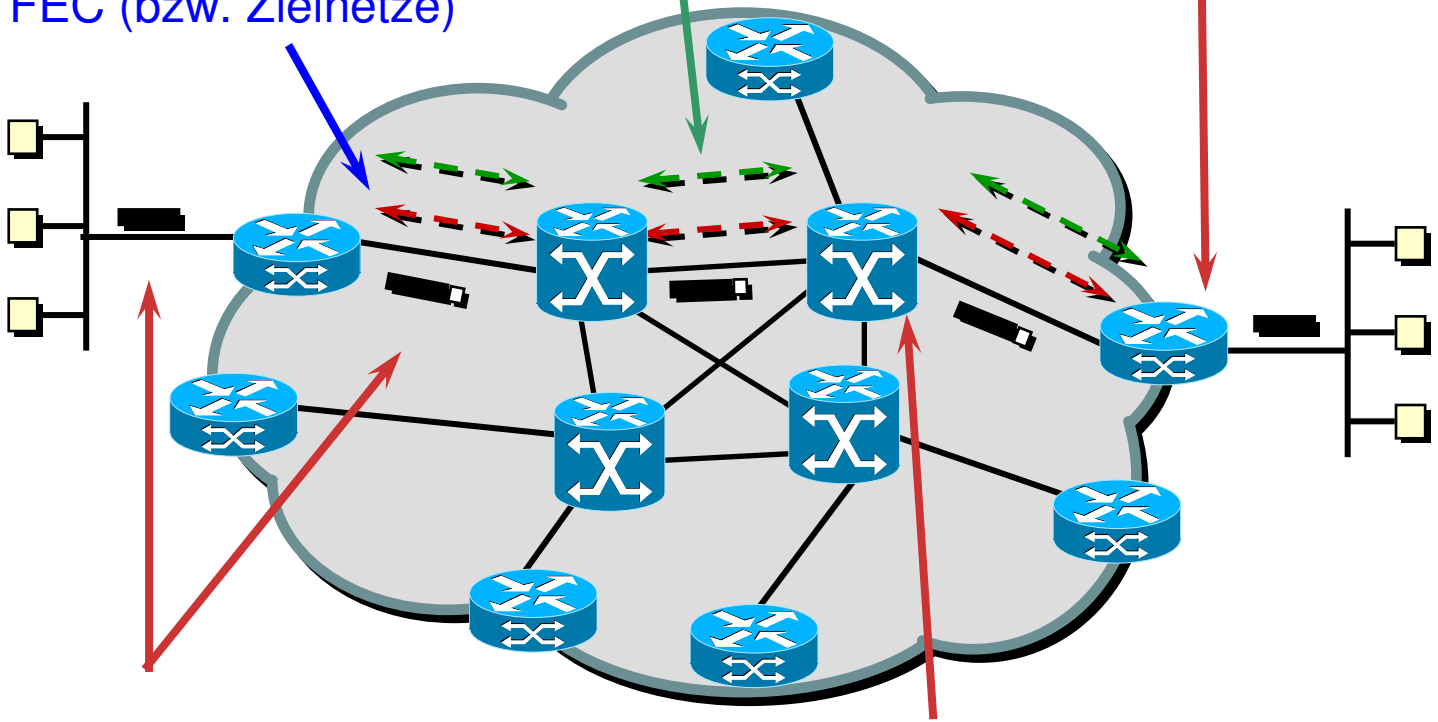


MPLS
Zusammenfassung

0a. Routing Protokolle (z.B. OSPF, IS-IS) stellen Routing zu den Zielnetzen sicher

0b. LDP verwaltet und verteilt Labels für FEC (bzw. Zielnetze)

3. LER erhält Paket, entfernt das Label und liefert Paket aus



1. LER erhält Paket, klassifiziert und "labelt" das Paket (falls erforderlich unter Nutzung von LDP)

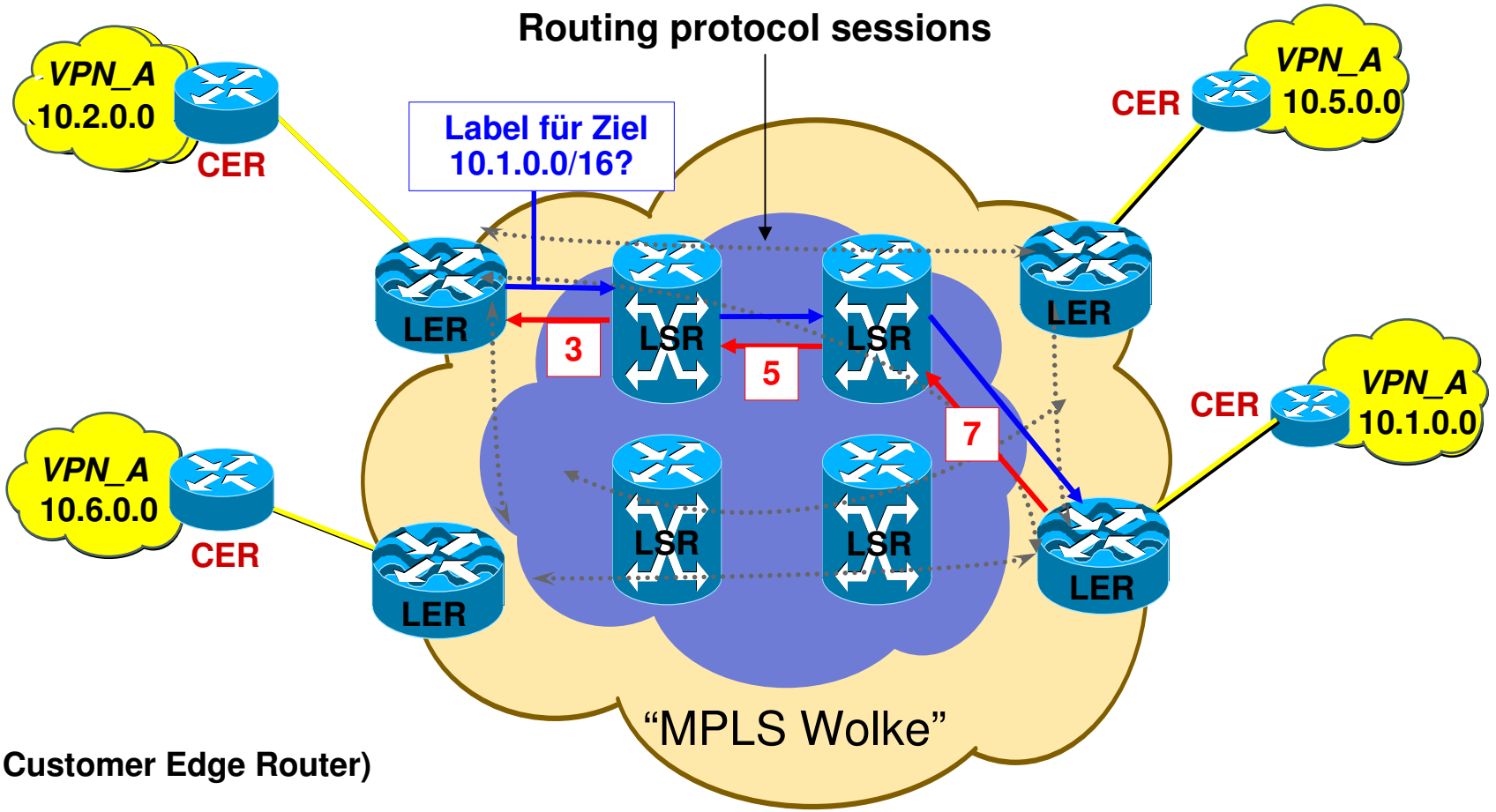
2. LSR leiten IP Pakete anhand der Labels durchs Netz (und tauschen dabei die Labels aus)

VPN‘s auf Basis von MPLS
Anforderungen und Charakteristika

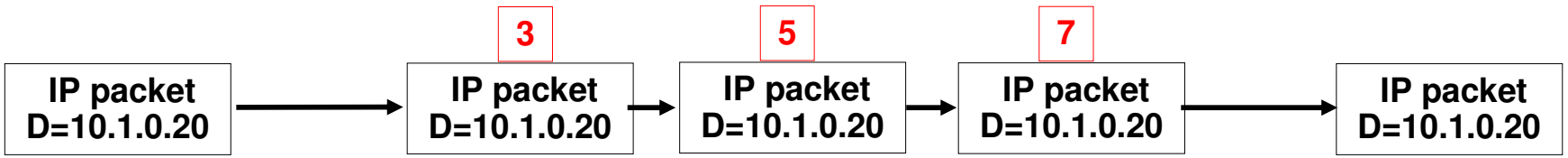
- siehe auch Vorlesung vom 08.05.08
- IP VPNs verwenden (pro Kunden !!!):
  - spezifische Adressierungsschemata
  - spezifische Routing-Policies
  - Ggf. überlappende IP-Netze
- Um IP-Pakete verschiedener VPNs (d.h. verschiedener Kunden) zu transportieren, muss ein MPLS-Netz folgendes sicherstellen:
  - Routing von IP-Adressen verschiedener VPNs
  - Eindeutigkeit von IP-Adressen über verschiedene VPNs
  - Unterstützung verschiedener Routingprotokolle

- Sicherstellung/Durchsetzung über MPLS Labels!

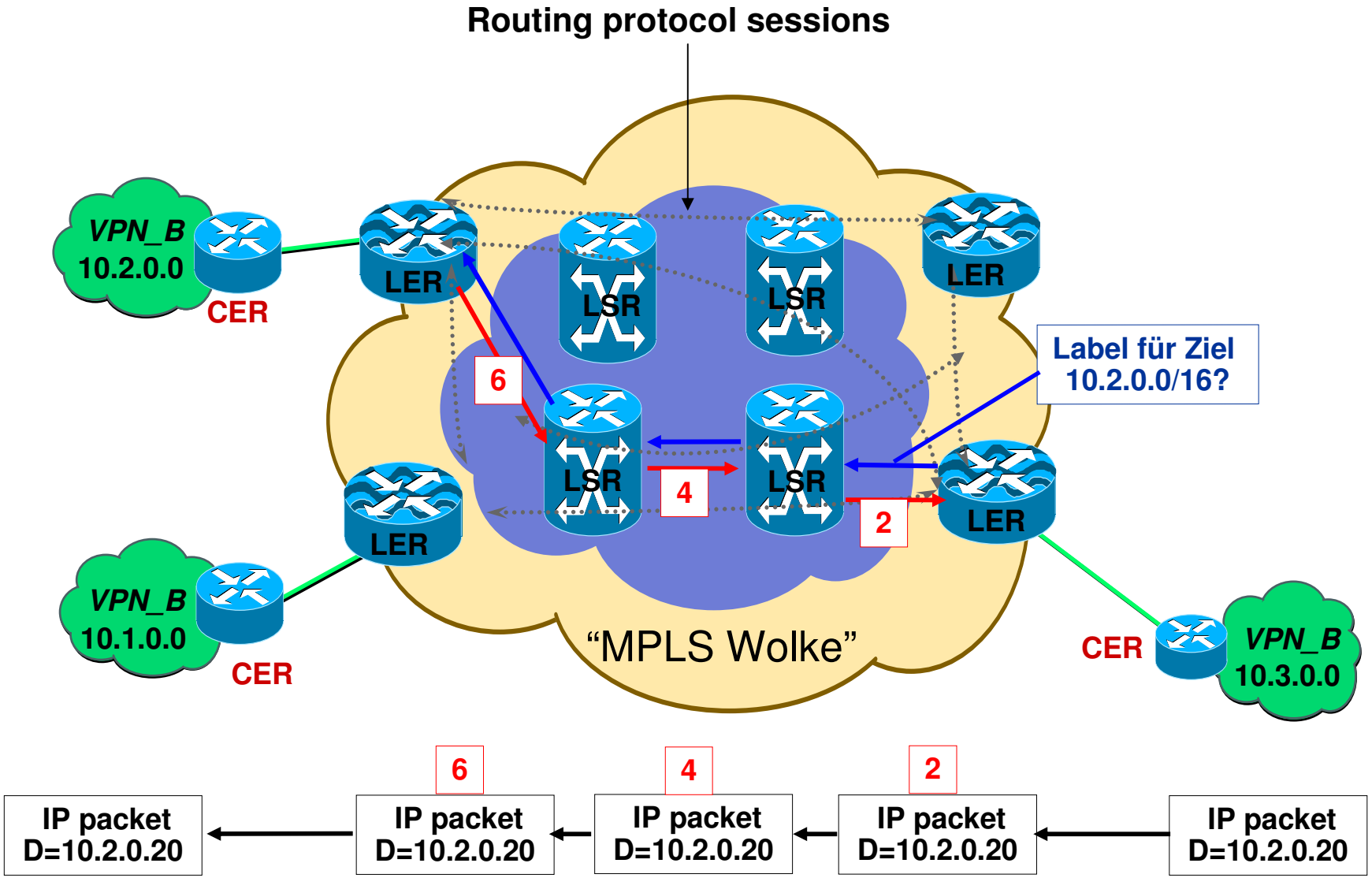
MPLS-basierte IP-VPN‘s
Routing/Packet Forwarding für Kunden A



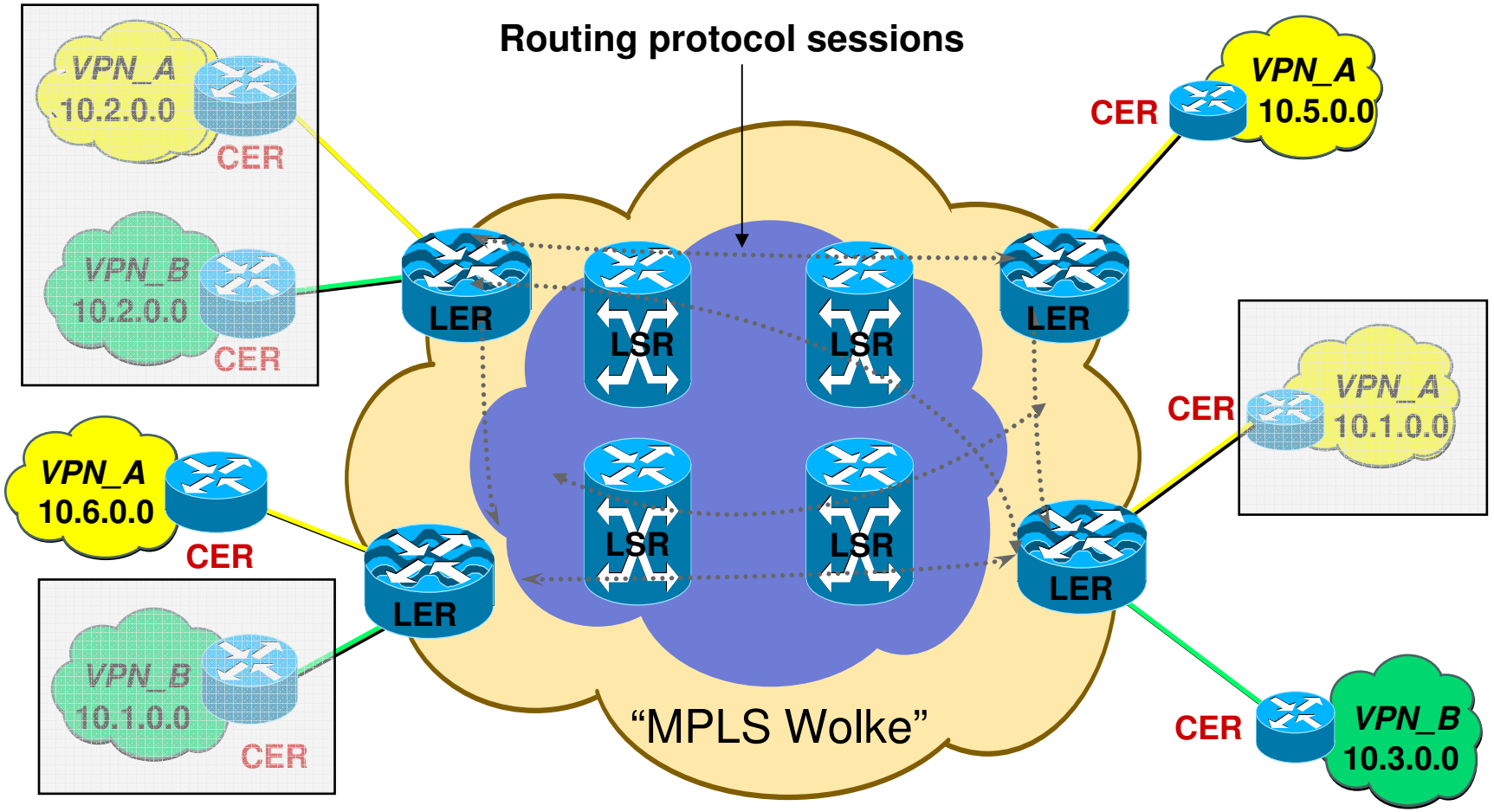
(CER: Customer Edge Router)



MPLS-basierte IP-VPN‘s
Routing/Packet Forwarding für Kunden B

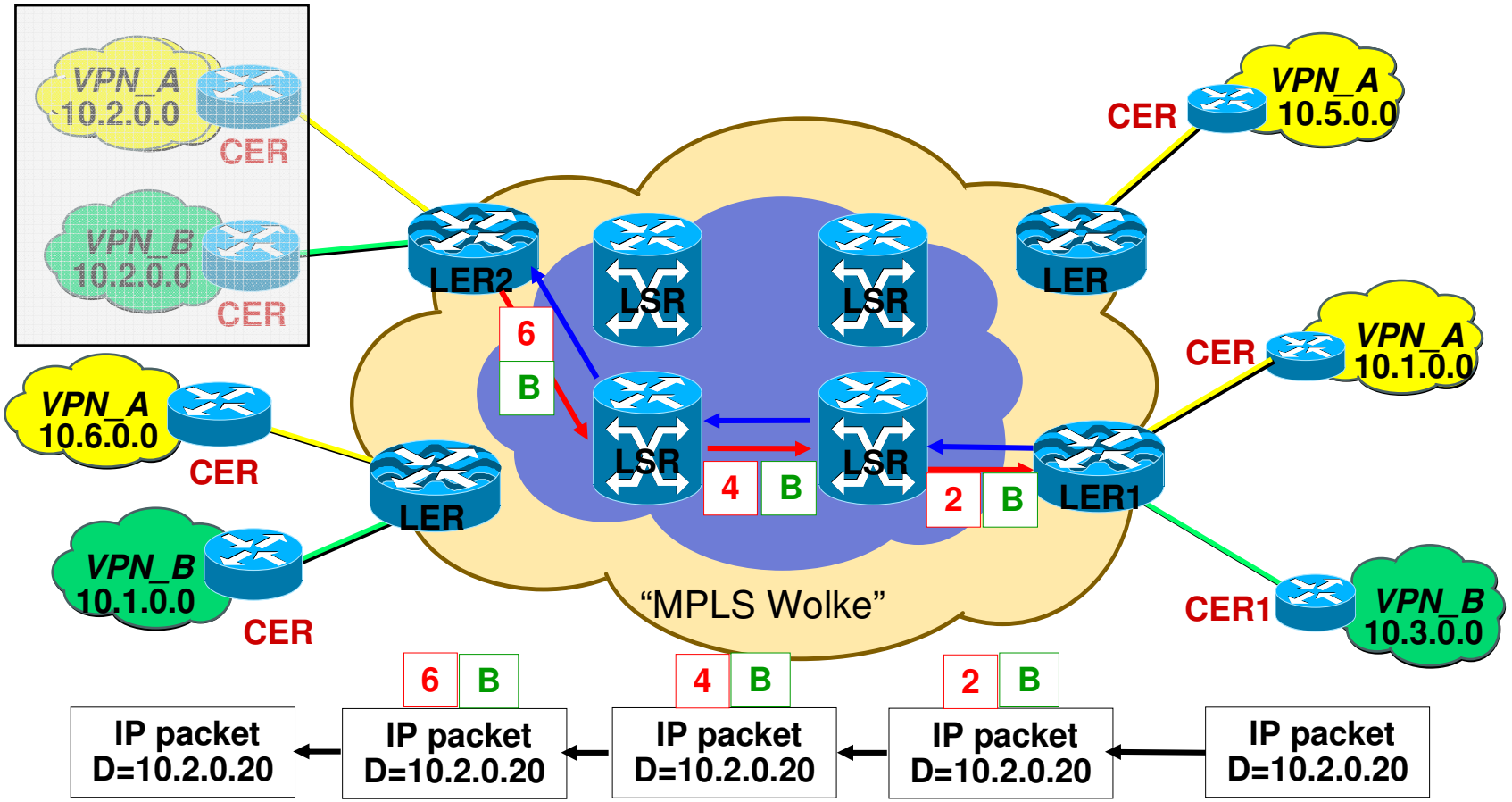


MPLS-basierte IP-VPN‘s
Beispielszenario mit Kunden A und B



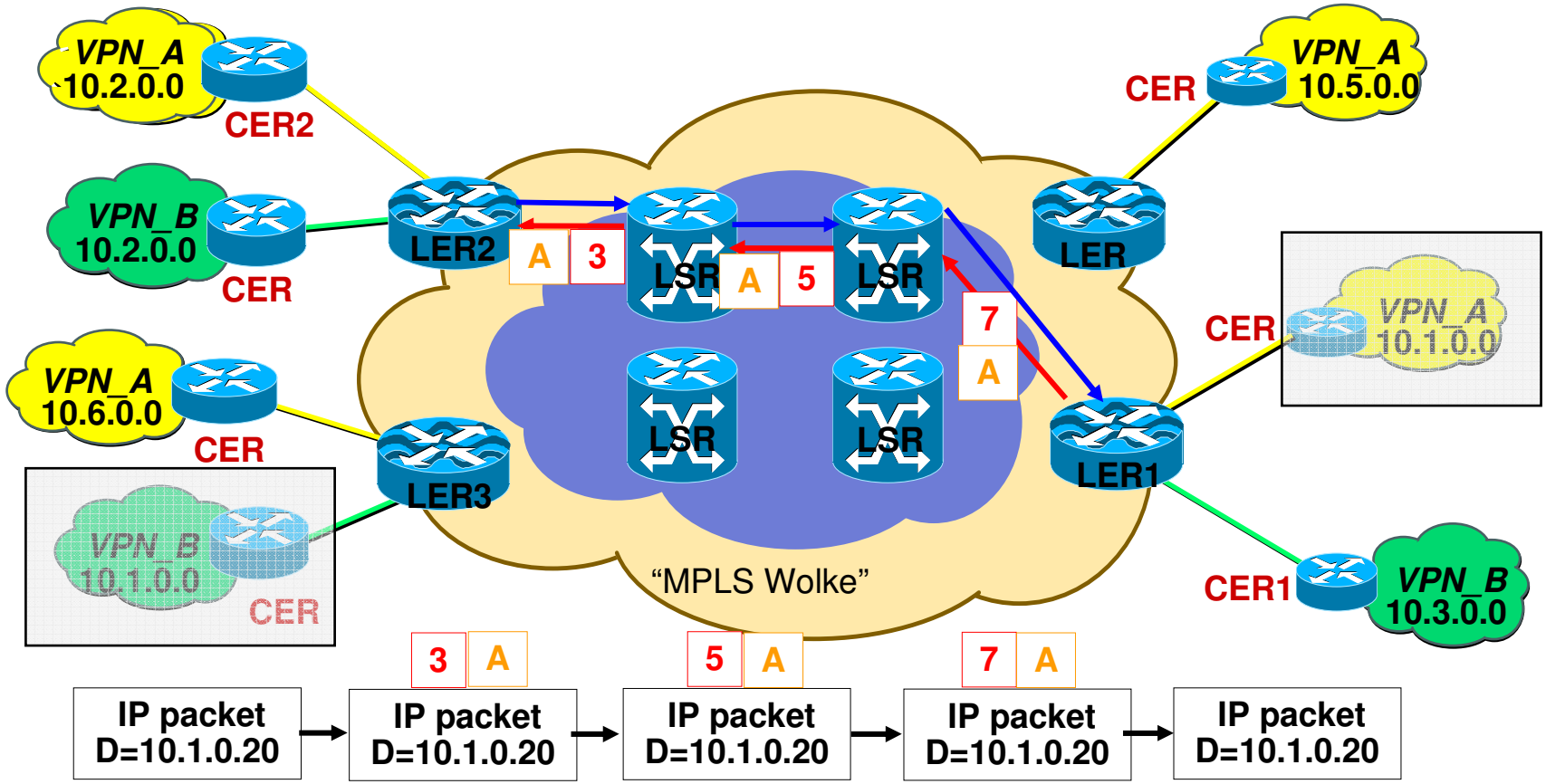
- Problem: Überlappende IP Adressbereiche für VPN_A und VPN_B
  - 10.2.0.0/16 am selben LER
  - 10.1.0.0/16 an verschiedenen LER‘s

MPLS-basierte IP-VPN‘s
Routing/Packet Forwarding für VPN_B



- LER1 erhält IP-Paket vom CER1 und fügt zwei Label an:
  - Interior Label: liefert Routing-Entscheidung (wechselt auf dem Weg)
  - Exterior Label: liefert VPN-Entscheidung (Kundenidentifikator)

MPLS-basierte IP-VPN‘s
Routing/Packet Forwarding für VPN_A



- LER2 erhält IP-Paket vom CER2 und fügt zwei Label an:
  - Interior Label: liefert Routing-Entscheidung (wechselt auf dem Weg)
  - Exterior Label: liefert VPN-Entscheidung (Kundenidentifikator)

Quality of Service (QoS) in MPLS-VPN's
Anforderungen und Charakteristika

- Anwendungen haben unterschiedliche Anforderungen an QoS, z.B.
  - Laufzeiten
  - Durchsatz
  - Verlustraten

- Ziel:
  - MPLS-Netz versorgt Anwendungen mit dem jeweils passenden, und/oder gewünschten QoS

- Zwei wichtige Modelle für Realisierung:
  - Integrated Services Model (Intserv)
  - Differentiated Services Model (DiffServ)

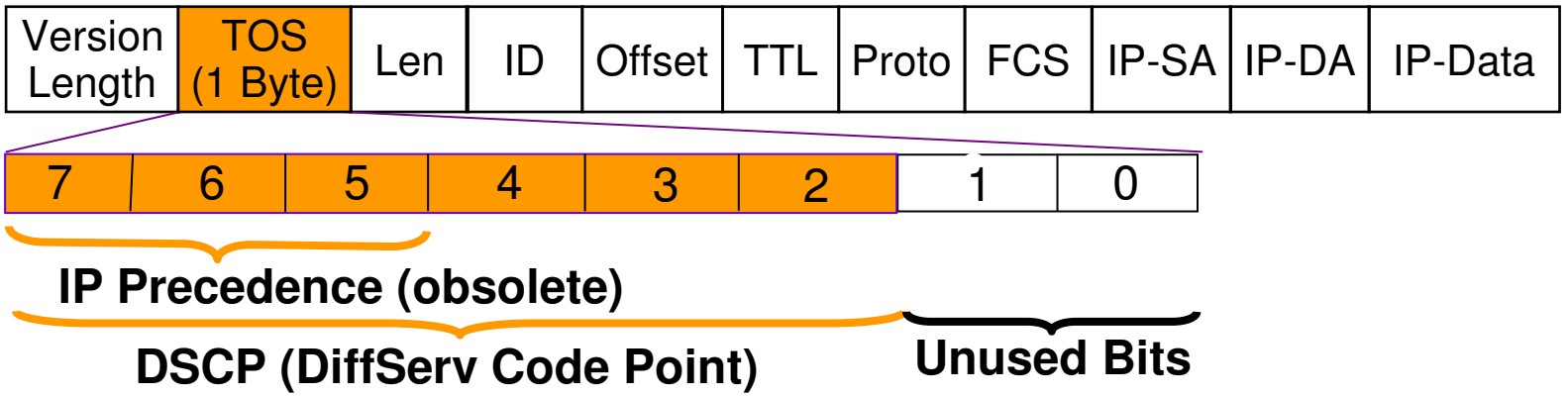
- Sicherstellung/Durchsetzung über MPLS Labels!

Quality of Service (QoS) in MPLS-VPN‘s
Überblick Integrated Services Model (RFC 2205)

- Anwendung fordert spezifischen QoS an
- Signalisierung via „Resource Reservation Protocol“ (RSVP)
- Nachteile:
  - Anwendung muss RSVP-fähig sein
  - Technische Komplexität bei Nutzung und Konfiguration
  - Schlechte Skalierung, da pro Verkehrsbeziehung Status (in den Routern) vorzuhalten ist
  - Umfangreicher Management- und Kontroll-Verkehr
  - Sämtliche Router auf dem Weg müssen RSVP-fähig sein
- Vorteile:
  - feine Granularität
  - Ressourcen und QoS sind Ende-zu-Ende garantiert

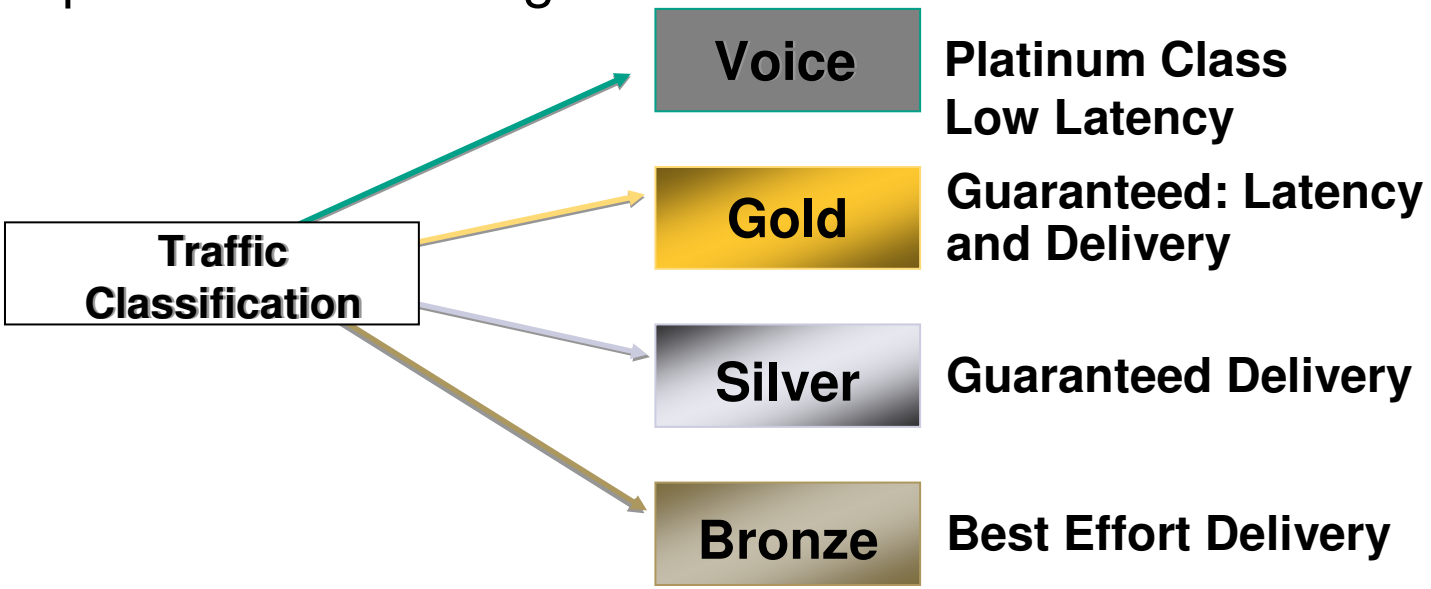
Quality of Service (QoS) in MPLS-VPN's
Überblick Differentiated Services Model (RFC 2475)

- QoS durch unterschiedliche Behandlung von (Klassen von) Paketen
- Klassifikation z.B. nach IP-Adressen oder Ports (TCP, UDP) etc.
- Keine explizite Anforderung oder Signalisierung durch Anwendung
- Nachteile:
  - Grobe Granularität, d.h. keine spezifische Behandlung pro Anwendung
  - Keine Ende-zu-Ende Garantien, nur auf „Per Hop Basis“
- Vorteile:
  - Einfache Konfiguration, keine Modifikation existierender Anwendungen
  - Gute Skalierbarkeit wegen grober Granularität
- Einordnung im IP Header (vgl. RFC 791):



Quality of Service (QoS) in MPLS-VPN‘s
Einsatz DiffServ in MPLS Netzen

- In MPLS-basierenden Netzen mit QoS kommt i.d.R. das Differentiated Services Model zum Einsatz
- Markierung der Pakete am Eingang zum MPLS-Netz (CER oder LER) oder durch Anwendung
- Kopieren der Markierung in MPLS-Label (Exp.Bits!!!)
- LSRs verwenden Label bzw. Exp.bits zur Entscheidung, in welche Output-Queue Paket genommen wird



Das wärs für heute...

- Fragen / Diskussion
- Verbesserungsvorschläge
- Die Folien von heute sind bereits auf die Web-Seite der Vorlesung
- Literatur: siehe Linkliste des letzten Vortrags

- Nächster Termin (29. Mai 2008):
  - Webzugang und Internet-Sicherheit, Teil 2

- Einen schönen Abend !!!