

# Design und Realisierung von E-Business- und Internet-Anwendungen

## „Virtuelle Private Netze“ Teil 2

Dr. Michael Nerb et al.,  
Prof. Dr. Heinz-Gerd Hegering  
SoSe 2005

DREIA  
Dr. M. Nerb,  
Dr. S. Heilbronner et al.  
(C) 2005  
Seite 2

## Virtuelle Private Netze Inhalte dieses Teils (verteilt auf zwei Termine)

Inhalte des letzten Termins (12.05.05):

- 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 Weitverkehrenetzen**

- **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**

## 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 „geschichten“ Infrastruktur
- Tunneling oder Tagging
- Transparent oder „Nicht-Transparent“ für Benutzer

## Klassifikation – Wiederholung VPN's nach OSI-Schichtenmodell

### Layer-2 Technologien:

- L2F, PPTP, L2TP, L2Sec

### Layer-3 Technologien:

- IPSec

### Layer-4-7 Technologien:

- SSH, SSL/TLS, SSL-VPN's

### VPN-Technologien in WAN's

- Virtuelle Verbindungen in Frame Relay Netzen
- Virtuelle Pfade und Kanäle in zellbasierten Netzen (z.B. ATM)
- Multiprotokoll Label Switching (MPLS)

Vertiefung der VPN's erfolgt anhand dieser Klassifikation

# 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

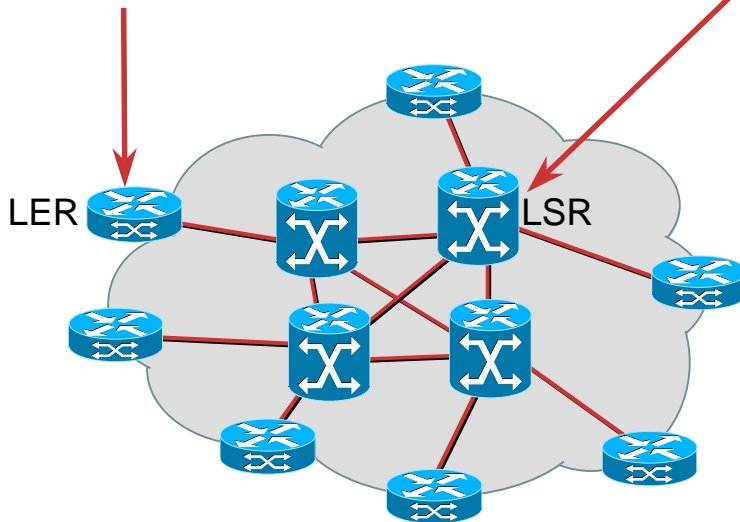
## Konzept – Überblick

### 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

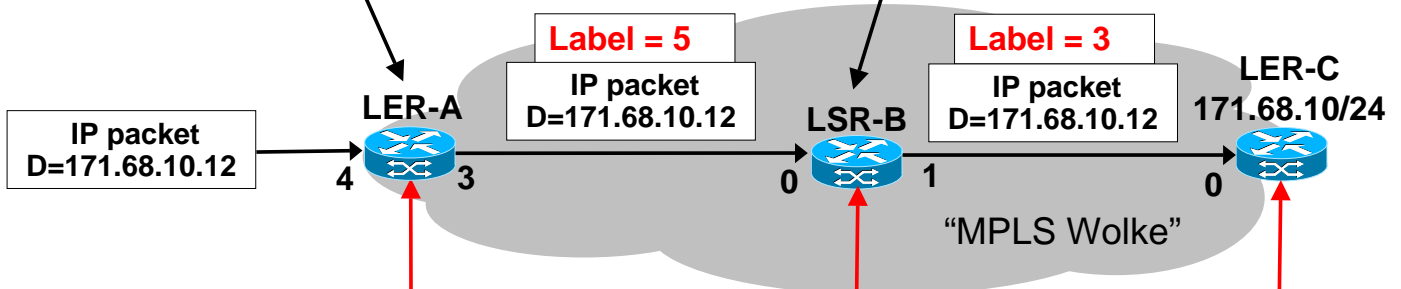
LSR: Label Switch Router

# MPLS

## Konzept – Paket Forwarding (vereinfacht)

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

In I/F	In Lab	Address Prefix	Out I/F	Out Lab
0	5	171.68.10	1	3
...	...	...	...	...



1) LER-A klassifiziert IP Paket in eine FEC und weist Label zu

2) LSR-B leitet IP Paket anhand des Labels weiter

3) Entfernt Label und liefert IP Paket aus

# 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

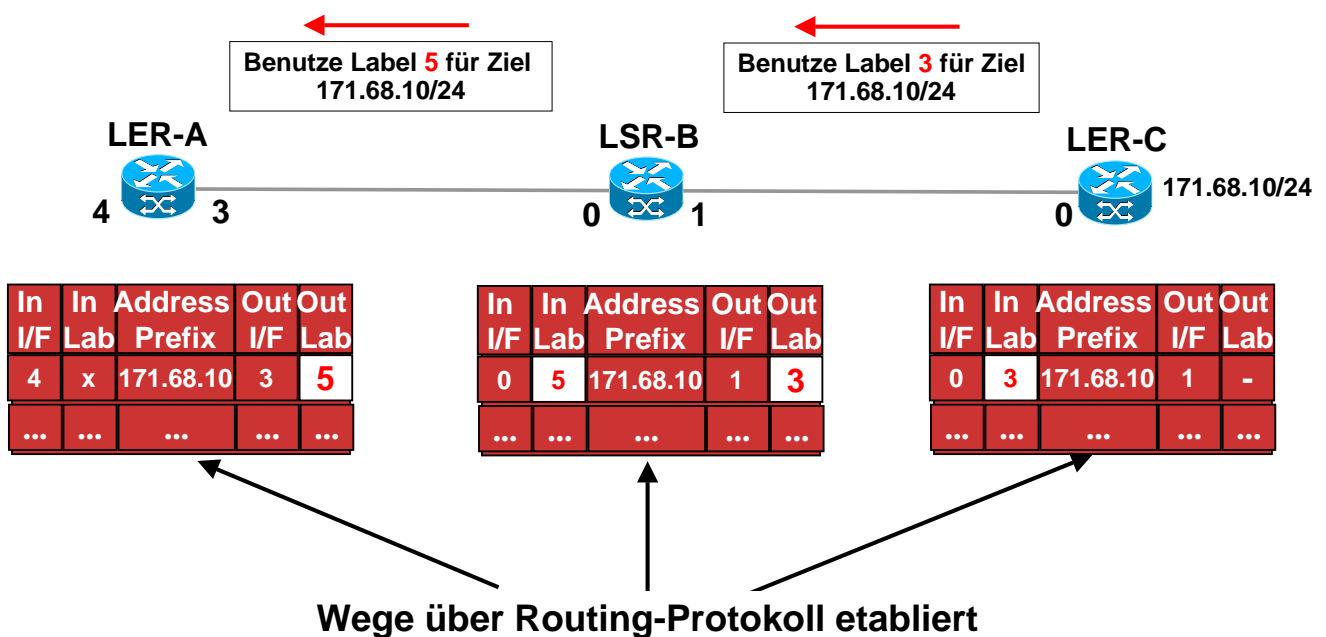
**Out-Label:** MPLS Router erfragen dies vom „Downstream LSR“ via LDP:

- 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
...	...	...	...	...

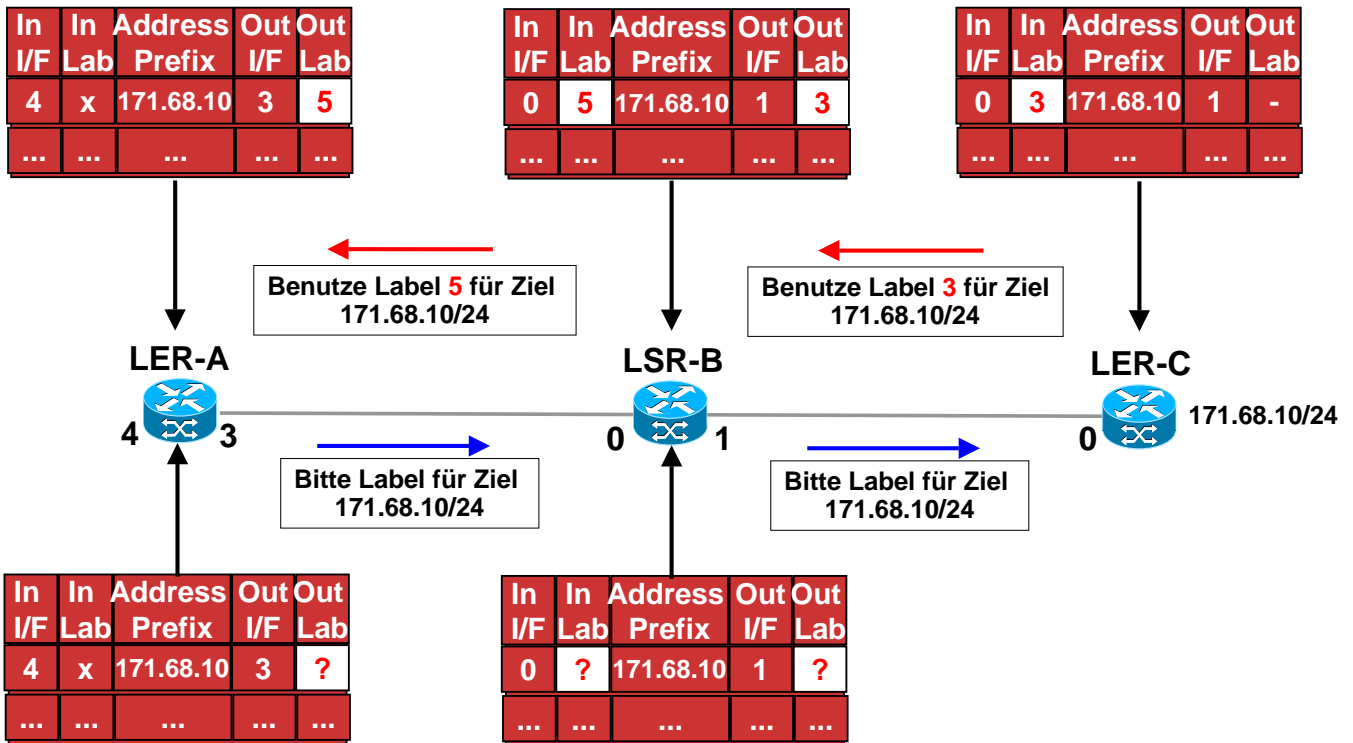
# MPLS

## Details – Unsolicited Downstream



# MPLS

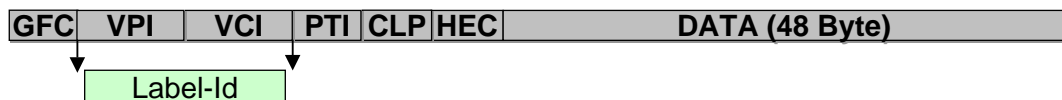
## Details – Downstream on Demand



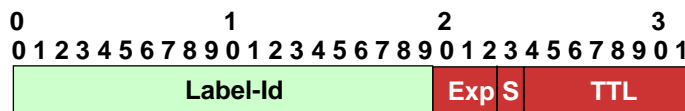
# MPLS

## Struktur und Einbettung der MPLS Labels

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

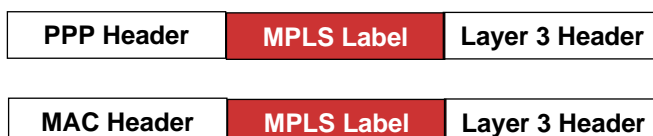


Ergänzung um zusätzliche Informationen (insg. 4 Byte, 32 bit):



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

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

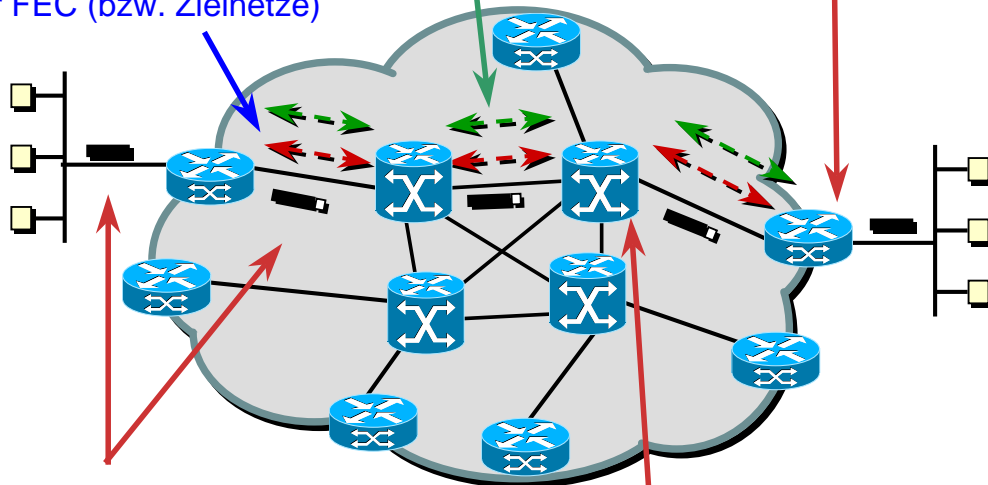


# MPLS Zusammenfassung

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 12.05.05

IP VPNs verwenden (pro Kunden !!!):

- spezifische Adressierungsschemata
- spezifische Routing-Policies
- Ggf. überlappende IP-Netze

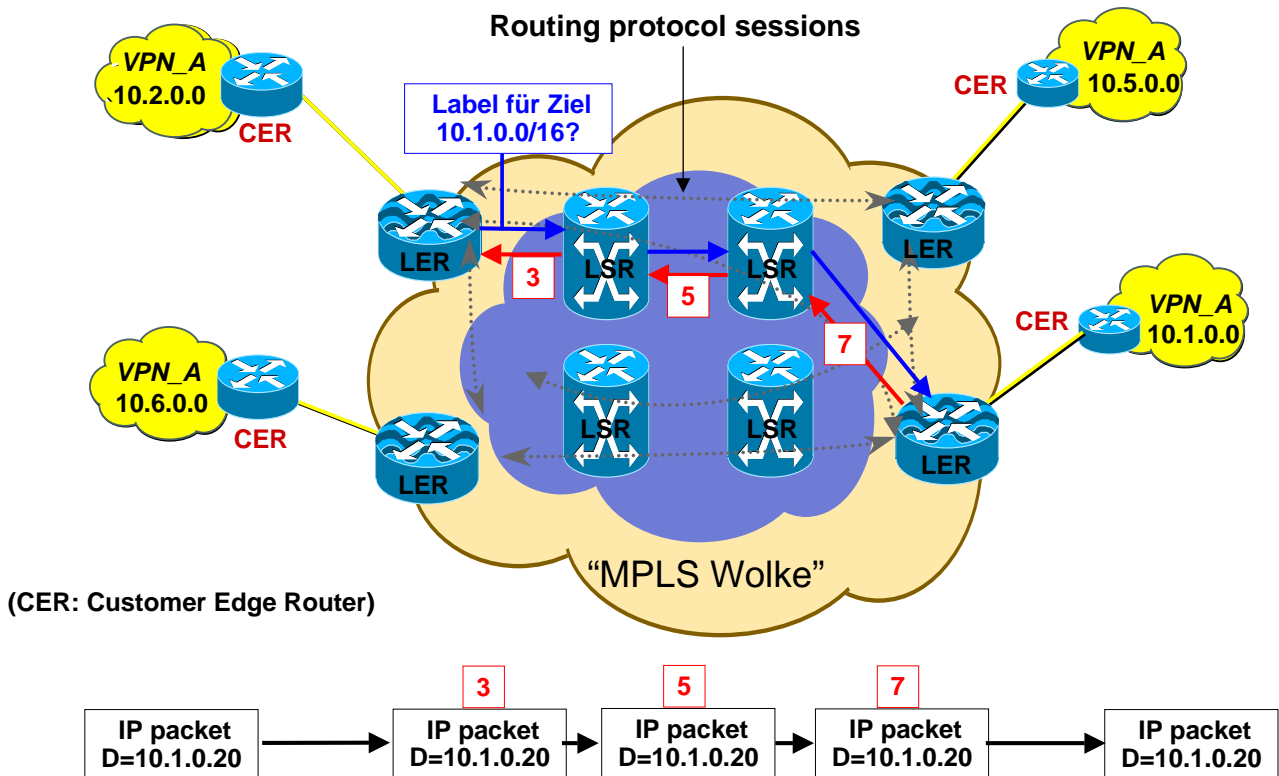
Um IP-Pakete verschiedener VPNs (d.h. verschiedener Kunden) zu transportieren, muss ein MPLS-Netz folgendes sicherstellen:

- Routing von IP-Adressen verschiedener VPNs
- Eindeutigkeit von IP-Adressen über verschiedene VPNs
- Unterstützung verschiedener Routingprotokolle

**Sicherstellung/Durchsetzung über MPLS Labels!**

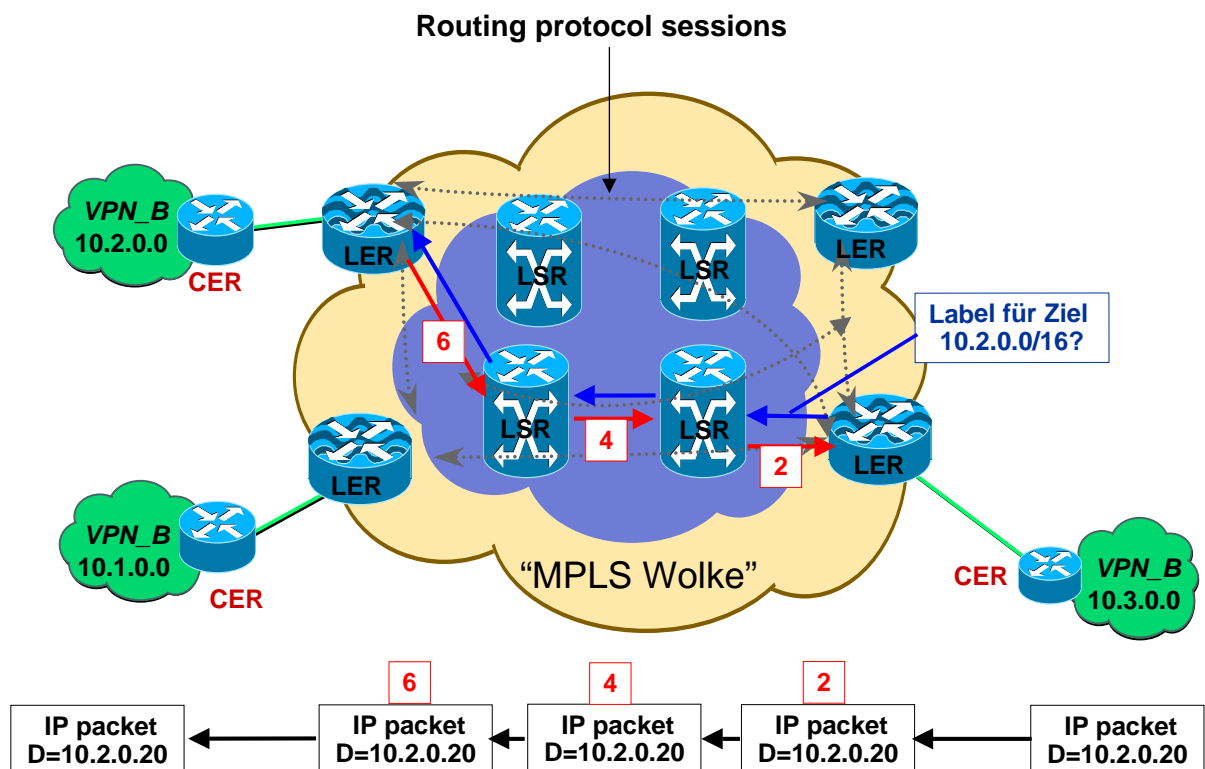
# MPLS-basierte IP-VPN's

## Routing/Packet Forwarding für Kunden A



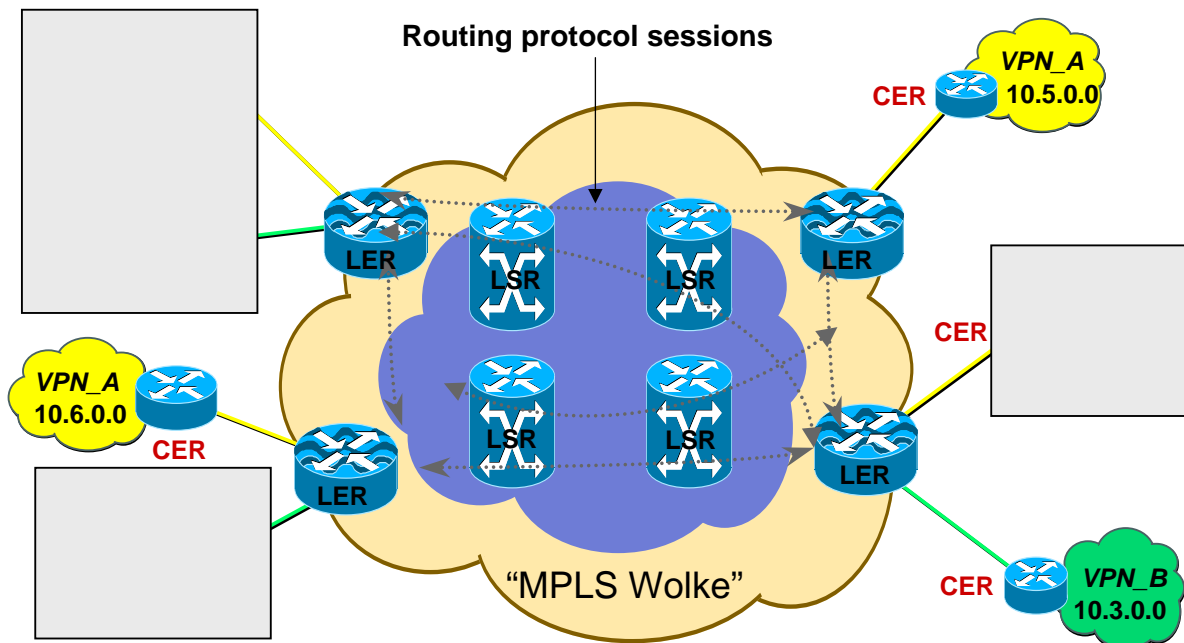
# MPLS-basierte IP-VPN's

## Routing/Packet Forwarding für Kunden B





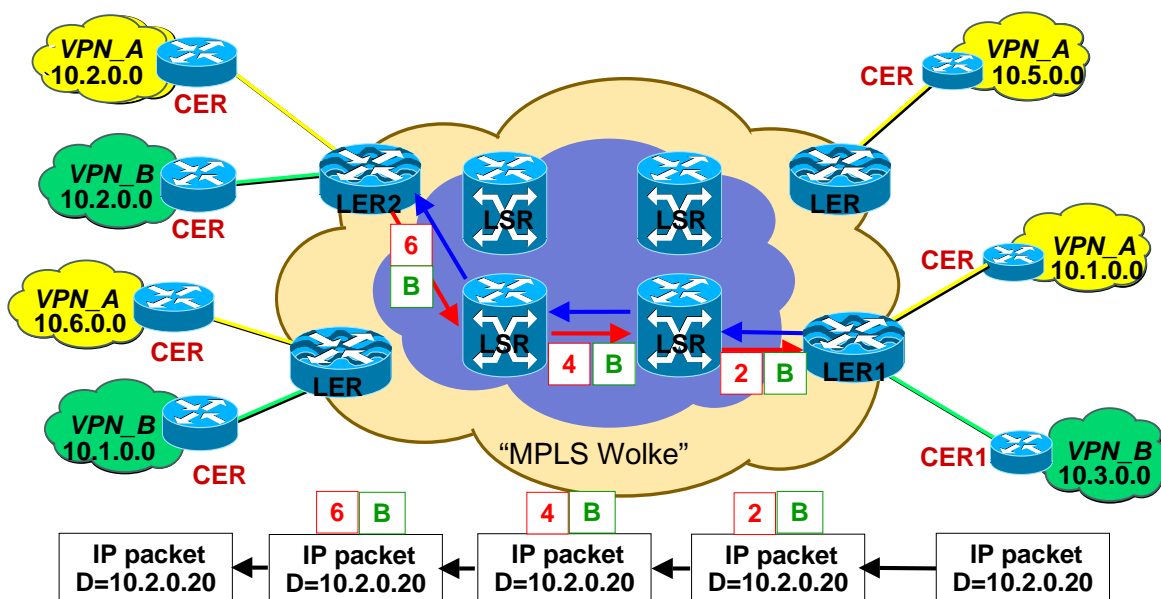
## MPLS-basierte IP-VPN's Beispielszenario mit Kunden A und B



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

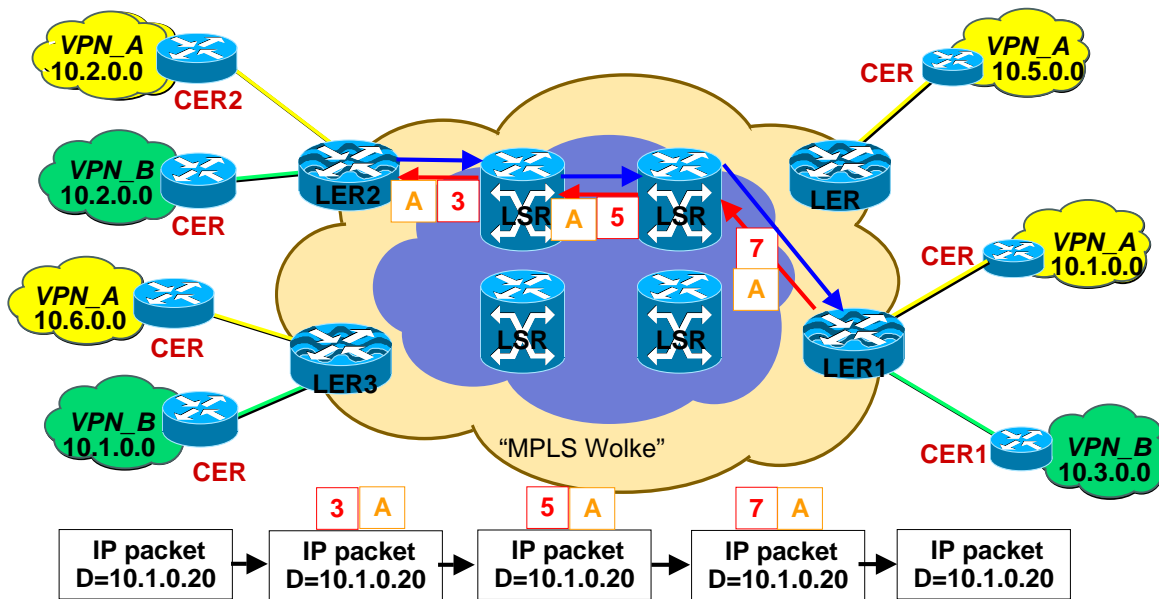
## MPLS-basierte IP-VPN's Routing/Packet Forwarding für VPN\_B



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):

Version Length	TOS (1 Byte)	Len	ID	Offset	TTL	Proto	FCS	IP-SA	IP-DA	IP-Data
-------------------	-----------------	-----	----	--------	-----	-------	-----	-------	-------	---------



IP Precedence (obsolete)

DSCP (DiffServ Code Point)

Unused Bits

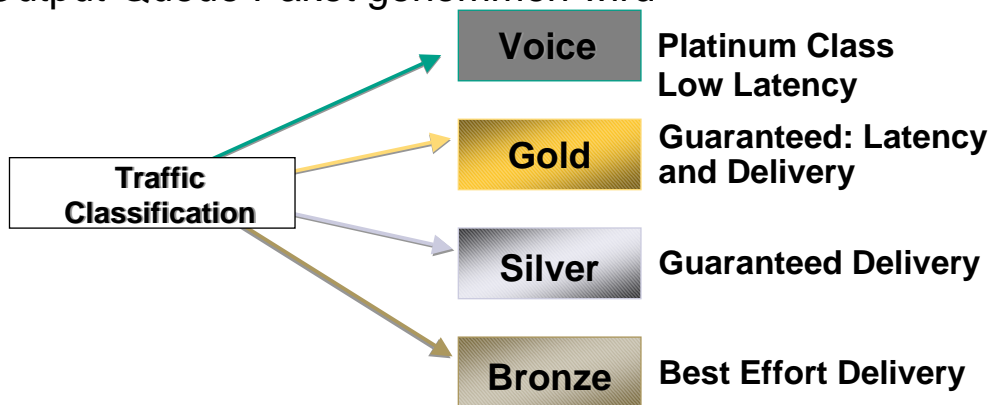
## Quality of Service (QoS) in MPLS-VPN's Einsatz DiffServ in MPLS Netzen

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 (02. Juni 2005):

- Referenten: Stefan Emilius und Christian Pauli
- Thema: „UMTS und WLAN“

Einen schönen Abend !!!