Rechnernetze II

SoSe 2025

Roland Wismüller
Betriebssysteme / verteilte Systeme
roland.wismueller@uni-siegen.de
Tel.: 0271/740-4050, Büro: H-B 8404

Stand: 8. April 2025

Rechnernetze II

SoSe 2025

4 IP-Routing: Spezielle Aspekte

4 IP-Routing: Spezielle Aspekte ...

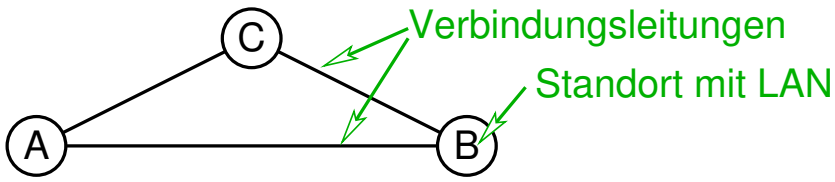
Inhalt

- Tunneling und VPN
- Multicast
- Mobile IP
- *Multiprotocol Label Switching*, MPLS

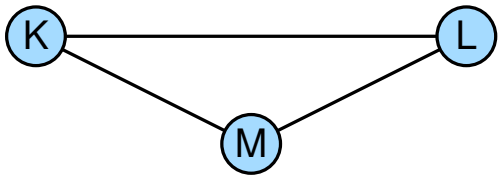
- Tanenbaum, Kap. 5.2.8, 5.2.9, 5.4.5, 5.6.2, 5.6.4
- Peterson, Kap. **4.2.5**, **4.3-4.3.4**, **4.4**, **4.5**
- J.F. Kurose, K.W. Ross: Computernetze. Pearson Studium, 2002. Kap. 4.8 (Multicast)
- CCNA, Kap. 5

4.1 Tunneling und virtuelle private Netze (VPN)

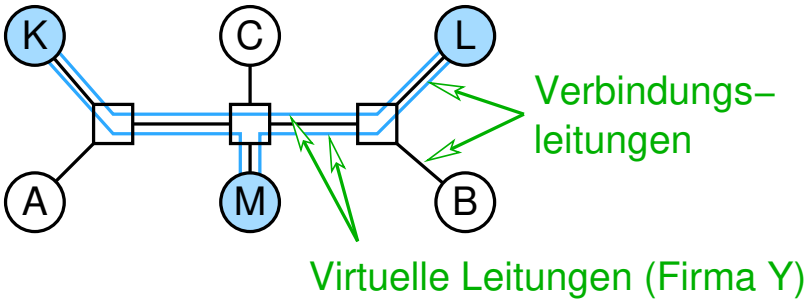
- Zwei private Netzwerke:
  - Firma X:



  - Firma Y:

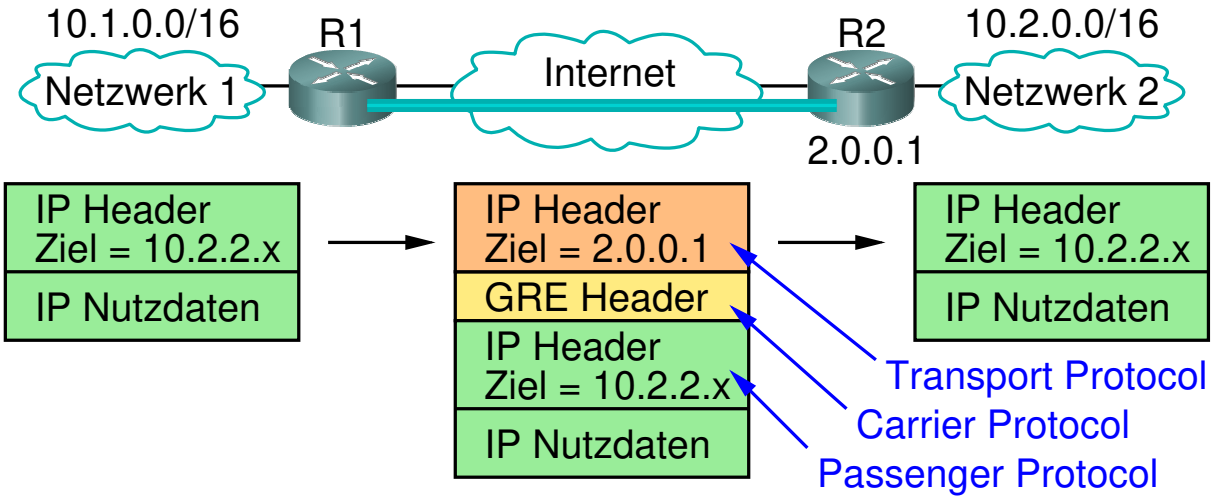


- Zwei VPNs:



4.1 Tunneling und virtuelle private Netze (VPN) ...

- Virtuelle Leitung simuliert eine Layer-2-Verbindung über ein Layer-3-Netz (z.B. Internet)
- Realisierung von virtuellen Leitungen: Tunnel



- Carrier-Protokoll kann ggf. auch fehlen
  - Aufgaben u.a. Multiplexing, Authentifizierung, Reihenfolge, ...

Anmerkungen zu Folie 125:

GRE (*Generic Routing Encapsulation*) ist ein einfaches, unsicheres Tunnel-Protokoll, das von CISCO entwickelt wurde.

Der GRE-Header enthält u.a. ein 16-Bit Feld zur Identifikation des *Passenger* Protokolls (IP hat nur ein 8-Bit Feld), einen anwendungsabhängigen Schlüsselwert und eine Sequenznummer.

4.1 Tunneling und virtuelle private Netze (VPN) ...

- Einsatz von Tunneln:
  - spezielle Fähigkeiten von R1, R2
    - *Overlay*-Netze, z.B. MBone (Multicast Backbone)
  - Kopplung von nicht-IP-Netzen über das Internet
  - VPNs: Verschlüsselung und Authentifizierung im Tunnel
- Arten von VPNs
  - *Site-to-site* VPN: verbindet z.B. zwei Standorte
    - statisch
    - VPN für interne Hosts nicht sichtbar
    - Realisierung durch Router (VPN *Gateways*), typ. mit IPsec
  - *Remote-access* VPN
    - externer Client verbindet sich dynamisch mit VPN *Gateway*
    - Lösungen über TLS (eingeschränkt) bzw. IPsec

4.2 Multicast

- Multicast: ein Sender sendet an Gruppe von Empfängern
- Anwendungen, z.B.:
  - Multimedia-Streaming (Video- / Audioübertragung)
  - Telekonferenzen
  - Nachrichtenticker, z.B. Börsenkurse
- Einfachste Realisierung:
  - Unicast an jedes Gruppenmitglied
  - verschwendet Bandbreite auf gemeinsamen Verbindungen
- Ziel:
  - Multicast-Unterstützung durch Router
  - Paket auf jeder Verbindung nur einmal übertragen

4.2.1 Adressierung beim Multicast

- Explizite Angabe aller Empfänger skaliert nicht
- Daher: indirekte Adressierung über Multicast-Gruppen
  - Gruppe wird in IPv4 durch Adresse der Klasse D adressiert

31	0
1 1 1 0	Multicast–Adresse

    - Adreßbereich 224.0.0.0 - 239.255.255.255
  - In IPv6: Adressbereich FF00::/8
- Fragen:
  - Wahl der Multicast-Adresse?
  - dynamisches Ein- und Austreten möglich?
  - kennen sich die Gruppenmitglieder?
  - wie erfolgt das Routing?

4.2.2 Management von Multicast-Gruppen

IGMP: *Internet Group Management Protocol* (IETF RFC 2236)

- Protokoll zwischen Host und lokalem Router
  - Informationsaustausch zwischen den Routern nur durch Routing-Protokolle
  - keine globale Information über Gruppenmitglieder!
- Nachrichtentypen:
  - *Membership_query*: Anfrage des Routers an lokales LAN
    - welche Gruppen haben Mitglieder im LAN?
    - ist ein Host Mitglied der angegebenen Gruppe?
    - versendet per LAN-Multicast
  - *Membership_report*: Host ist Mitglied der Gruppe
    - als Antwort auf *Membership_query* oder spontan
  - *Leave_group*: Host verlässt Gruppe (optional)

IGMP: Anmerkungen

- Wahl der Multicast-Adresse erfolgt **nicht** durch IGMP
- Router muß nur wissen, ob es im LAN einen Rechner in einer gegebenen Gruppe gibt
  - Pakete werden lokal mit LAN-Multicast geschickt
- Bei *Membership_query*: Feedback-Unterdrückung:
  - Host wartet vor Antwort zufällige Zeit
  - wenn Host Antwort im LAN sieht: eigene Antwort verwerfen
- Soft-State-Registrierung:
  - Registrierung hat nur bestimmte Lebensdauer
  - periodische *Membership_query*-Anfragen des Routers

Anmerkungen zu Folie 130:

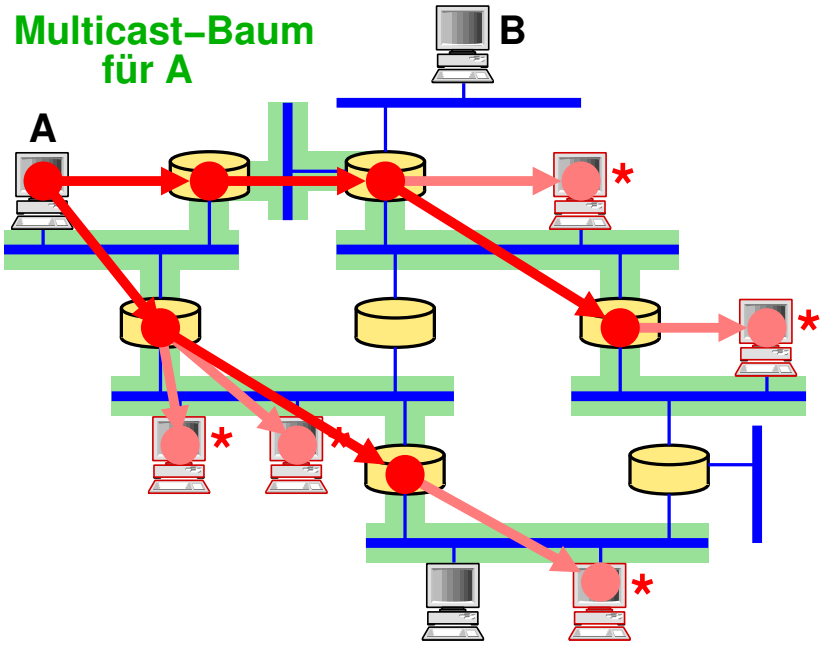
- Für Ethernet-LANs spezifiziert RFC 1112 eine feste Abbildung von IP-Multicast-Adressen auf Ethernet Multicast-Adressen: die untersten 23 Bit der IP-Adresse werden in die Multicast-Adresse 01:00:5E:00:00:00 eingetragen. Obwohl diese Zuordnung mehrdeutig ist, ermöglicht sie doch eine Vorfilterung des Multicast-Verkehrs durch die Netzwerk-Karten.
- Die IGMP-Nachrichten (*Membership_query*, *Membership_report* und *Leave_group*) werden als Multicast (an die Adresse 224.0.0.22) mit einer TTL von 1 gesendet. Das heißt, die Nachrichten gehen an alle Rechner (die Multicast nutzen) im LAN. Die Antwort auf eine *Membership_query* ist daher für alle betroffenen Rechner im LAN sichtbar, auch wenn das LAN mit Hilfe von Switches aufgebaut ist.

4.2.3 Multicast-Routing

(Animierte Folie)

Beispiel-Netzwerk

- (Rot) markierte Rechner gehören zur Multicast-Gruppe
- A sendet: Nachrichten entlang eines aufspannenden Baums mit Wurzel A verteilen

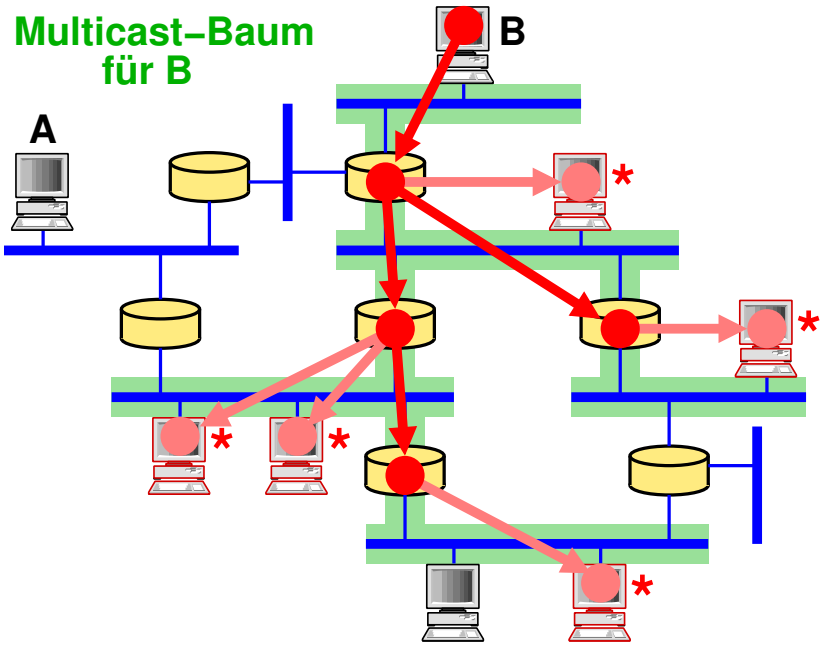


4.2.3 Multicast-Routing ...

(Animierte Folie)

Beispiel-Netzwerk

- (Rot) markierte Rechner gehören zur Multicast-Gruppe
- B sendet: Nachrichten entlang eines aufspannenden Baums mit Wurzel B verteilen



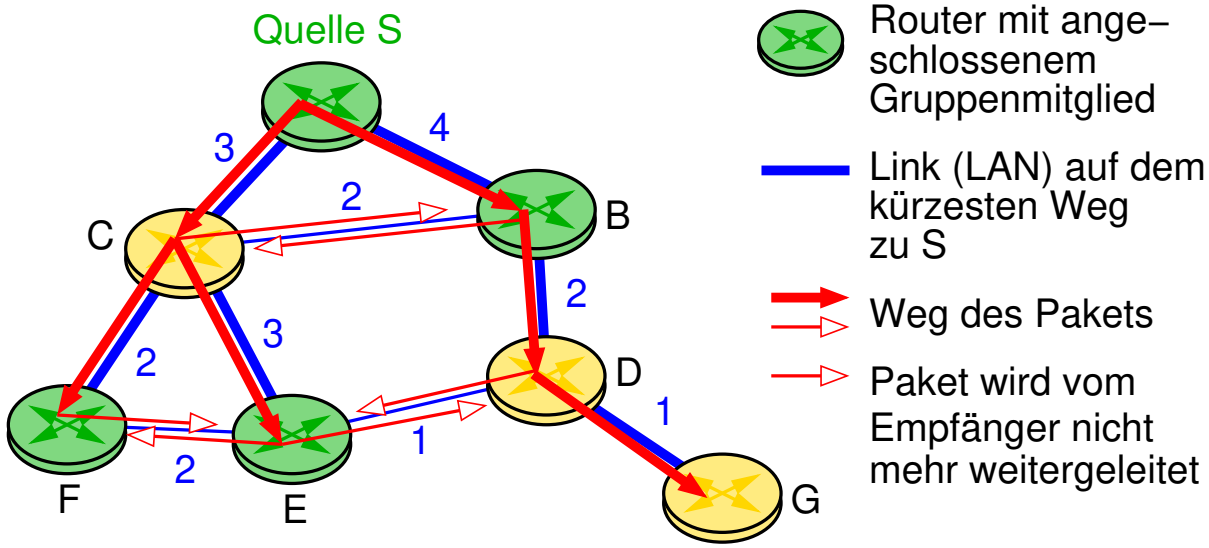
Link-State-Multicast Routing

- Erinnerung:
  - Durch *Reliable Flooding* erhält jeder Router Information über das Gesamtnetz
  - Berechnung kürzester Wege durch Dijkstra-Algorithmus
- Für Multicast-Routing:
  - Link-State-Pakete geben für jedes LAN an, für welche Gruppen Mitglieder im LAN sind
  - jeder Router berechnet spannenden Baum mit kürzesten Wegen im Gesamtnetz
    - von jeder Quelle zu jeder Gruppe!

Distanzvektor-Multicast (IETF RFC 1075)

- Erinnerung: Distanzvektor-Routing
  - Router kennen globalen Netzwerkgraph nicht
  - jeder Router hält Tabelle mit Einträgen <*Ziel, Kosten, nextHop*>
  - Router tauschen <*Ziel, Kosten*> Nachrichten aus
- Grundprinzip: *Reverse Path Forwarding* (RPF)
  - wenn ein Router ein Paket von Quelle S über Link L erhält:
    - Paket an alle Links außer L weiterleiten (wie bei Flooding)
    - **aber nur**, wenn L der Link auf dem kürzesten Weg zu S ist (das Paket also vom *nextHop* in Richtung S kam)

Beispiel zum *Reverse Path Forwardng*



Anmerkungen zu Folie 135:

Die überflüssigen Übertragungen des Pakets finden nur beim ersten Paket statt. Danach werden sie durch *Pruning* verhindert (siehe nächste Folie).

Im Beispiel würde etwa Router E eine *Prune*-Nachricht an die Router F und D senden (und umgekehrt).

Distanzvektor-Multicast ...

- *Pruning*
  - ein „Blatt“-Router, der Pakete empfängt, aber kein Gruppenmitglied im LAN hat (im Beispiel: G), sendet einen *Prune*-Nachricht an seinen Upstream-Router (im Beispiel: D)
  - ein Router, der von allen Downstream-Routern *Prune* empfangen hat, sendet *Prune* upstream weiter
  - Rückgängigmachen des *Pruning* durch *Timeout* oder explizite *Join*-Nachricht
- Verfeinerung: *Reverse Path Broadcast* (RPB)
  - wenn an ein LAN mehrere Router angeschlossen sind, sendet nur einer davon Multicast-Pakete in das LAN
- Einsatz in MBone (*Multicast Backbone*)

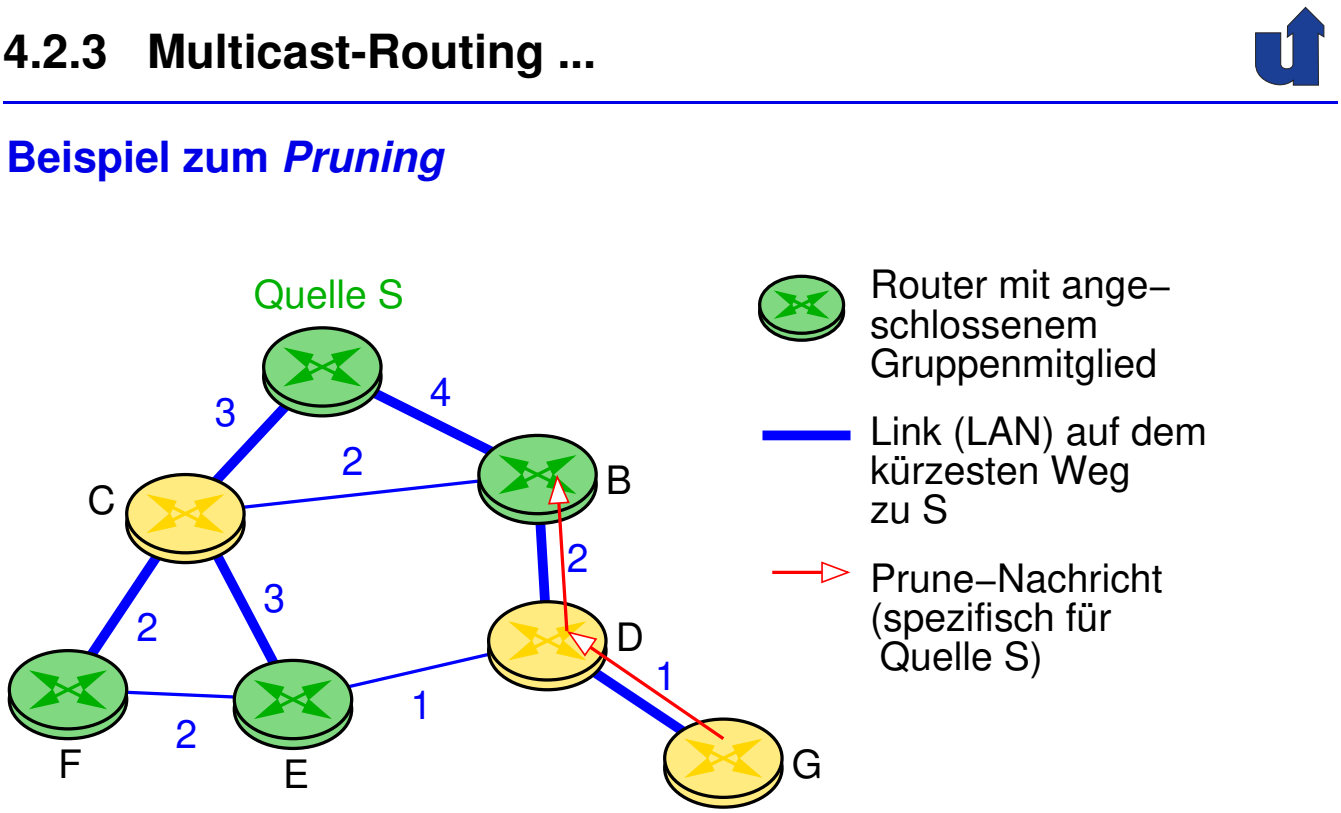
Anmerkungen zu Folie 136:

Die Prune-Nachricht ist quellenspezifisch und wird nur bei Bedarf erzeugt, d.h., erst wenn das erste Multicast-Paket von S eintrifft.

Durch den periodischen Austausch der Distanzvektoren weiß jeder Router für jedes seiner angeschlossenen LANs, ob er im quellenspezifischen Multicast-Baum der Parent-Router für dieses LAN ist. Er ist genau dann der Parent-Router, wenn er von allen Routern in diesem LAN den kürzesten Abstand zur Quelle hat. In diesem Fall ist der Router dafür zuständig, Multicast-Pakete in das LAN weiterzuleiten. Damit weiß der Router auch, welche anderen Router Child-Router (d.h. Downstream-Router) für eine bestimmte Quelle sind, nämlich alle, die an ein LAN angeschlossen sind, für das der Router zuständig ist.

Literatur

S. Deering: *Multicast Routing in Internetworks and Extended LANs*, ACM SIGCOMM Computer Communication Review, 25(1), Jan. 1995 (Abschnitt 5.2)



Beispiel zum *Pruning*

PIM: *Protocol Independent Multicast* (IETF RFC 2362)

- Problem bei RPF: Skalierbarkeit
  - Default-Verhalten: **jeder** Router erhält das Paket
  - meist aber nur wenige Router wirklich betroffen
- Bei PIM daher zwei Modi:
  - *dense*: Ansatz wie bei RPF (mit *Pruning*)
  - *sparse*: Router muß sich explizit registrieren
- Im Folgenden: *sparse*-Modus

PIM: Aufbau des Multicast-Baums

- Für jede Gruppe wird ein spezieller Router (**Rendezvouspunkt**, RP) ausgewählt
- Router senden *Join* bzw. *Prune*-Nachrichten an RP, um sich zu registrieren bzw. abzumelden
- Durch den Weg der *Join*-Nachrichten wird ein Baum aufgebaut (mit RP als Wurzel)
  - unabhängig vom verwendeten Routing-Protokoll (⇒ **PI**M)
  - ein gemeinsamer Baum für alle Quellen

Anmerkungen zu Folie 139:

Der RP kann manuell konfiguriert oder durch ein spezielles Protokoll zwischen den Routern gewählt werden (RFC 2363, Abschnitt 2.6).

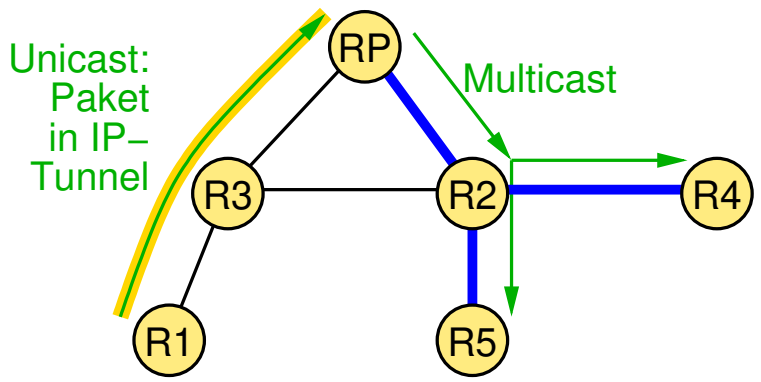
Jeder Router kennt die Zuordnung zwischen Multicast-Adresse (bzw. Adreß-Präfix) und RP.

PIM: Routing eines Multicast-Pakets

- Ablauf beim Senden eines Multicast-Pakets:
  - Quelle sendet Paket über Tunnel an RP
  - RP sendet Paket über Baum an Multicast-Gruppe
- Optimierungen (bei entsprechendem Verkehrsaufkommen):
  1. RP sendet quellenspezifischen *Join* an Quelle
     - damit kennen dazwischenliegende Router den Pfad, kein IP-Tunnelling mehr notwendig
     - Pfad gilt nur für die im *Join* angegebene Quelle
  2. Empfänger senden quellenspezifischen *Join* an Quelle
     - Aufbau eines quellenspezifischen Baumes (mit Quelle als Wurzel)

(Animierte Folie)

PIM: Beispiel



R1 sendet Paket an Gruppe:

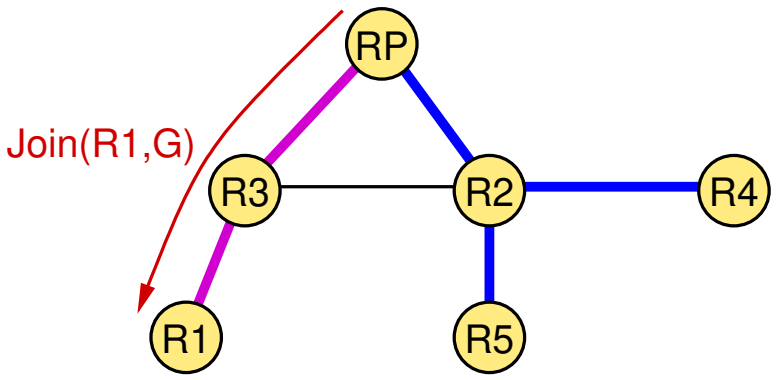
a) R1 sendet Paket über Tunnel an RP

b) RP sendet Paket über Multicast

Gemeinsamer Multicast–baum

(Animierte Folie)

PIM: Beispiel

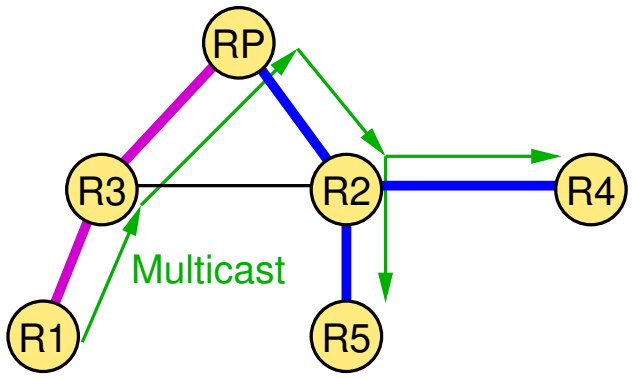


Pfad R1–RP wird zum Baum hinzugefügt

- Gemeinsamer Multicast–baum
- Quellenspezifischer Multi–castbaum für R1

(Animierte Folie)

PIM: Beispiel

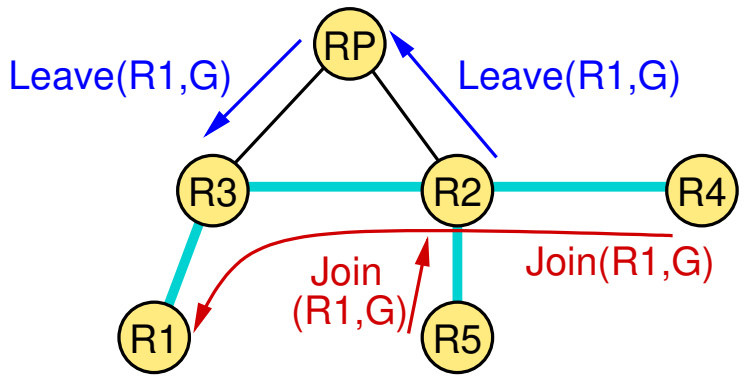


R1 sendet Paket über Multicast–Baum

- Gemeinsamer Multicast–baum
- Quellenspezifischer Multi–castbaum für R1

(Animierte Folie)

PIM: Beispiel



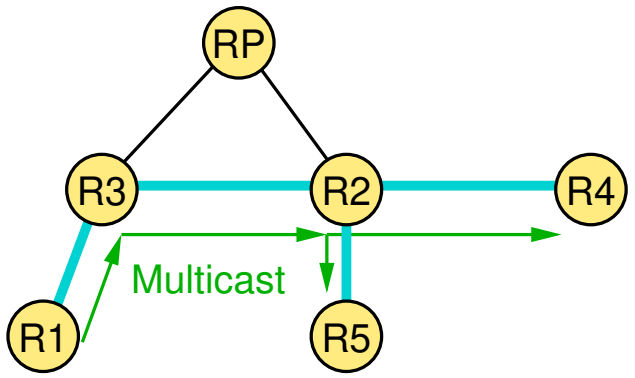
Pfade R1–R3–R2–R4 und R2–R5 werden in quellen–spezifische Baum von R1 aufgenommen

R2 und RP melden sich für Quelle R1 ab

Quellenspezifischer Multi–castbaum für R1

(Animierte Folie)

PIM: Beispiel



R1 sendet Paket über quellenspezifischen Baum

Quellenspezifischer Multi–castbaum für R1

Anmerkungen zu Folie 145:

Wenn im Beispiel nur R4 einen quellenspezifischen Join an R1 gesendet hätte, würde dieselbe Situation entstehen: R2 gibt diesen quellenspezifischen Join ja an R1 weiter und weiß damit, daß er die Muticast-Pakete von R1 „direkt“ erhält statt über den RP. Er wird sich also auch in diesem Fall vom RP für die Quelle R1 abmelden.

In unserem Beispiel kann sich auch der RP für die Quelle R1 abmelden, da er keinen Nachbarn mehr hat, dem er die Pakete weiterleiten muß. Das wird im allgemeinen aber nicht der Fall sein. Der RP bleibt dann im quellenspezifischen Baum und gibt die Pakete über den gemeinsamen Multicast-Baum an alle Router weiter, die noch keinen quellenspezifischen Join geschickt haben.

145-1

4.2.4 Multicast: Zusammenfassung

Zwei Aspekte:

- Verwaltung von Multicast-Gruppen
  - An- und Abmelden von Teilnehmern (IGMP)
  - Wahl der Multicast-Adresse (durch *out-of-band*-Mechanismen)
- Multicast-Routing
  - Verteilung der Pakete über aufspannenden Baum
    - gemeinsamer Baum für alle Quellen
    - quellenspezifische Bäume
  - Erweiterung existierender Routing-Protokolle oder Protokoll-unabhängiger Multicast

4.3 Mobile IP

Erinnerung: IP-Routing

- IP-Adressen sind aufgeteilt in
  - Netzadresse
  - Hostadresse (und ggf. Subnetz-Adresse)
- Router im Internet betrachten nur Netzadresse
  - Vorteil: bessere Skalierbarkeit
  - Problem: Host ist nur in „seinem“ Netz erreichbar
- Mobile Rechner (Laptops) werden in verschiedenen Netzen betrieben
  - neue IP-Adresse über DHCP ist nicht immer eine Lösung
    - bestehende Verbindungen werden unterbrochen

4.3 Mobile IP ...

Ziele von *Mobile IP* (IETF RFC 3344)

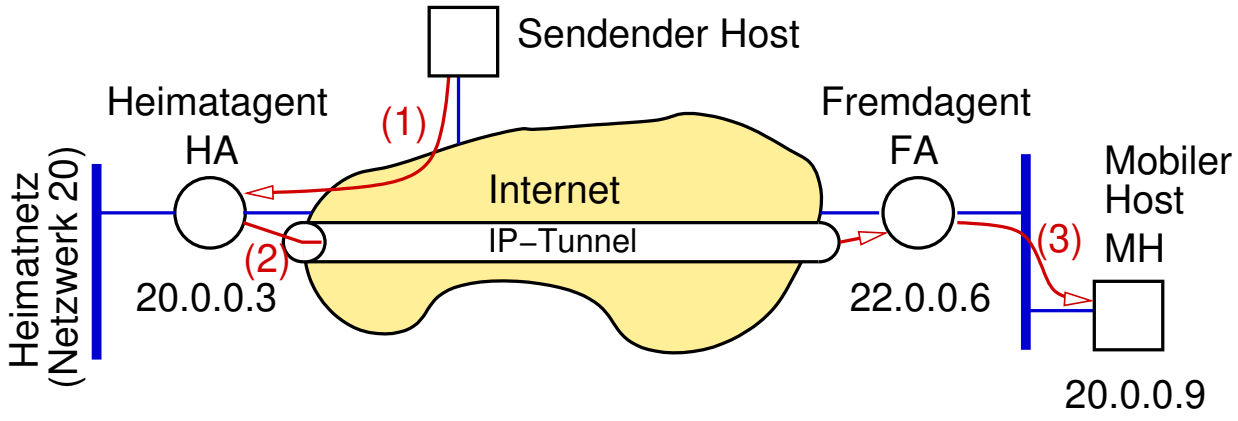
- Rechner kann (drahtloses) Netz wechseln („*Roaming*“)
  - ohne IP-Adresse zu wechseln
  - ohne Abbruch existierender Verbindungen
- Lösung darf keine Änderung
  - der über IP liegenden Software der mobilen Hosts
  - einer Vielzahl von Internet-Routern

  benötigen

Funktionsweise

- Ein bzw. zwei Router mit speziellen Fähigkeiten
  - **Heimatagent** (HA): im Heimatnetz des mobilen Hosts
    - permanente IP-Adresse (Heimatadresse) des mobilen Hosts liegt im Netz dieses Routers
  - **Fremdagent** (FA): im aktuellen Netz des MH
- HA und FA senden regelmäßig *Advertisements*
  - enthalten IP-Adresse des Routers
- Im Heimatnetz: mobiler Host (MH) erhält Adresse des HA
- Im Fremdnetz:
  - MH registriert sich bei FA, sendet Adresse des HA
  - FA sendet c/o-Adresse des MH (i.d.R. Adr. des FA) an HA

Routing eines Pakets an mobilen Host



1. Host sendet an MH: Paket wird an HA geroutet
2. HA sendet Paket über IP-Tunnel an c/o-Adresse (d.h. FA)
3. FA sendet Paket an MH (über MAC-Adr. aus Registrierung)

Anmerkungen zum Routing

- Was, wenn das Paket nicht über HA ins Heimatnetz kommt?
  - z.B. Sender im Heimatnetz oder zweiter Router
  - Lösung: ***Proxy ARP***
    - HA sendet ARP-Paket (IP-Adr. MH, MAC-Adr. HA)
    - ohne Anfrage durch Host / Router: ***Gratuitous ARP***
- MH kann selbst die Funktion des FA übernehmen
- Optimierung: HA kann Sender anweisen, Folgepakete (über IP-Tunnel) direkt an FA zu senden (IPv6 *Binding-Update*)
  - falls sich MH weiterbewegt:
    - *Binding-Warning* durch FA, wenn Paket eintrifft
    - zusätzlich: begrenzte Lebenszeit (falls MH selbst FA ist)

Anmerkungen zu Folie 151:

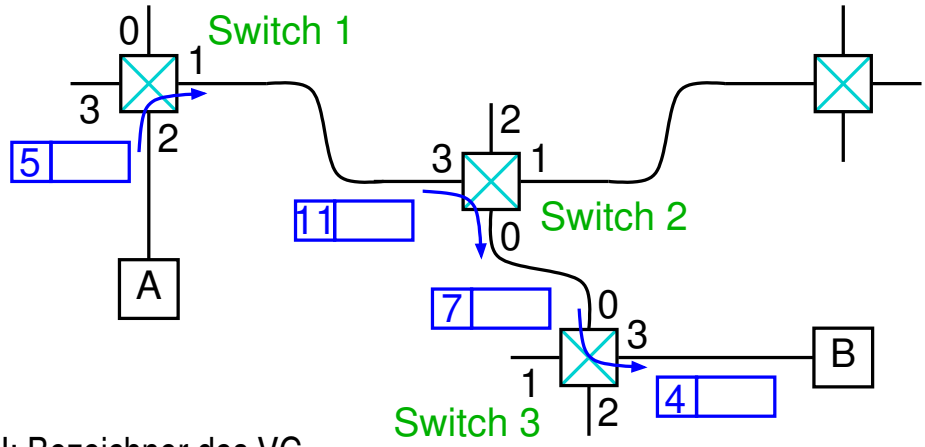
Zur Sicherheit von mobile IP:

- Der mobile Knoten, der Heimatagent und der Fremdagent müssen sich mit Hilfe von IPsec (☞ **5**) authentifizieren, so daß ein Angreifer keine gefälschten Nachrichten an den Heimatagenten senden kann, um Pakete umzuleiten.
- Die Vertraulichkeit kann z.B. ebenfalls über IPsec gewährleistet werden.

Siehe dazu auch RFC 3344 und `http://www.cu.ipv6tf.org/pdf/mobileip-sec.pdf`

Erinnerung: Virtuelle Leitungsvermittlung

- Kurze, link-spezifische Label statt langer Zieladresse



VCI: Bezeichner des VC

	Eingangsport	Eingangs–VCI	Ausgangsport	Ausgangs–VCI
Switch 1:	2	5	1	11
Switch 2:	3	11	0	7
Switch 3:	0	7	3	4

Anmerkungen zu Folie 152:

Der Eingangsport kann, muß aber nicht zusammen mit dem Eingangs-VCI als Schlüssel zum Auffinden von Ausgangsport und Ausgangs-VCI dienen. Viele Router verwenden nur den Eingangs-VCI als Schlüssel. Der Eingangs-VCI ist dann einfach der Index des zugehörigen Eintrags in der Routingtabelle.

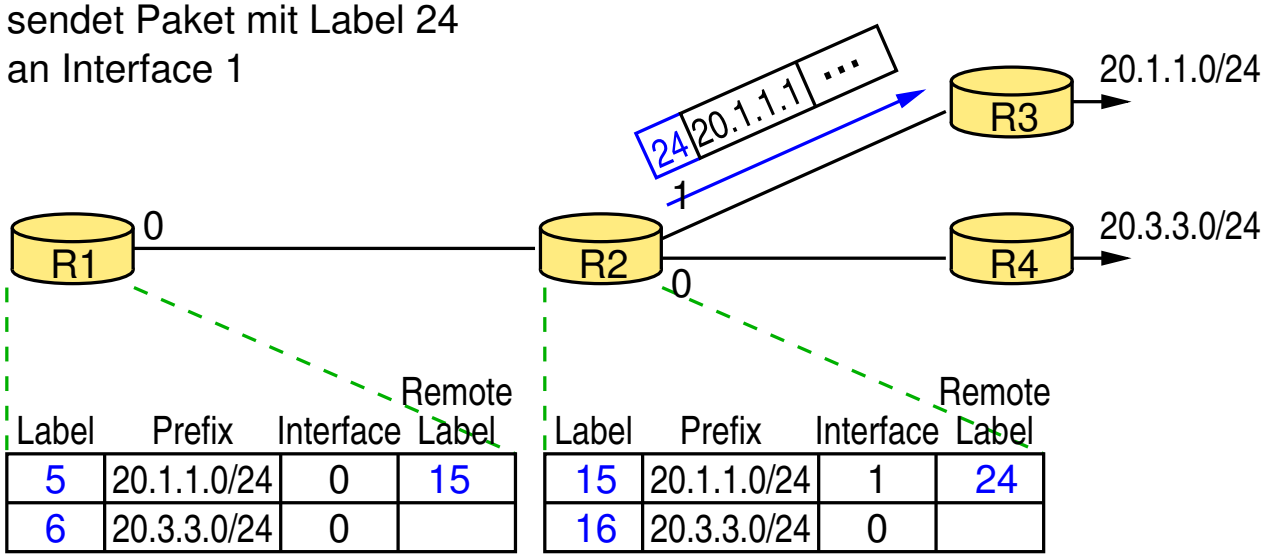
Ziel von MPLS (IETF RFC 3031)

- Vorteile der virtuellen Leitungsvermittlung für IP nutzen
- Ursprüngliche Motivation: effizientere Weiterleitung
  - IP: Suche des längsten Präfixes (CIDR!) aufwendig
  - Label ist typischerweise Index in Weiterleitungstabelle
    - schnelle Weiterleitung, Hardware-Implementierung
- Einsatz von MPLS heute:
  - Weiterleitung von IP-Paketen entlang expliziter Routen
  - Realisierung von Tunneln und virtuellen privaten Netzen
  - IP-Unterstützung für Switches, deren Hardware keine IP-Pakete verarbeiten kann

(Animierte Folie)

Funktionsprinzip von MPLS

R2 betrachtet nur Label, sendet Paket mit Label 24 an Interface 1



Label	Prefix	Interface	Remote Label
5	20.1.1.0/24	0	15
6	20.3.3.0/24	0	

Label	Prefix	Interface	Remote Label
15	20.1.1.0/24	1	24
16	20.3.3.0/24	0	

Anmerkungen zu Folie 154:

Die Information, welches IP-Netz über welches MPLS Label erreicht werden kann, wird durch das *Label Distribution Protocol* LDP (RFC 5036-5038) weitergegeben.

154-1

4.4 *Multiprotocol Label Switching ...*

Einfügen des Labels

- Bei den meisten Schicht-2-Protokollen (Ethernet, PPP, ...):
  - Einfügen zwischen Header von Schicht 2 und IP-Header:

PPP Header	Label Header	IP Header

  - MPLS ist „Schicht 2,5-Protokoll“

- Aufbau des MPLS-Headers (*MPLS Shim Header*):

0 … 20	20 … 23	23	24 … 31
Label	TC	S	TTL

  - **TC:** Traffic Class (für *Quality-of-Service*)
  - **S:** *Bottom of Stack*, kennzeichnet letztes Label

Anmerkungen zu Folie 155:

Im Schicht-2 Header wird dabei durch einen speziellen Protokolltyp gekennzeichnet, daß ein MPLS-Header folgt (z.B. im Ethernet durch den *Ethertype* 0x8847 für MPLS Unicast).

Dagegen steht im MPLS-Header nicht explizit, welcher Schicht-3 Header folgt. RFC 3032 legt fest, daß sich das Schicht-3 Protokoll immer eindeutig aus dem Label ergeben muß (indem z.B. für IP immer bestimmte Label verwendet werden).

155-1

4.4 *Multiprotocol Label Switching ...*

Explizite Routen

- MPLS ermöglicht Festlegung expliziter Pfade
  - analog zur virtuellen Leitungsvermittlung
  - Festlegung der Pfade z.B. über *Resource Reservation Protocol* (RSVP, siehe später: QoS)
    - RSVP-Nachrichten führen zur Reservierung von Puffer und Bandbreite auf dem ausgewählten Pfad
- Damit möglich z.B.:
  - quellenabhängige Routen
  - schnelles Rerouting bei Ausfall von Links
  - Dienstgütegarantien, z.B.:
    - Auswahl einer Route mit bestimmter Bandbreite
    - Nutzung der Route, auf der Ressourcen reserviert wurden

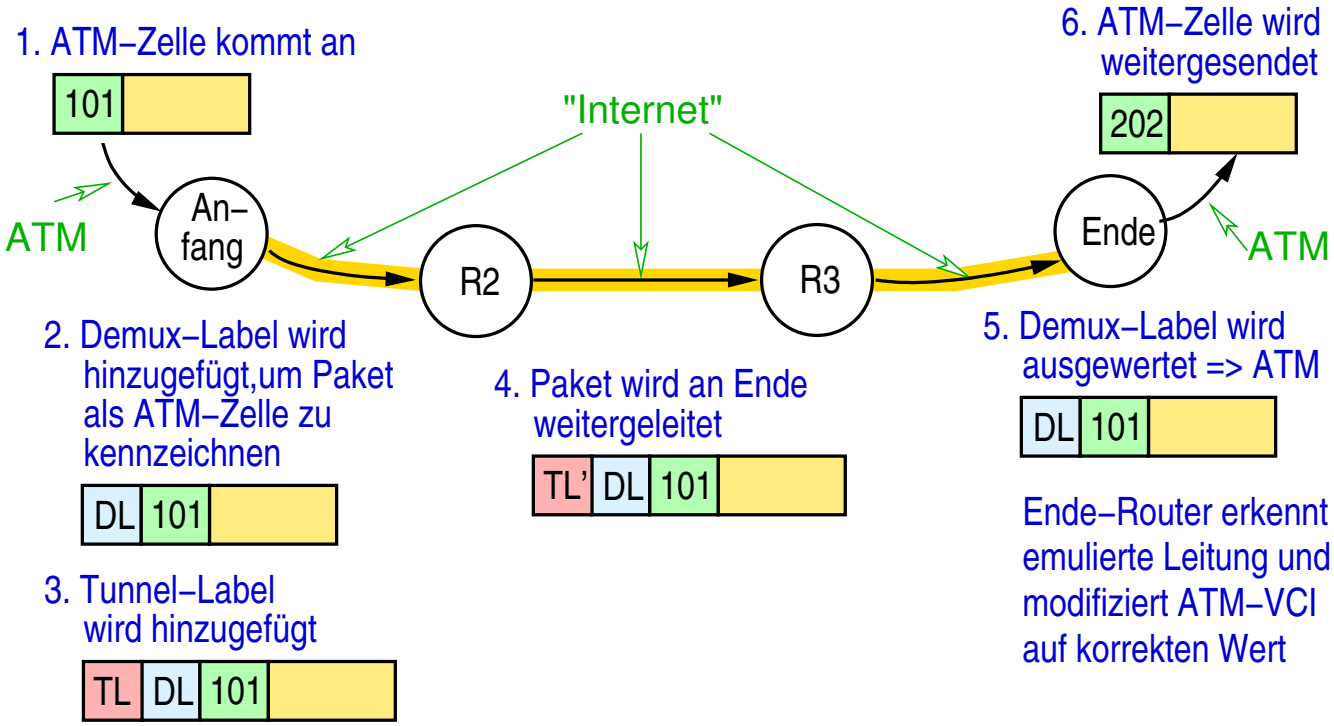
Tunnel und VPNs

- Prinzip wie bei IP-Tunnel:
  - Paket wird am Eingang des Tunnels mit MPLS-Label versehen, am Ausgang wird Label entfernt
- Vorteil gegenüber IP: Label ist kürzer als IP-Header
- Zum Demultiplexen am Tunnelende: weiteres MPLS-Label
  - letztes Label durch spezielles Bit gekennzeichnet
  - Tunnel damit für mehrere Verbindungen nutzbar
- Anwendung z.B.
  - Emulation von Schicht-2-Diensten, z.B. ATM über Internet
  - Realisierung von Schicht-3-VPNs
    - virtuelle, private IP-Netzwerke über Internet

Anmerkungen zu Folie 157:

Um bei Schicht-3-VPNs die Last des letzten MPLS-Routers zu verringern, wird typischerweise bereits vom vorletzten Router das MPLS Tunnel-Label entfernt (*Penultimate Hop Popping*). Ohne diese Maßnahme müsste der Router am Ende des Tunnels einen Label-Lookup durchführen, nur um festzustellen, daß er das Ziel ist und das Label entfernen muß, um das angekommene IP-Paket weiterbearbeiten zu können. Wenn bereits der vorletzte Router das Label entfernt, ist dieser Lookup nicht nötig.

Beispiel: Tunnelling von ATM-Zellen



Fazit

- MPLS kombiniert
  - label-basierte Weiterleitung der virtuellen Leitungsvermittlung

  mit
  - Routing- und Kontrollprotokollen von IP-Datagramm-Netzen
- Ergebnis:
  - Netzwerkklasse irgendwo zwischen leitungs- und datagrammvermittelnden Netzen

4.5 Zusammenfassung / Wiederholung

IP-Routing: Spezielle Aspekte

- IP Multicast
  - IGMP: Anmeldung und Abmeldung
    - Router erfährt, welche Gruppen im LAN vertreten sind
  - Link-State-Multicast
    - Berechnung spannender Bäume mit kürzesten Wegen
  - Distanzvektor-Multicast (*Reverse Path Multicast*)
    - Broadcast mit Zyklenvermeidung und *Pruning*
  - *Protocol Independent Multicast* (PIM), *Sparse Mode*
    - Wege der *Join*-Nachrichten ergeben Multicast-Baum
    - zunächst mit fester Wurzel (Rendezvous-Punkt)
    - Optimierung: quellenspezifische *Joins* bzw. Bäume

4.5 Zusammenfassung / Wiederholung ...

IP-Routing: Spezielle Aspekte ...

- Mobile IP
  - Heimatagent (HA) leitet Pakete über IP-Tunnel an Router des Fremdnetzes (oder mobilen Host (MH) selbst)
  - Proxy ARP: HA fängt Pakete an MH im lokalen Netz ab
- MPLS (*Multiprotocol Label Switching*)
  - Kombination von IP Datagramm-Vermittlung mit Weiterleitung aus virtueller Leitungsvermittlung
  - IP-Paket wird Label vorangestellt; Weiterleitung nur aufgrund des Labels
  - Einsatz: explizite Routen, Tunnels und VPN, ATM-Switches als *Label Switching Router*