

# IT2221 - Netzwerktechnik

Dozentin:

Gabriele Schrenk

[e\\_schrenk@doz.hwr-berlin.de](mailto:e_schrenk@doz.hwr-berlin.de)

## Insgesamt 10 Online-Vorlesungen mit BBB

1. Grundlagen, IP-Adressierung OSI-Modell, Ethernet (Labor)
2. Layer 1 und 2 an den Beispielen Ethernet und WLAN
3. Layer 3 am Beispiel von IPv4 und Routingprotokollen
4. Layer 3 Routen zusammenfassen, IPv6 und DSL
5. Layer 4 (TCP und UDP), Layer 3 NAT, L7 DNS
6. Troubleshooting, Routingprotokoll BGP, Weitverkehrsnetze (MPLS)
7. Weitverkehrsnetze, Ausfallsichere Netze
8. Netzwerksicherheit
9. Wiederholung, offene Fragen, Bewertung Vorlesung/Labore
10. Prüfungsvorbereitung

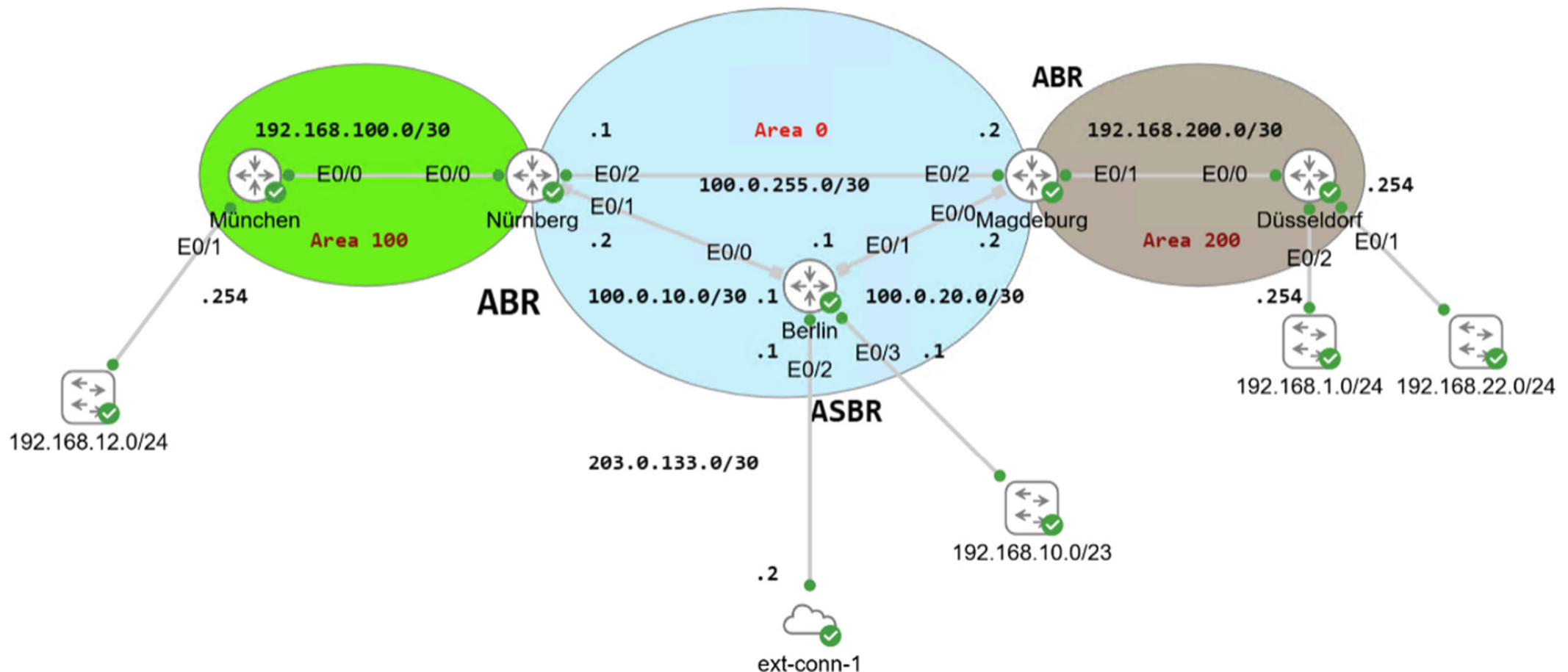
Klausur im Stundenplan, **Mo., 4. Mai 2026** von **14:00 bis 16:00 Uhr**  
in den Räumen **6B.369** und **6B.371** statt.

- Raum **6B.369** ist länger reserviert für Nachteilsausgleich
- Betreuer: Schrenk und Albaradie

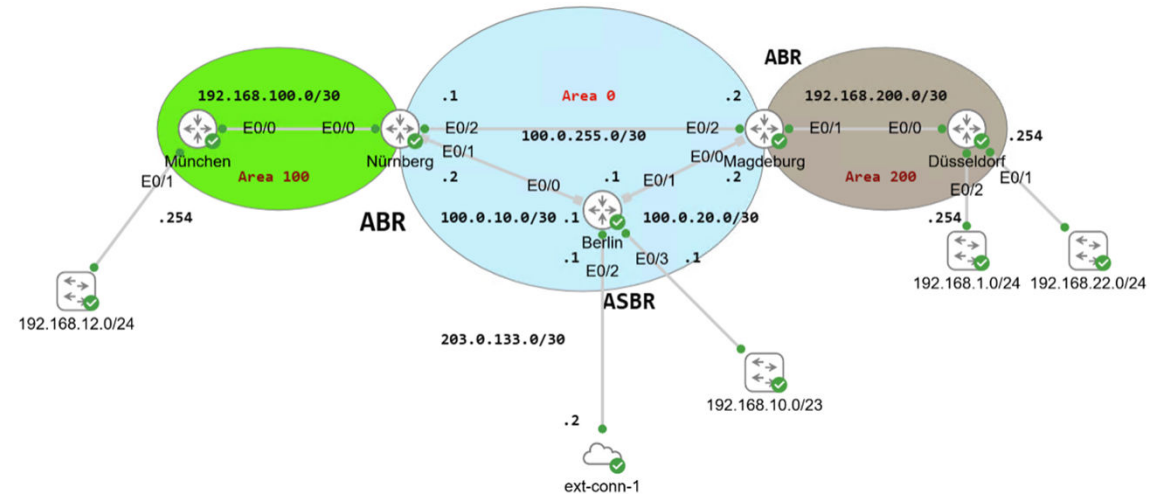
Eine praktische Prüfung ist nicht vorgesehen laut Curriculum

Im Curriculum ab dem **Jahr 2025 (IT25)** ist die Prüfungsleistung eine kombinierte Prüfung mit einer Klausur (K) im Bereich „Netzwerke“ und einer Laborausarbeitung (L) im Bereich „Labor Netzwerke“

## Netzwerke können Fehler enthalten



- PC bekommt keine IP Adresse
- PC erreicht einen bestimmten anderen PC nicht
- Router in Magdeburg und Düsseldorf bauen keine OSPF-Nachbarschaft auf



**Schritt 1:** Problem definieren (Was funktioniert nicht?)

**Schritt 2:** Informationen sammeln (Befehle anzeigen)

**Schritt 3:** Daten analysieren (Routingtabellen,  
Nachbarzustände)

**Schritt 4:** Hypothese formulieren (Welche OSI-Schicht?)

**Schritt 5:** Hypothese testen (Paketmitschnitte, PCAPs)

**Schritt 6:** Korrektur planen/implementieren

**Schritt 7:** Überprüfen, bzw. testen und dokumentieren

## Statusinformationen der Router und Switches

show ip route

show ip interface / show interface

show ip ospf neighbor /database

show dhcp server leases

## Nutzung von Netzwerk-Diagnose-Tools

Ping

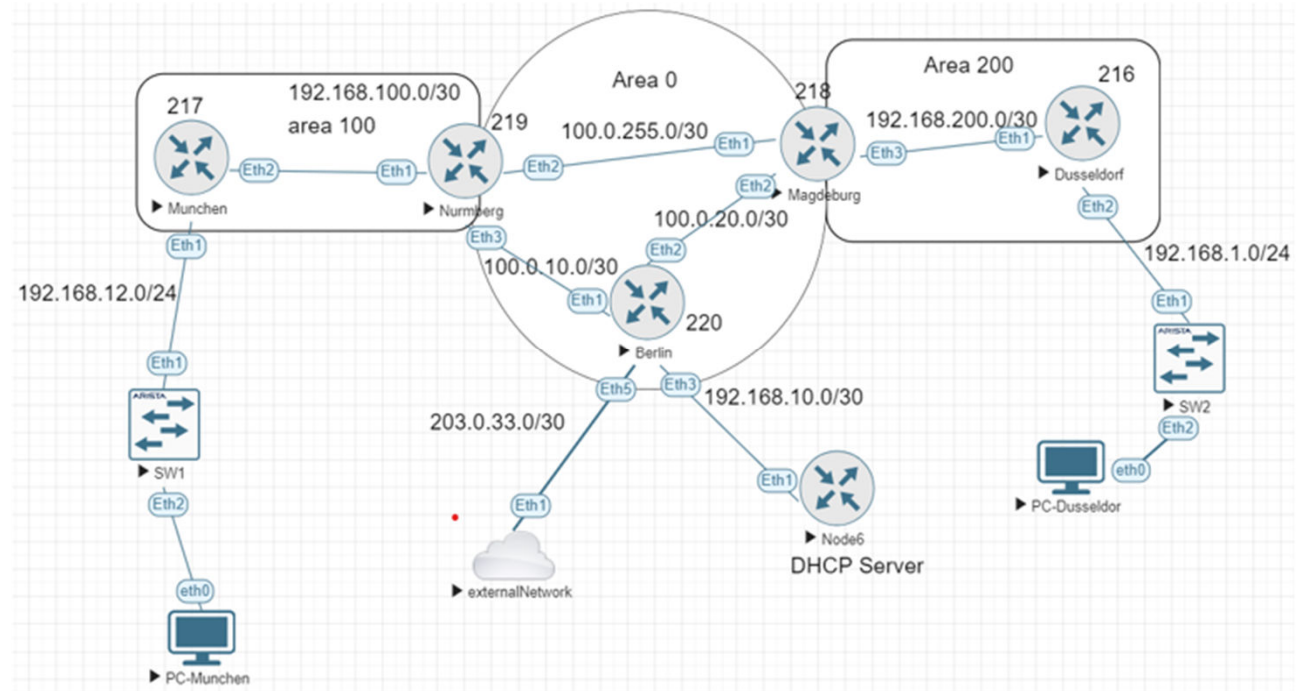
Traceroute

Packet Capture (PCAP)

1. PC bekommt keine IP Adresse

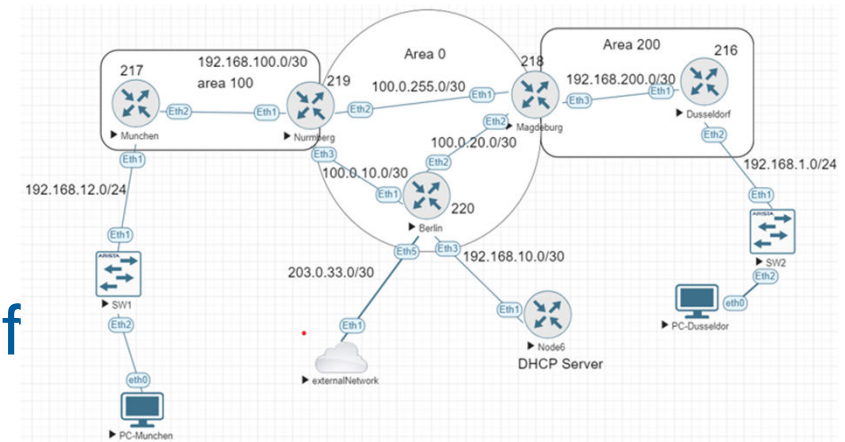
2. PC erreicht einen anderen PC nicht

3. Router in Magdeburg und Düsseldorf bauen keine OSPF-Nachbarschaft auf



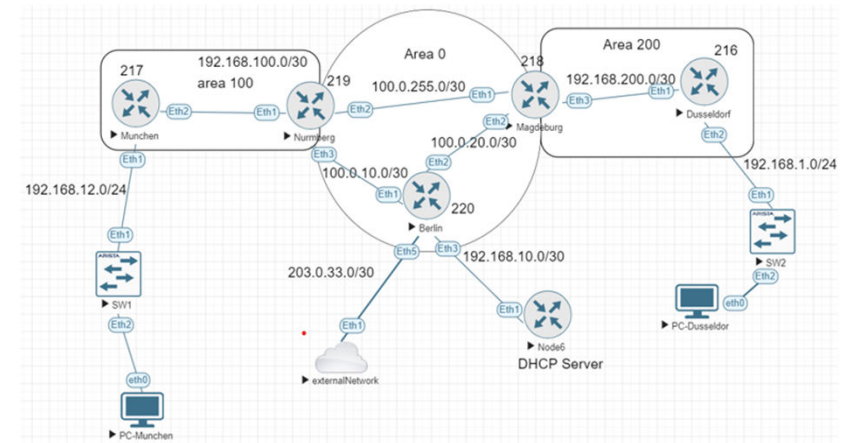


- PC München kann keine IP-Adresse beziehen:
  - Fehler A – Helper-Adresse auf falschem Interface
    - Discover-Pakete wurden auf der Verbindung SW1–München empfangen, es wurde jedoch nichts nach Nürnberg weitergeleitet
  - Fehler B – Helper-Adresse verweist auf die falsche IP-Adresse
    - Relayed Discover wurde auf der Verbindung München–Nürnberg empfangen, jedoch mit der falschen Ziel-IP-Adresse. Es wird kein Angebot zurückgesendet.
    - PC München bekommt keine IP Adresse



## 2. Troubleshooting Szenario

- PC München kann PC Düsseldorf nicht erreichen:
  - Fehler A – OSPF-Area Mismatch
    - Keine Nachbarschaft zwischen München und Nürnberg
    - Überprüfen der OSPF-Hello-Pakete
  - Fehler B – Fehlende OSPF-Aktivierung auf dem Interface für Magdeburg
    - Keine OSPF-Hello-Pakete



### 3. Troubleshooting Szenario

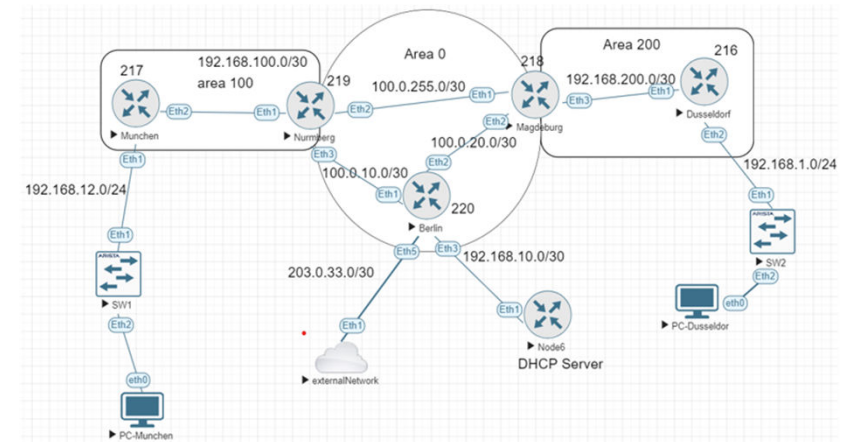
- Magdeburg und Düsseldorf sind keine OSPF-Nachbarn:

- Failure A — OSPF  
Hello/Dead Timer Mismatch

- OSPF-Hello-Nachrichten werden zwar ausgetauscht, jedoch nicht mit derselben Häufigkeit, und es werden keine Nachbarschaften gebildet

- Failure B — Falsche Subnetzmaske auf dem München–Nürnberg-Link

- OSPF Hellos werden ausgetauscht, aber keine Nachbarschaft gebildet



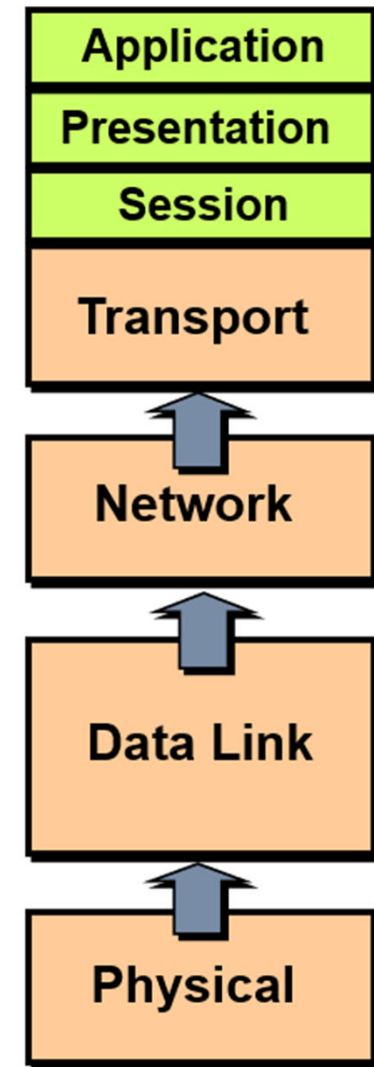
Application Layer - Anwendungsschicht

# LAYER 7

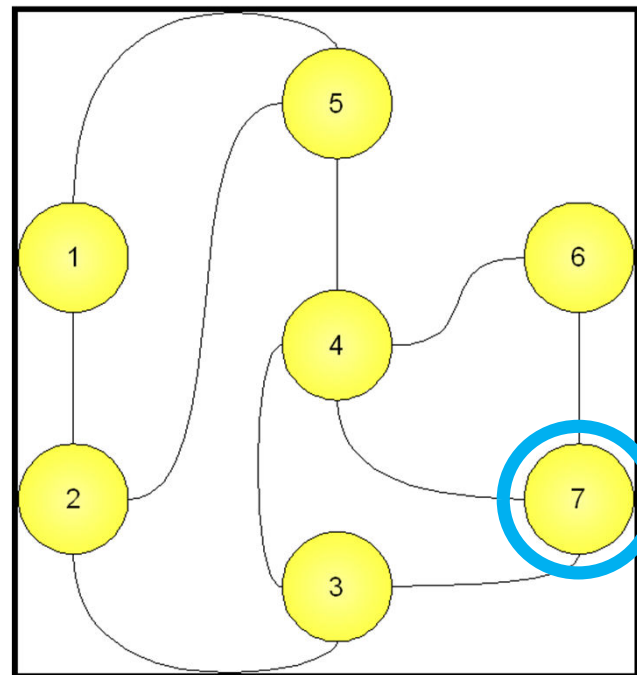
- Anzahl der Netze (Prefixes): 1.064.462 (947.805)
- Anzahl Routing-Tabellen-Einträge: 600.307 (530.557)
- Anzahl der Autonomen Systeme: 78.423 (75.746)
- Größtes AS:  
Anzahl Prefixes: 16.509 Amazon-02, US
- Größte Anzahl Adressen: 227.731.200/32 AS749 DNIC  
United States Department of Defense (DoD), US  
IP-Adressbereiche, die ein AS über BGP meldet

täglich aktuelle Zahlen: <https://www.cidr-report.org>

- Standardisiert IETF RFC 4271 von Januar 2006
- Routing Protocol
  - Path Vector Protocol
- **kommuniziert über TCP-Port 179**
- überträgt Netzmasken (Classless)
- Nachbarschaften müssen konfiguriert werden
- Kein Load Balancing
- Routen müssen stabil sein
- Authentifizierung der Nachbarn möglich
- Router kann nur zu einem AS gehören



- Router kennen die Pfade durch das Netz vollständig
- Schleifen werden dadurch erkannt
- Routingtabelle klein halten
  - Weitergeben des kürzesten Pfades pro Interface



Element	Vektor
1	4 - 5 - 1
1	3 - 2 - 1
1	6 - 4 - 5 - 1
2	3 - 2
2	4 - 3 - 2
2	6 - 4 - 3 - 2
3	3
3	4 - 3
3	6 - 4 - 3
4	4
4	3 - 4
4	6 - 4
5	3 - 2 - 5
5	4 - 5
5	6 - 4 - 5

Quelle Wikipedia <https://de.wikipedia.org/wiki/Pfadvektorprotokoll>

- Metrik: Anzahl der AS auf dem Weg
- Routen-Auswahl erfolgt in 9-stufigem Verfahren
- Konvergenzzeit liegt bei einigen Minuten
- BGP trägt immer nur eine Route pro Netz in die allgemeine Routing-Tabelle ein
- Schleifenvermeidung: Es werden keine Routen akzeptiert, in deren AS\_Path das eigene AS auftaucht.



## 1 – OPEN

- Erste Nachricht nach Aufbau der TCP Verbindung
- Keepalive als Antwort auf ein Open

## 2 – UPDATE

- Enthalten die Routing Informationen der Peers
- Erlauben ein Sicht auf die Topologie inkl. aller AS
- Erkennen von Routing-Schleifen
- Zurückziehen von nicht mehr aktuellen Routen

## 3 – NOTIFICATION

- Mitteilung von Fehlersituationen (z.B. Timer Expiry) -> Abbruch BGP Verbindung

## 4 – KEEPALIVE

- Periodische Nachrichten zum Erhalt der Verbindung

- LOCAL\_PREF
  - wählt den bevorzugten Weg, um Daten aus dem AS zu senden
  - höchster Wert gewinnt
- AS\_PATH
  - wählt bei Verbindungen zu mehreren AS dasjenige aus, über welches Daten empfangen werden sollen
  - mehrfaches Anhängen der eigenen AS-Nummer
- Multi\_Exit\_Disc (MED)
  - wählt aus mehreren Verbindungen zu einem Nachbar-AS diejenige aus, über die Daten empfangen werden sollen
  - niedrigster Wert gewinnt

1. **Bevorzuge Weg mit höchster LOCAL\_PREF.**
2. Bevorzuge Routen, die von dem aktuellen Router stammen.
3. **Bevorzuge Weg mit kürzestem AS\_PATH.**
4. Bevorzuge Weg mit kleinstem ORIGIN Wert (IGP vor EGP).
5. **Bevorzuge Weg mit kleinstem MED-Wert (MULTI\_EXIT\_DISCRIMINATOR). (Eingang in das AS von extern)**
6. **Bevorzuge Routen aus eBGP vor Routen aus iBGP.**
7. Bevorzuge Weg über den kürzesten IGP-Nachbarn.
8. Bevorzuge den Nachbarn mit der kleinsten Router-ID.
9. Bevorzuge den Nachbarn mit der kleinsten IP-Adresse.

## Transit

- Übermittlung von Daten zwischen einem AS und dem Internet gegen Bezahlung

## Peering

- Vereinbarung zum gegenseitigen Austausch von Daten zwischen zwei AS und der an sie angeschlossenen Systeme (in der Regel ohne Bezahlung).
- privates oder öffentliches Peering

Einteilung der Internet Service Provider (ISPs)

Tier 1 (Deutsche Telekom, AT&T, Orange, NTT etc.)

- landesweiter oder internationaler Provider
- nur Peering

Tier 2 (Vodafone, Swisscom, 1&1, DFN etc.)

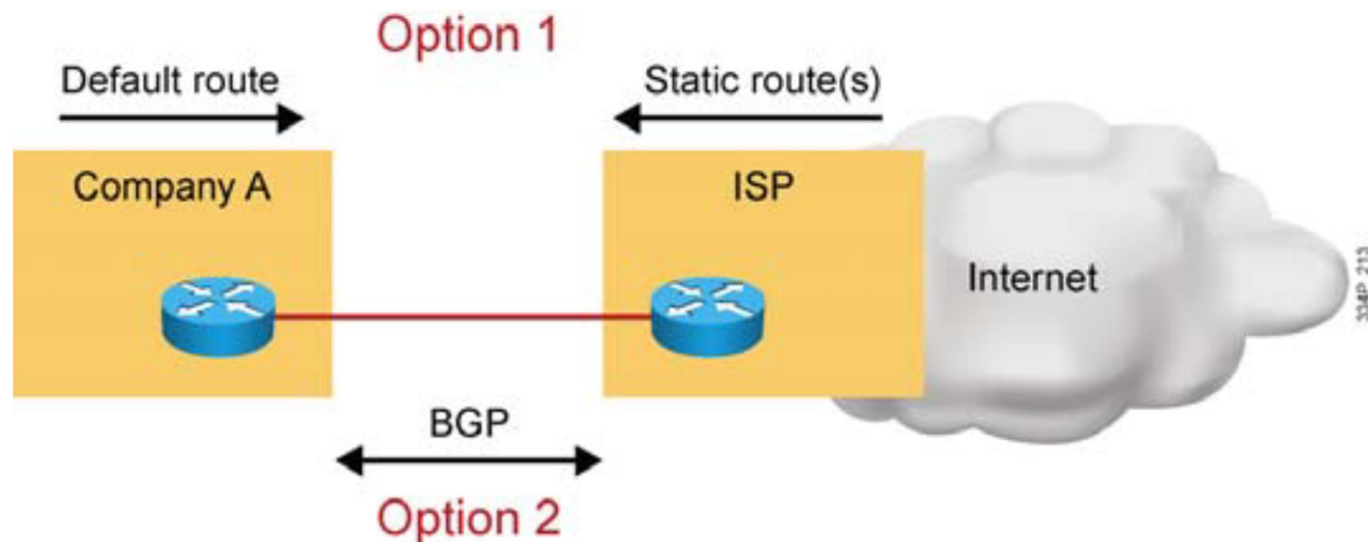
- landesweiter Provider
- Peering und Transit

Tier 3 (z. B. wilhelm.tel, M-Net, EWE TEL, etc.)

- regionaler oder lokaler Provider
- hauptsächlich Transit, selten Peering

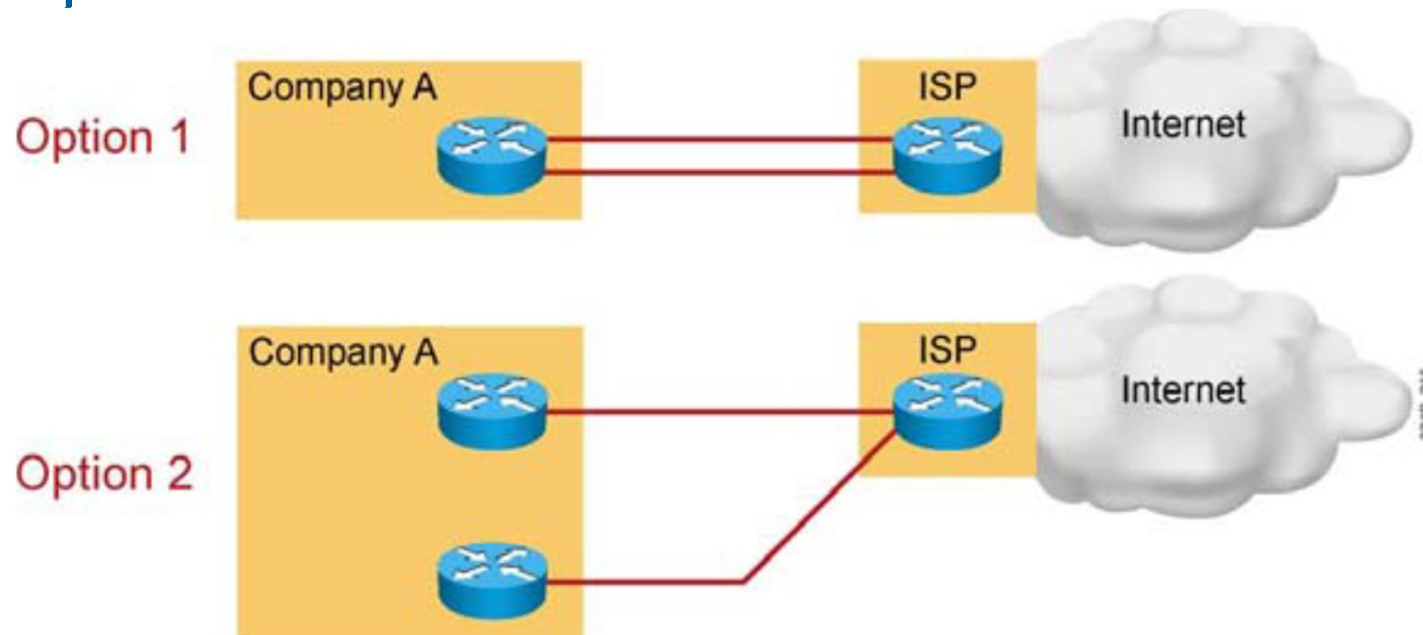
## BGP: Anbindung an Provider

- Single Homed
  - statische Routen oder
  - BGP, falls öffentliches Netz mit häufigen Änderungen
  - private AS-Nummer



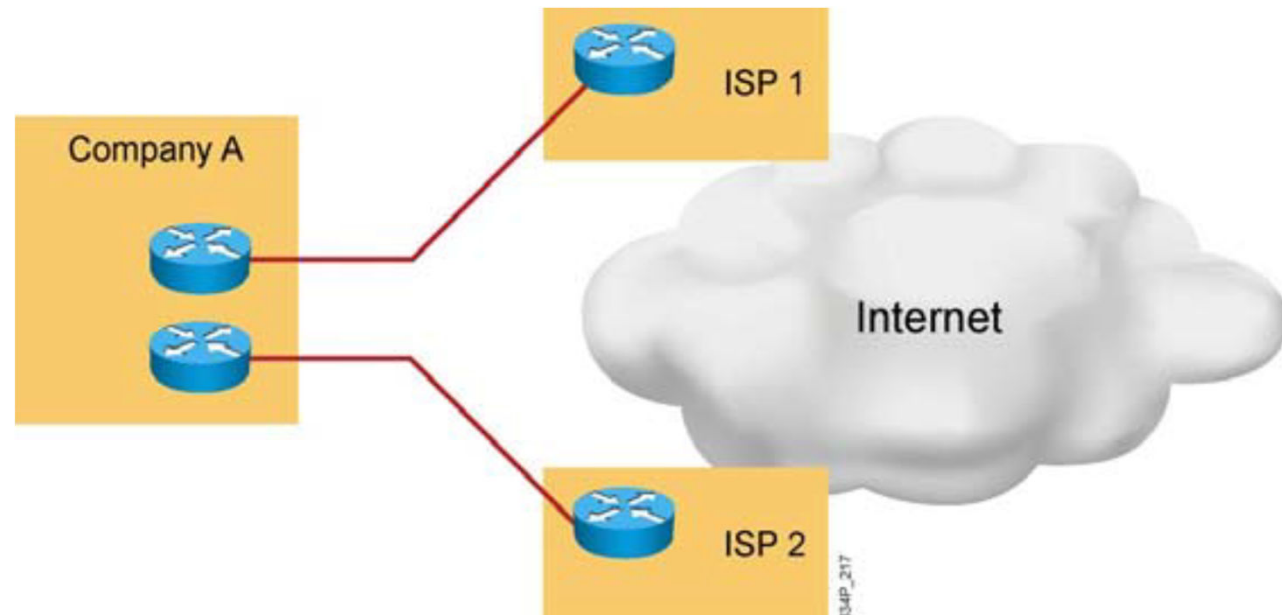
## BGP: Anbindung an Provider

- Dual Homed
  - mehrere Verbindungen zu einem Provider
  - BGP oder statische Routen
  - private AS-Nummer



## BGP: Anbindung an Provider

- (Dual) Multi Homed
  - Verbindungen zu mehreren Providern
  - BGP-Routing
  - öffentliche AS-Nummer

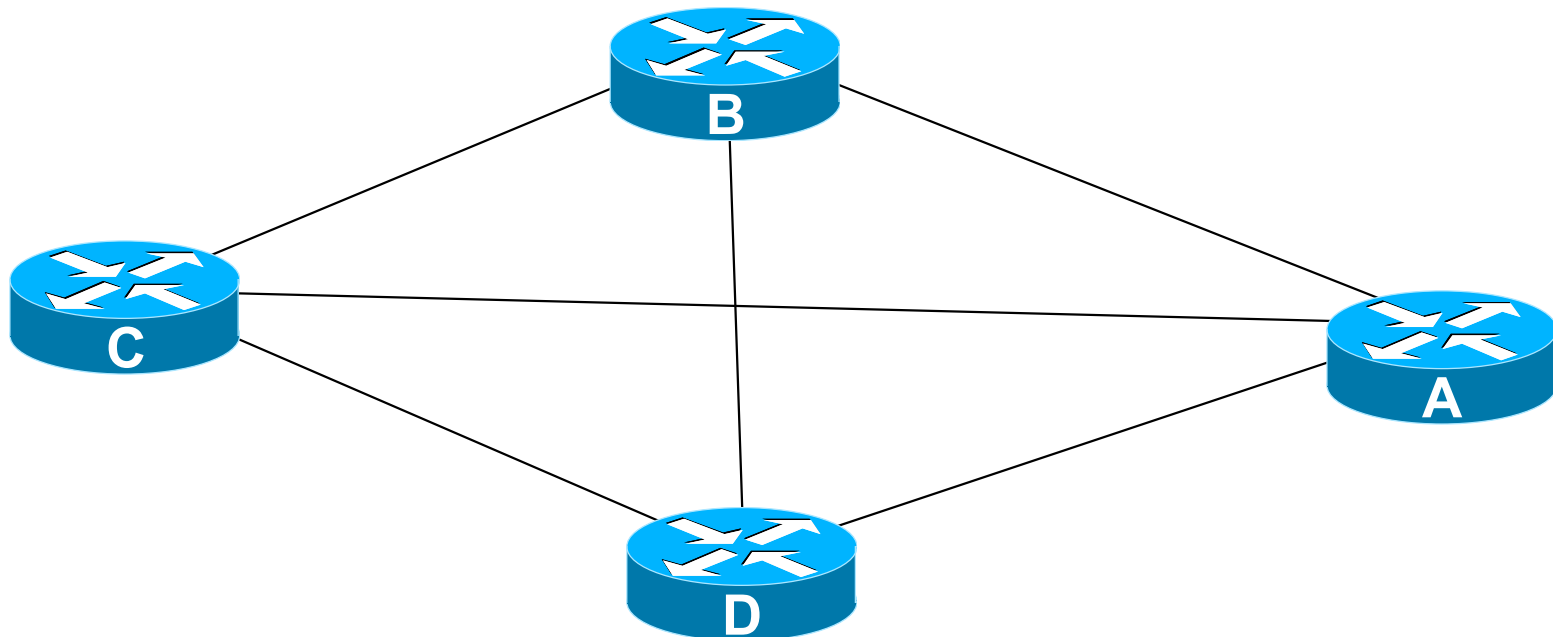




- Internes BGP innerhalb des ISPs
- alle BGP-Router eines AS müssen miteinander kommunizieren
  - iBGP = beide Nachbarn gleiche AS
  - eBGP = beide Nachbarn unterschiedliche AS
- bei eBGP sind Nachbarn direkt verbunden
- bei iBGP Erreichbarkeit über IGP (OSPF/IS-IS)

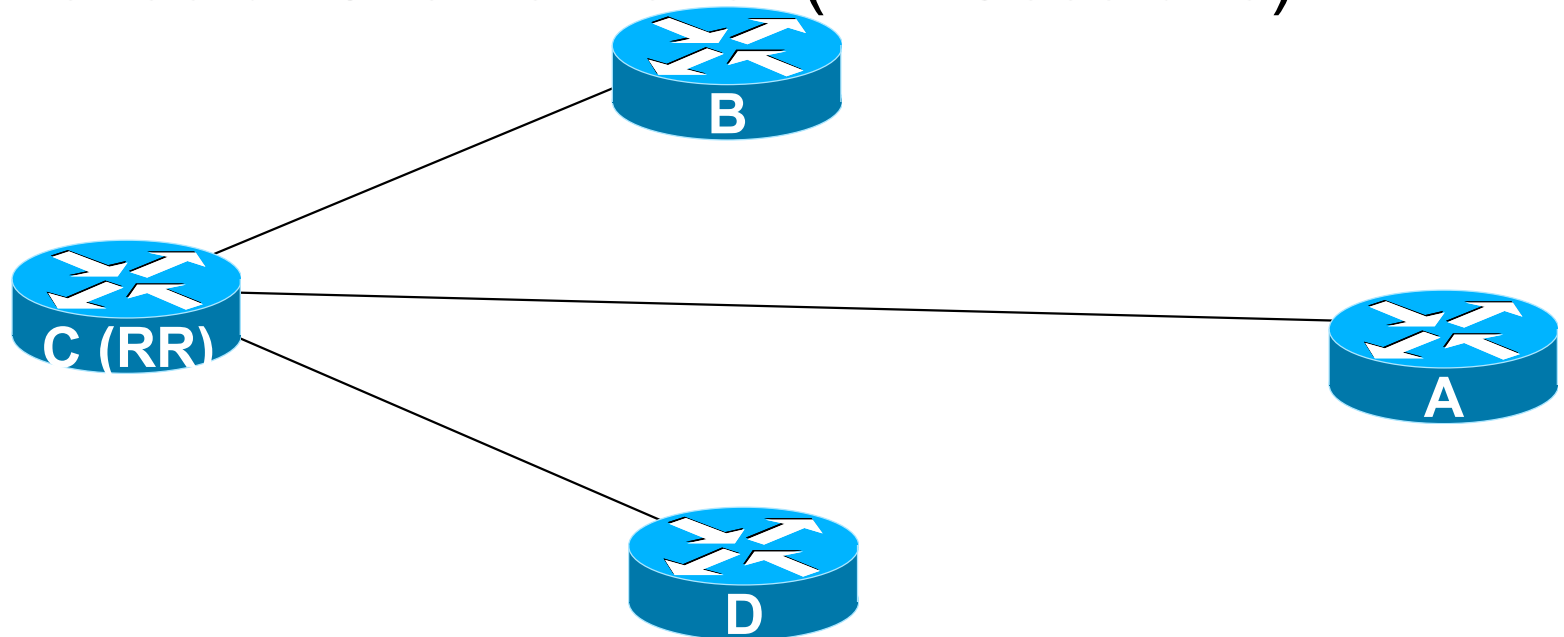
## iBGP: Route-Reflector

- Problem:  
Jeder BGP-Router in einem AS muss mit allen anderen BGP-Routern eine Nachbarschaft aufbauen (Vollvermaschung,  $n*(n-1)/2$  Sessions).



## iBGP: Route-Reflector

- Lösung:  
Jeder BGP-Router in einem AS baut nur mit einem Router (Route Reflector) eine Nachbarschaft auf. Dieser leitet empfangene BGP-Messages an die Route-Reflector Clients weiter (n-1 Sessions).

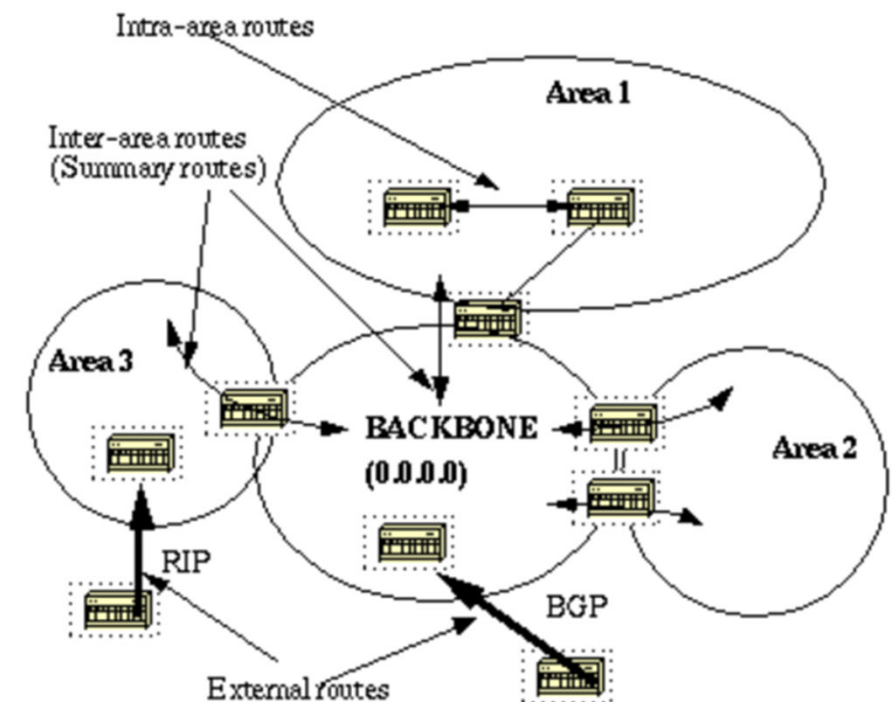


## Auswahl des besten Pfades

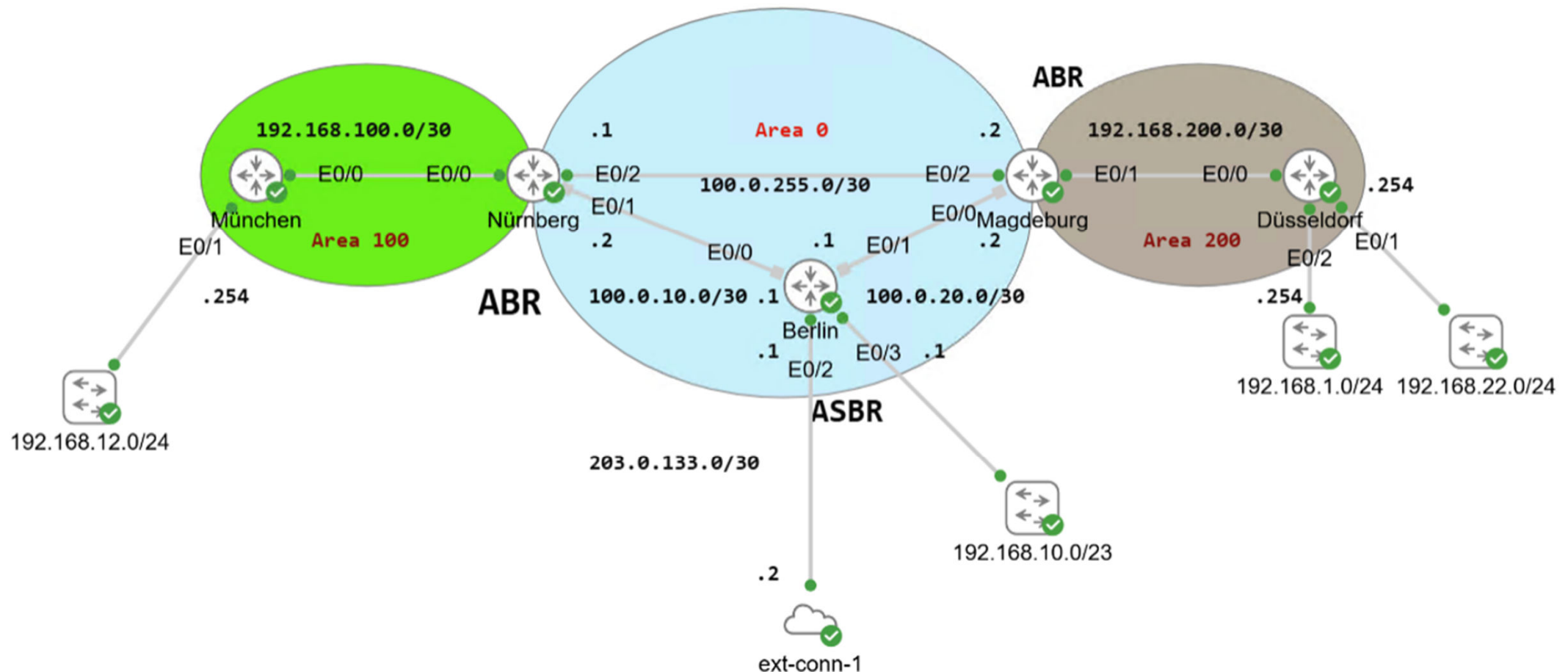
- Kriterium zur Bestimmung der Verwendung
  - Routing-Protokoll falls mehrere Protokolle Routen zum gleichen Ziel besitzen.
  - Mittel zur Vertrauenswürdigkeit der Quelle
  - Lokale Bedeutung, nicht genutzt bei Routing-Updates
- Umrechnung zwischen unterschiedlichen Metriken nicht möglich
- Administrative Distanz legt Reihenfolge der Routing Protokolle fest

• Connected interface:	0
• Static route:	1
• EIGRP (Enhanced Interior Gateway Routing Protocol)	
Summary route:	5
• External BGP:	20
• Internal EIGRP:	90
• IGRP (Interior Gateway Routing Protocol):	100
• OSPF (Open Shortest Path First):	110
• IS-IS (Intermediate System-to-Intermediate System):	115
• Routing Information Protocol (RIP):	120
• Exterior Gateway Protocol (EGP):	140
• External EIGRP:	170
• Internal BGP:	200
• Unknown:	255

- Verbinden verschiedener Routing Protokolle
- Verteilung IGP Routen (z.B. OSPF) zu BGP
- Befehl „redistribute“ mit Angabe des Protokolls:
  - `redistribute connected`
  - `redistribute ospf`
- Es müssen immer beide Richtungen konfiguriert sein!



- Verbinden verschiedener OSPF-Areas
- Verbindung nach extern über BGP

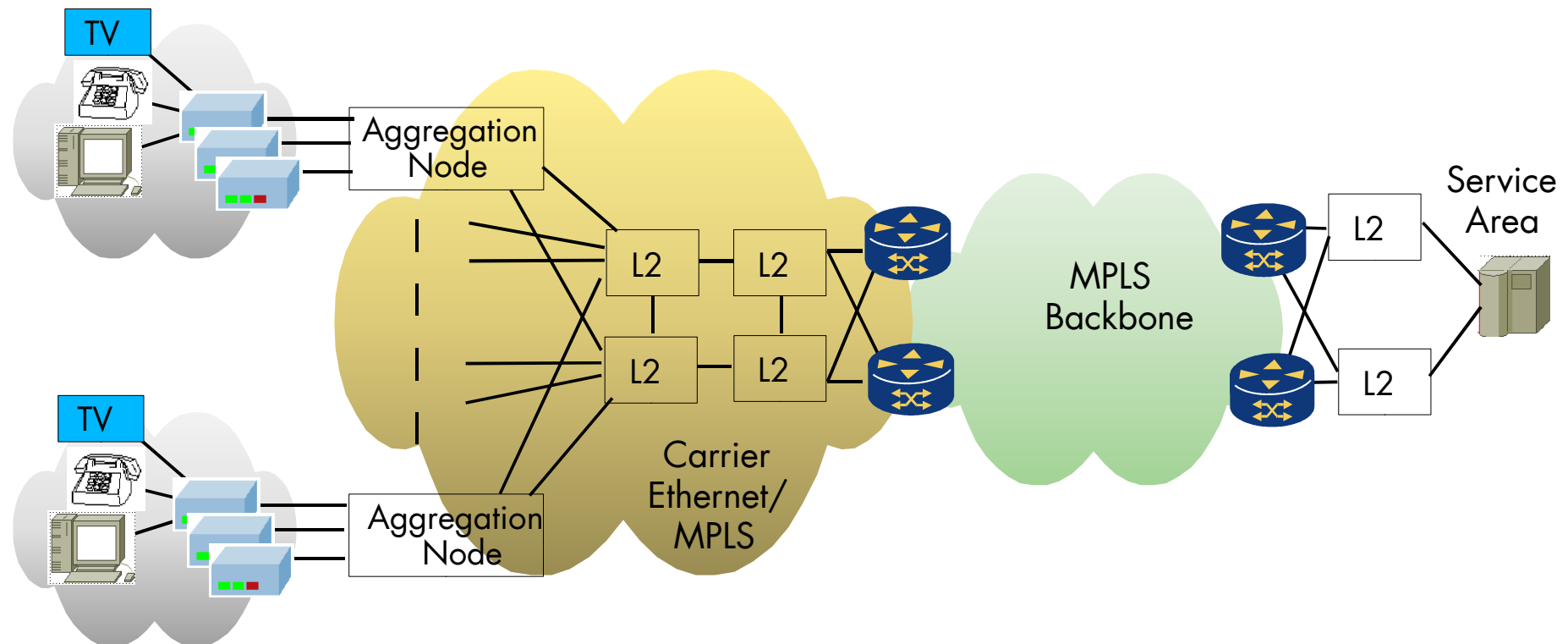


Network Layer - Vermittlungsschicht

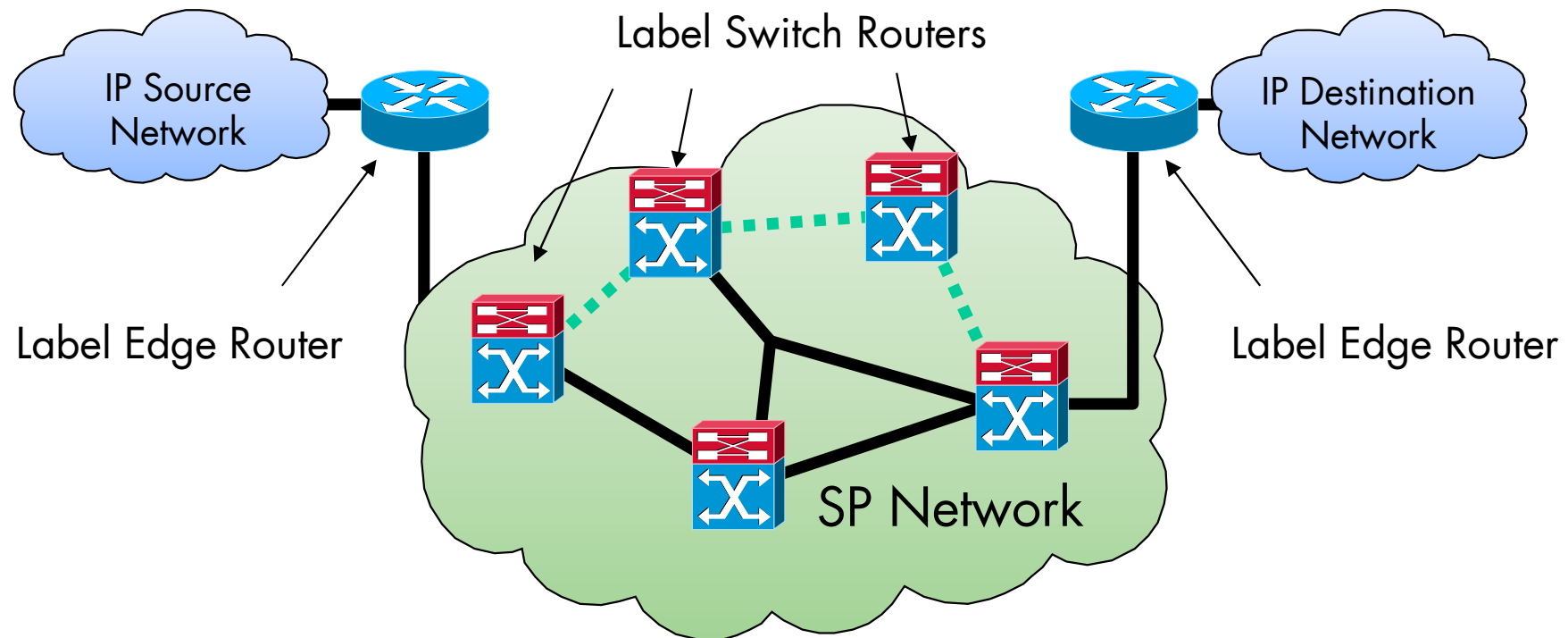
# LAYER 3



- Unternehmen und private Haushalte sehen in der Regel keinen MPLS Verkehr
- Bietet Mechanismen für Ethernet und IP Virtual Private Networks (VPNs) für Layer 2 und Layer 3



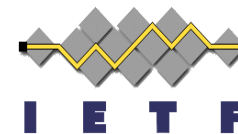
- MPLS nutzt Labels für die Wegewahl der Datenpakete
- Überträgt Daten über Label Switched Paths (LSPs)
  - Pfade werden über Signalisierungsprotokolle aufgebaut
- Bietet Fast Reroute Protection (unter 50ms)



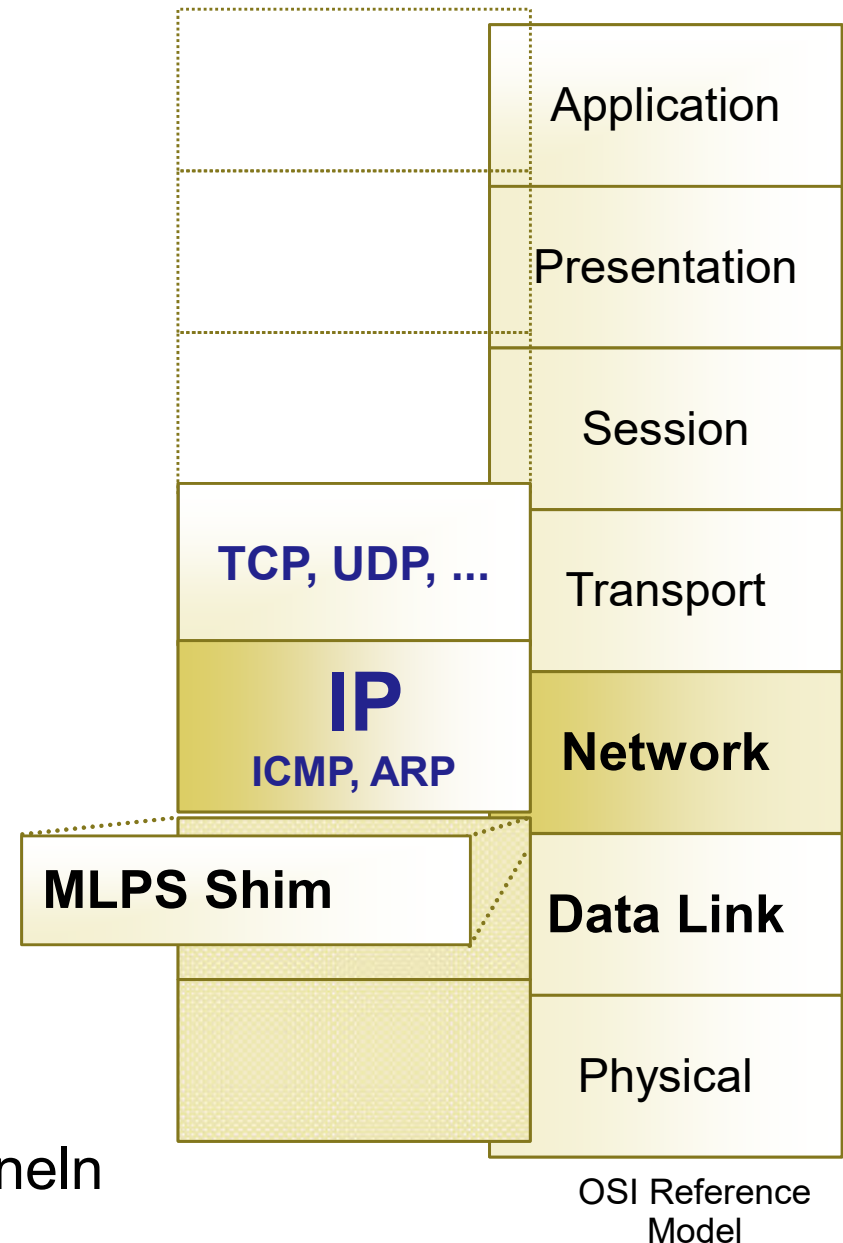
- MPLS weit verbreitet in IP Carrier / SP Netzen

	IP	MPLS
Data Plane	<ul style="list-style-type: none"><li>• Routing table</li><li>• Lookup for outgoing (egress) interfaces</li></ul>	<ul style="list-style-type: none"><li>• Label pushing, swapping and popping</li></ul>
Control Plane	<ul style="list-style-type: none"><li>• Routing protocols</li></ul>	<ul style="list-style-type: none"><li>• Extended routing protocols (OSPF-TE, ISIS-TE)</li><li>• Label distribution protocols (LDP, RSVP-TE)</li><li>• Discovery protocols (BGP)</li></ul>

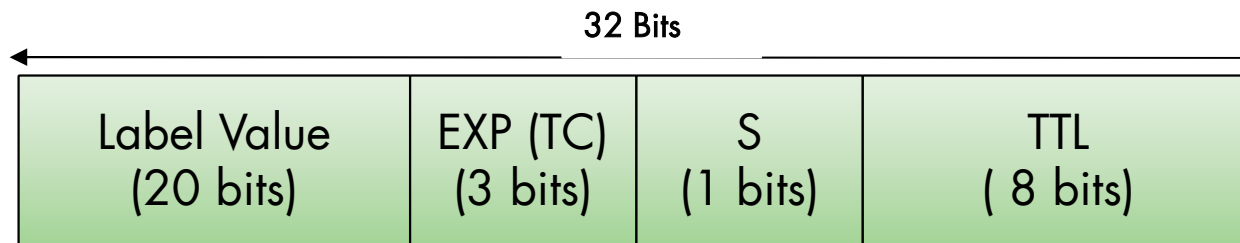
- IETF Standardisiert MPLS in diversen RFCs
- <https://datatracker.ietf.org/wg/mpls/documents/>



- Routing-Entscheidung nicht mehr für jedes Paket einzeln
- Route wird am Eintrittspunkt festgelegt (Ingress-Router)
- Alle zusammengehörigen Pakete erhalten einheitliches Label
- Label wird am Austrittspunkt (Egress-Router) entfernt
- Ingress und Egress Router müssen sich kennen (IGP)
- Signalisierung der Route über LDP, Label Distribution Protocol
- Aufbau von Layer-2 oder Layer-3 Tunneln

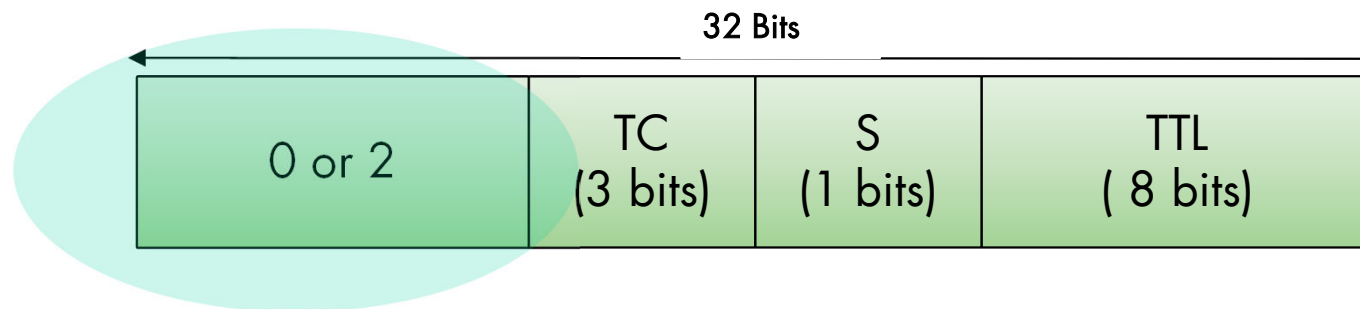


- IETF RFC 3032, “MPLS Label Stack Encoding”
- Besteht aus 4 Feldern
  - Label: Label Value - 20 bits
  - EXP: Experimental Use - 3 bits;
  - In RFC 5462 renamed to Traffic Class (TC)
  - S: Bottom of Stack - 1 bit
  - TTL: Time To Live - 8 bits

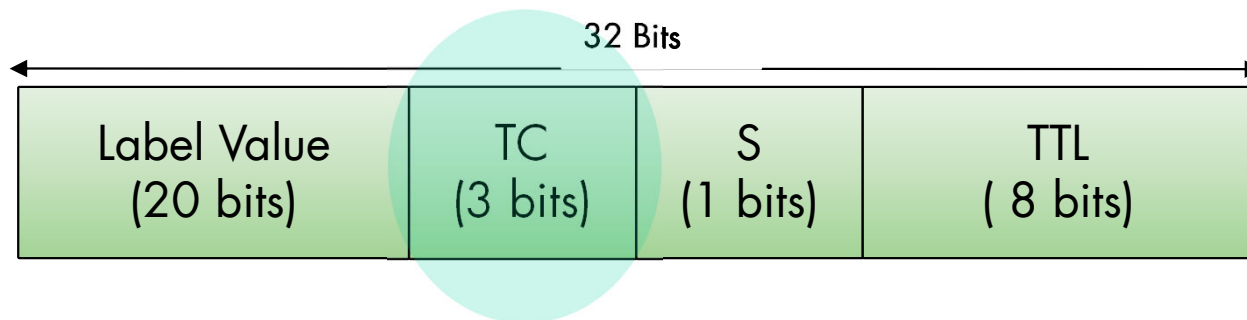


- Values 0 and 2
  - Explicit null labels
- Value 1 - Router Alert Label
  - Forward packet to local software instance
- Value 3
  - Implicit null label
- Values 4 - 15
  - Are reserved for future use – RFC 3032
  - Value 13
    - Reserved as Generic Associated Channel(GAL) – RFC 5586
  - Value 14
    - Reserved as the OAM Alert Label – RFC 3429
- Values 16 -  $2^{20}$ 
  - Normal label swap operation between incoming and outgoing labels

- Values 0 and 2
  - **Identifiziere den Inhalt des Pakets nach dem MPLS Label Stack**
    - Muss das unterste Label auf dem MPLS Stack sein
    - Eventuell Pushed am Ingress – zusätzlich zum LSP label
    - Muss entfernt werden am Penultimate Hop – danach Weiterleitung auf Basis IP header
  - Value 0 – IPv4 header
  - Value 2 – IPv6 header

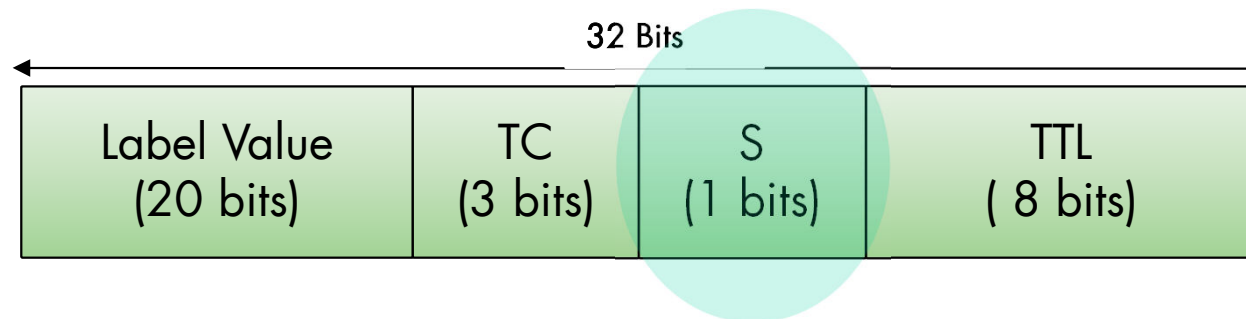


- Verwendet bei MPLS DiffServ (Differentiated Services)
- DiffServ nutzt das Feld zur Speicherung der Class of Service Information
  - DiffServ speichert hier die Drop Precedence oder CoS ID
  - Wenn MPLS DiffServ deaktiviert – keine Bedeutung

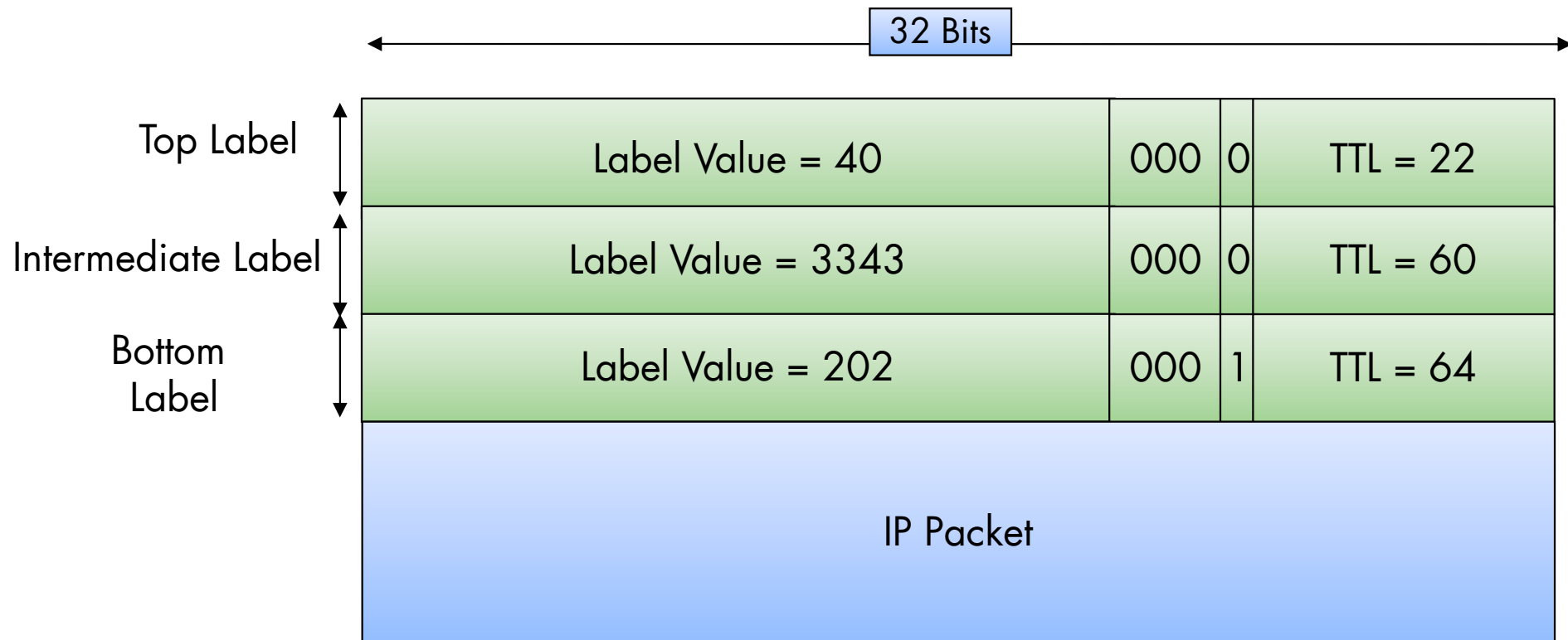




- Ein MPLS Paket kann mehrere Labels besitzen
  - “Label stack”
  - Erlaubt Bildung von LSP Hierarchien
- Bottom of Stack gesetzt auf 1
  - Identifiziert das letzte Label auf dem Label Stack
  - Ist nur ein Label vorhanden, muss das S Bit auf 1 gesetzt sein
  - LSR prüft das Bit, bevor das Label entfernt wird



- Das S-Bit aller Label auf 0 gesetzt
- Nur beim letzten Label wird S-Bit auf 1 gesetzt.



- Jeder LSR pflegt eine MPLS Forwarding Matrix
  - Ein im Netz vorhandener LSR weist Incoming und auch Outgoing Label zu

FEC	In Label	Out Label	Next Hop	Action
10.1.1/24	50	40	LSR4	Swap

FEC = Forwarding Equivalence Class

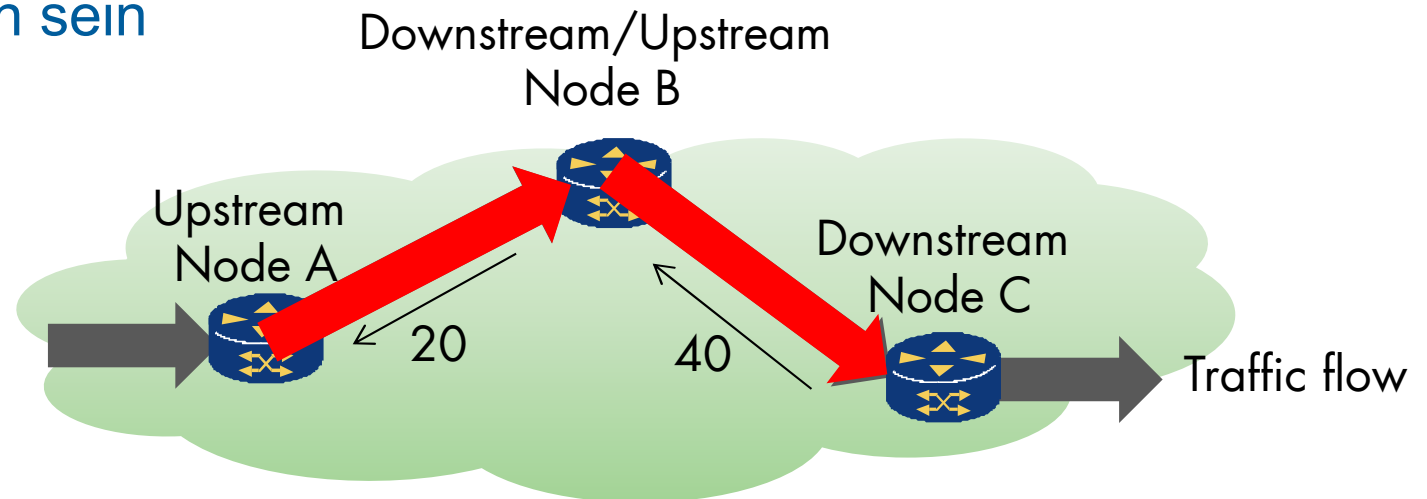
- Am Eingang (Ingress) LSR/LER, Matrix ohne Incoming Label

FEC	In Label	Out Label	Next Hop	Action
10.1.1/24	-	20	LSR2	Push

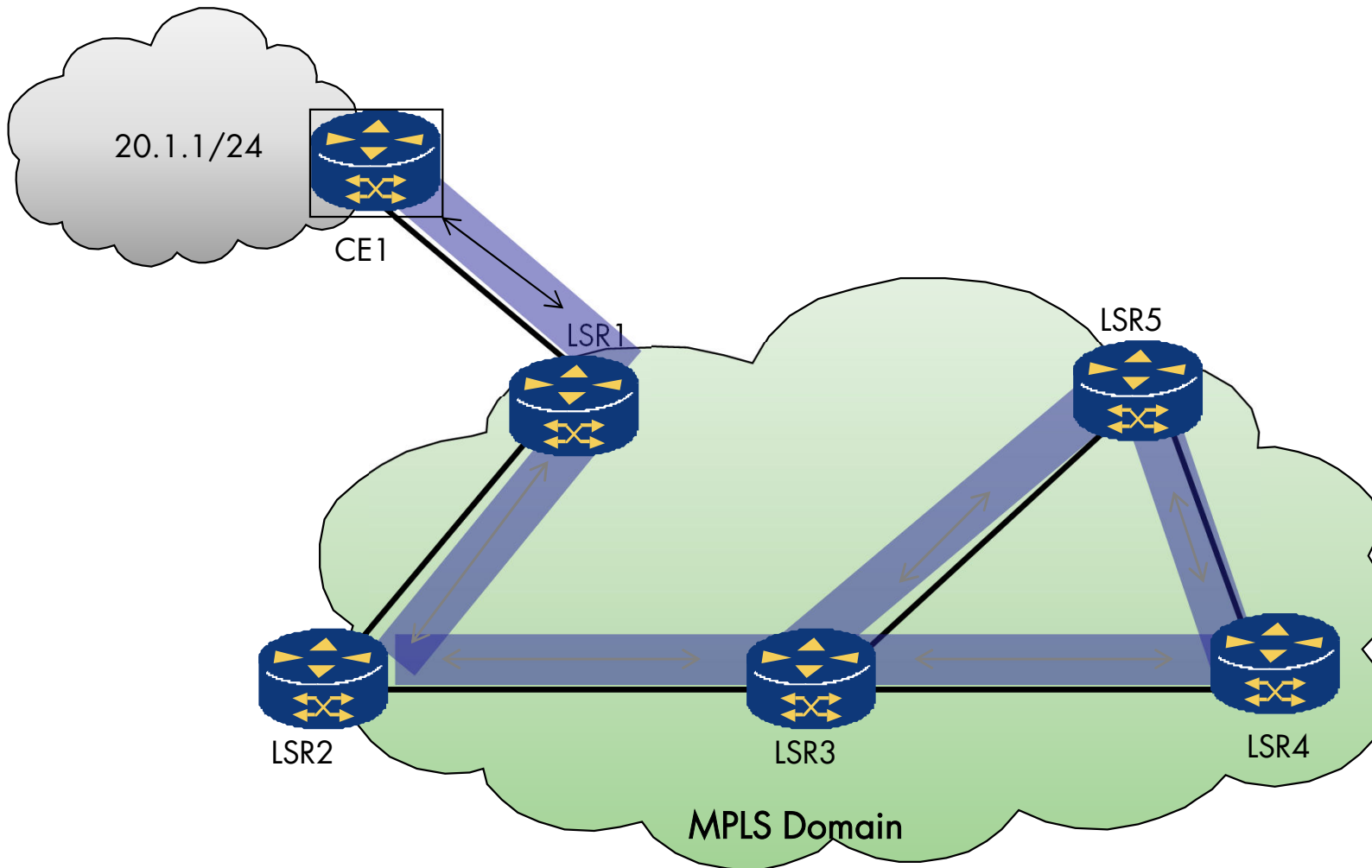
- Am Ausgang (Egress) LSR/LER, Matrix ohne Outgoing Label

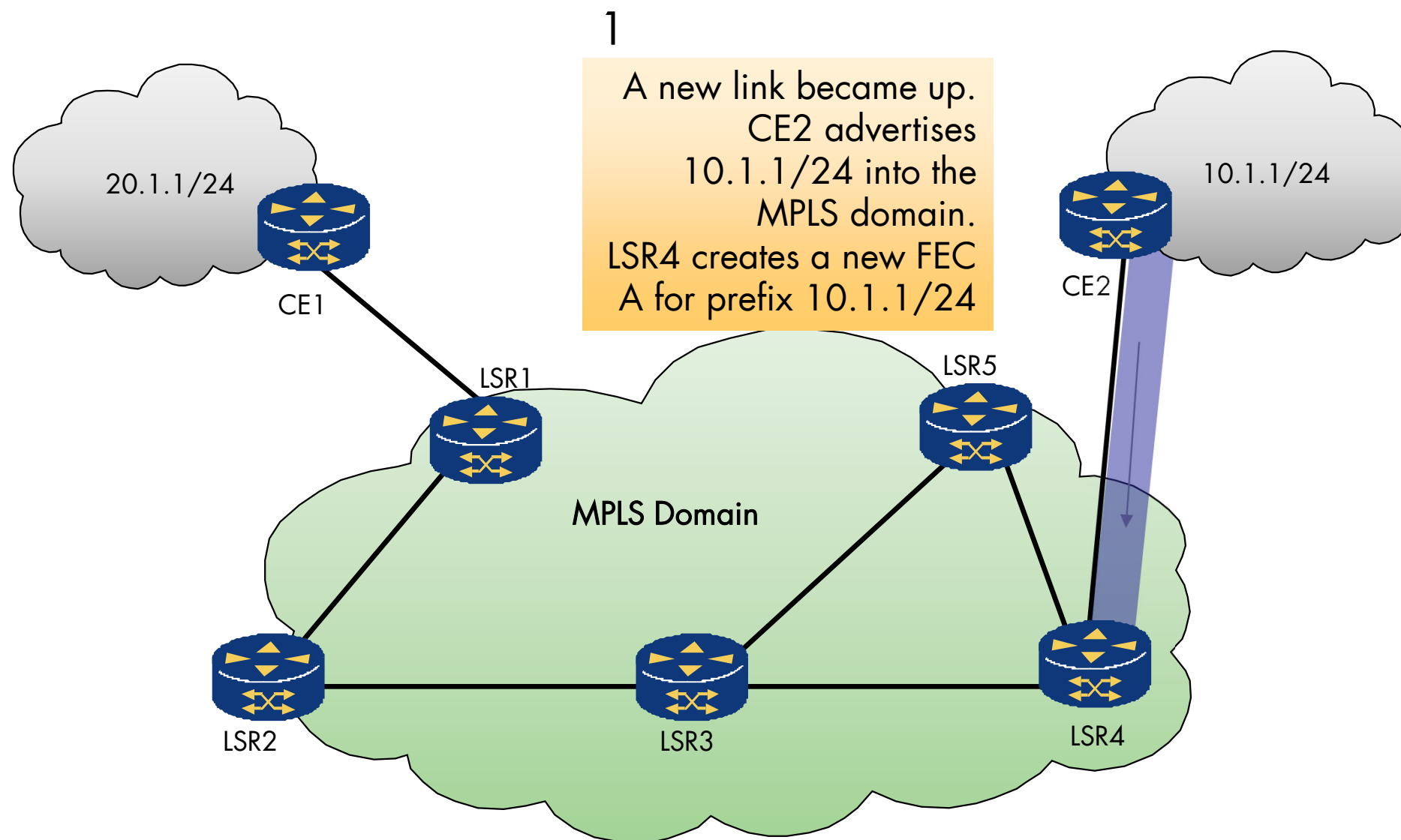
FEC	In Label	Out Label	Next Hop	Action
10.1.1/24	40	-	CE2	Pop/ Route

- Bidirektionale Kommunikation im MPLS-Netz
  - Aufbau von zwei Label Switched Paths (LSPs)
    - Hinrichtung (Forwarding Path), Anfrage durch LER A
    - Rückrichtung (Reverse Path), Anfrage durch LER C
  - Label Request / Label Mapping
  - Weg durch IGP bestimmt
  - Rückweg kann unterschiedlich sein



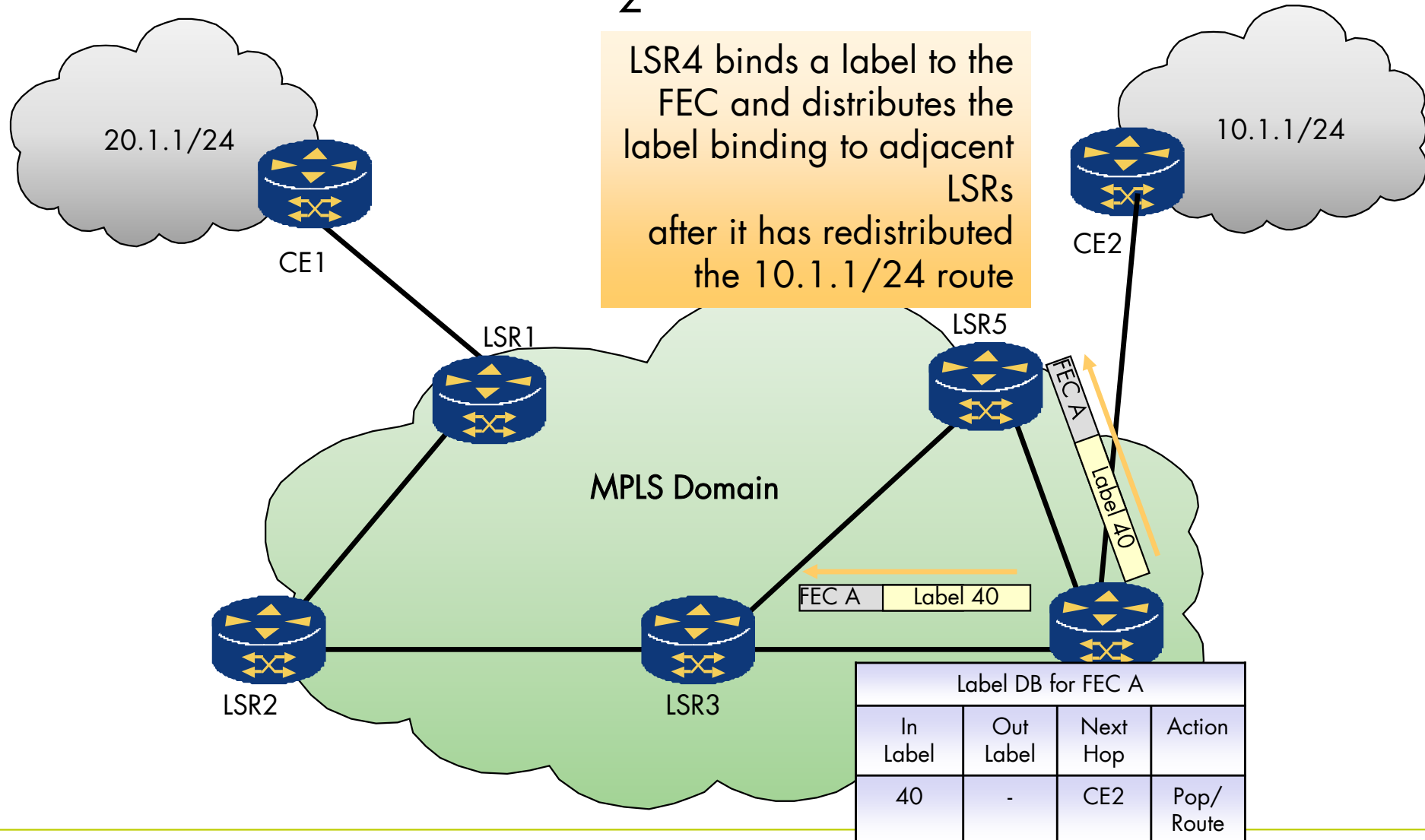
- LSRs lernen über Routing-Protokolle
- Labels werden während des Routings verteilt





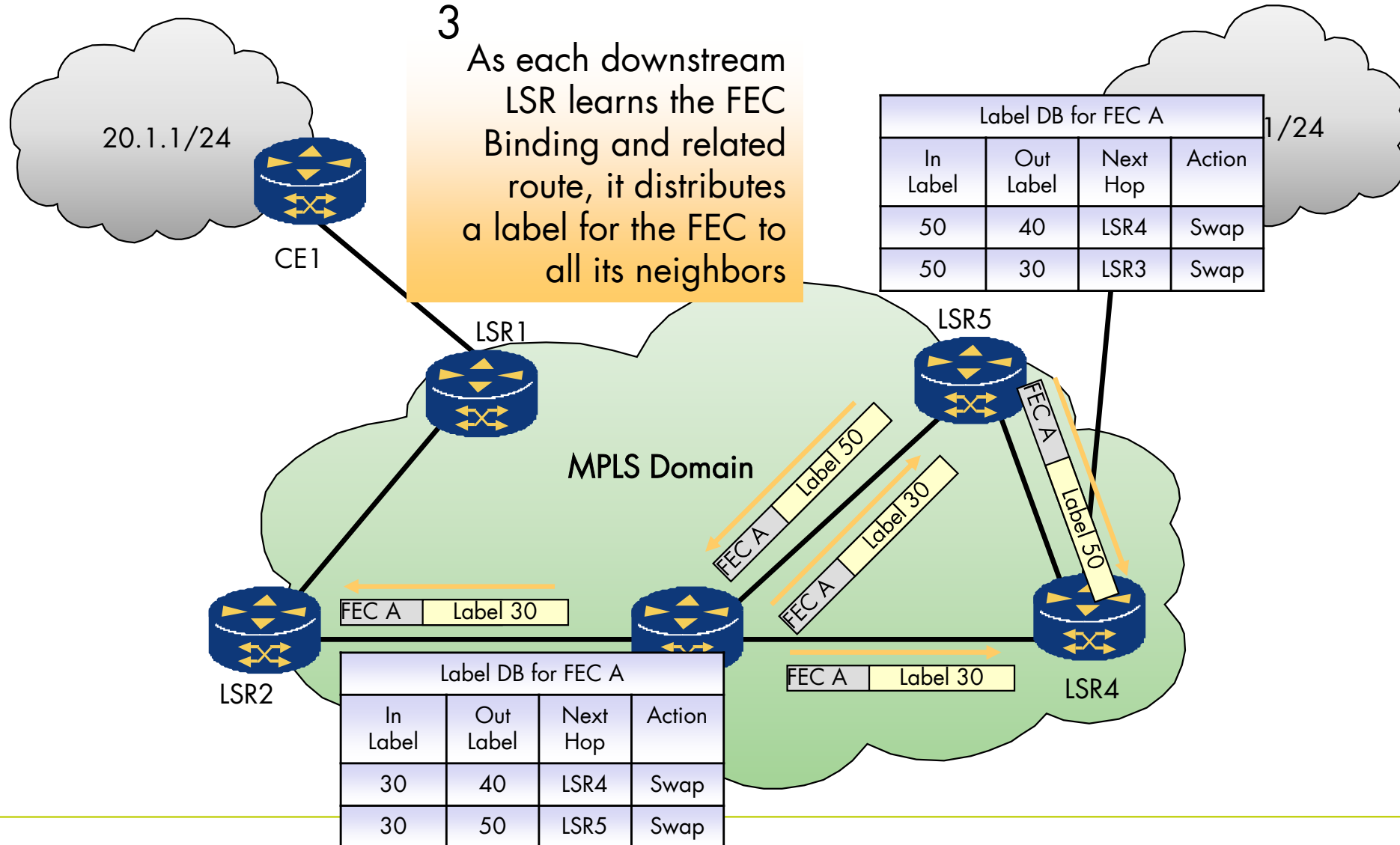
2

LSR4 binds a label to the FEC and distributes the label binding to adjacent LSRs after it has redistributed the 10.1.1/24 route

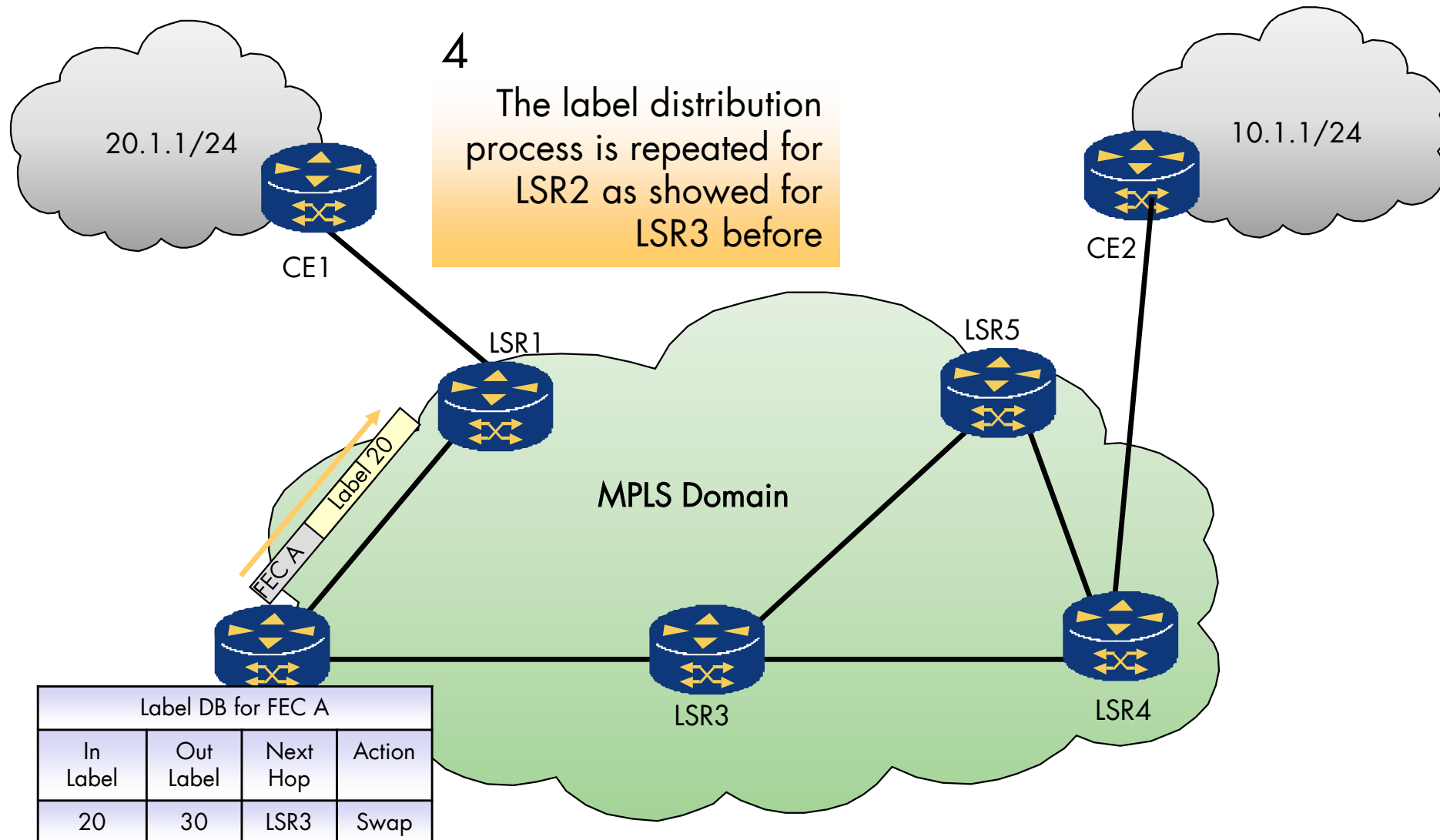


3

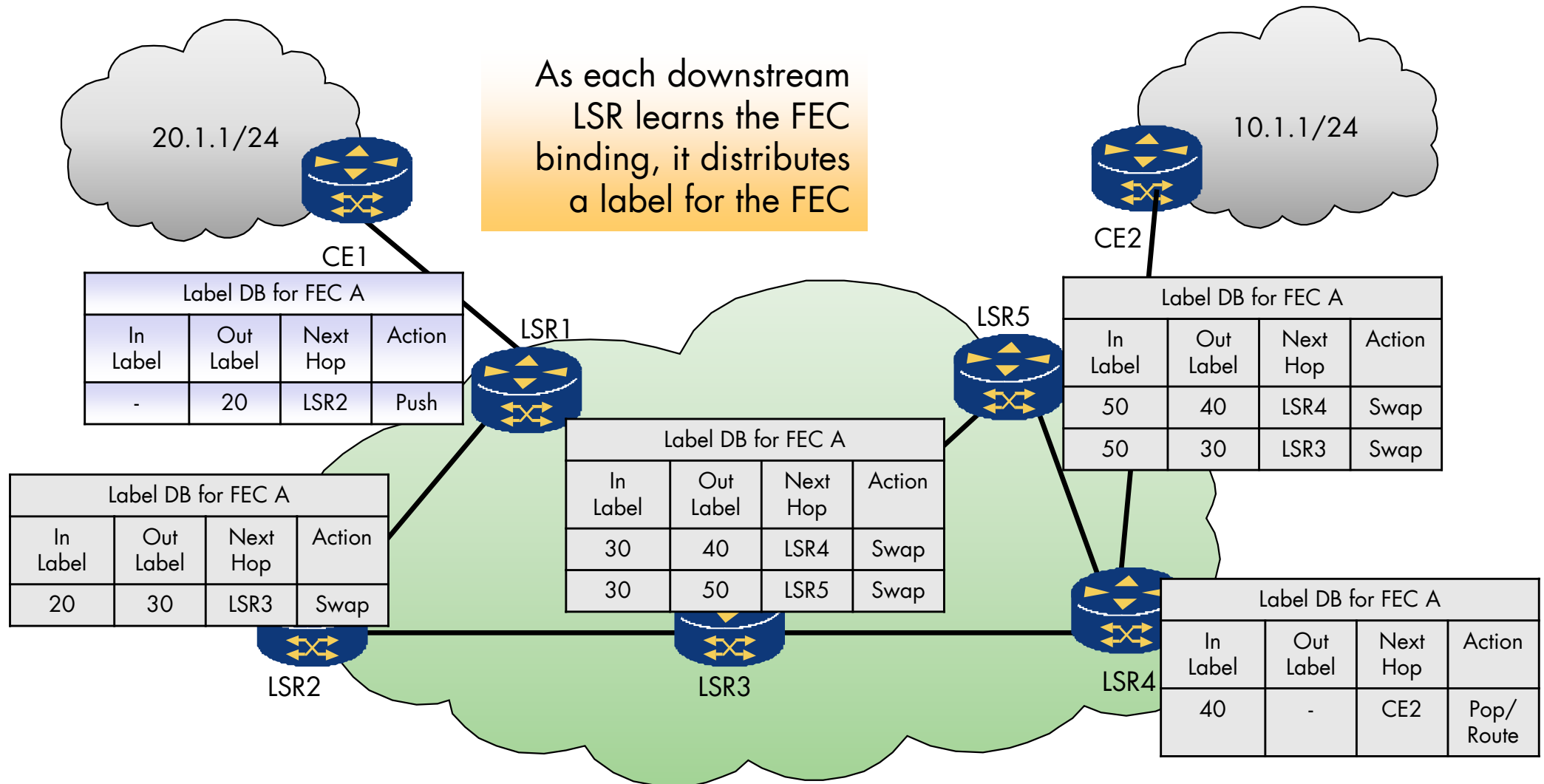
As each downstream LSR learns the FEC Binding and related route, it distributes a label for the FEC to all its neighbors





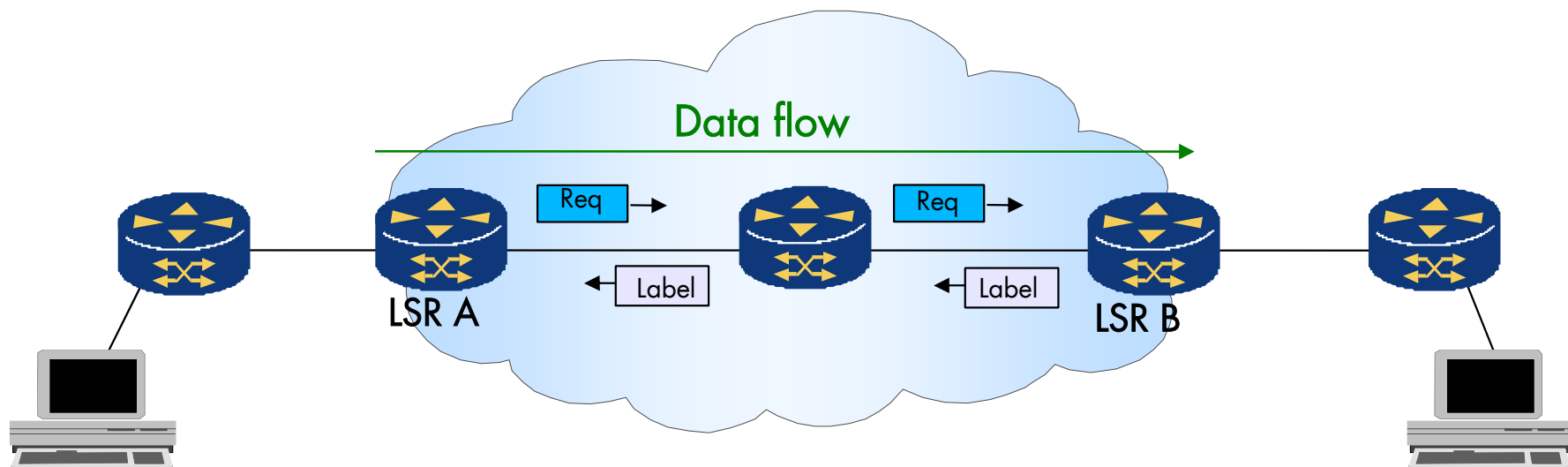


As each downstream LSR learns the FEC binding, it distributes a label for the FEC



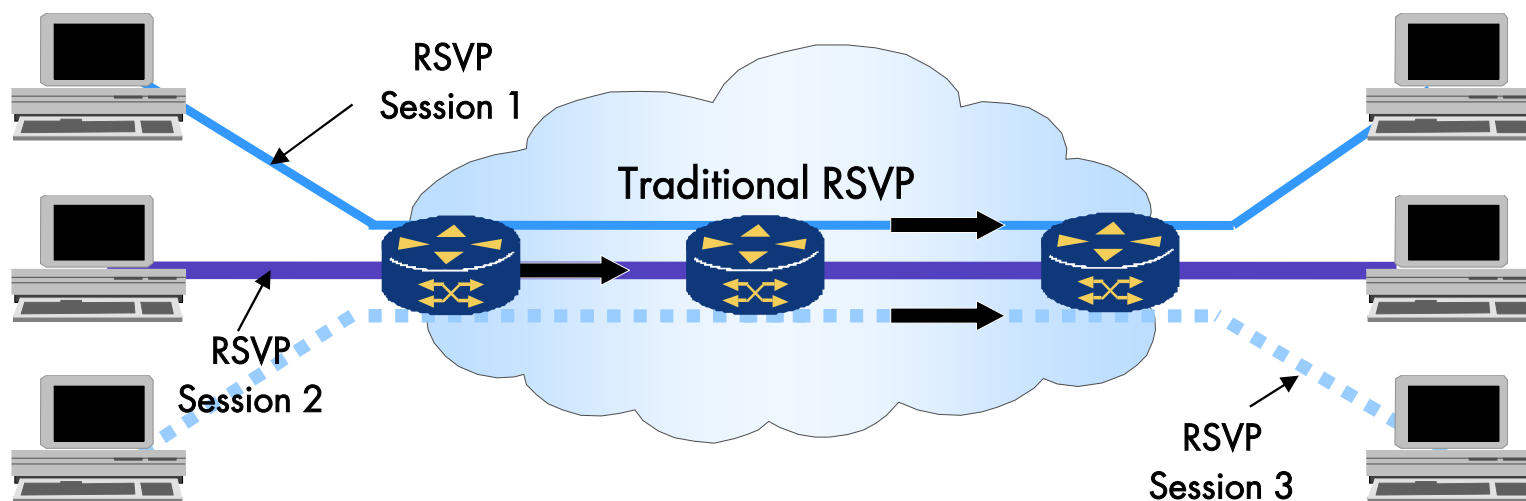
- RSVP-TE
  - Wird in Netzwerken mit aktiviertem TE für Transport-LSPs verwendet
- LDP
  - Wird in Netzwerken ohne TE zur Signalisierung von Transport-LSPs verwendet.
  - Wird in Layer-2 und Layer3-VPNs zur Signalisierung
- MP-BGP – BGP+Label-Erweiterung
  - Wird in Layer-3-VPNs zur Signalisierung eines bestimmten Kundenservice-Labels verwendet
  - Wird an der Grenze zwischen autonomen Systemen verwendet
  - Manchmal als Ersatz für LDP in Layer-2-VPNs

- Unidirektionaler Aufbau eines LSPs downstream
  - Zwei Arten der Label-Zuweisung für jeden LSP
    - Statisch (manuell)
    - Dynamisch mittels Signalisierungsprotokoll
  - LDP (Label Distribution Protocol)
  - RSVP-TE (Resource Reservation Protocol – Traffic Engineering)
  - MP-BGP (Multiprotocol Border Gateway Protocol)

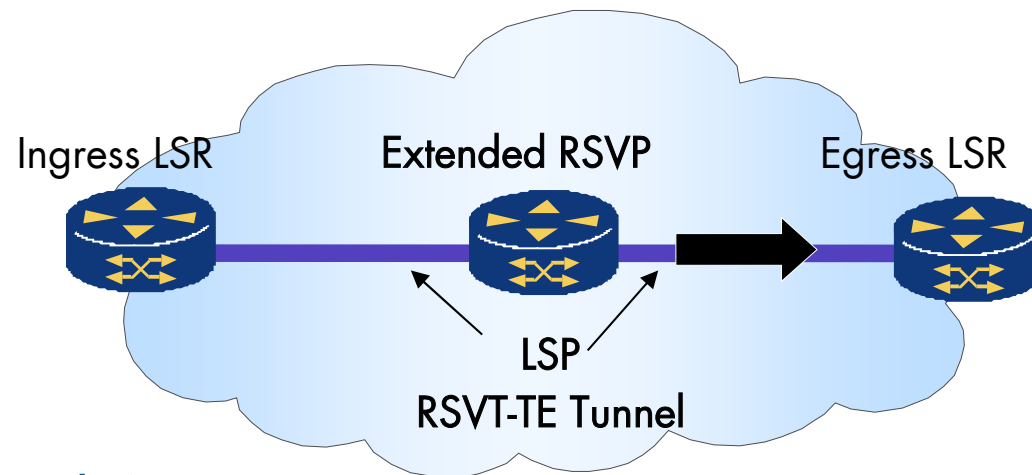


- Aktueller Einsatz der Verbindungsaufbauprotokolle
  - **LDP: Für einfache Label-Verteilung**
    - Am weitesten verbreitet, wenn keine TE oder QoS Anforderungen
    - Verwendet in einfachen MPLS-Topologien
  - **RSVP-TE: Für Traffic Engineering und QoS-Anforderungen**
    - Erlaubt die Reservierung von Ressourcen für z.B. Echtzeitanwendungen
    - Große Unternehmen- und SP-Netze, die Anforderungen haben
  - **MP-BGP: Für MPLS-VPNs und Inter-Domain-Routing**
    - Verwendet für MPLS-VPNs und Traffic Engineering zwischen autonomen Systemen
    - Skaliert über große Netze
    - Weiterer Einsatz für Inter-Domain-Routing und komplexe Netze mit mehreren AS
- Wann startet der LSP-Aufbau
  - **Topology-Driven: LSPs basieren auf der Netzwerk-Topologie (z.B. mit LDP)**
  - **Data-Driven: LSPs werden dynamisch basierend auf den aktuellen Datenströmen angepasst (z.B. mit RSVP-TE)**

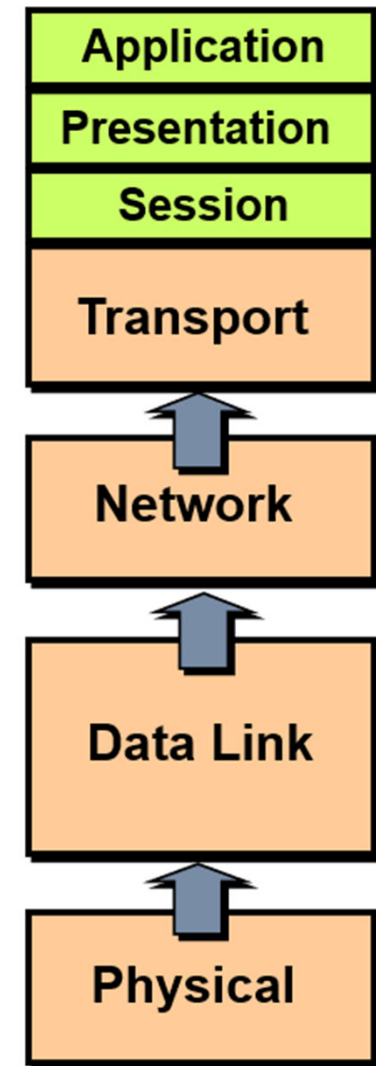
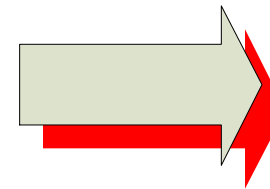
- RSVP wurde 1997 in RFC2205 und RFC2209 standardisiert.
  - QoS-Signalisierungsprotokoll für IP
  - Reserviert die verfügbaren Netzwerkressourcen
  - Hop-by-Hop-Behandlung für den individuellen Datenverkehr
  - Wenige Verbreitung in Dienstbieternetzwerken
  - Schlechte Skalierbarkeit
  - Beinhaltet die Signalisierung für Traffic-Engineering-Attribute



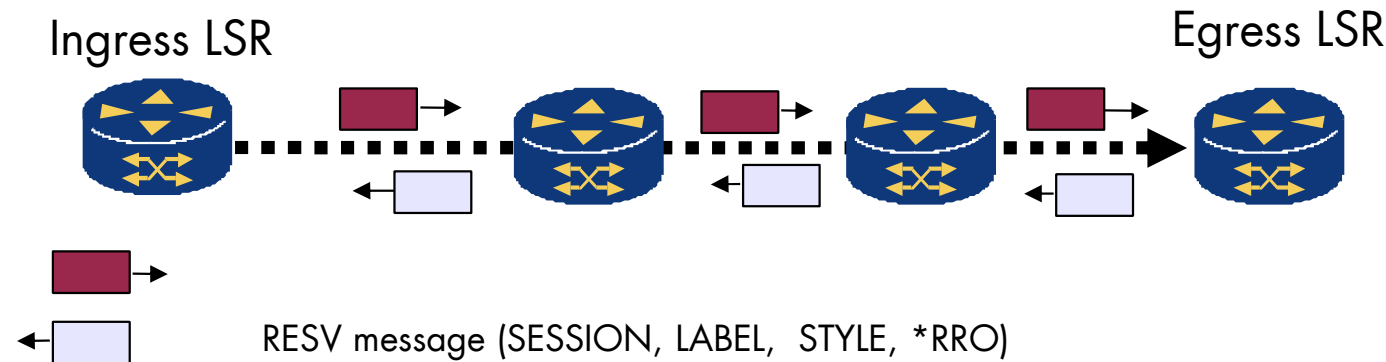
- Resource Reservation Protocol Traffic Engineering (RSVP-TE)
  - Spezifiziert in RFC 3209
  - Erstellt und verwaltet explizit signalisierte LSPs
  - Initiiert und beendet an MPLS-Edge-LSRs
  - Signalisiert LSPs und deren benötigte Ressourcen, jedoch nicht FEC
  - Die Zuordnung des Datenverkehrs zu einem LSP erfolgt lokal durch den Eingangs-LSR
  - Daher wird bei RSVP-TE-LSPs der Begriff „Tunnel“ verwendet



- RSVP-TE auf Network Layer (Layer 3)
  - Wird über IP übertragen (Protokollnr. 46)
  - Signalisierungsnachrichten in regelmäßigen Abständen erneut senden
  - Sicherstellen, dass die Reservierungen aktiv bleiben
  - Wenn ein Router keine Antwort auf eine gesendete Nachricht erhält, kann er die Nachricht erneut senden







\* ERO - Explicit Route Object, \*RRO – Record Route Object

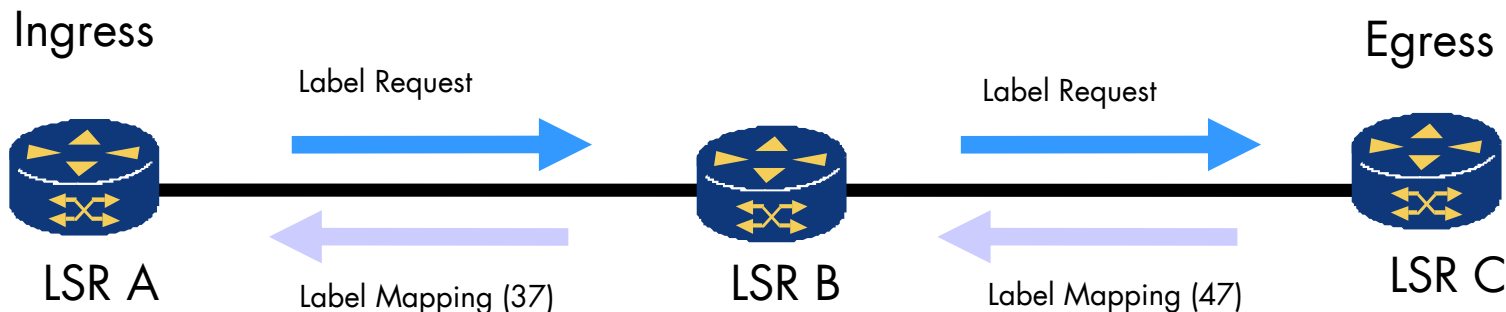
- PATH-Nachricht

- Initiiert vom Ingress-LSR und adressiert an den Egress-LSR
- Fordert die Erstellung eines LSP und QoS bei jedem LSP-Hop an
- Der Ingress-LSR kann eine explizite Route angeben
- Der Ingress-LSR kann Informationen über die genaue Route erhalten

- RESV-Nachricht

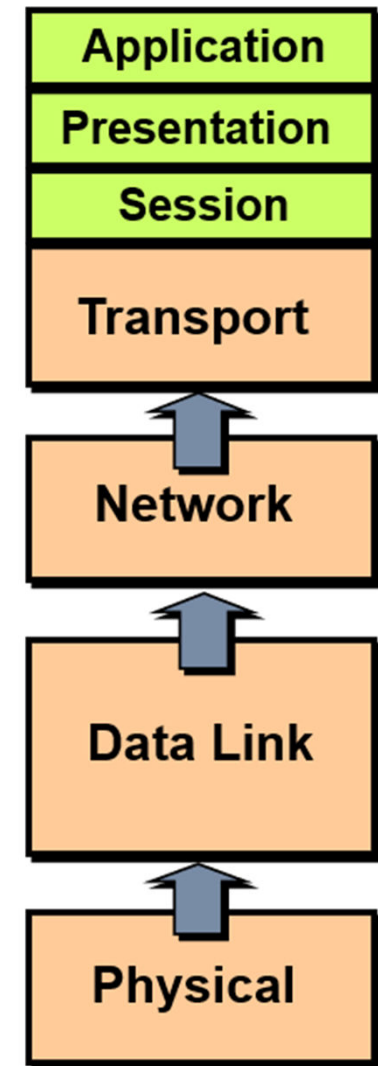
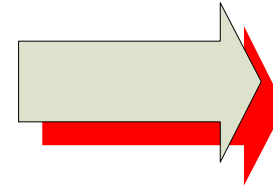
- Adressiert an den vorherigen Hop der PATH-Nachricht
- Zeigt eine erfolgreiche Ressourcenreservierung an
- Gibt den QoS-Nutzungsstil an
- Labelerstellungprozess: Wird ausgeführt, wenn der Ingress-LSR als Ergebnis einen gültigen RESV für seine PATH-Anfrage erhält

- LDP (Label Distribution Protocol) – ein weiteres LSP-Signalisierungsprotokoll
- Nutzt die vom Hello-Protokoll empfangenen Informationen zum Aufbau von TCP-Sitzungen zwischen LSRs
  - Setzt eine zuverlässige Verteilung von LDP-Nachrichten voraus
  - Baut für jede LDP-Sitzung zwischen LSRs eine TCP-Sitzung auf
  - Immer nur eine Sitzung pro Nachbar
  - Kein kontinuierlicher Austausch von Statusinformationen



- Ursprünglich entwickelt, um IP-Routing-Präfixe mit Labels zu verknüpfen
  - Router tauschen Labels aus, anstatt zu routen
  - Label-Switching und Routing gleichzeitig
  - Wenn das IP-Präfix mit einem Label verknüpft ist, wechselt der Router, andernfalls führt er normales Routing durch
  - Zwei Betriebsmodi werden unterstützt:
    - L(Link)-LDP – eine LDP-Sitzung zwischen zwei direkt benachbarten Routern.
    - T(Targeted)-LDP – eine LDP-Sitzung zwischen zwei nicht direkt benachbarten Routern.
  - Zwischen den beiden Routern können mehrere IP-Hops oder Netzwerke liegen

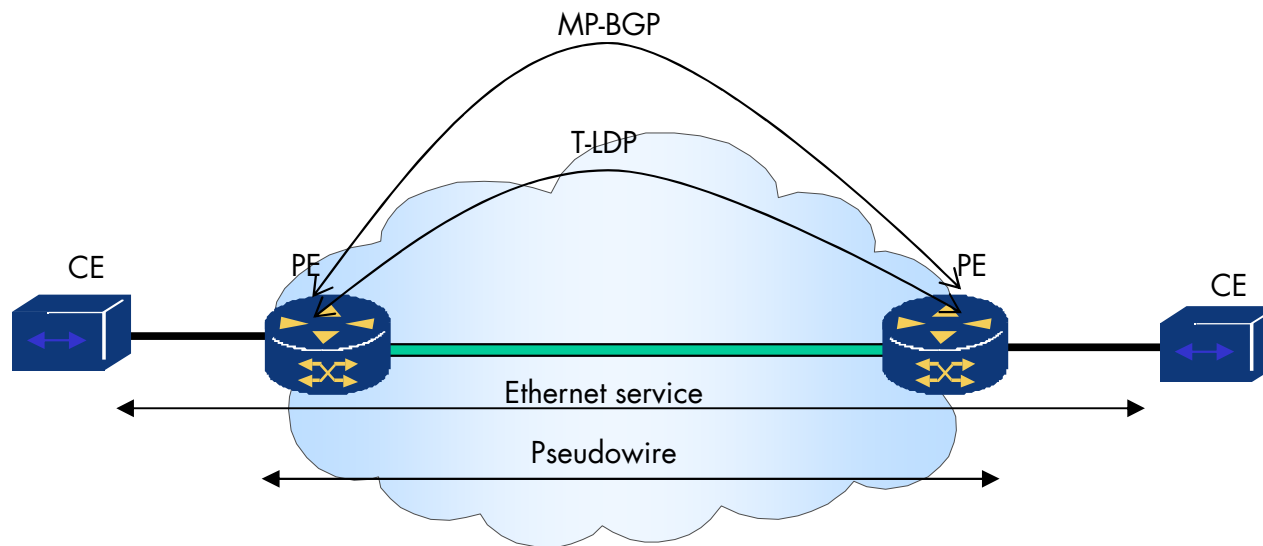
- LDP auf Schicht 7, nutzt Transportschicht (Layer 4)
  - Wird über TCP übertragen (Port 646)
  - Tauscht regelmäßig HELLO Nachrichten aus
    - Dient der Nachbarschaftserkennung und Bestätigung
  - TCP sorgt für die zuverlässige Übertragung, ist aber nicht einsetzbar, um benachbarte Router zu entdecken und Aktivität zu überprüfen
  - Verwendung von Hello-Nachrichten in LDP für Aufrechterhaltung der Nachbarschaftsbeziehung
  - TCP als Basis für zuverlässige Datenübertragung



- LDP-Sitzung zwischen direkt benachbarten Routern
  - Router müssen sich direkt erreichen können
  - Müssen im selben Layer-2- oder Layer-3-Netzwerk sein
- Nachbarschaftserkennung zum Aufbau einer LDP-Sitzung
  - Verwendet Hello-Nachrichten zur Identifizierung von LDP-Peers in MPLS-Netzwerken
- Informationen über die verfügbaren Labels austauschen
  - Nach Aufbau TCP Austausch von Label Mapping-Nachrichten
    - Label: Label, das einem bestimmten Ziel zugewiesen wird  
Router kann ein Label für einen bestimmten Pfad oder Dienst vorschlagen
    - FEC (Forwarding Equivalence Class): Beschreibt die Gruppe von IP-Paketen, die identisch behandelt werden (z.B. Pakete, die an das gleiche Ziel gesendet werden)
    - FEC definiert, welche Pakete das zugewiesene Label verwenden sollen
    - Next Hop: Die IP-Adresse des nächsten Routers, an den das Paket mit dem zugewiesenen Label weitergeleitet werden soll

- LDP-Sitzung zwischen nicht direkt benachbarten Routern
  - Einrichtung einer LDP-Sitzung zwischen zwei Routern, die nicht direkt benachbart sind
  - Ermöglicht, dass zwischen den beiden Routern mehrere IP-Hops oder Netzwerke liegen können
- LDP-Sitzung wird durch die Angabe eines spezifischen Nachbarn (Target) initiiert
  - Router A (in einem Netzwerk) baut eine LDP-Sitzung mit Router C (in einem anderen Netzwerk) auf
  - Router B kann als Zwischenrouter fungieren
  - Sitzung wird über Routing und IP-Adressen aufgebaut, nicht über eine direkte physische Verbindung

- Multiprotocol BGP wird bei MPLS-L3-VPNs häufig eingesetzt
  - VPN-Labels auszutauschen
  - Lernen der Kundenstandorte Routen über ein MPLS-Netzwerk
  - Unterscheidung verschiedener Kundenstandorte, wenn der Datenverkehr von den anderen Kundenstandorten zum Provider Edge Router (PE-Router) zum Routing gelangt

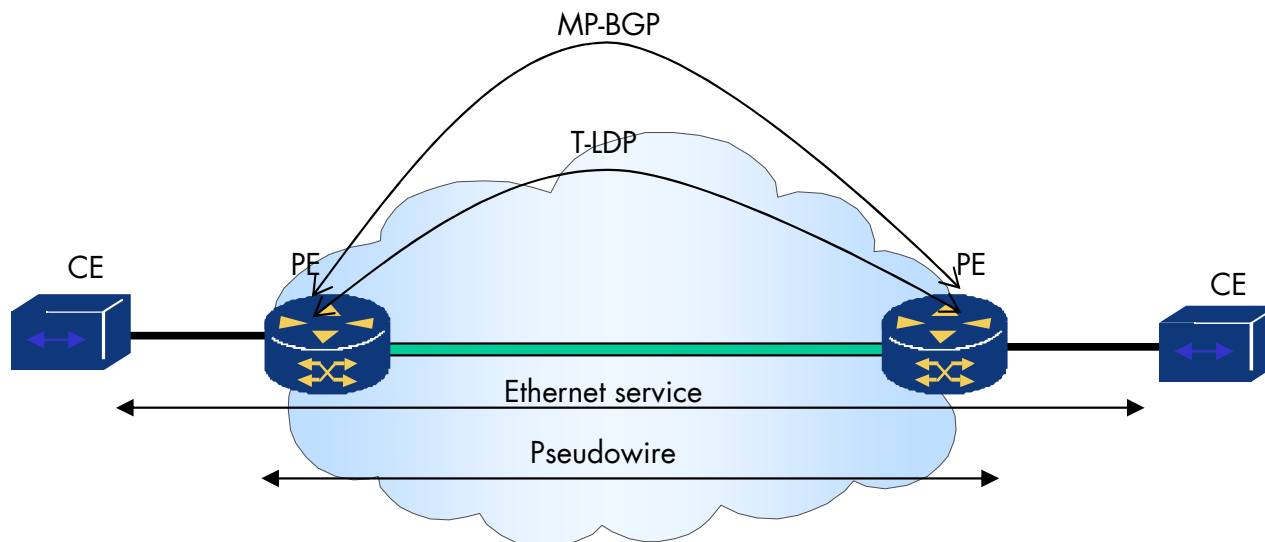


- Multiprotocol Border Gateway Protocol für Aufbau LSPs
  - Unterstützt IPv4, IPv6 und MPLS
- Nachbarschaftsbildung
  - Verwendet TCP (Port 179) zur Bildung von Nachbarschaften
  - Aufbau erfolgt über den TCP-Handshake -> keine Hello-Pakete
  - Nach Aufbau der TCP-Verbindung senden von BGP-Updates
- Routen-Austausch
  - BGP-Update-Nachrichten für Routing-Informationen
- Multiprotokoll-Unterstützung
  - Verwendet verschiedene Adressfamilien für unterschiedliche Protokolle und Adressformate



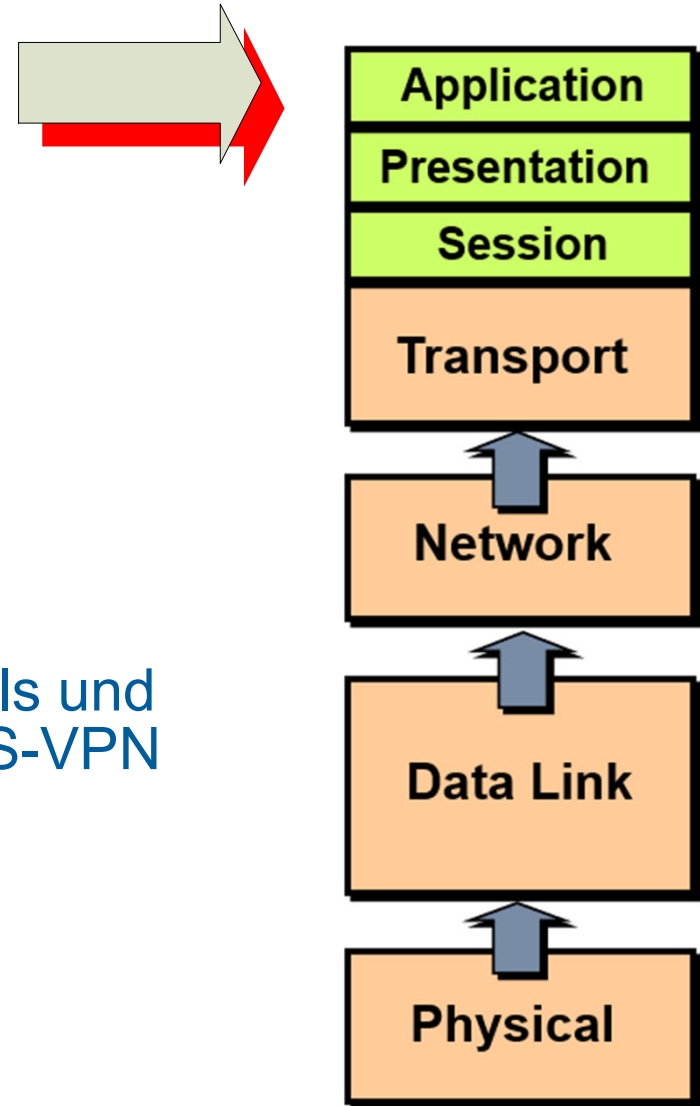
- AFI (Address Family Identifier)
  - 16-Bit-Wert, welche Adressfamilie verwendet wird
    - 1 für IPv4
    - 2 für IPv6
    - 25 für MPLS (für VPNs)
- SAFI (Subsequent Address Family Identifier)
  - 8-Bit-Wert für die spezifische Art des Dienstes
    - 1 für unicast
    - 128 für VPNv4 (VPN IPv4)
    - 132 für VPNv6 (VPN IPv6)
- VPN-Label
  - Label in den Update-Nachrichten wenn in MPLS-VPNs genutzt
- Route-Distinguisher (RD)
  - Attribut für VPN-Routen
    - Sicherstellung der Eindeutigkeit der IP-Adressen in verschiedenen VPNs
    - Wird als Präfix zu einer IP-Adresse hinzugefügt.

- Zwei Signalisierungsprotokolle
  - Targeted-LDP (T-LDP)
  - Multiprotocol-BGP (MP-BGP)
- Kein Unterschied in der Forwarding Plane
- Unabhängig von der Signalisierung des Transport LSPs
  - Dieser kann über RSVP-TE aufgebaut werden
- Signalisierungssession zwischen den LERs / PEs



LER = PE (Provider Edge)  
• Ingress/Egress  
LSR = P (Provider) Router  
CE = Customer Edge

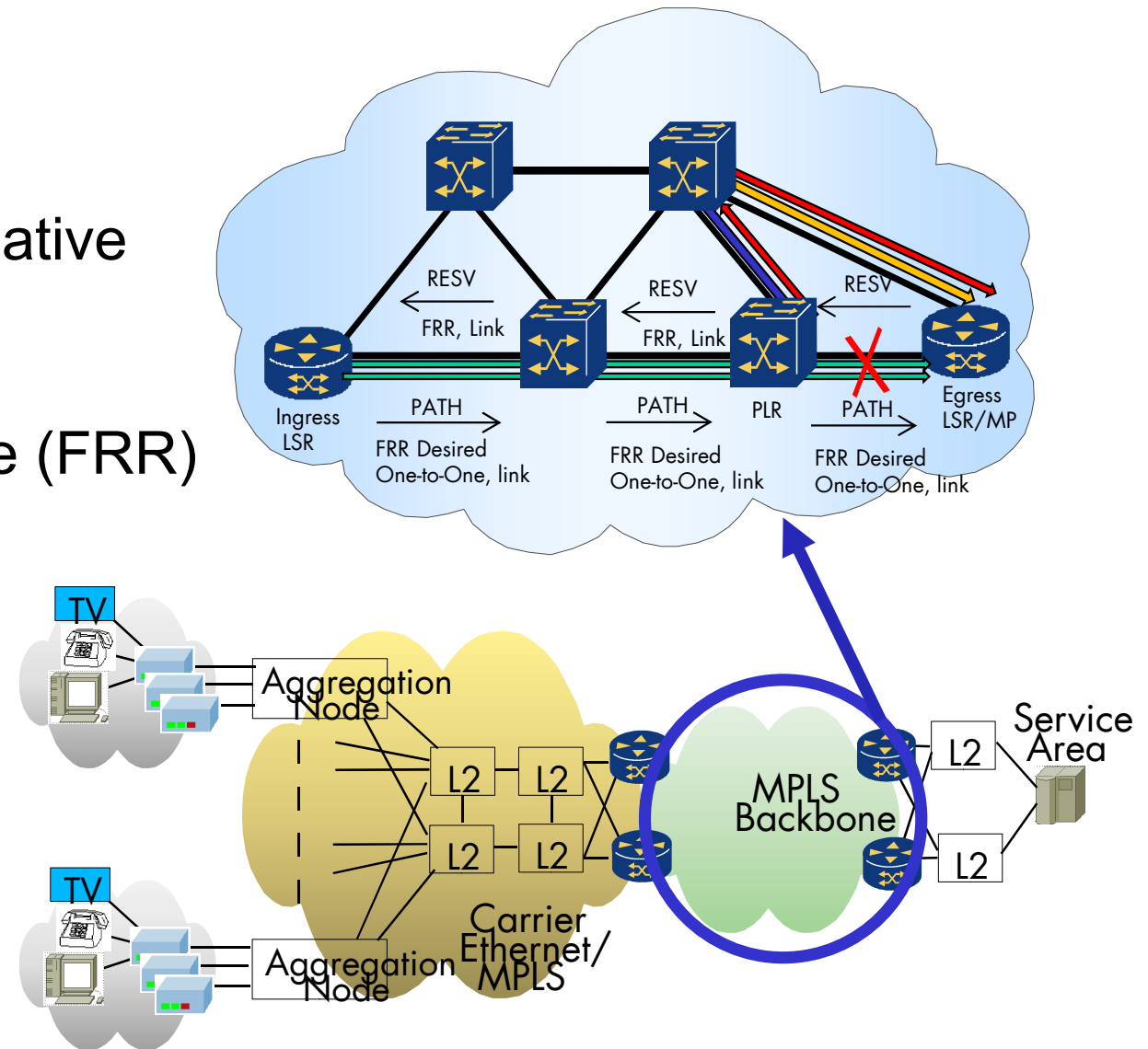
- MP-BGP auf Schicht 7, nutzt Transportschicht (Layer 4)
  - Erweiterung des BGP-Protokolls
  - Nutzt TCP mit Portnummer 179
  - Verwendung von TCP für MP-BGP
    - In dynamischen Netzen mit häufigen Änderungen der Routing-Informationen bleibt die Integrität gewährleistet
  - Labels für VPN-Routen zuweisen
- MP-BGP für den Austausch von Labels und Routing-Informationen in einem MPLS-VPN



Network Layer - Vermittlungsschicht

# LAYER 3

- Fehlererkennung
- Schnelle Konvergenz
- Umschalten auf alternative Wege
- BFD und Fast Reroute (FRR)



- Netzwerkprotokoll zur schnellen Erkennung von Fehlern
  - Kann in verschiedenen Kontexten eingesetzt werden, einschließlich Layer 2 MPLS und Layer 3 MPLS
- BFD operiert auf der Transport- und Netzwerk-Schicht
  - Transport-Schicht (Layer 4): BFD verwendet UDP als Transportprotokoll, um seine „Hello“-Pakete zwischen den Geräten zu versenden
  - Diese Pakete werden typischerweise an einen speziellen Port (standardmäßig Port 3784 für BFD) gesendet
  - Netzwerk-Schicht (Layer 3): Da BFD auch IP-Pakete verwendet, um seine Nachrichten zu transportieren, ist es ebenfalls relevant auf der Netzwerk-Schicht, da es mit IP-Adressen und Routing-Protokollen interagiert

- Sendet regelmäßige „Hello“-Nachrichten zwischen zwei Endpunkten
  - Überprüft, ob Verbindung aktiv und funktionsfähig
- L2 MPLS
  - BFD überwacht Verbindung zwischen PE-Routern und CE
    - Schnelle Erkennung von Verbindungsfehlern erlaubt schnell auf Ausfälle zu reagieren
    - Alternative Pfade zu verwenden, um die Verfügbarkeit der Dienste sicherzustellen
- L3 MPLS
  - BFD überwacht IP-basierte Dienste
    - Verbindungen zwischen Routern mit IP-Routing-Protokollen (z. B. OSPF oder BGP)
    - Schnellere Konvergenz der Routing-Protokolle, bevor diese zu Routing-Problemen führen
    - Verbessert die Netzwerkleistung und die Benutzererfahrung, da Ausfallzeiten minimiert werden

- RFC 5880: "Bidirectional Forwarding Detection"
  - Veröffentlichungsdatum: August 2010
  - Definiert grundlegende Mechanismen und Protokolle für BFD
  - Einschließlich der Nachrichtenformate, der Zustandsmaschinen und der Anwendungsfälle
- RFC 5881: "Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6"
  - Veröffentlichungsdatum: August 2010
  - Beschreibt die speziellen Implementierungen von BFD für IPv4- und IPv6-Umgebungen
  - Einschließlich der spezifischen Details zur Verwendung von BFD in diesen Protokollen



- Nachrichtenaustausch
  - Verwendet UDP-Pakete als BFD-Nachrichten
  - Nachrichten enthalten Informationen über den Status der Verbindung
  - Einschließlich der Identität der Endpunkte und der Zeitstempel für die letzte erfolgreiche Kommunikation
- Zustandsmaschinen
  - Down: Die Verbindung ist nicht aktiv oder erreichbar
  - Init: Die Verbindung hat gerade begonnen, Nachrichten auszutauschen
  - Up: Die Verbindung ist aktiv und funktionsfähig
- Nach Timeout wird die Verbindung auf Down gesetzt

- Heartbeat-Mechanismus
  - Sendet regelmäßig „Hello“-Pakete (Heartbeat-Nachrichten)
  - Pakete haben i.d.R. eine sehr kurze Intervalldauer (z. B. 50 ms)
- Timeout-Mechanismus
  - Timeout-Wert bestimmt, wie lange er auf BFD-Nachricht warten
  - Wenn keine Nachrichten empfangen, Verbindung ausgefallen
- Schnelle Reaktion
  - Kann so konfiguriert werden, dass es sehr schnell auf Verbindungsprobleme reagiert
  - Ermöglicht, alternative Pfade sofort zu aktivieren

- Statusmeldung
  - Wenn Router erkennt, dass die Verbindung zu anderen Routern inaktiv ist (z. B. weil der Timeout überschritten wurde)
  - Benachrichtigung der entsprechenden Routing-Protokolle (wie OSPF oder BGP), um die Routen zu aktualisieren oder zu entfernen
- Umschaltung auf Backup-Pfade
  - Wenn Redundanz vorhanden, kann Router automatisch auf einen Backup-LSP (Label-Switched Path) oder einen alternativen Pfad umschalten
  - Benutzer oder die Anwendung bemerken keine Unterbrechung

- IP Routing Protocols
  - Schneller Trigger für Rerouting, schneller als die IGP's
- Multi-Hop BFD, wenn Systeme nicht direkt verbunden
  - Adresse des zu überwachenden Routers eingeben
- MPLS LSP und Pseudowire Fehlererkennung
  - Health Monitoring
  - Trigger Umschaltung auf Backup LSP durch MPLS FRR
  - Trigger Umschaltung auf Backup Pseudowire, falls vorhanden

- Schutz des Tunnel-LSP (Transport)
  - Gegen Verbindungs- oder Knotenausfälle
- Ermöglicht SDH-ähnliche Ausfallsicherheit
  - Im 50-ms-Bereich für IP Routing Protocols
- Traffic-Engineering-Erweiterung (TE) für Interior Gateway Protocols (IGP)
  - Link-State-Protokoll
  - Verteilung zusätzlicher Verbindungsinformationen
- RSVP-Erweiterungen für LSP-Tunnel (RSVP-TE)
  - Übertragung der MPLS-Labelinformationen

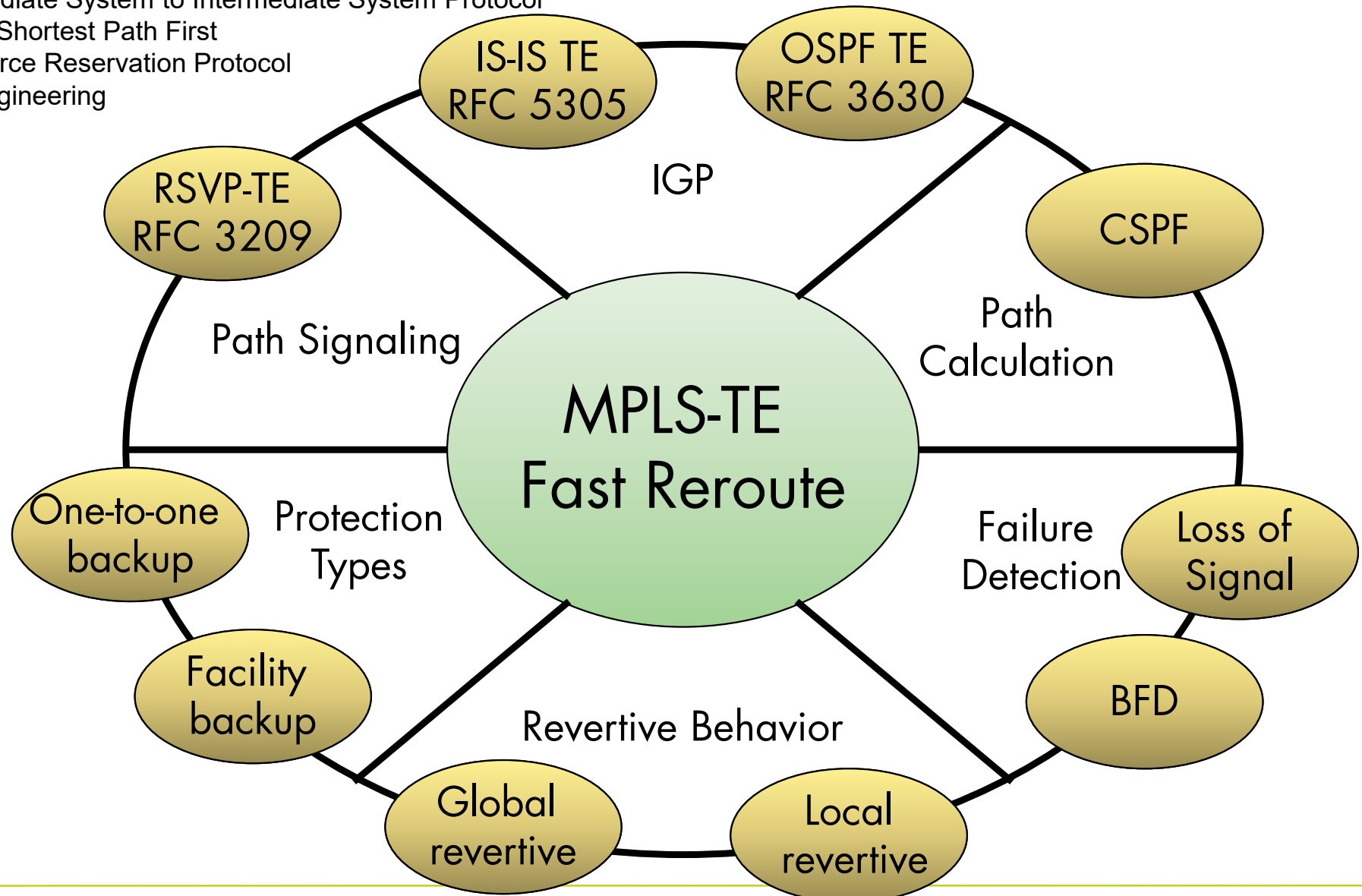
CSFP - Constrained Shortest Path First

IS-IS - Intermediate System to Intermediate System Protocol

OSPF - Open Shortest Path First

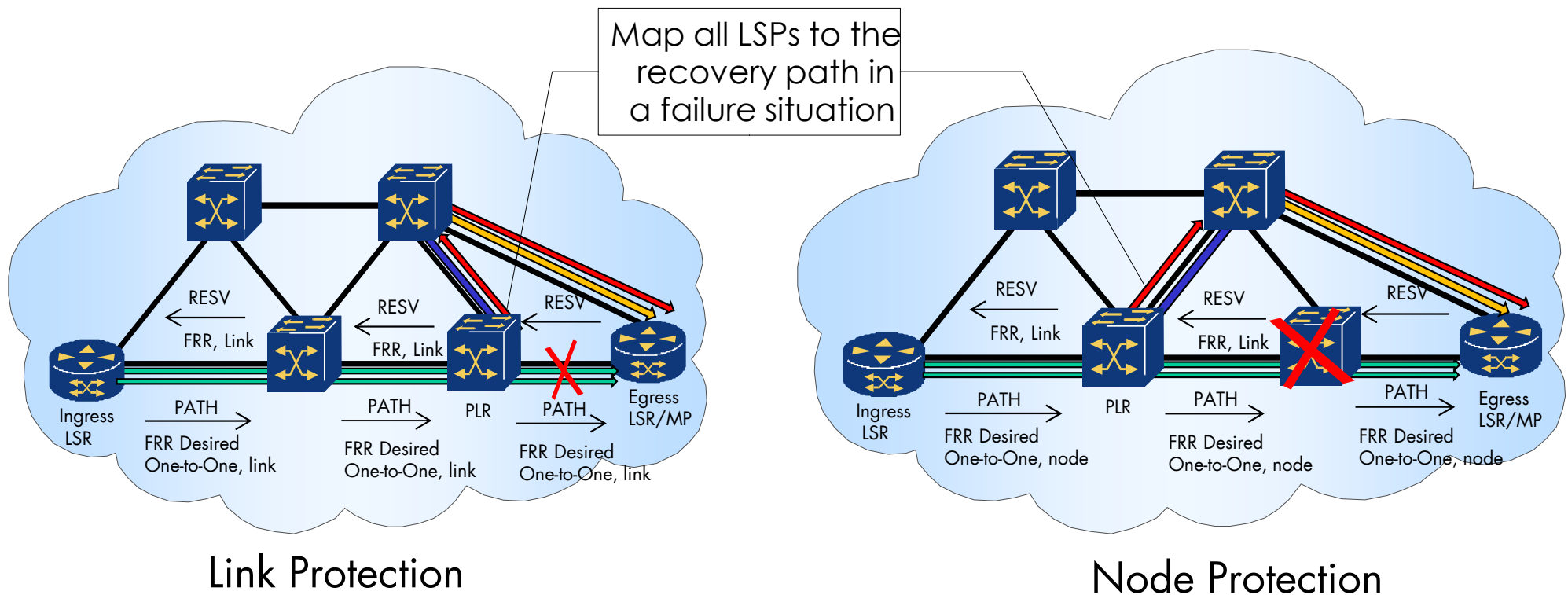
RSVP - Resource Reservation Protocol

TE - Traffic Engineering



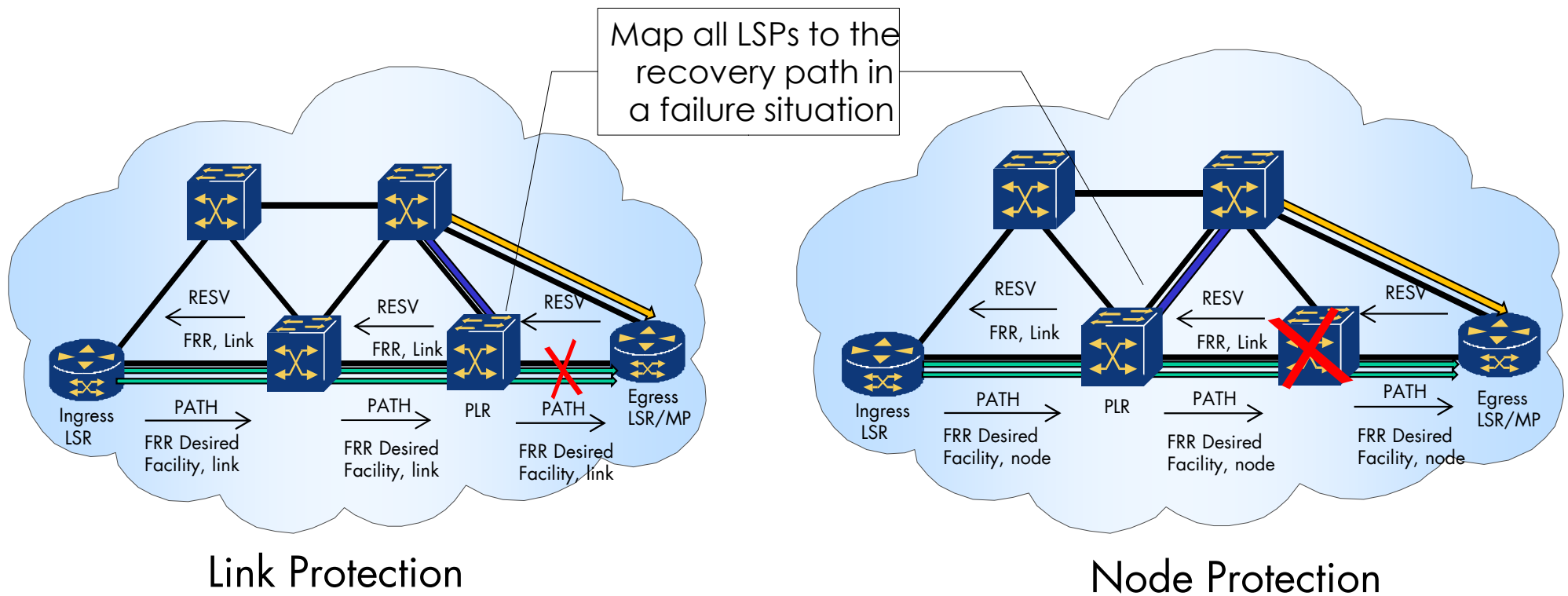
- Zwei neue Objekte
  - **FAST\_REROUTE-Objekt** in der PATH-Nachricht eingefügt
    - Steuert den Backup-Pfad
    - Gibt Prioritäten, Sitzungsattribute, Filter und Bandbreite an
    - Ermöglicht die Anforderung einer bestimmten lokalen Schutztechnik (node, link)
  - **DETOUR** wird bei Eins-zu-eins-Backups verwendet
    - Identifiziert den Detour-LSP mit einem Knotenpaar {Point of Local Repair (PLR) und Merge Point (MP)}
- Zwei erweiterte Objekte
  - **SESSION\_ATTRIBUTE, Record Route Object (RRO)**
    - Geben z.B. die gewünschte Bandbreite an
    - Informationen über die LSPs am Ausfallpunkt und den Aufbau neuer End-to-End-LSPs sowie den gewünschten Schutz an

Jeder LSP-Pfad verfügt über einen eigenen Satz  
vorsignalisierter Backup-LSPs



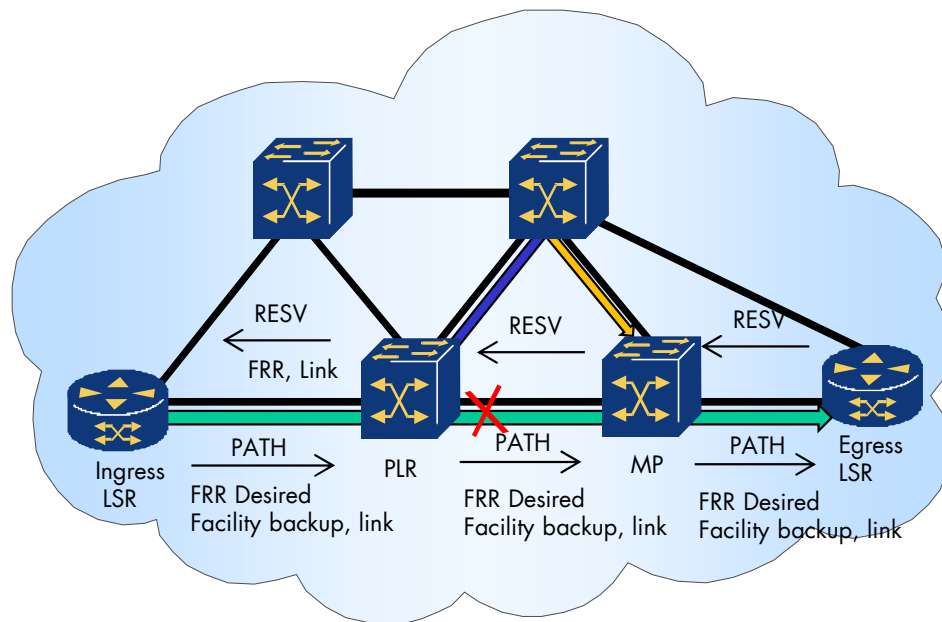


Alle geschützten LSPs im gemeinsamen Netzwerksegmenten teilen sich denselben Bypass-Tunnel



## Local Repair

1. Local repair
2. Nutze denselben LSP-Path



## Global Repair

- 1. Zuerst Local repair
- 2. PLR sendet zum Ingress LSR "PATH ERROR "
- 3. Ingress LSR Re-Set-Up neuen optimalen LSP-Path

