

IT2221 - Netzwerktechnik

Dozentin:

Gabriele Schrenk

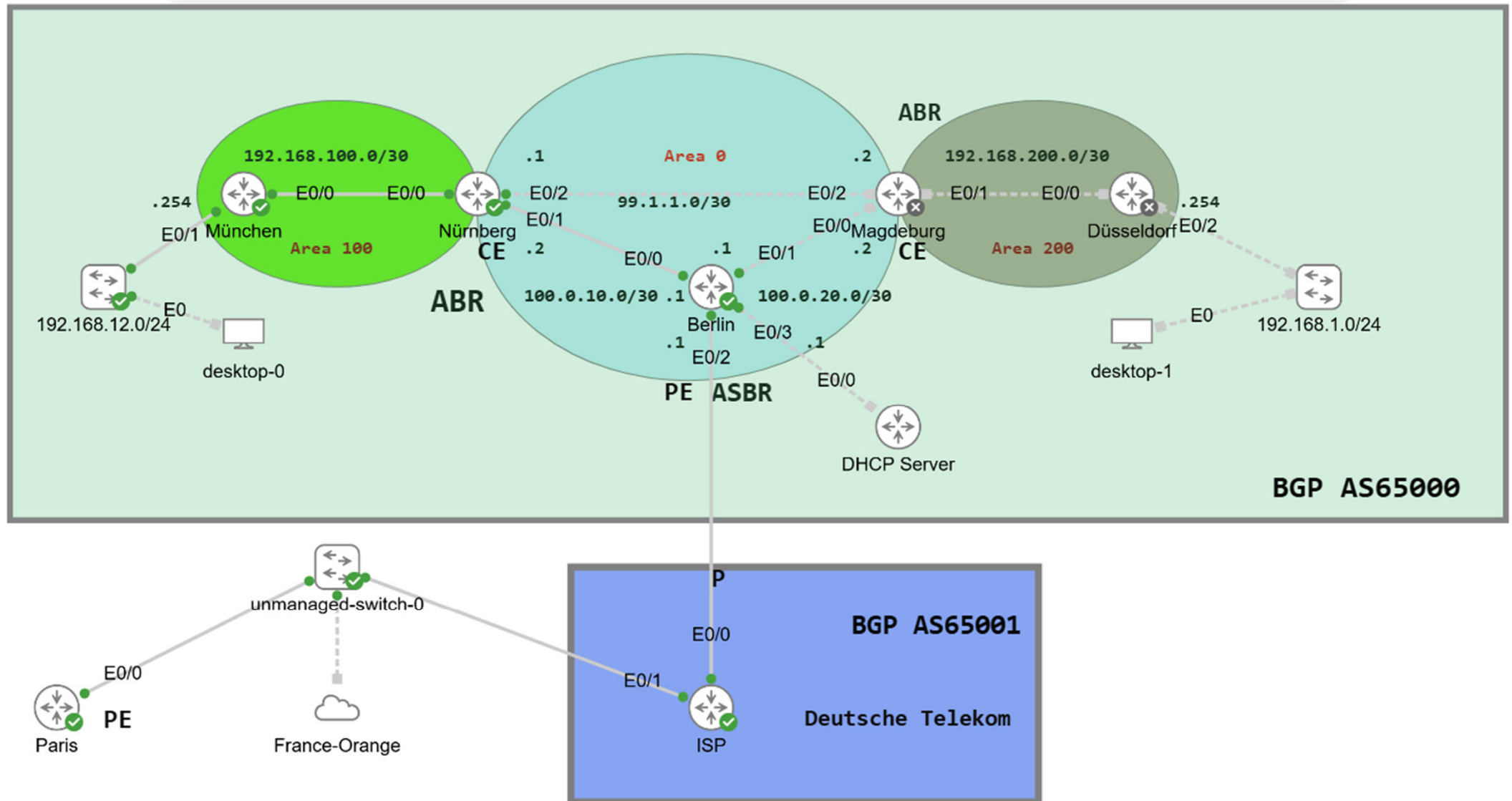
e_schrenk@doz.hwr-berlin.de

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 MPLS, L2/L3 VPNs über MPLS, Segment Routing
8. Segment Routing, Ausfallsichere Netze, Netzwerksicherheit
9. Netzwerksicherheit, Carrier, Ethernet, Ausblick Autonomous Networks
10. Bewertung Vorlesung/Labor, Prüfungsvorbereitung
11. Prüfungsvorbereitung / offene Fragen (29.4.26)

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



Network Layer - Vermittlungsschicht

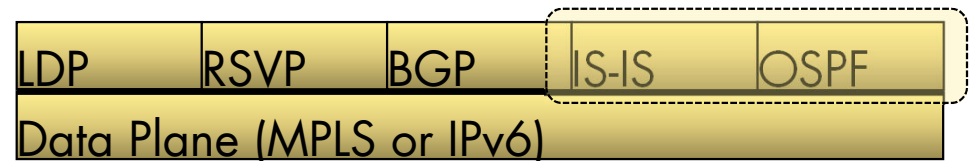
LAYER 3

Source routing

Der Eingangsrouter (Ingress-Knoten) wählt den gesamten Pfad durchs Netz
Der Weg wird also nicht „Hop by Hop“ von jedem Router neu berechnet,
sondern vom ersten Router festgelegt
Der Pfad (Weg) wird als geordnete Liste dargestellt, die „Segmente“
(Segments) genannt wird

Segment

Ein Segment ist eine Anweisung für den Router, Beispiel:
„Sende zum Knoten X über den kürzesten Pfad“
IGP Segment: Prefix-/Node-SID (global), Adjacency-SID (lokal)



Data Plane Agnostic

Vorhandene Data Planes (MPLS or IPv6) / Routing Protokolle (IS-IS, OSPF)

Control Plane Vereinfachung

- Weniger Control-Plane-Protokolle, die betrieben werden müssen
- Weniger Wechselwirkungen/Abhängigkeiten zwischen Control-Plane-Protokollen
- Automatischer Traffic-Schutz für beliebige Topologien, ohne dass für jeden einzelnen Flow im Netz Signalisierung nötig ist

Traffic Engineering

- Vermeidung von zustandsbehafteten Einträgen (States) pro Flow im Kernnetz;
- Vermeidung der manuellen Konfiguration von Traffic-Engineering-Pfaden
Pfade werden automatisch berechnet oder durch einen Controller vorgegeben

Software-Defined Networking

- Weiterentwicklung bestehende Technik, keine komplette „Revolution“ oder Neukonstruktion
- Hybrider Ansatz zwischen zentralisierter und verteilter Control Plane (per Controller)
- Netzwerk-Programmierbarkeit über Southbound-Schnittstellen, z. B. PCEP
Ein Controller kann über solche Schnittstellen Pfade/Policies im Netz vorgeben

PCEP steht für Path Computation Element Communication Protocol

In Software-defined Networking (SDN) ist es ein standardisiertes Protokoll (IETF)

Genutzt vom SDN-Controller (PCE), um Pfade durch ein Netz für Datenströme zu berechnen und zu verwalten

IETF standardization in Source Packet Routing in Networking working group

Architektur und Use Cases

RFC 8402 and RFC 9256



Segment Routing über MPLS und über IPv6

SR-MPLS (RFC 8660) und SRv6 (RFC 9886)

Protokol-Erweiterungen in einzelnen Working Groups

Zum Beispiel (nicht vollständig):

Source Packet Routing in Networking (SPRING)

Path Computation Element (PCE)

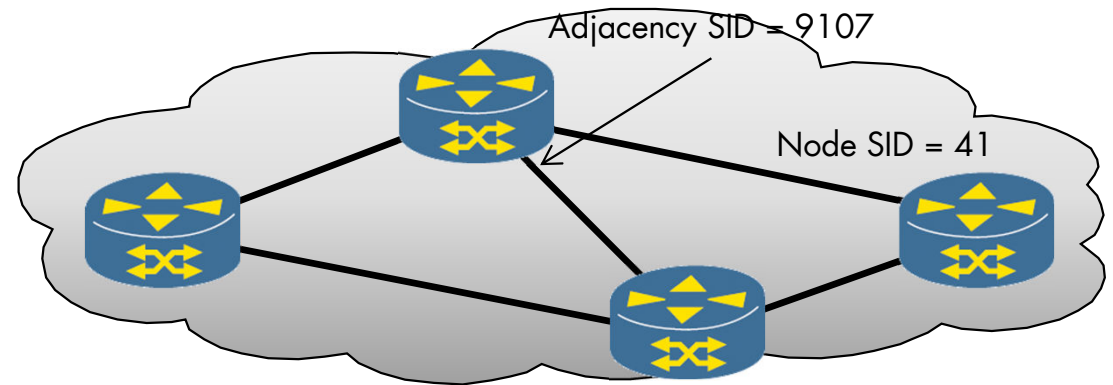
Inter-Domain Routing (IDR)

IPv6 Maintenance (6MAN)

<https://datatracker.ietf.org/wg/spring/documents/>

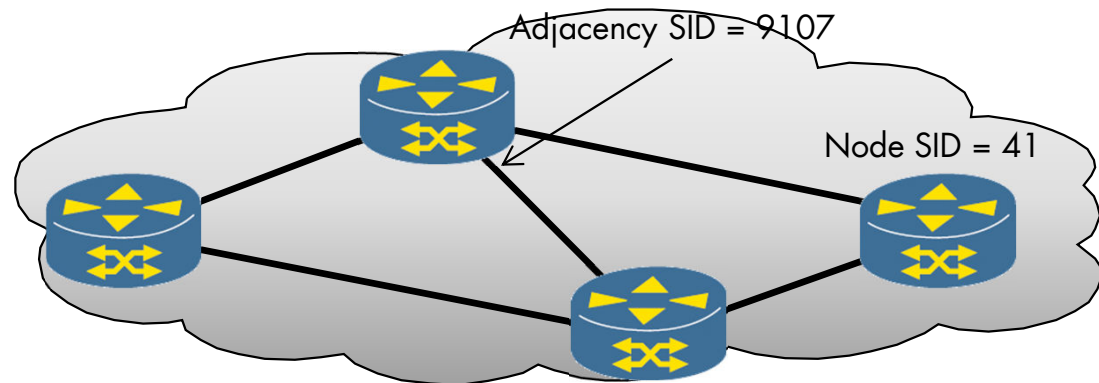
Prefix/Node Segment

- Global gültig innerhalb der gesamten Segment-Routing-Domäne
Jeder Router im SR-Netz versteht dieselbe SID gleich
- Alle Knoten leiten das Paket zu diesem Präfix/Knoten über den kürzesten IGP-Pfad weiter (normales SPF-Routing, über die SID)
- Wird als relativer Wert (Index) angekündigt
Die SID ist ein Index, der innerhalb eines reservierten Bereichs interpretiert wird
- Verwendet einen pro Knoten reservierten SID-Bereich (ab 16.000)
Segment Routing Global Block, SRGB
- Jeder Router hat einen SRGB; in Kombination mit dem Index ergibt sich die konkrete Label-/SID-Nummer



Adjacency Segment

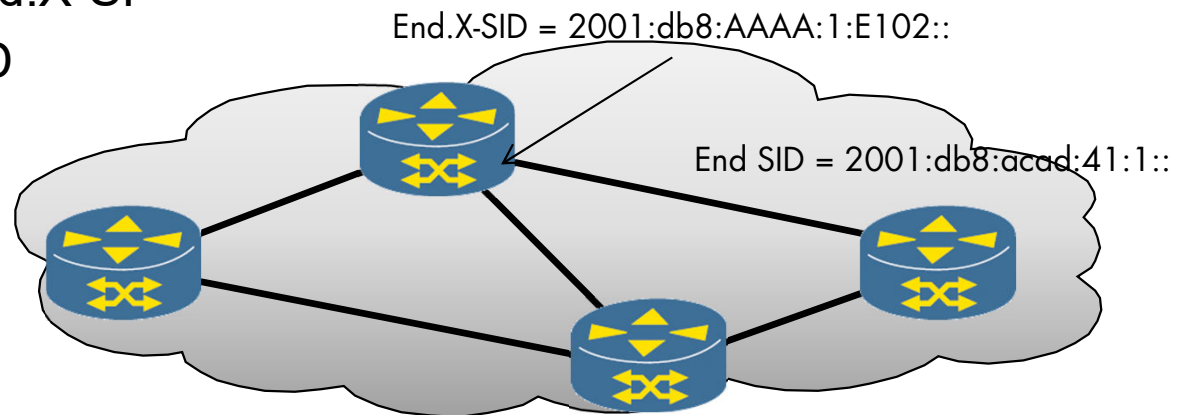
- Nur lokal auf dem Knoten gültig, der das Segment vergibt
Andere Router verwenden diese SID nicht für ihre eigene Weiterleitung
- Der Knoten wertet die SID aus und leitet das Paket explizit über diese bestimmte Nachbarverbindung weiter
 - Source Routing
- Wird als absoluter Wert angekündigt.
Die SID ist direkt die konkrete Label-/SID-Nummer, kein Index innerhalb eines SRGB
- Prefix-SID
Index mit SRGB addiert
(16.000 + 41 = 16.041)
- Adj-SID
Absoluter Wert ist direkt die Label-Nummer



Kein SRGB nur noch IPv6-Adressen

- Die SID (Segment ID) nicht mehr als 20-Bit-MPLS-Label übertragen, sondern als komplette 128-Bit-IPv6-Adresse
- IPv6-Adressen sind global eindeutig und im gesamten Netz routbar
- Daher braucht es keinen reservierten Label-Block (SRGB)
- Die SID ist die IPv6-Adresse

- Adjacency-SID in SRv6: End.X-SI
- Node-SID in SRv6: End-SID
- Prefix-SID in SRv6:
End.DT4 / End.DT6



SR-MPLS nutzt die MPLS-Weiterleitungsebene wieder

- SR-MPLS steht für Segment Routing über die MPLS-Datenebene (gemäß RFC 8660)
- Verwendet Standard-MPLS-Header

Segmente werden als MPLS-Labels kodiert

- Jede SID ist MPLS-Label aus dem Segment Routing Global Block (SRGB)
- Die Segmentliste wird als MPLS-Label-Stack dargestellt

Forwarding behavior auf dem Pfad/Weg

- Der Headend-Router wendet den vollständigen SR-Label-Stack für den gewählten Pfad oder die SR Policy
- Der Ausgangsrouter entfernt das letzte SR-Label und leitet die Daten weiter

Koexistenz mit “classic” MPLS

- SR-MPLS nutzt dieselbe Data Plane wie LDP/RSVP-TE-LSPs
- Migrationsoptionen: SR- und LDP-Tunnel können koexistieren

Was ist SRv6?

- SRv6 steht für Segment Routing over IPv6 und ist in RFC 8986 definiert
- Es nutzt die Standard-IPv6-Forwarding-Plane mit einem optionalen Segment Routing Header (SRH)
- Jede SID wird als IPv6-Adresse und nicht als MPLS-Label kodiert

Struktur und Typen von SRv6-SIDs

- Eine SID ist üblicherweise wie folgt strukturiert: Locator :: Funktion :: Argumente (High-Level-Format)
- Der Locator identifiziert den Knoten oder Standort; der Funktionsteil definiert das auszuführende Verhalten

SRv6 “network programming” Konzept

- Jede SID repräsentiert ein Verhalten, nicht nur den nächsten Hop
- SRv6 und SR-MPLS nutzen dieselbe SR-Architektur

Classic MPLS

- MPLS verwendet Label-Switched Paths (LSPs), die über Protokolle wie LDP und RSVP-TE signalisiert/aufgebaut werden
- Mehrere Control-Plane-Protokolle (IGP + LDP + RSVP-TE) erhöhen den Betriebsaufwand und erschweren die Fehlersuche
- Eine große Anzahl von LSPs erzeugt viel Zustandsinformation (State) im Kernnetz und kann CPU und Speicher der Core-Router stark belasten

Segment Routing (SR)

- Segment Routing nutzt Source-Routing:
Der Ingress-Router legt den Pfad fest und codiert ihn als Segmentliste im Paket
- Segmente (SIDs) werden direkt über IGP/BGP verteilt; es ist kein separates Label-Distributionsprotokoll wie LDP nötig (vereinfachte Control Plane)
- Zustandsinformationen pro Flow werden nur am Ingress der SR-Domäne gehalten (Die Core-Router sehen nur generische SIDs/Labels, aber keinen separaten State für jeden einzelnen Flow/LSP)
- Integriertes Traffic Engineering: Pfade über geeignete Segmentlisten explizit gesteuert, ohne separate TE-LSPs via RSVP-TE

Grundidee Segment Routing

- Segment Routing (SR) nutzt *source-based routing*
- Jeder Segment Identifier (SID) kodiert eine Instruktion, z.B. “go to this node” oder “use this link”
- Per-Flow State wird nur am Ingress gehalten

Haupttypen der Segmente

- Node / Prefix SID: Zeigt die Shortest-Path-Route zu einem Knoten oder Prefix
- Adjacency SID: Zeigt einen spezifischen ausgehenden Link zwischen Knoten
- Binding SID: Repräsentiert einen kompletten, vorberechneten Pfad oder eine Policy mit einer einzigen SID (Label oder IPv6 Adresse: Route über A, dann B, dann C)

Wie werden SIDs verteilt und übertragen?

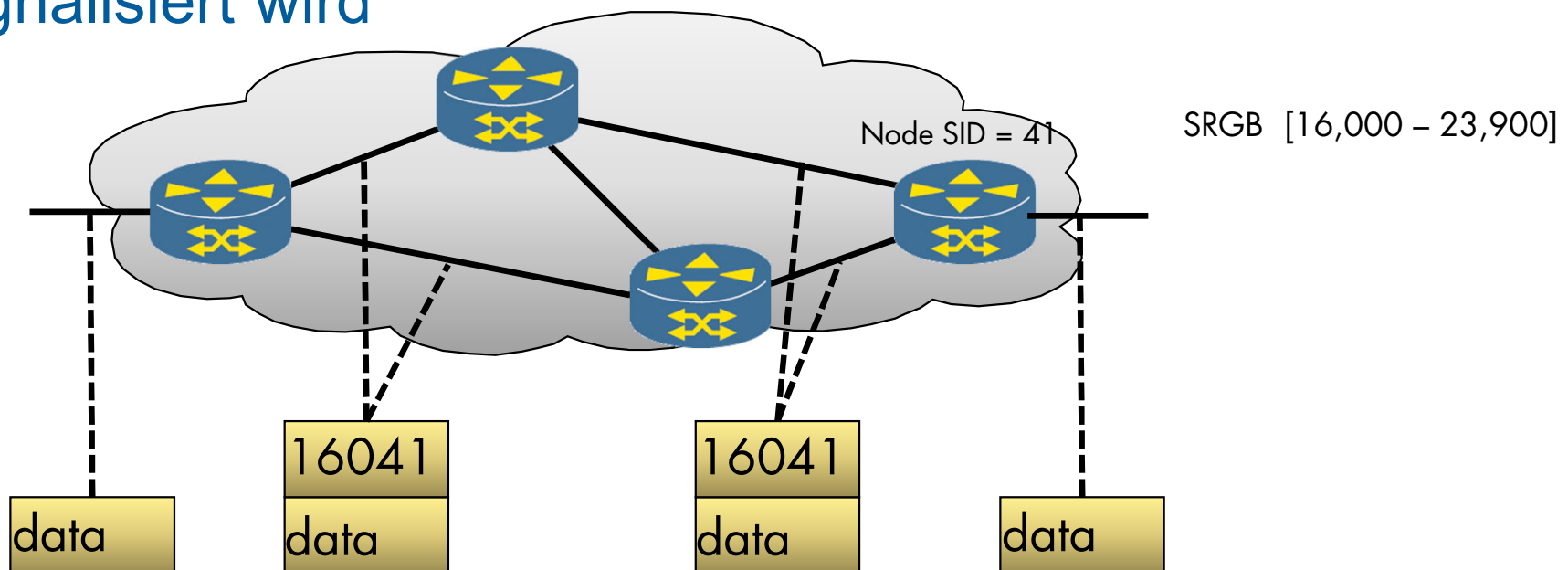
- IGPs (IS-IS, OSPF) und BGP weisen SIDs zu, über standardisierte Erweiterungen
- In SR-MPLS, SIDs sind MPLS-Labels innerhalb eines SR Label Ranges (SRGB)
- In SRv6, SIDs sind IPv6-Adressen

Weiterleitung entlang des kürzesten IGP-Pfades

Nutzung des ECMP-Lastausgleichs

Durchführung einer Swap-Operation im Core

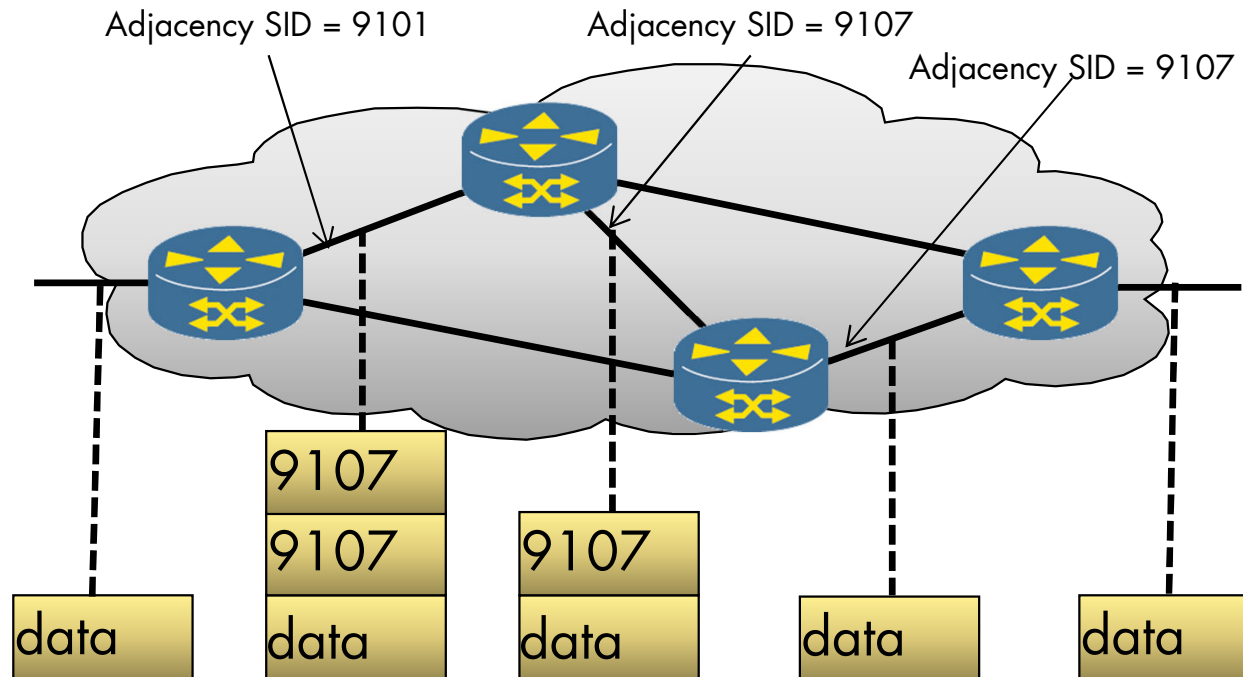
Der vorletzte Hop kann eine Pop-Operation (PHP) durchführen, wenn dies vom Ausgangs-LSR signalisiert wird



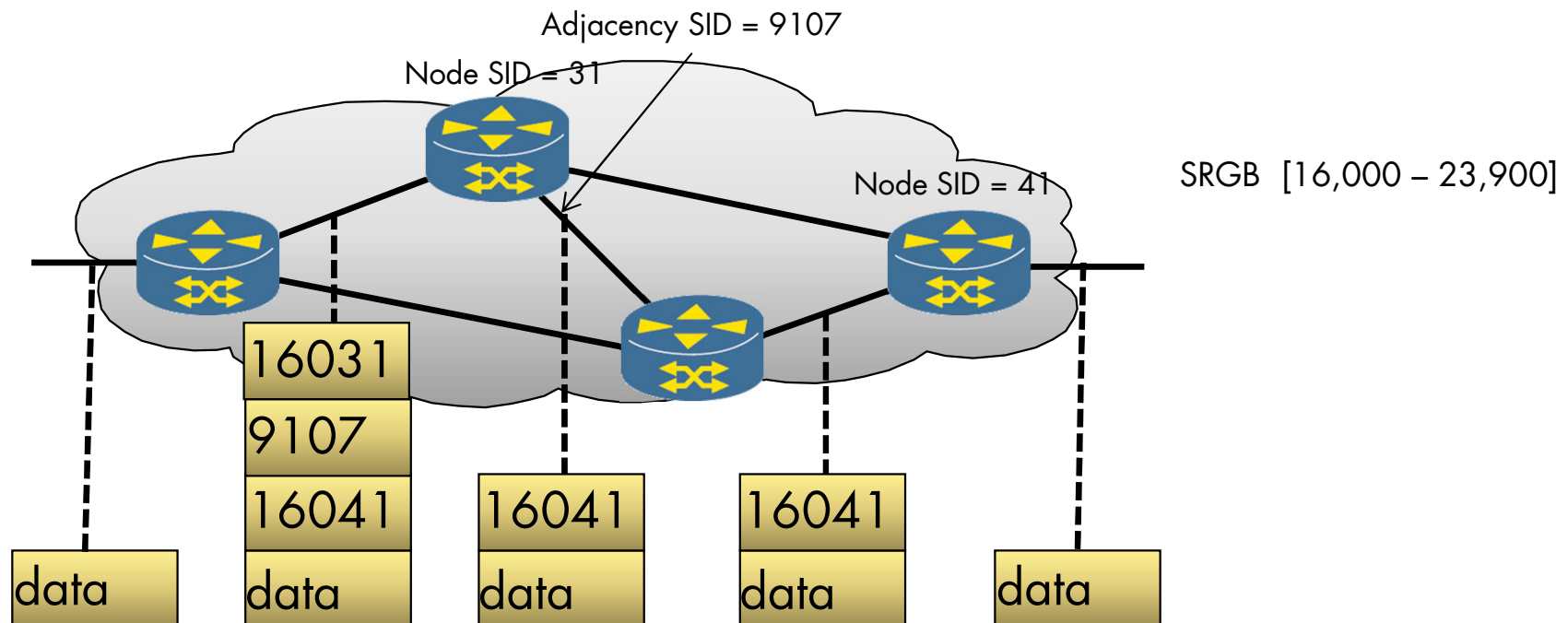
Weiterleitung entlang der IGP-Nachbarschaft

Ausführung der Pop-Operation

Der vorletzte Hop entfernt immer die letzte Adjacency ID



Weiterleitung basierend auf dem Label-Stack
Per-flow Status nur am Eingangs-SR-Knoten

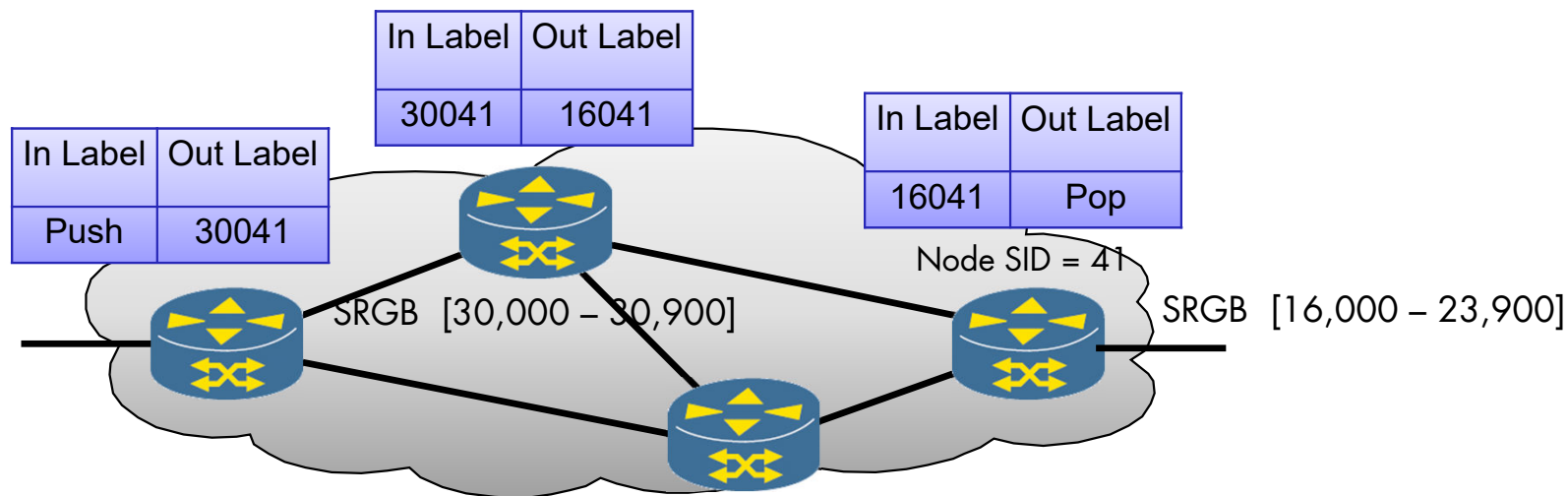


Building Blocks: Segment Routing Global Block (SRGB)

Die Node-SID wird als relativer (Index-)Wert angegeben

Der Index stellt einen Offset vom SRGB-Basiswert dar
und ist global eindeutig

Der SRGB-Wert kann zwischen den Knoten variieren



Beschreibung	SR-MPLS	SRv6
Identifizier	20 Bit MPLS Label	128 Bit IPv6 Adresse (SID)
Kompletter Pfad	MPLS Label Stack	IPv6 Header plus Segment Routing Header
Mapping	Label zeigt auf IP Adresse	Adresse Selbst enthält die Anweisungen
Protokoll/Hardware	MPLS mit Labelzuweisung	Plain IPv6
Use Case	Upgrade bestehender Netze	Neue Netze komplett auf IPv6

- Bei SR-MPLS kann das Netz IPv4 oder IPv6 sein.
- IPv6-Adresse wird unterteilt in logische Blöcke
 - Locator: Routbarer Teil der Adresse
 - Function: z.B. Paket an Interface A senden, oder in VRF A weiterleiten
 - Arguments: Zusatzinformationen wie Flow-Parameter, Multicast-Infos

Flex Algo (Flexible Algorithm) ist aktuell eine Schlüsseltechnologien für moderne Weitverkehrsnetze (WAN) und Rechenzentren

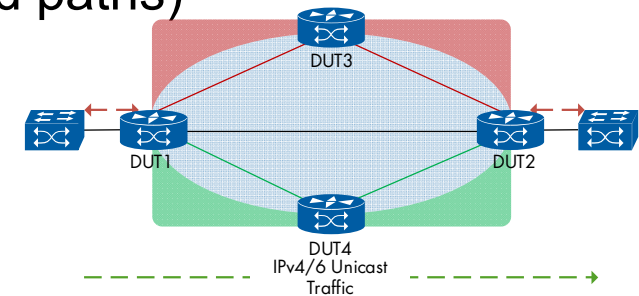
- Es wird heute standardmäßig eingesetzt, um Netzwerke effizient zu "schneiden" (Network Slicing) und Traffic Engineering zu vereinfachen.
- Anstatt mühsam jeden Pfad einzeln zu konfigurieren, erlaubt Flex Algo dem Routing-Protokoll (OSPF oder IS-IS), automatisch mehrere "logische Topologien" auf derselben physischen Infrastruktur zu berechnen

Warum Flex Algo genutzt wird

- Automatisches Traffic Engineering: Router berechnen Pfade basierend auf Verzögerung (Latency) statt nur auf Bandbreite, notwendig für Echtzeitanwendungen (Cloud-Gaming oder autonomes Fahren)
- Network Slicing für 5G & AI: Betreiber nutzen Flex Algo für dedizierte virtuelle Netzwerke (z. B. eine „Low Latency“-Slice und eine „High Throughput“-Slice)
- Im Vergleich zu alten Methoden (wie RSVP-TE) braucht es keinen zentralen Controller für die Pfadberechnung – die Intelligenz liegt direkt in den Routern

- Flexible Algorithm erlaubt über Routing Protokolle (IGPs):

- Benutzerdefinierte Pfade (constraint-based paths)
- Nicht den kürzesten nach IGP
- Pfade können Latenzen, Bandbreite, oder Farben (Colors) berücksichtigen



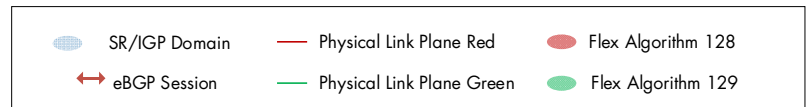
- Routing ohne externen Controller

- Wird direkt auf Router konfiguriert

- Flex-Algo definiert eine logische Topologie

- Nutzt ggf. nicht das komplette physische Netz
- Nutzt Metriken/Constraints innerhalb derselben IGP-Domain

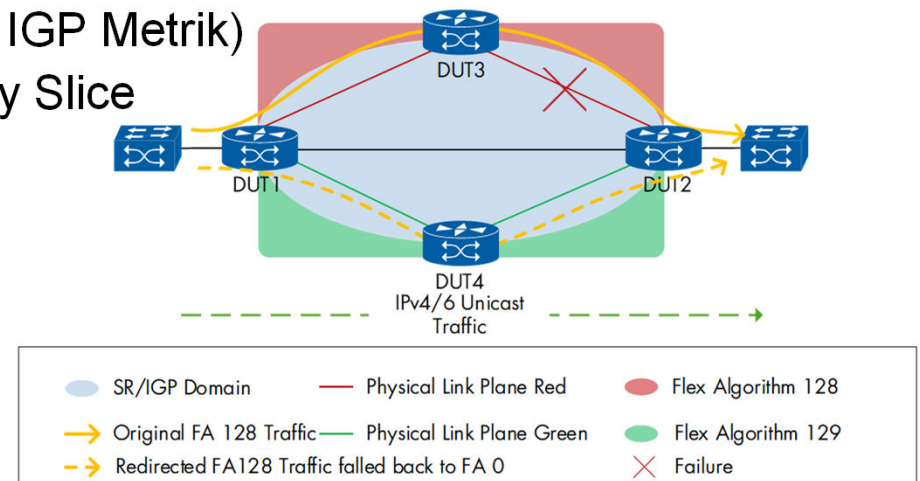
- Verbunden mit Segment Routing (SR) und erlaubt SR-MPLS und SRv6 durch Zuweisen von Algorithm-Specific SIDs/locators zu Flex-Algo



- **Flexible Algorithm Definition (FAD) definiert:**
 - z.B. minimale Latenz
 - Der Betreiber definiert einen oder mehrere Flex-Algorithmen (IDs) mit Parametern wie Metriktyp (IGP, TE, Latenz), ein-/ausgeschlossenen „Linkfarben“ (Colors) usw.
- **Identifikation über eine Zahl von 128-255**
 - Ausgewählte Knoten veröffentlichen FADs im IGP; anschließend führen sie separate SPF-Berechnungen pro Flex-Algorithmus durch
- **Berechnung**
 - Jeder Router berechnet Pfad mit Berücksichtigung der Einschränkung
 - Knoten veröffentlichen Präfix-SIDs/SRv6-Locators pro Flex-Algorithmus, sodass jeder Knoten mehrere SIDs haben kann, eine für jeden Algorithmus (z. B. Standard, niedrige Latenz)
- **Weiterleitung durch Segment Routing durch das Netz**
 - Das IGP stellt automatisch TE-optimierte Pfade für jeden Flex-Algorithmus bereit

Typische Use Cases

- Erstelle “virtual topologies” für verschiedene Dienste:
 - Algo 0 - default best-effort (Standard IGP Metrik)
 - Algo X - Low-Latency oder Low-Delay Slice
 - Algo Y – Pfad zur Vermeidung von spezifischen Links oder Knoten

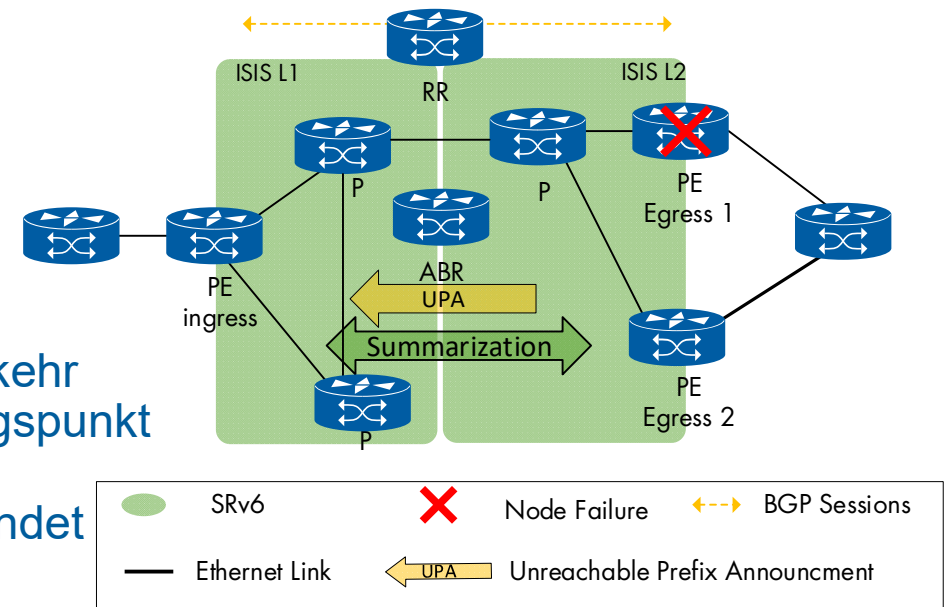


- Einfaches Traffic Engineering in SR-Netzwerken ohne vollständigen SR-TE-Controller – besonders attraktiv für kleinere oder regionale Implementierungen
- Verwenden von Flex-Algo-spezifischen SIDs direkt (z. B. „Traffic über Low-Latency-Algorithmus senden“) oder als Bausteine in SR-Richtlinien und TI-LFA-Backup-Pfaden

Unreachable Prefix Announcement (UPA)

Was ist UPA?

- eine IGP-Funktion, die den Verlust der Erreichbarkeit eines bestimmten Präfixes, explizit ankündigt
- Ziel: Remote-Router sollen den Datenverkehr schnell von einem ausgefallenen Ausgangspunkt umleiten selbst wenn eine Präfix-/Locator-Zusammenfassung verwendet



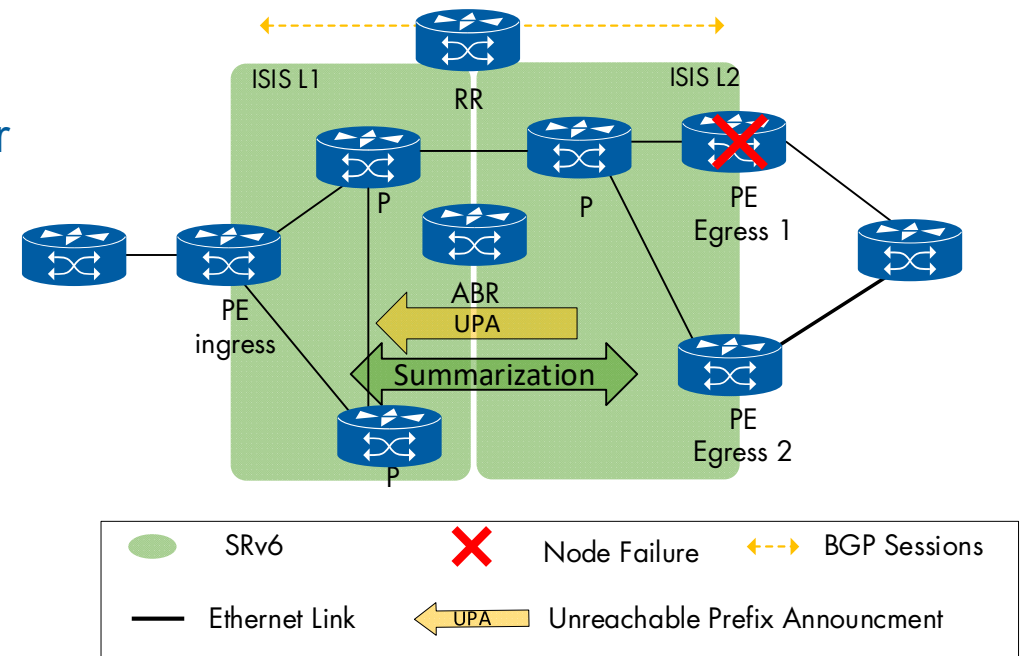
Funktionsweise von UPA auf IGP-Ebene

- Wenn ein ABR/ASBR feststellt, dass ein einzelnes Präfix nicht mehr erreichbar ist, erzeugt er eine UPA für dieses Präfix
- Die UPA wird wie eine normale IGP-Ankündigung über alle Bereiche/Ebenen verteilt
- Zwischenrouter leiten die UPA einfach weiter; nur ABRs und Ingress-PEs müssen sie verstehen und darauf reagieren

Warum braucht es Unreachable Prefix Announcement (UPA)

Wie UPA die BGP/SR-Dienste unterstützt

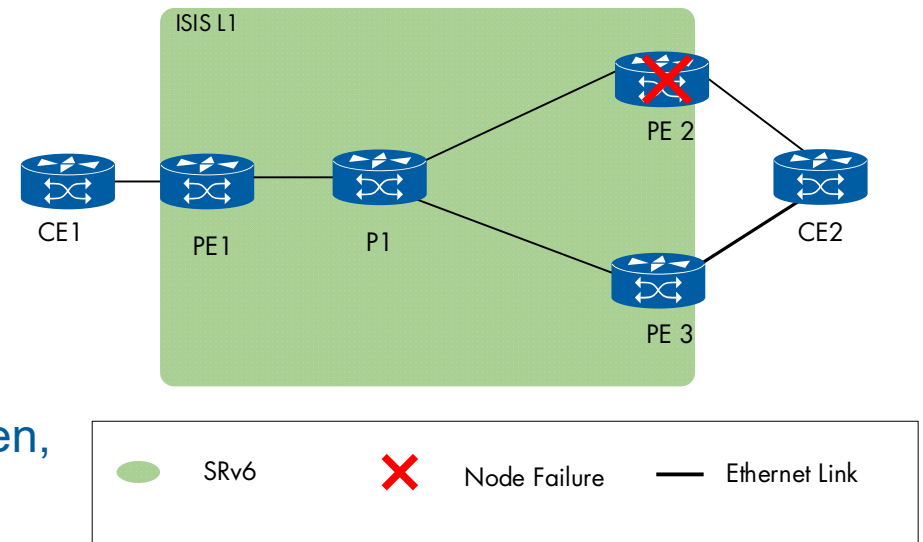
- Ingress-PEs, die eine UPA empfangen, markieren das entsprechende Ausgangspräfix als nicht erreichbar und lösen ein schnelles BGP FRR für Routen aus, die diesen Ausgangspunkt hinter der Route Summarization verwenden



- Schnelle Umschaltung auf den Backup-Pfad
- Dadurch wird ein langes Blackholing vermieden, wenn ein SRv6/SR-MPLS-Ausgang hinter einer Route Summarization liegt

Schnelle Fehlererkennung mit BFD

- Bidirectional Forwarding Detection (BFD) ermöglicht die Fehlererkennung von
- Oft sogar unter 50 ms, unabhängig von IGP/BGP-Hello-Timern
- BFD-Sitzungen sind an IGP-Nachbarschaften, BGP-Sitzungen und teilweise auch an SR-Tunnel gebunden



BGP PIC (Prefix Independent Convergence)

- BGP PIC berechnet Backup-Next-Hops im RIB/FIB vor, sodass bei einem Next-Hop- oder Egress-Fehler lediglich eine kleine Zeigeränderung (Pointer auf die Route) erforderlich ist und nicht alle Präfixe neu verarbeitet werden müssen
- Ein Core-/Edge-PE-Fehler oder der Verlust des Next-Hops löst eine schnelle Umschaltung auf Backup-Pfade aus
- Unerlässlich für die Hochverfügbarkeit von L3VPN-, EVPN- und Internetdiensten über SR-Pfade

Ziel von IGP Fast Reroute (FRR)
Lokaler Schutz:

- Umleitung des Datenverkehrs um eine ausgefallene Verbindung/einen ausgefallenen Knoten innerhalb von Millisekunden, noch vor der vollständigen IGP-Konvergenz
- Der Schutz wird pro primärem Next-Hop vorab berechnet

Grundlagen von Loop-Free Alternates (LFA)

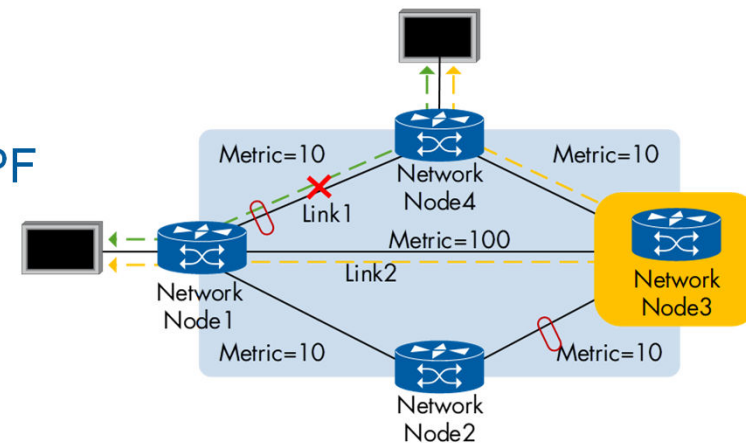
- LFA wählt einen Nachbarn als Backup-Next-Hop aus, sofern dieser die Schleifenfreiheitsbedingung erfüllt
- Remote-LFA erweitert LFA, indem der Datenverkehr über einen Backuptunnel zu einem PQ-Knoten geleitet wird, um die Abdeckung über direkte Nachbarn hinaus zu verbessern (P-Space = Source Side, Q-Space = Destination Side)
 - Knoten, die den Source-Router und Destination-Router erreichen ohne Ausfall
- Zwischenrouter leiten die UPA einfach weiter; nur ABRs und Ingress-PEs müssen sie verstehen und darauf reagieren

Interaktion mit Segment Routing (vor TI-LFA)

- In SR-MPLS-/SRv6-Netzwerken können LFA/Remote-LFA SR-SIDs/Labels als Backup-Tunnel verwendet werden
- IGP berechnet primäre Next-Hops und LFA/Remote-LFA-Backups
- Im Fehlerfall wechselt der Router zum Backup-Next-Hop oder zum SR-basierten Backuptunnel
- LFA / Remote-LFA bleiben grundsätzlich nützlich
- TI-LFA verallgemeinert dies für Segment Routing
- Verwendet explizite SR-Segmentlisten, um die Abdeckung (Backups) zu maximieren

Ziele von TI-LFA

- Fast Reroute Mechanismus für IS-IS/OSPF
- Berechnet SR-Backuppfade (Segmentlisten) vorab
- Lokale Reparatur in SR-MPLS- und SRv6-Netzwerken unter 50 ms



Funktionsweise von TI-LFA

- Für jeden primären Next-Hop berechnet der Router einen Shortest Path Tree, der die geschützte Ressource (Link/Knoten) ausschließt
- Der Backuppfad wird als SR-Segmentliste (MPLS-Labels oder SRv6-SIDs) kodiert und vorab in die FIB eingetragen
- Im Fehlerfall greift der Router auf die vorinstallierte SR-Backupliste zurück
- Vorteile gegenüber klassischem LFA/Remote-LFA:
 - Einheitlicher Mechanismus
 - Integration mit TE & FlexAlgo

Aktuelle MPLS-Netzwerke im Brownfield-Umfeld

- Viele SP- und DC-Backbones nutzen LDP und/oder RSVP-TE über MPLS mit umfangreichen VPN/EVPN- und Internetdiensten
- Diese Netzwerke sind stabil, aber betrieblich komplex
- Betreiber wünschen sich SR-MPLS/SRv6 für einfacheres TE, Automatisierung und verbesserte Hochverfügbarkeit

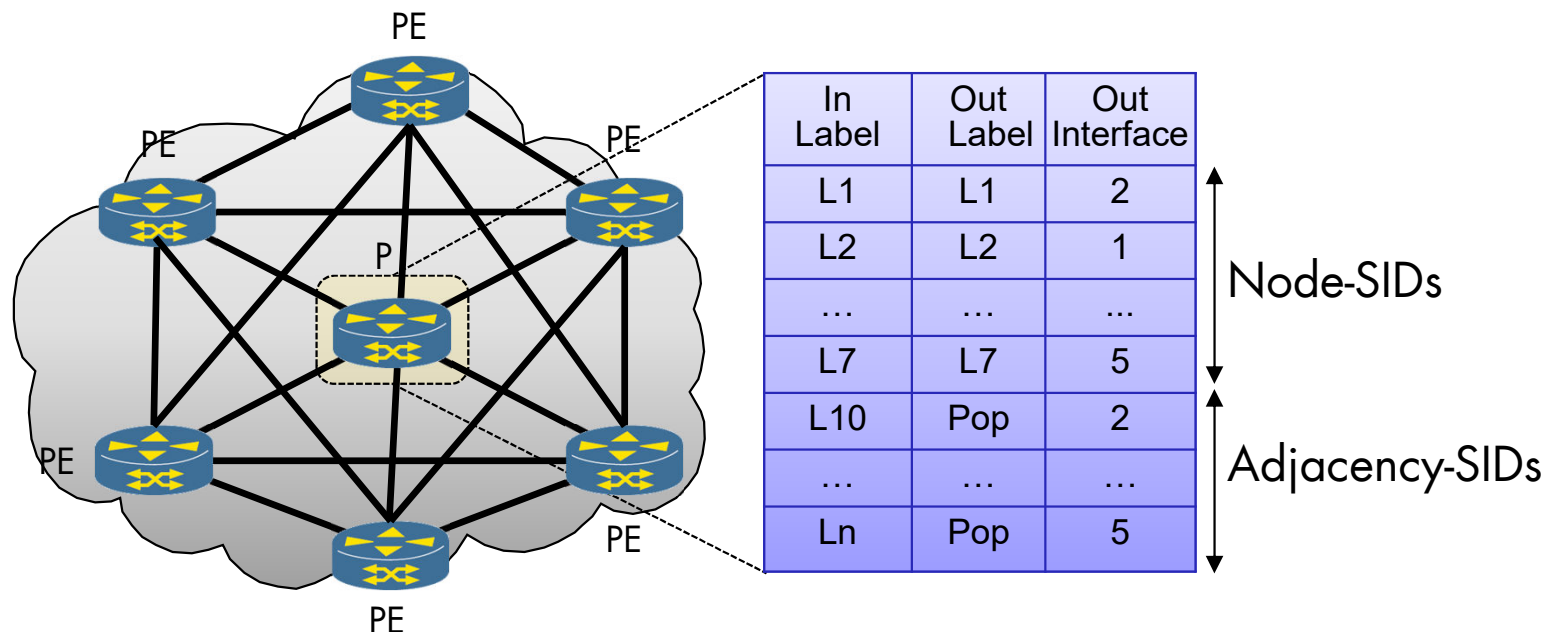
Koexistenz ist der übliche erste Schritt

- Die MPLS-Architektur ermöglicht den gleichzeitigen Betrieb mehrerer Label-Control-Planes
- Interworking-Mechanismen ermöglichen die durchgängige Übertragung von Datenverkehr zwischen SR- und Legacy-MPLS-Tunneln
- Sinnvoll während der Migration

Label Forwarding Information Base (LFIB) zugewiesen
über IGP (ISIS / OSPF)

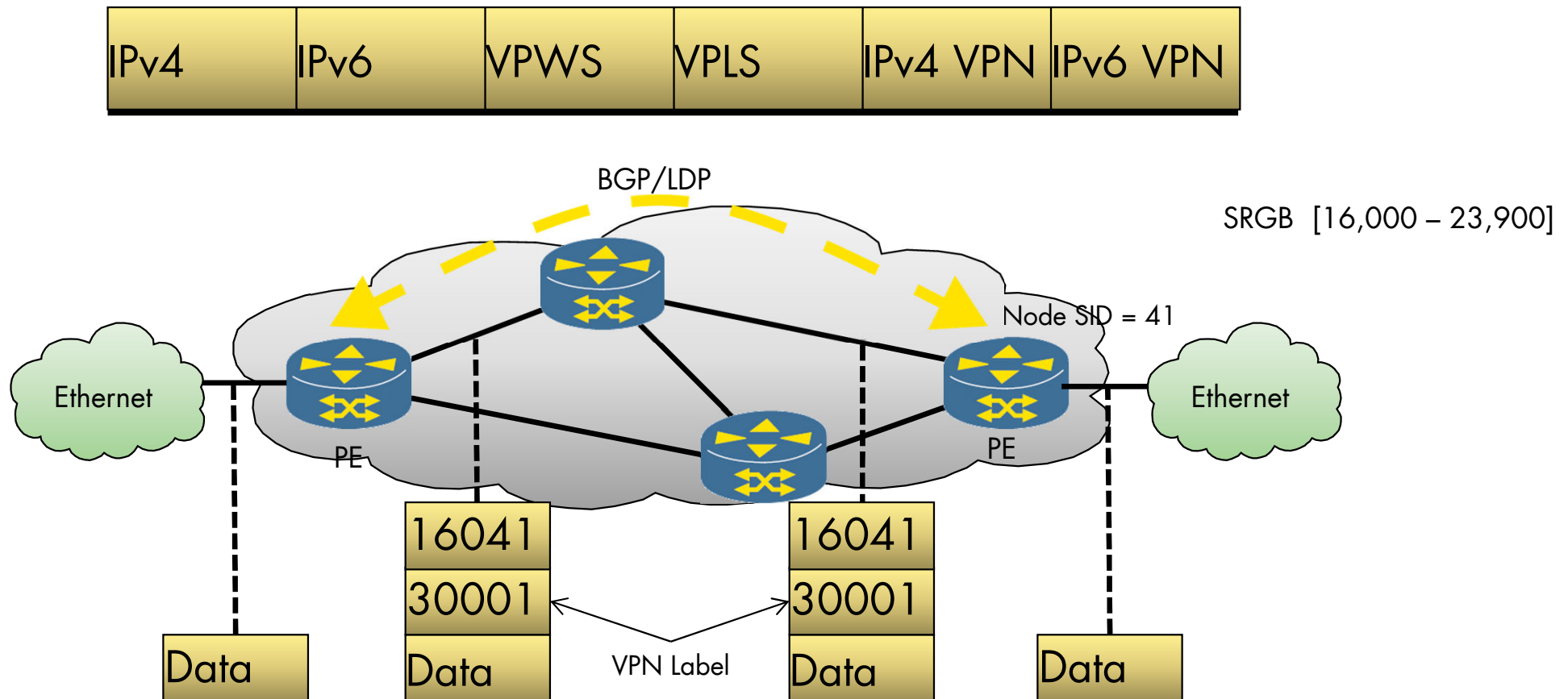
Die MPLS Architektur erlaubt die gleichzeitige Nutzung
von verschiedenen Label Distribution Protokollen

Forwarding table bleibt konstant (Nodes + Adjacencies)
unabhängig von der Anzahl der Pfade



Nutzen aller MPLS services

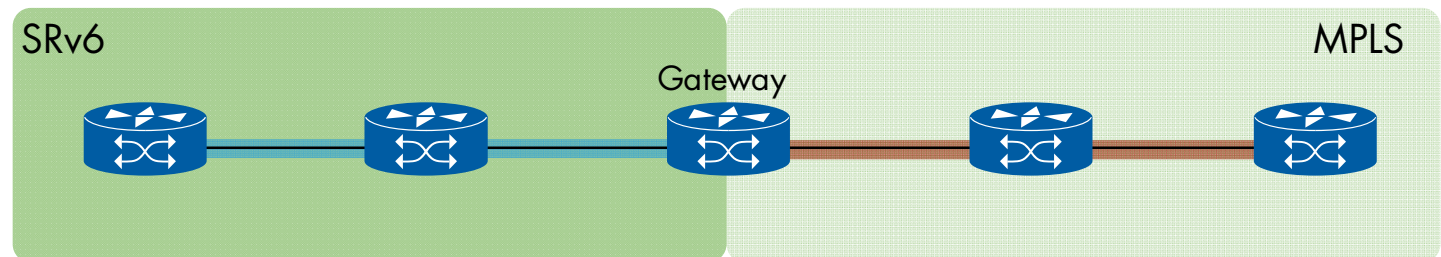
Keine Änderungen an der MPLS-Control oder Forwarding-Plane



Was ist ein SRv6-MPLS-Interworking-Gateway?

- Ein Gateway-Router, der sowohl BGP-SRv6-basierte als auch BGP-MPLS-basierte L2/L3-Dienste für dieselbe Serviceinstanz (VRF, EVPN EVI) unterstützt
- Grenze zwischen einer SRv6-Domäne und einer MPLS/SR-MPLS-Domäne
- Genutzt für L3VPN, EVPN-L3 und EVPN VPWS über SRv6- / MPLS-Netzwerke während der Migration

Migrationsrolle



- Das Gateway baut BGP-Sitzungen zu beiden Seiten auf
 - Zu SRv6-PEs: Ankündigung von L2/L3-Servicerouten mit SRv6-Service-SIDs
 - Zu MPLS-PEs: Ankündigung derselben VPN/EVPN-Präfixe mit MPLS-Service-Labels
- Für jedes gelernte Präfix installiert das Gateway dieses in der Dienstinstanz und kündigt es mit dem anderen Kapselungstyp erneut an

Verfügbarkeit in Netzen

BERECHNUNG

- Ausfallsicherheit der Komponenten erhöhen
 - redundante Komponenten
 - redundante Spannungsversorgung
 - USV
 - regelmäßige Wartung
 - Hot-Plugging
 - kontrollierte Umgebungsbedingungen
- Ausfallzeit reduzieren
 - Ersatzteile bevorraten
 - Überwachung
 - Wartungsverträge

- Netztopologie
 - logische Funktionsblöcke (Cluster)
 - Redundante Netzwerkpfade
 - Layer 2 oder Layer 3 Anbindung
- First Hop Redundancy
 - Redundanz im Access Layer
 - Kombination mit redundanten Netzwerkpfaden
- Routing Protokolle
 - Protokollauswahl, Wiederherstellungszeiten berücksichtigen
 - Kombination mit redundanten Netzwerkpfaden

Verfügbarkeit (Anzahl von 9s)	Verfügbarkeit (%)	Ausfallzeit pro Jahr	Ausfallzeit pro Monat
1	90%	36,5 Tage	72 Stunden
2	99%	3.65 Tage	7.2 Stunden
3	99.9%	8.76 Stunden	43.8 Minuten
4	99.99%	52.56 Minuten	4.38 Minuten
5	99.999%	5.26 Minuten	26,3 Sekunden
6	99.9999%	31,5 Sekunden	2.59 Sekunden

Maximale Ausfallzeit pro Jahr = $(1 - \text{Verfügbarkeit}) * \text{Gesamtzeit}$

100 % Verfügbarkeit = $365 \text{ d} * 24 \text{ h} * 60 \text{ Min} * 60 \text{ Sec} = 31.536.000 \text{ Sec}$

- $365 \text{ Tage} = 8760 \text{ Std.} = 525.600 \text{ Min.} = 31.536.000 \text{ Sec}$

Berechnung für 99,9% Verfügbarkeit

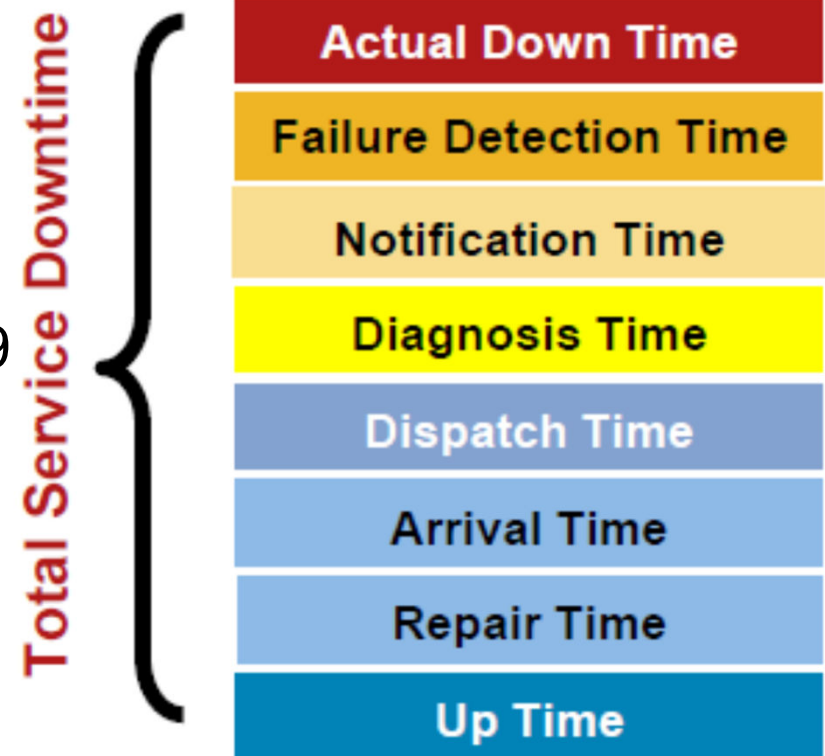
Bedeutet, dass nur 0,1% der Zeit Ausfallzeiten zulässig sind

- Gesamtzeit pro Jahr: 8760 Stunden
- Gesamtzeit pro Monat: 730 Stunden
- Ausfallzeit pro Jahr: $(1 - 0.999) * 8760 \text{ Std.} = 8,76 \text{ Stunden}$
- Ausfallzeit pro Monat: $(1 - 0.999) * 730 \text{ Std.} = 0,73 \text{ Stunden}$
 $0,73 \text{ Std.} * 60 \text{ Min} = 43,8 \text{ Minuten}$

- Geplante Zeiträume
 - Systeme offline aufgrund von Wartungsarbeiten, Upgrades, etc.
- Perioden sind geplant und im Voraus angekündigt
- Unternehmen rechnen oft die Verfügbarkeit inkl. Wartung
 - Beispiel: geplante Wartung, 2 Stunden pro Monat offline
 - Zeit wird von der Gesamtverfügbarkeit abgezogen
- Service Level Agreement (SLA) inkl. Wartungsfenster
 - Wartung 2 Stunden pro Monat (24 Stunden pro Jahr)
 - Ungeplante Ausfallzeit: 10 Stunden pro Jahr
 - Ausfallzeit: 24 Std. (Wartung) + 10 Std. (Fehler) = 34 Stunden

- Geplante Wartungsfenster
 - 2 Stunden pro Monat (24 Stunden pro Jahr)
- Ungeplante Ausfallzeit: 10 Stunden pro Jahr
- Ausfallzeit: 24 Std. (Wartung) + 10 Std. (Fehler)
 - Gesamte Ausfallzeit 34 Stunden
 - Gesamtzeit pro Jahr: 365 Tage = 8.760 Stunden
 - $\text{Verfügbarkeit (\%)} = (1 - (34 \text{ Std.} / 8760 \text{ Std.})) * 100$
 - 99,61% Verfügbarkeit

- Das Netz darf maximal einen Arbeitstag (8 Std.) ausfallen
 - Wie hoch muss die Verfügbarkeit im Jahr mindestens sein?
 - $8 \text{ Std.} = 8 * 60 * 60 = 28.800 \text{ Sec}$
 - $28.800 \text{ Sec} / 31.536.000 \text{ Sec} = 0,0009$
 - Maximale Ausfallzeit = 0,09 %
- Verfügbarkeit = 99,91 %



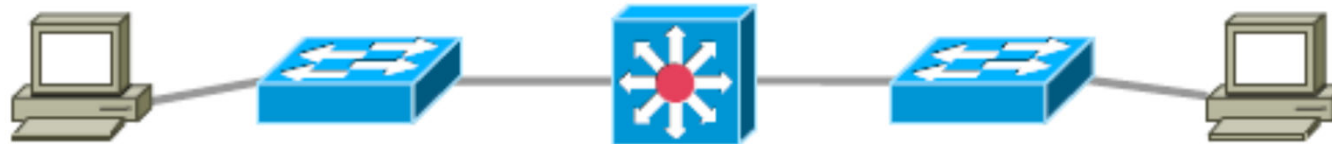
MTBF (Mean Time Between Failures) und MTTR (Mean Time to Repair)



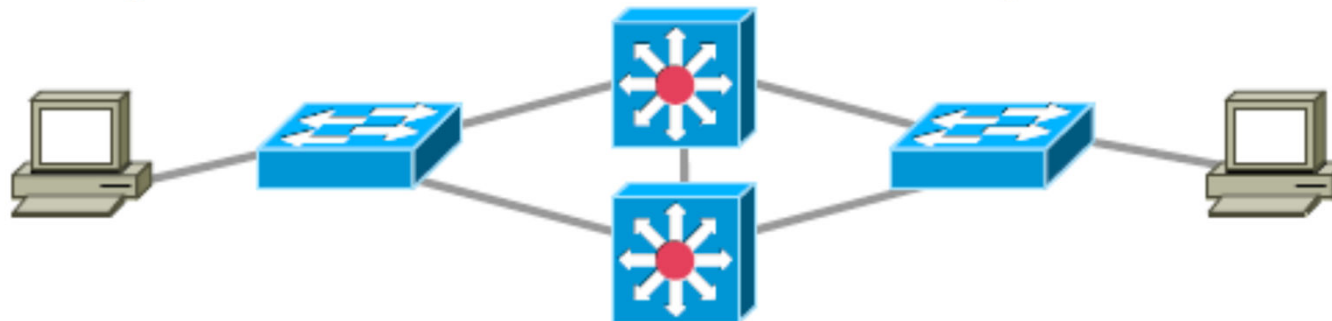
- MTBF
 - Durchschnittliche Zeit, die ein System oder eine Komponente zwischen zwei aufeinanderfolgenden Ausfällen arbeitet
 - Verwendet, um die Zuverlässigkeit eines Systems zu messen
- MTTR
 - Durchschnittliche Zeit, um ein System oder Komponente nach einem Ausfall zu reparieren und wieder in Betrieb zu nehmen
- Ausfallzeit
 - Zeit, in der ein System nicht betriebsbereit ist
 - Setzt sich aus MTBF und MTTR zusammen
- Gesamte Ausfallzeit
 - $\text{Gesamte Ausfallzeit} = \text{Anzahl der Ausfälle} * \text{MTTR}$

- MTBF: 200 Stunden
- MTTR: 2 Stunden
- Anzahl der Ausfälle pro Jahr: 10
- Gesamte Ausfallzeit pro Jahr = Anzahl der Ausfälle * MTTR
- $V (\%) = (1 - (\text{Gesamte Ausfallzeit} / \text{Gesamtzeit})) * 100$
 - Gesamte Ausfallzeit: 20 Stunden
 - Gesamtzeit pro Jahr: 8760 Stunden (365 Tage * 24 Stunden)
 - $V (\%) = (1 - (20 / 8760)) * 100$
 - $V (\%) = (1 - 0.002283) * 100$
 - $V (\%) = 0.997717 * 100 \approx 99.77\%$

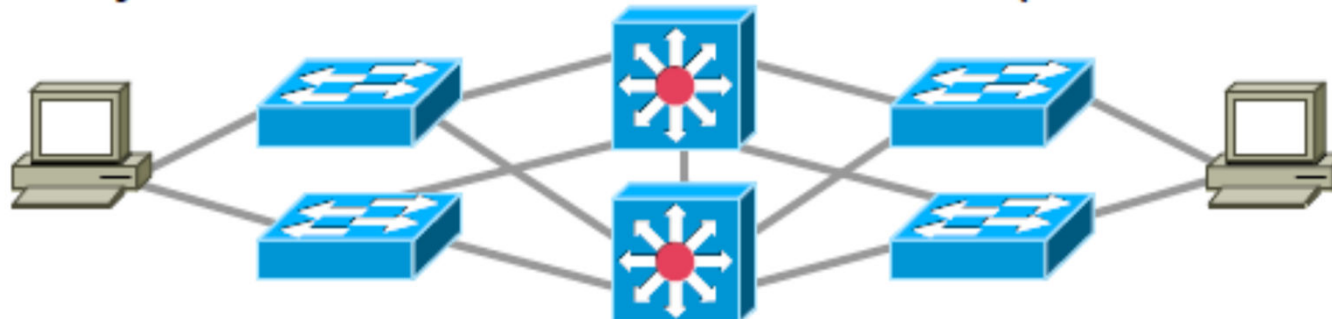
Reliability = 99.938% with Four Hour MTTR (325 Minutes/Year)



Reliability = 99.961% with Four Hour MTTR (204 Minutes/Year)



Reliability = 99.9999% with Four Hour MTTR (30 Seconds/Year)

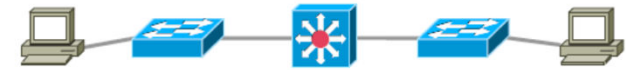


- Verfügbarkeit: 99,938% (0,99938)
- Gesamtzeit pro Jahr: 8760 Stunden (oder 525.600 Minuten)

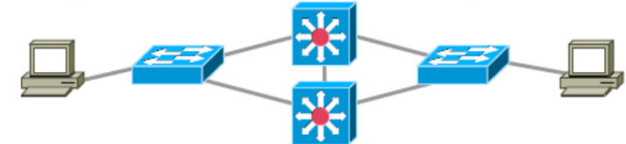
- Gesamte Ausfallzeit: 325 Min/Jahr

- Verfügbarkeit = 99,938% = 0,99938
- Gesamtzeit pro Jahr = 525.600 Minuten
- Erlaubte Ausfallzeit = $(1 - \text{Verfügbarkeit}) * \text{Gesamtzeit}$
- Erlaubte Ausfallzeit = $(1 - 0.99938) * 525600$
- Erlaubte Ausfallzeit = $0.00062 * 525600 = 326,112$ Minuten
- MTTR = Gesamtzeit / Anzahl der Ausfälle
- MTTR = 325 Minuten / n Ausfälle

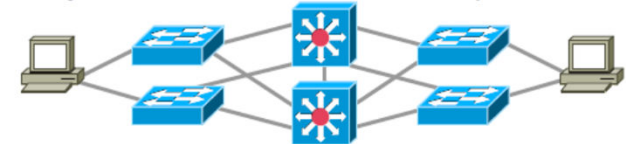
Reliability = 99.938% with Four Hour MTTR (325 Minutes/Year)



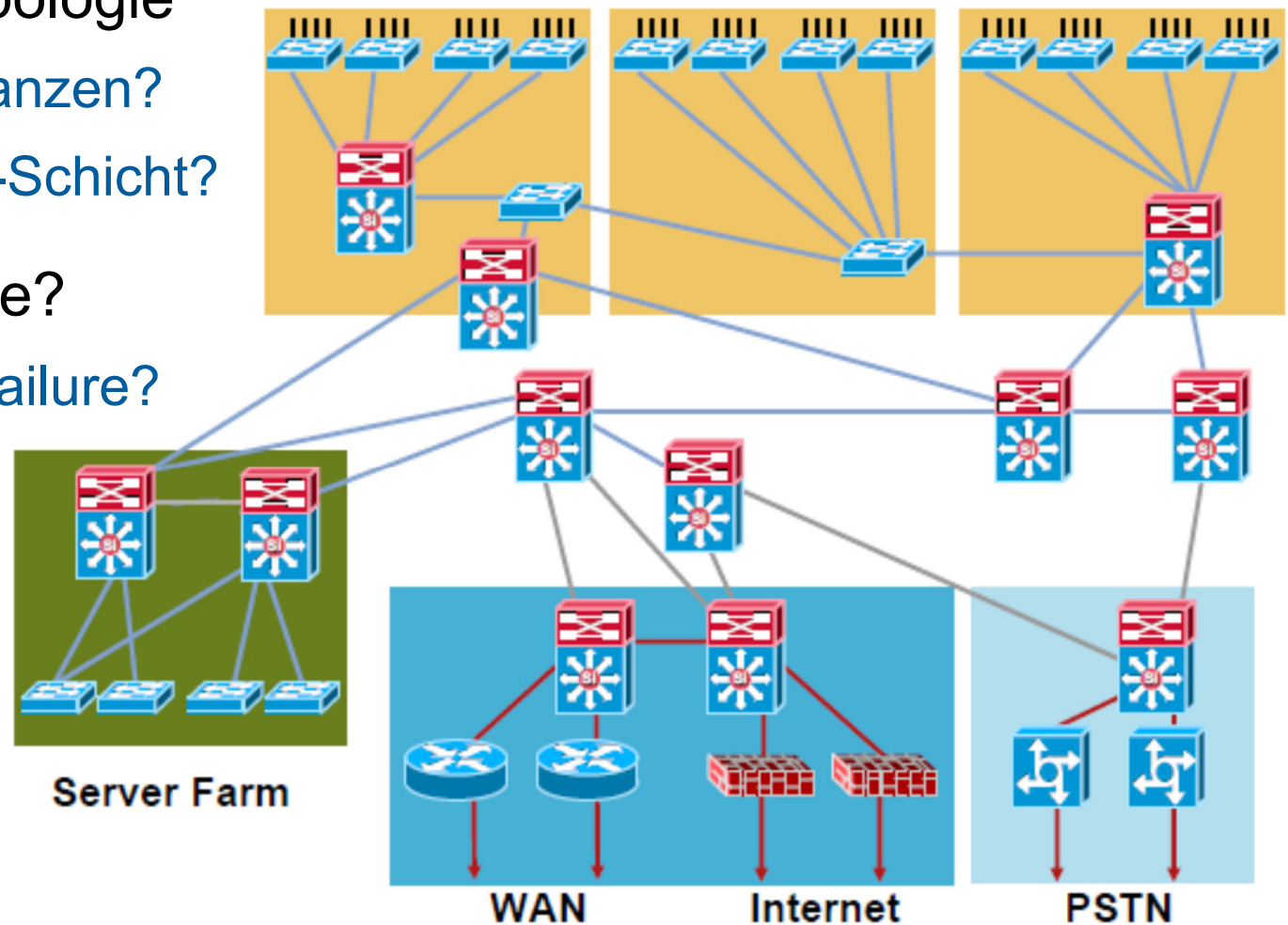
Reliability = 99.961% with Four Hour MTTR (204 Minutes/Year)



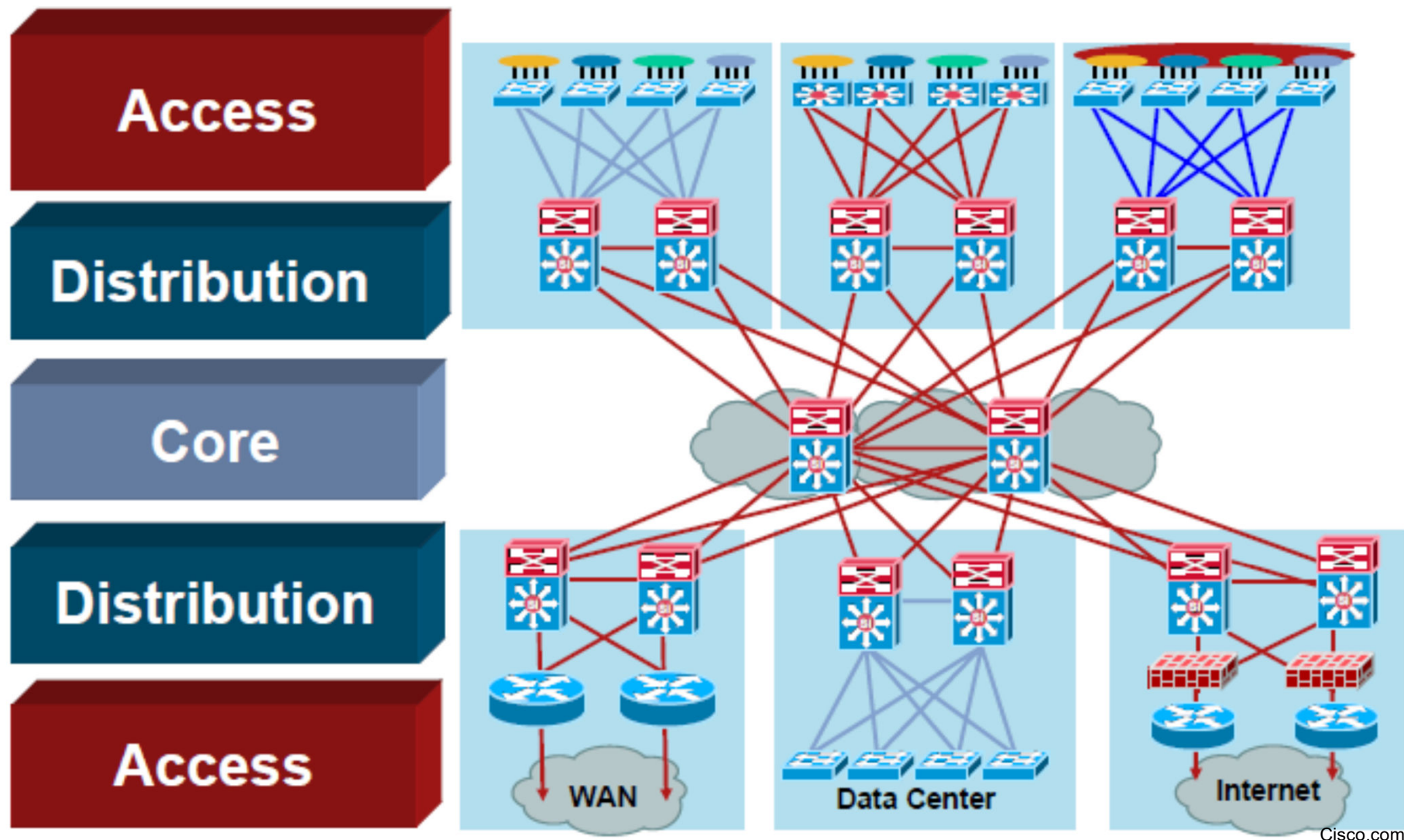
Reliability = 99.9999% with Four Hour MTTR (30 Seconds/Year)



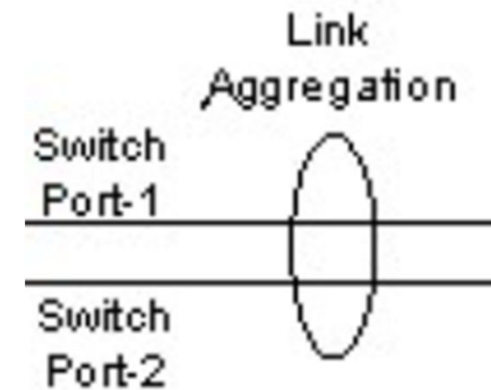
- Gegebene Netztopologie
 - Welche Redundanzen?
 - Auf welcher OSI-Schicht?
- Sinnvolle Topologie?
 - Single Point of Failure?



Cisco.com



- Standard IEEE 802.3ad und später 802.1AX-2008
 - Sub-Layer in OSI-Schicht 2
 - Statisch oder dynamisch konfiguriert
 - Dynamisch mittels Protokoll LACP (Link Aggregation Control Protocol)
- Zusammenfassen von verschiedenen Verbindungen
 - Aggregation (Bündelung) von Ports zu einer logischen Verbindung
 - Erhöhung der zur Verfügung stehenden Bandbreite
 - Redundanz durch mehrere Ports
 - Loadbalancing zwischen den physikalischen Ports
 - Für gestackte Switches auch über Ports auf mehreren Switches



- Bildung einer LACP-Gruppe durch Linkzuordnung
- Maximale Anzahl der LAG-Ports im Portchannel (1-8)
- LACPDUs (Link Aggregation Control Protocol Data Units)
 - Versendet an die Multicast Gruppe 01:80:C2:00:00:02
 - Verwendet für Statusinformationen (Link aktiv?, Prioritäten)
- LACP Pakete werden jede Sekunde versendet
 - Keepalive Mechanismus (default 30s, schnell 1s)
 - Loadbalancing kann eingestellt werden
 - Quell- und Ziel-IP-Hash, berechnet einen Hash-Wert basierend auf Quell-, Ziel-IP-Adresse
 - Layer 4 (TCP/UDP)-Hash
Hash-Wert auf Basis der Quell- und Ziel-IP-Adressen sowie der Quell- und Ziel-Ports (TCP oder UDP) berechnet

Virtual Router Redundancy Protocol (VRRP)

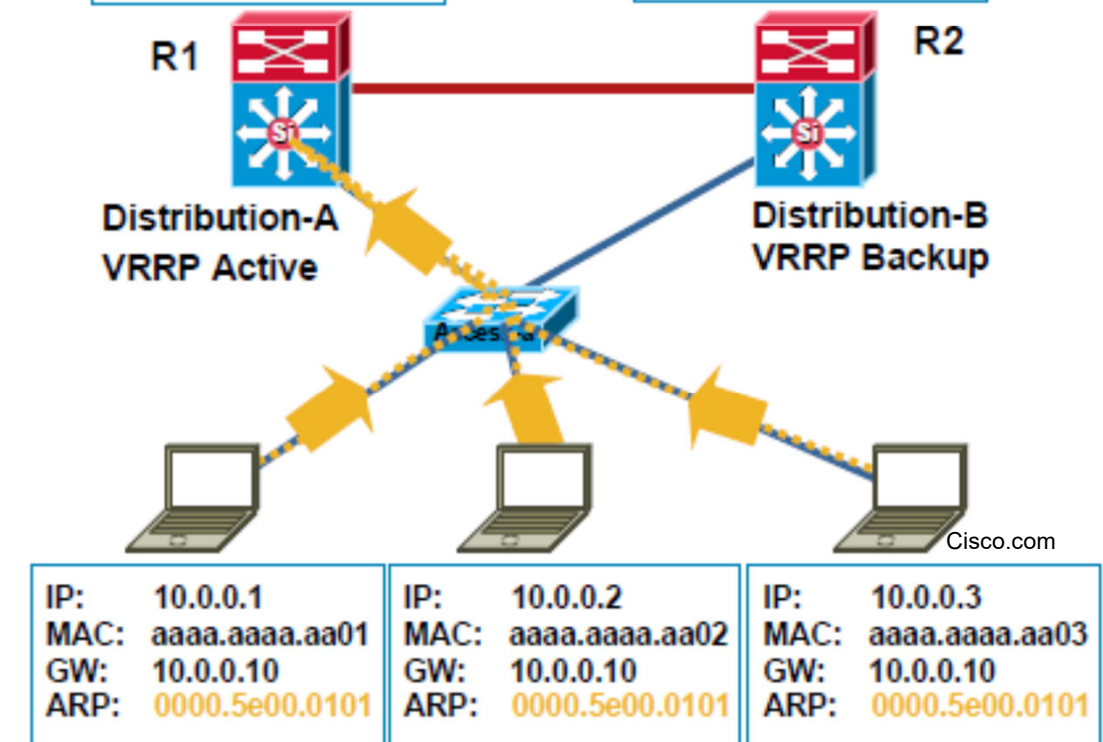
IETF Standard RFC 2338 (April 1998)

- A group of routers function as one virtual router by sharing ONE virtual IP address and one virtual MAC address
- One (master) router performs packet forwarding for local hosts
- The rest of the routers act as "back up" in case the master router fails
- Backup routers stay idle as far as packet forwarding from the client side is concerned

R1—Master, Forwarding Traffic; R2,—Backup
VRRP ACTIVE **VRRP BACKUP**

IP: 10.0.0.254
MAC: 0000.0c12.3456
vIP: 10.0.0.10
vMAC: 0000.5e00.0101

IP: 10.0.0.253
MAC: 0000.0c78.9abc
vIP:
vMAC:



- Virtuelle IP-Adresse
 - Switch kennt virtuelle IP-Adresse (VIP), verwendet von VRRP
 - Leitet den Verkehr zu dieser VIP an den Master Router
- MAC-Adresse
 - VRRP konfiguriert eine virtuelle MAC-Adresse
 - Zugeordnet dem Master Router
- Wechselt der Master Router, übertragen der VIP auf Backup
- Switches verwenden MAC-Adresstabellen
 - Erfährt indirekt vom Ausfall des Master Routers
 - Bekommt eine ARP-Nachricht des neuen Master Routers
 - Aktualisiert die MAC-Adresstabelle auf den anderen Port

