

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, Carrier Ethernet, Ausblick Autonomous Networks
9. Netzwerksicherheit
10. Bewertung Vorlesung/Labore, Prüfungsvorbereitung
11. Prüfungsvorbereitung / offene Fragen (29.4.26)

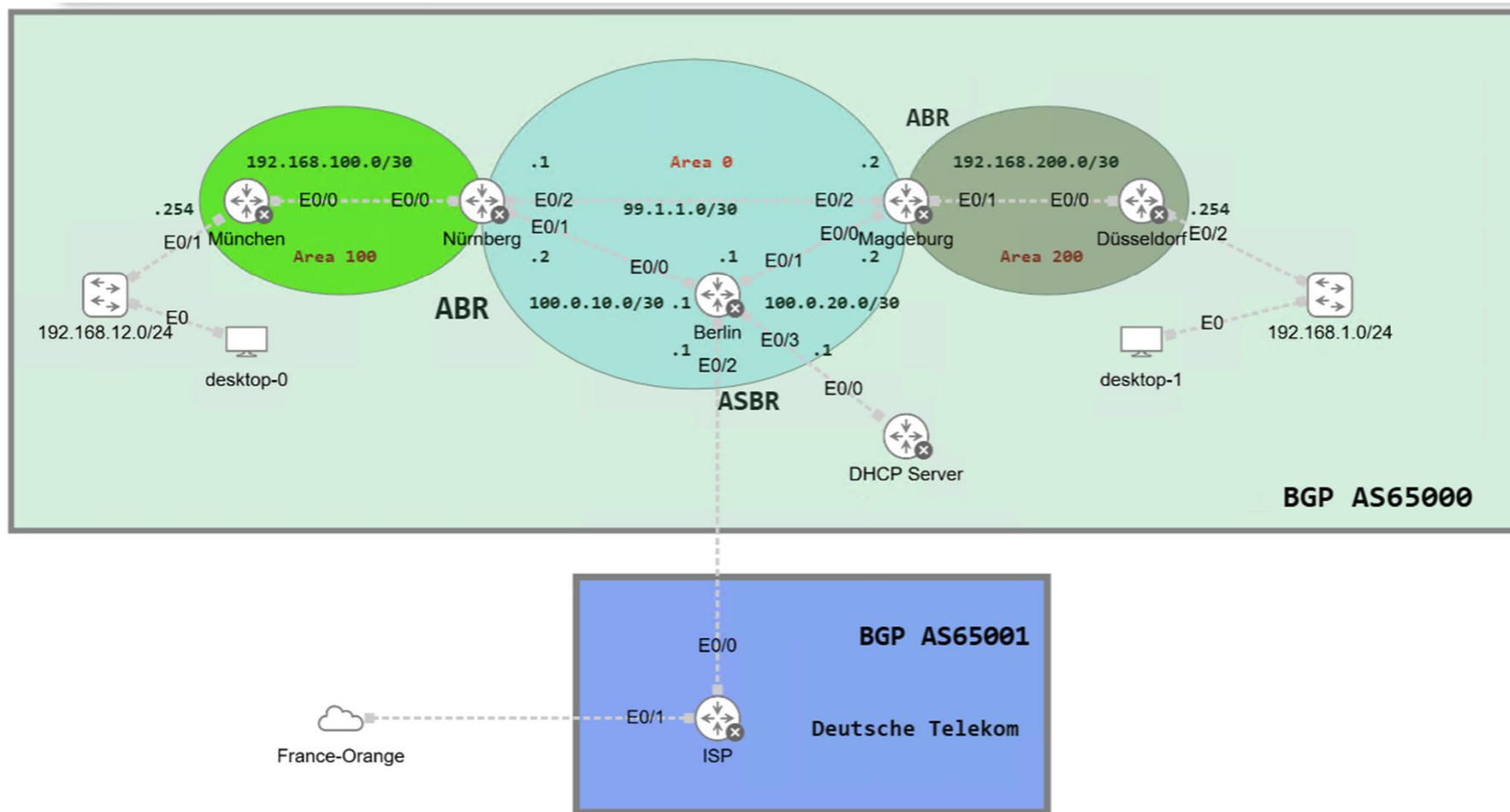
Klausur im Stundenplan, **Mo., 4. Mai 2026** von **14:00 bis 16:00 Uhr**
in den Räumen **6B.369** und **6B.371** statt.

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

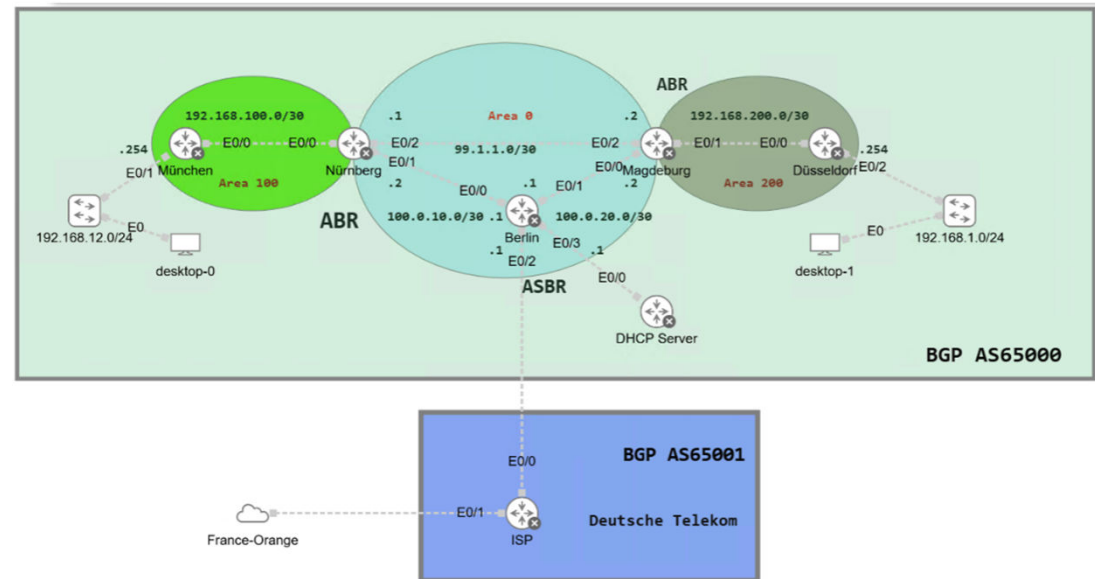
Eine praktische Prüfung ist nicht vorgesehen laut Curriculum

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“

In der aktuellen Woche: DHCP, NAT und BGP



- PC bekommt keine IP Adresse
- PC erreicht einen bestimmten anderen PC nicht



- Mögliche Fehler
 - OSPF-Nachbarschaft/Routing
 - BGP Redistribution
 - Interfaces falsch eingestellt (MTU Size, Adressen....)
 - Und verschiedene andere Fehler ☺

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)

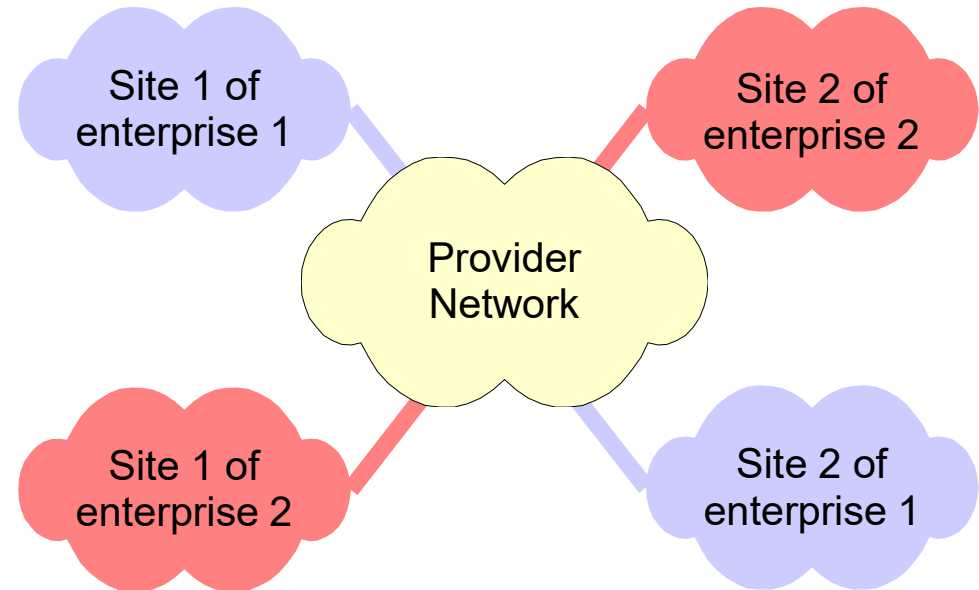
Schritt 6: Korrektur planen/implementieren

Schritt 7: Überprüfen, bzw. testen und dokumentieren

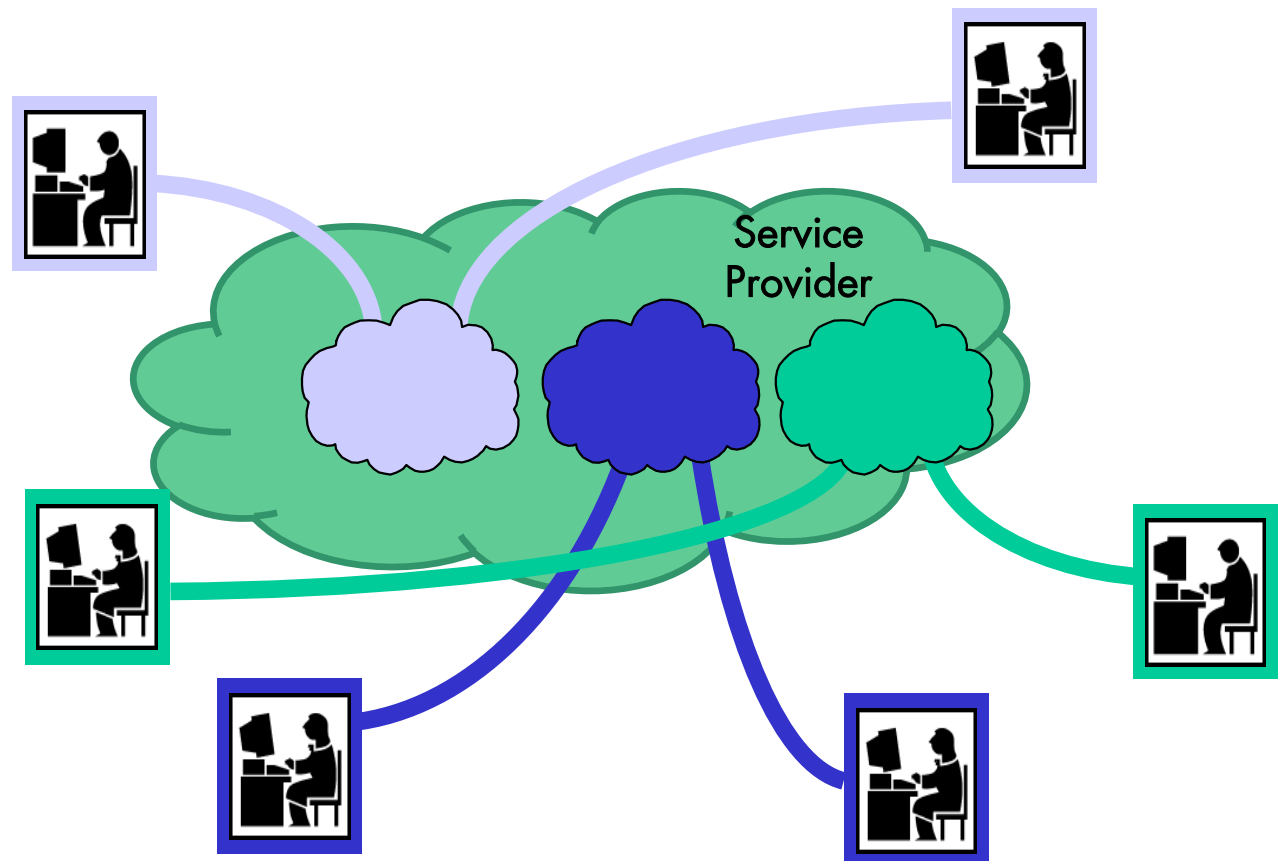
Network Layer - Vermittlungsschicht

LAYER 3

- Verschiedene Standorte mehrerer Unternehmen verbunden über einen SP-Backbone
 - Vorhandenen SP-Backbone verwenden
 - Überlappende Adressräume
 - Verwendung privater und öffentlicher Adressen
 - VPN-Isolierung der Daten
 - Einfache Verwaltung
 - Skalierung
 - Quality of Service

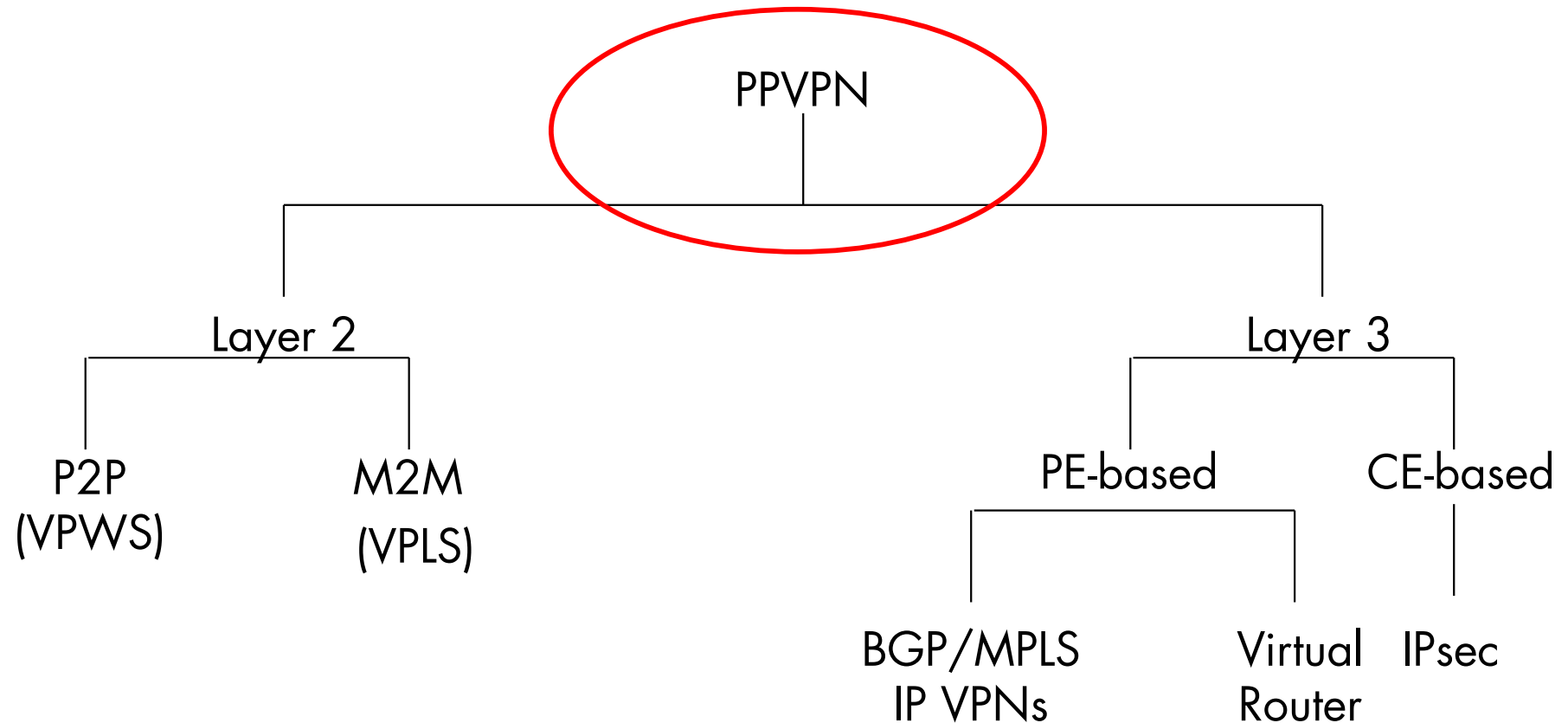


- Verbindet Kundennetze an verschiedenen Standorten
- Alle VPNs teilen sich die SP-Netzinfrastruktur
- Sind voneinander getrennt
- RFC 4026, Provider Provisioned Virtual Private Network (VPN)

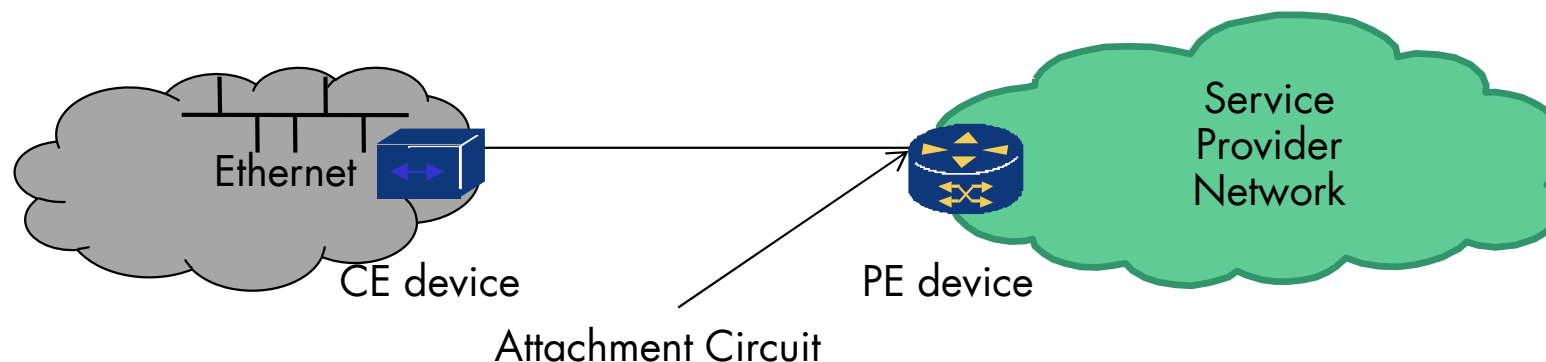


- MPLS wird als Basis für den Backbone beibehalten
 - Bereit für Transport, Resiliency und Traffic Engineering
 - Verbindungsorientierte Charakter gewährleistet QoS, TE
 - Interoperabilität mit allen L1-, L2- und L3-Protokollen
- Label Stacking (Kapselung)
 - Erlaubt Hierarchien, Trennung der Ebenen
- Angemessene Sicherheit
 - Verkehrstrennung verschiedener Kunden
- Qualität der Dienstleistung
 - Bandbreiten- und Performance-Management einfacher
 - Signalisierung von Bandbreiten- und QoS-Anforderungen

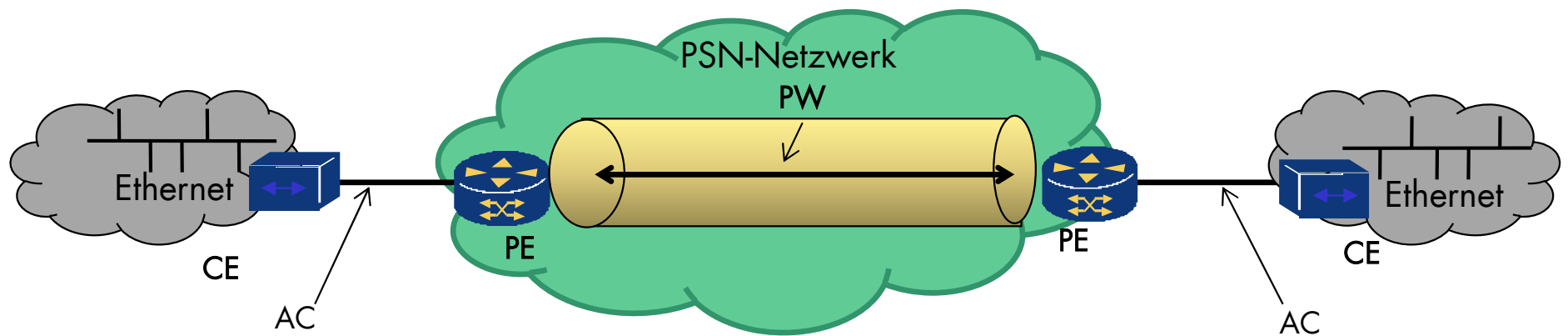
- RFC 4026, Provider Provisioned Virtual Private Network (VPN)



- Physischer oder logischer Anschluss zwischen einem Endgerät (z. B. einem Router oder Switch) und einem Provider Edge (PE) Router
 - Frame Relay DLCI
 - ATM VPI/VCI
 - Ethernet Port
 - VLAN
 - PPP-Verbindung auf einer physikalischen Schnittstelle
 - MPLS LSP, etc.
- Stellt Verbindung her, über die Daten übertragen werden

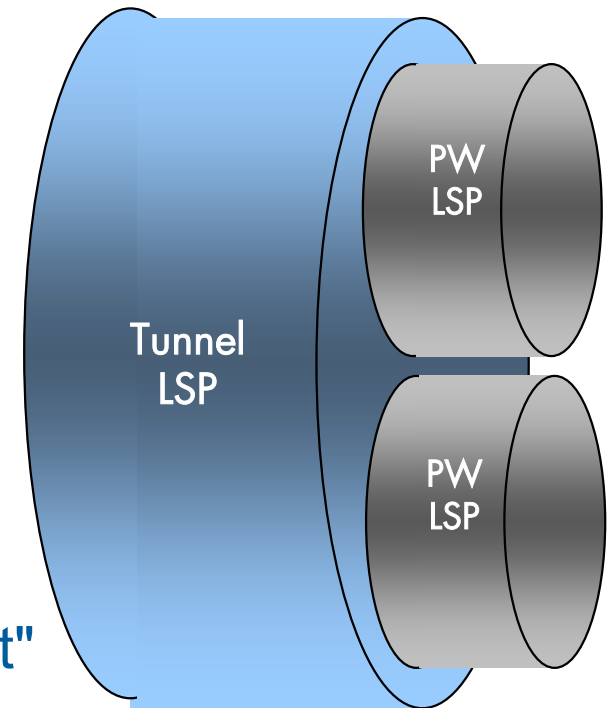


- Definiert für verschiedene ACs (Attachment Circuits)
 - ATM, TDM, Frame Relay, Ethernet usw.
- Definiert Kapselungsmechanismus für L2-Daten von AC -> PW
- Ist nur an den Endpunkten, also an zwei PEs bekannt
- PW wird über einen Tunnel transportiert
 - Allen LSRs entlang des Weges, zwischen PEs bekannt

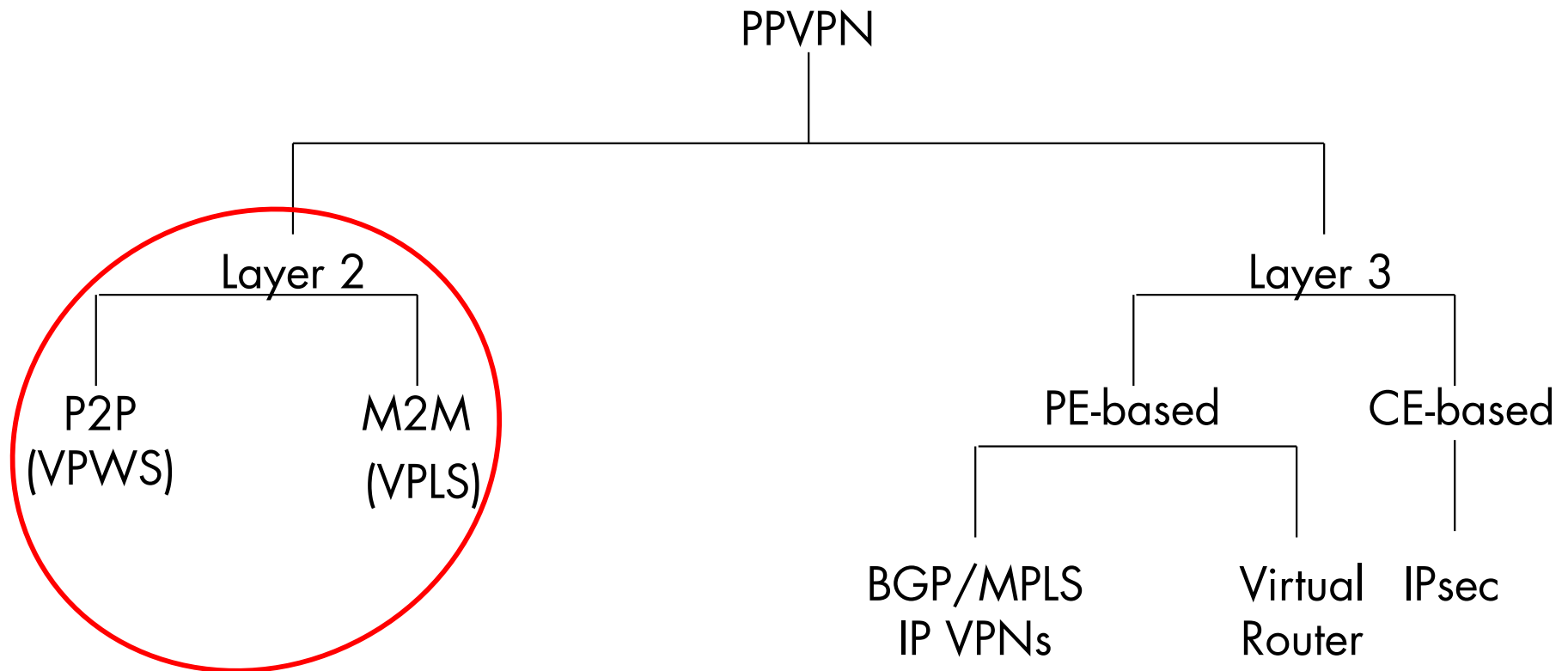


* Der Tunnel ist unidirektional

- Aggregiert mehrere PW LSPs zwischen zwei PEs
 - Nur PEs kennen die L2VPN (Pseudowires)
- Zwei stacked Labels
 - Innere Bezeichnung: Pseudowire LSP
 - Äußeres Label: Tunnel LSP
- Verstecken von Signalisierungsnachrichten
 - Aufbau und Verwaltung der Pseudowires werden innerhalb Transporttunnels "versteckt"
 - Nachrichten mit äußerem Label versehen
 - Werden von LSRs oder P-Routern nicht als spezifische Pseudowire-Nachrichten erkannt.
 - P-Router konzentriert sich nur auf das äußere Label



- RFC 4026, Provider Provisioned Virtual Private Network (VPN)



VPWS - Virtual Private Wire Service

VPLS - Virtual Private LAN Service

- VPLS (Virtual Private LAN Service)
 - Ermöglicht Verbindung mehrerer Standorte über MPLS-Netz
 - **Multipoint-to-Multipoint** - Agieren wie ein Ethernet-LAN
 - Angeschlossene Standorte tauschen Ethernet-Frames direkt aus, als wären sie physisch im selben LAN
- VPWS (Virtual Private Wire Service)
 - **Point-to-Point**-Dienst für transparente Verbindung zwischen zwei Standorten über ein MPLS-Netz
 - Im Gegensatz zu VPLS nur eine dedizierte, bidirektionale Verbindung für den Datenverkehr zwischen zwei Endpunkten
- Beide Dienste nutzen MP-BGP
 - Für Verwaltung der MAC-Adressen und Label-Zuweisungen

Ethernet/Frame Relay/ATM Pseudowires oder
Virtual Private Wire Service (VPWS)

Definiert in RFC 4875 als zentraler Standard

Virtual Private LAN Service (VPLS)

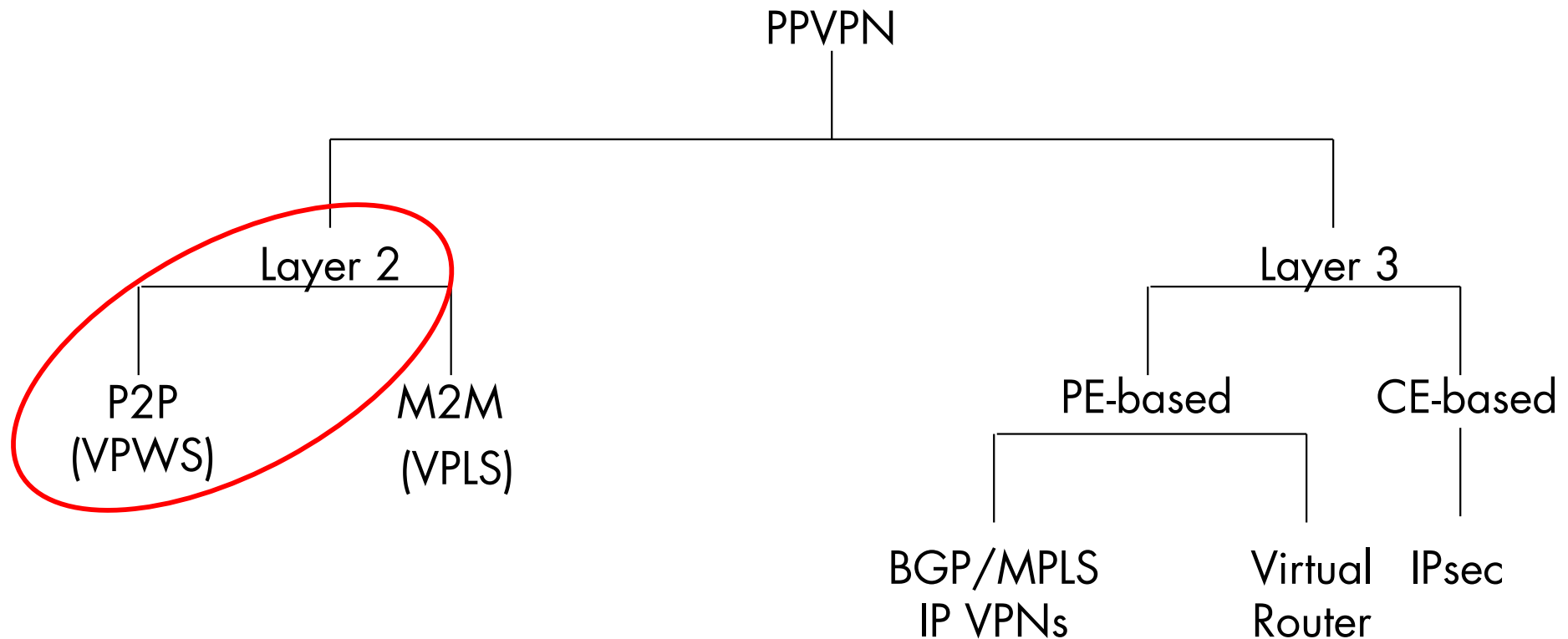
Definiert in RFC 4761 (BGP) und 4762 (LDP)

OAM requirements for VPLS – RFC 6136

Multicast over VPLS – RFC 5501

VPLS Interoperability with Customer Edge (CE)
Switches – RFC 6246

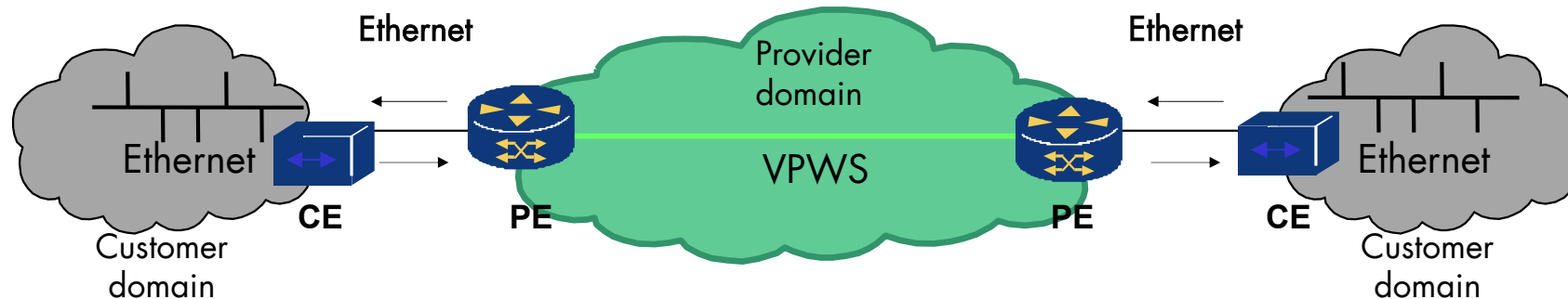
- RFC 4026, Provider Provisioned Virtual Private Network (VPN)



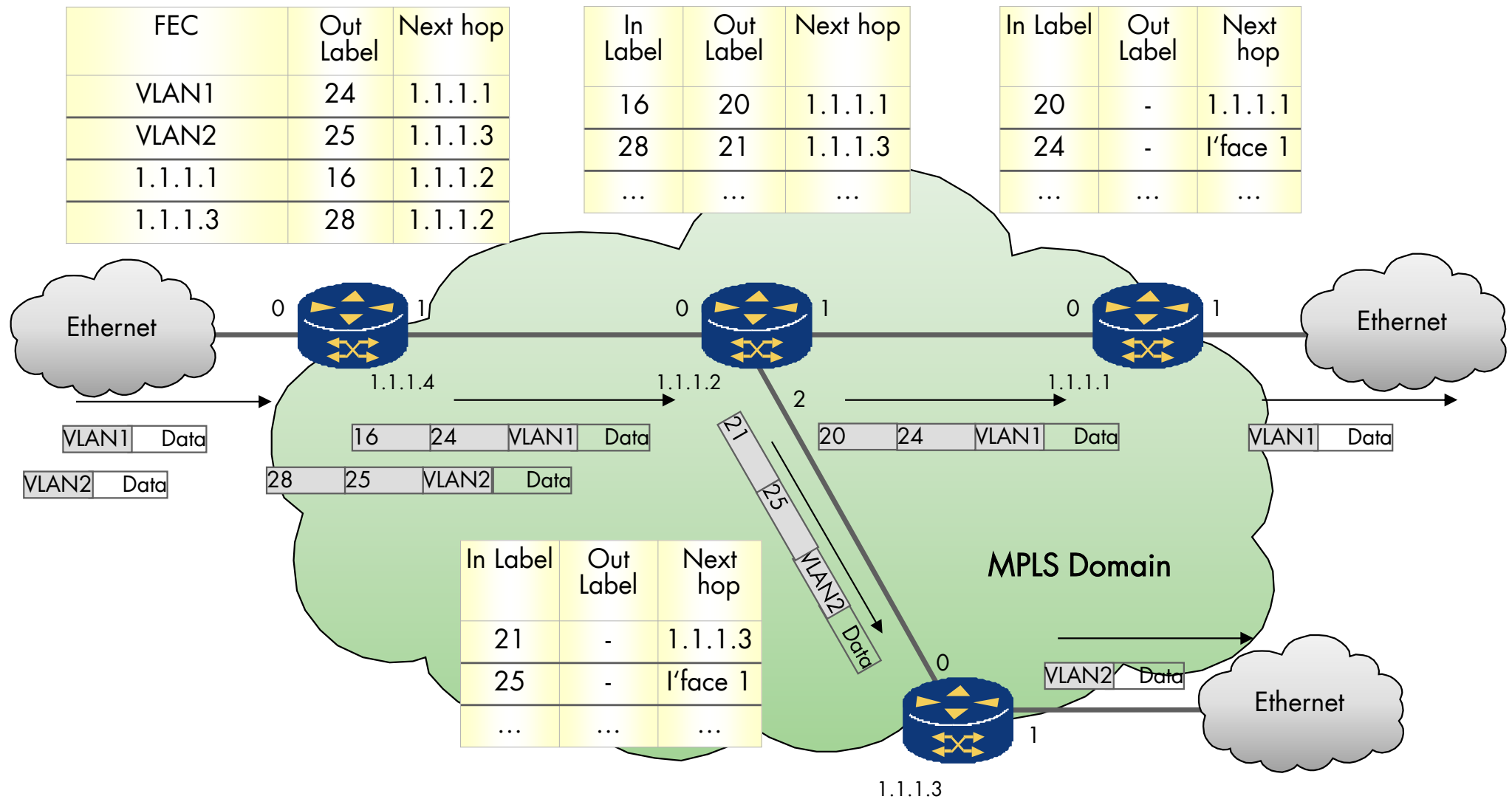
VPWS - Virtual Private Wire Service

VPLS - Virtual Private LAN Service

- VPWS ist ein Punkt-zu-Punkt-VPN-Dienst
 - Bindet genau einen AC an genau einen PW (pt-2-pt)
 - MPLS definiert die Labelverteilung und Encapsulierung
 - Aufbau von Pseudowires und Transport LSPs
 - Provider Edge (PE) verwaltet Ethernet-Port zum Kunden
 - Zuordnung von Ethernet-Frames des Kunden zu MPLS PWs basierend auf MAC-Adressen/Ports/VLANs



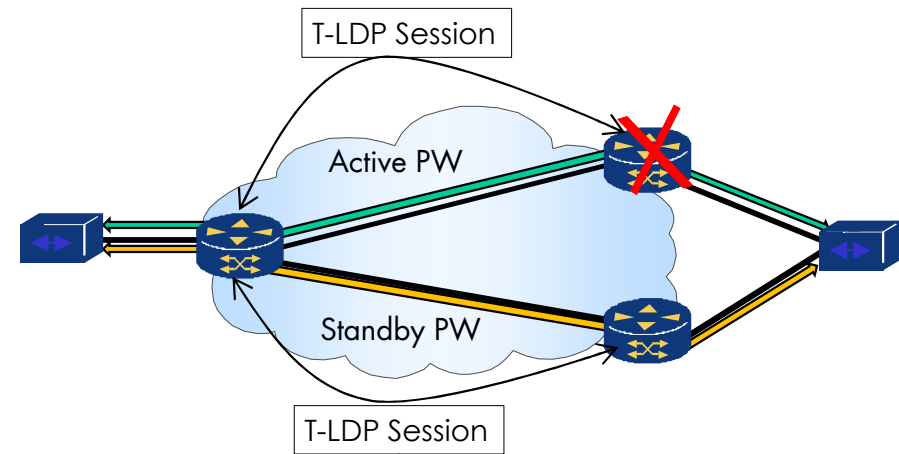
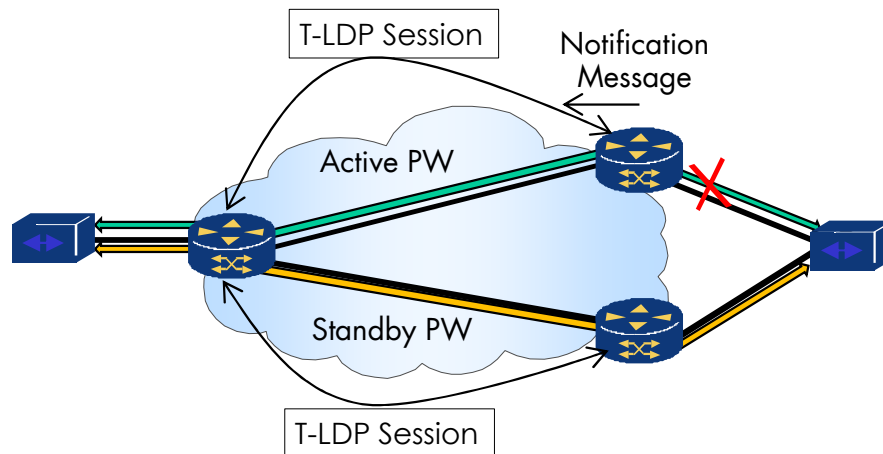
MPLS Forwarding von VPWS Frames ■ EANTC



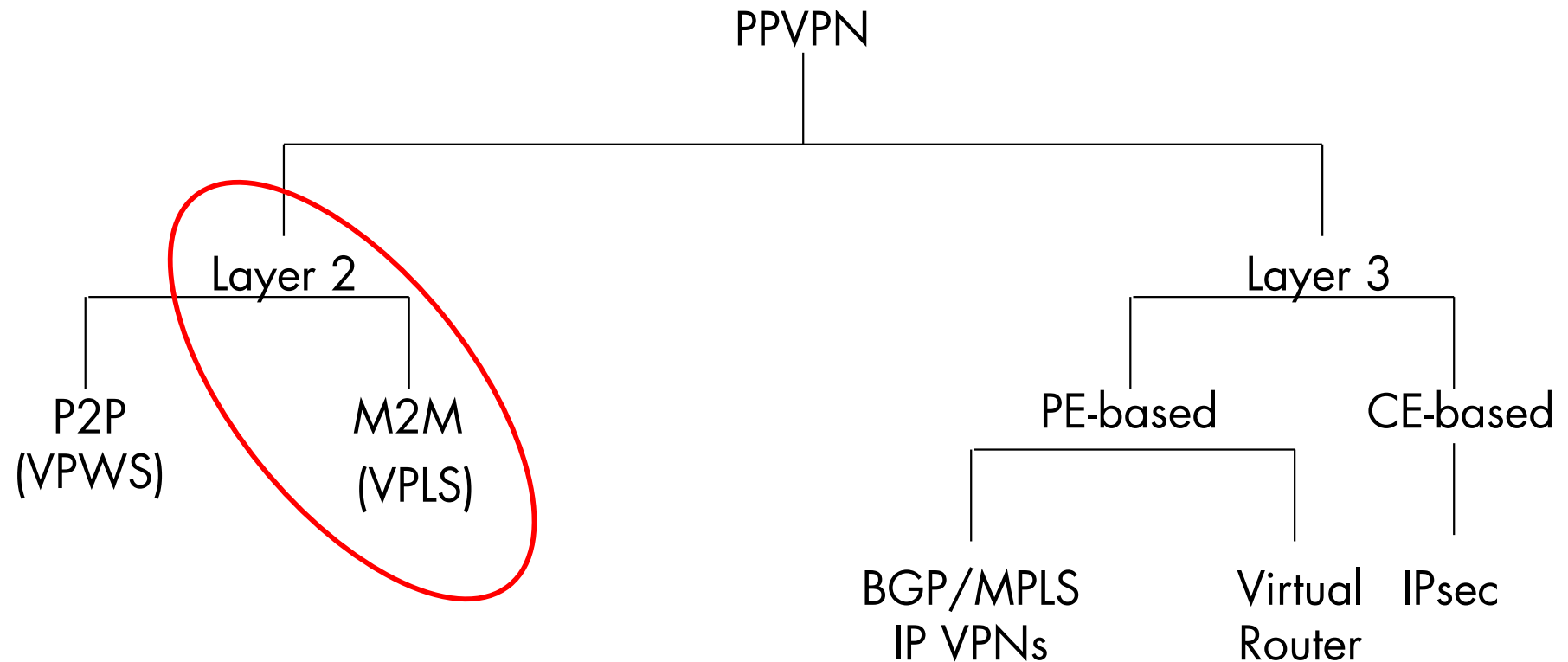
- Ein PW ist ein Tunnel, der auf zwei LSPs basiert
 - ein Tunnel pro Richtung
 - PW LSP ist aktiv, wenn Tunnel-LSP zwischen PEs eingerichtet und aktiv ist
- PW Status ist betriebsbereit, wenn beide PEs:
 - Unidirektionale LSPs sind etabliert und aktiv
 - Mindestens einer dem PW zugeordneter AC ist an jedem PE vorhanden
- Signalisierungsprotokolle
 - Für die Labelverteilung werden LDP (Targeted Mode) oder MP-BGP verwendet

Ereignisse, die eine Umschaltung auslösen können, sind:

- Manuelle Änderung des PW-Vorrangswerts (Presedence) für bevorzugten Pfad
- Der Status des PW ändert sich
- Benachrichtigung vom Remote-Peer
- Der aktive PW fällt aus



- RFC 4026, Provider Provisioned Virtual Private Network (VPN)



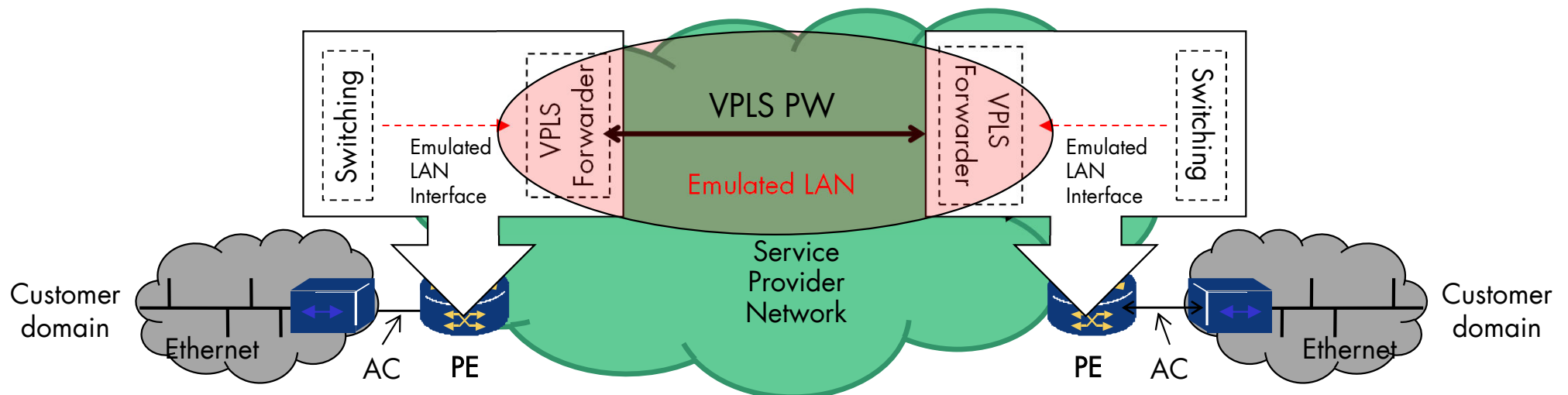
VPWS - Virtual Private Wire Service

VPLS - Virtual Private LAN Service

Virtual Private LAN Services

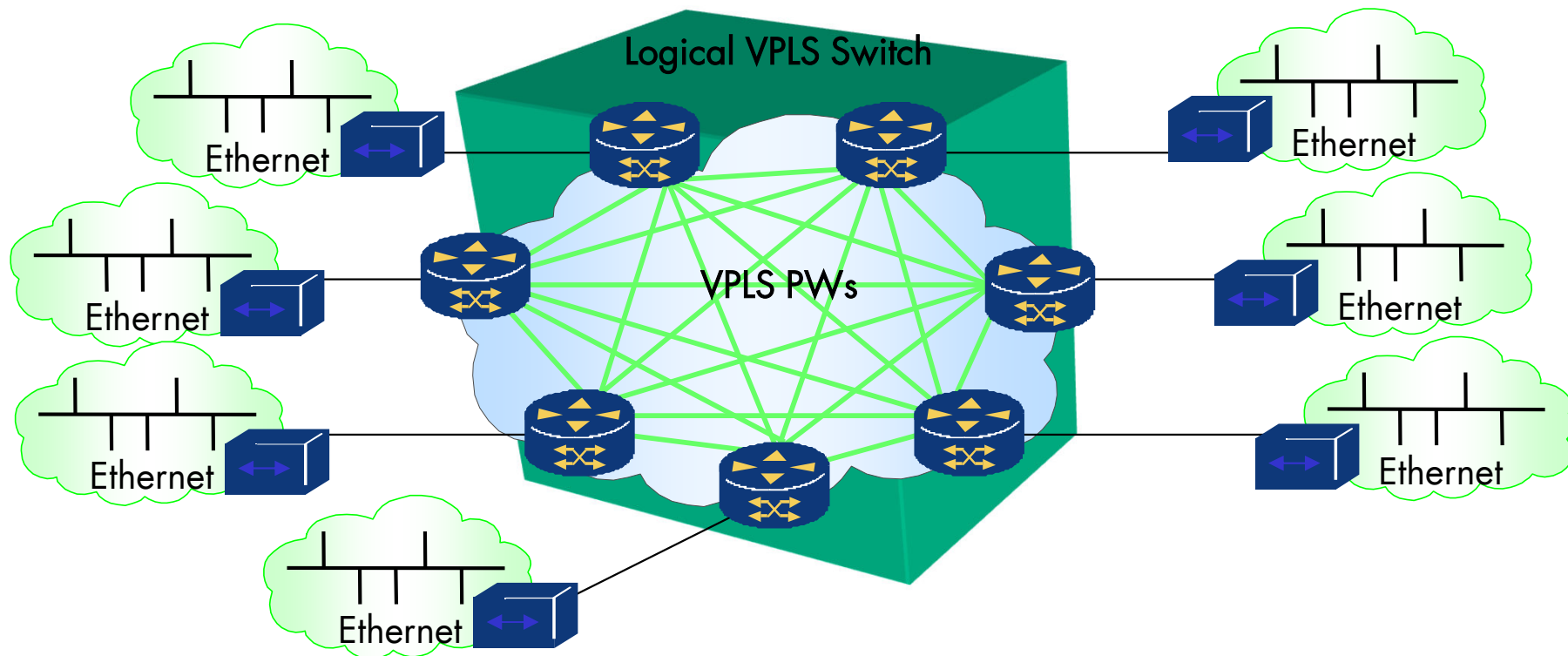
Ein PE besteht aus einem Switch-Modul

- Das Switch-Modul verbindet den AC über eine „emulierte LAN-Schnittstelle“ mit einem emulierten LAN
- Das emulierte LAN besteht aus mehreren ACs, die jeweils mit einem PW verbunden sind
- Teil eines gemeinsamen Ethernet-LANs

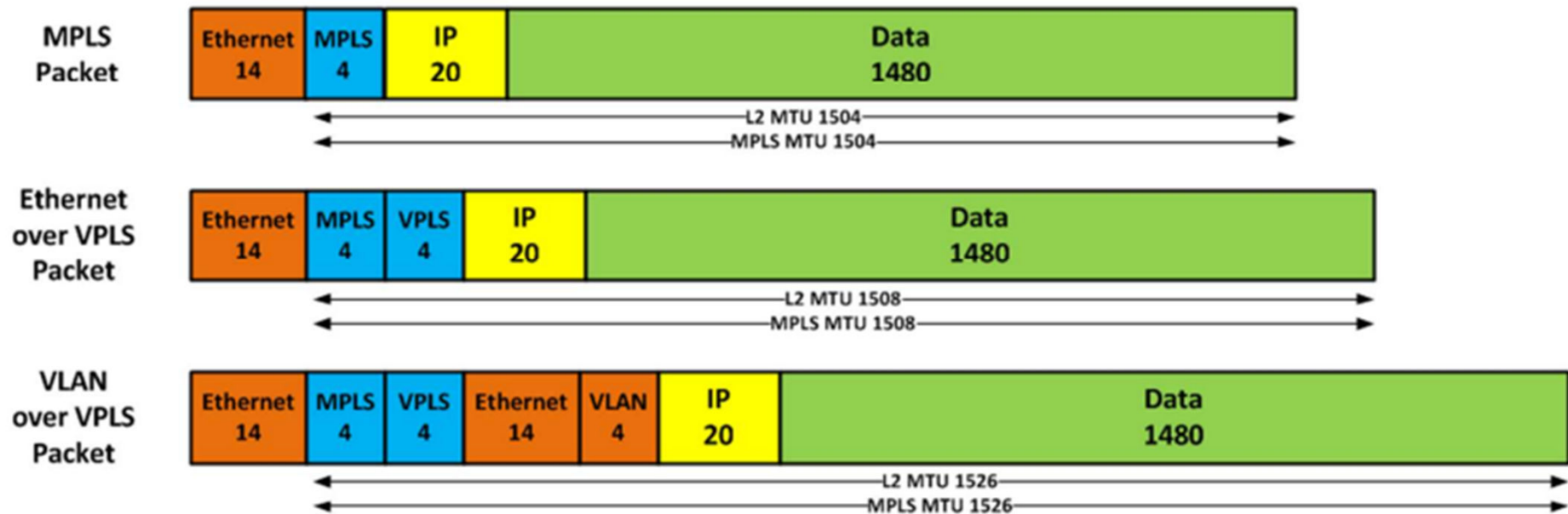


Switched verschiedene Kundenstandorte

- Multipoint-to-Multipoint Ethernet VPN Verbindungen
- Erstellt verschiedene Pseudowire für die Verbindungen



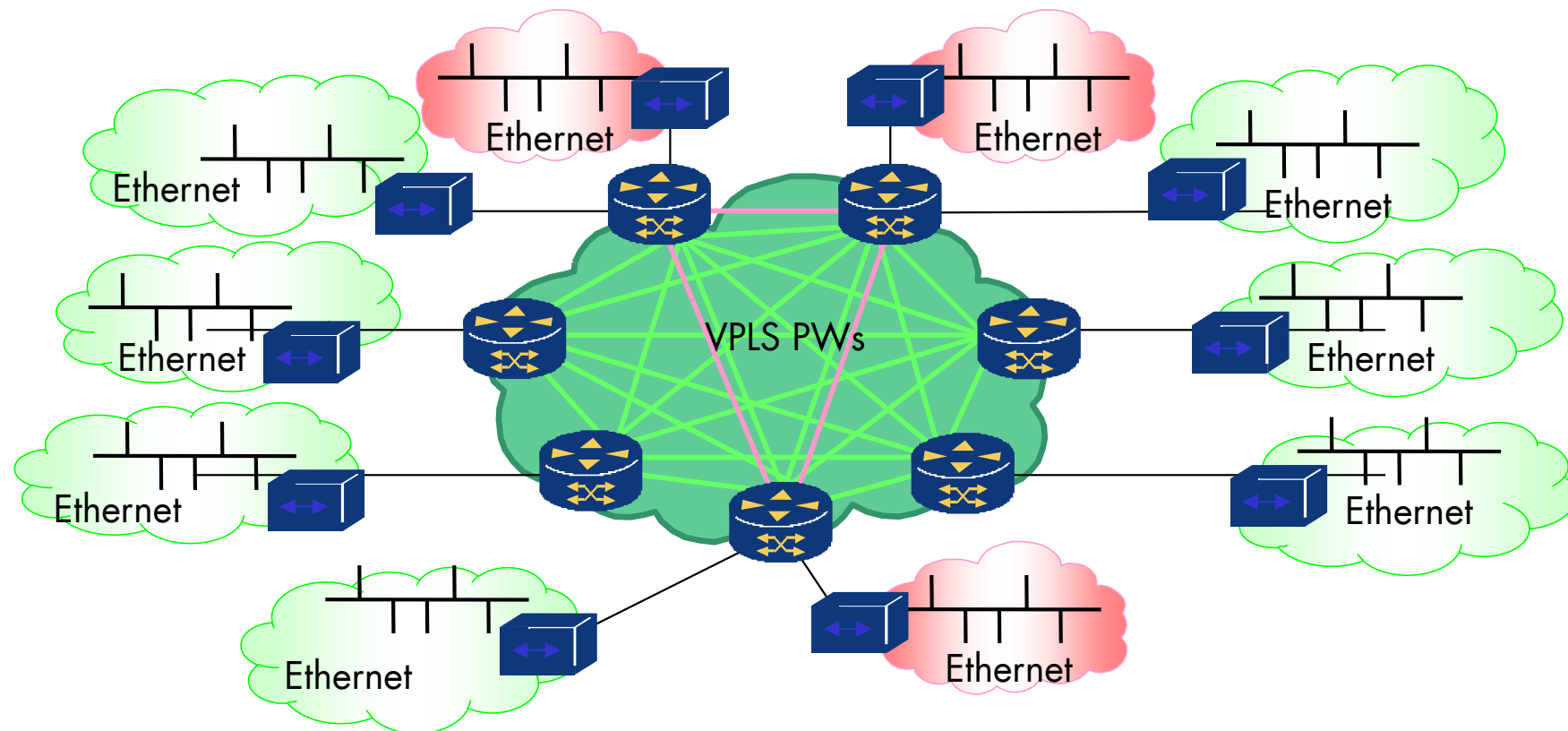
VPLS erhöht die MTU Size



Quelle: Business Technology Group (BTG), Andrew Thrift

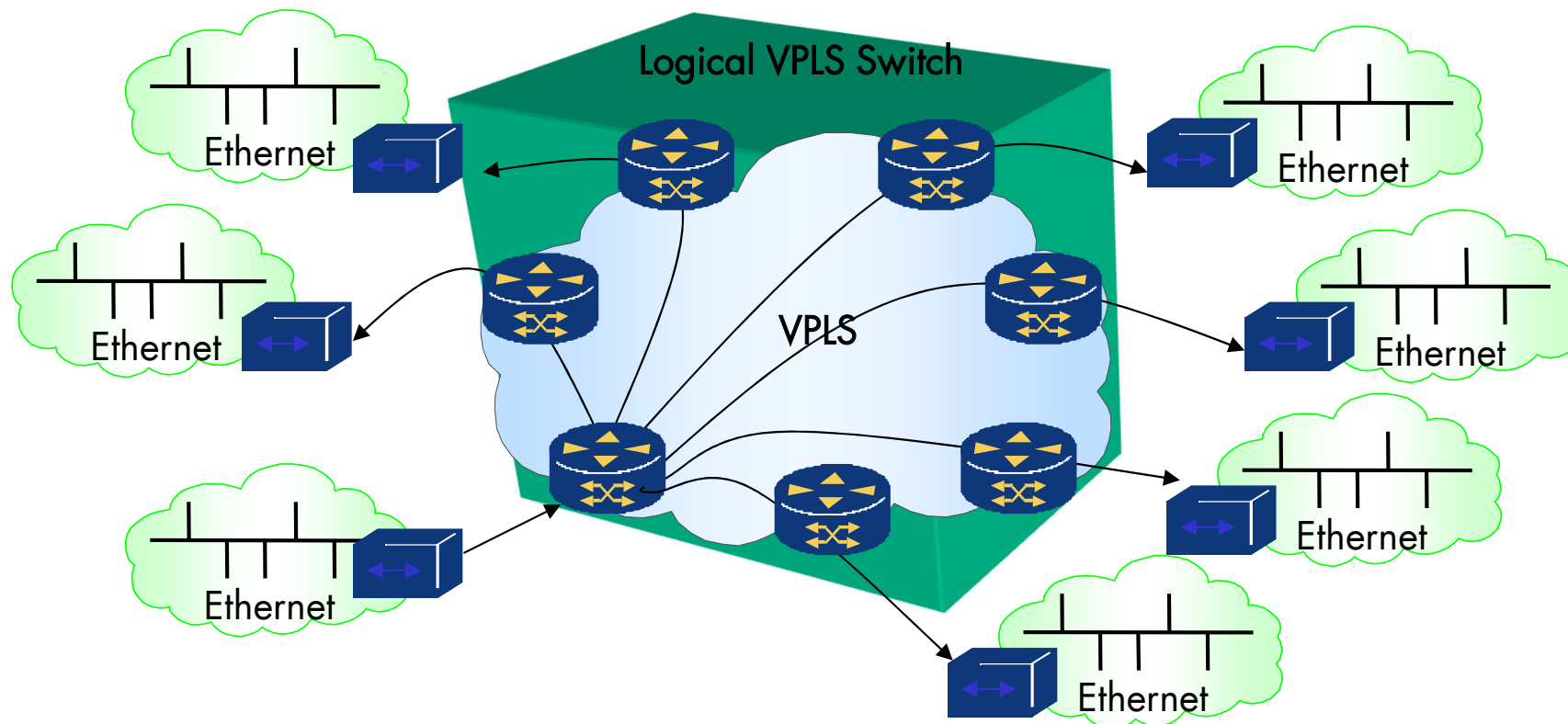
Mehrere Kunden im gleichen Netz, aber separiert

- Aufgebaut mit Targeted LDP oder MP-BGP
- Vollvermaschte Pseudowires pro Kunde und Kundenstandort



Vollvermaschung bedeutet Replikation an allen PEs

- Hierarchien einführen
- Daten werden aggregiert und zentral verwaltet

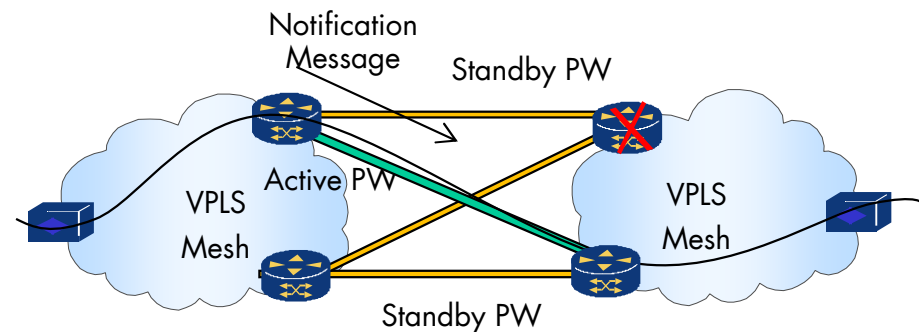
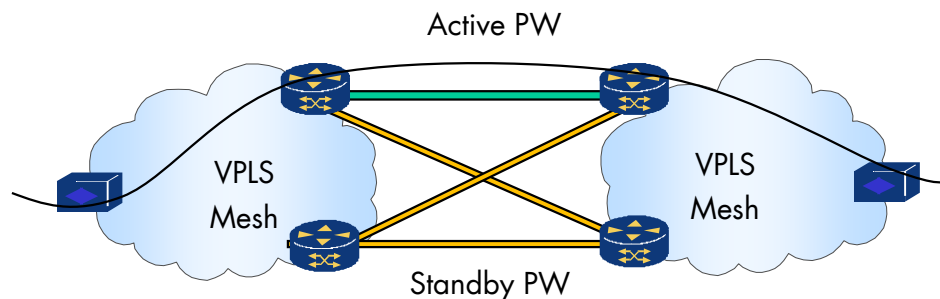


Targeted-LDP verwendet den PW-Statuscode (0x00), um den aktiven Status zu signalisieren

Baut Backup-LSPs ebenfalls über T-LDP auf

Damit der Backup-LSP im Falle eines Ausfalls des primären LSPs aktiviert wird

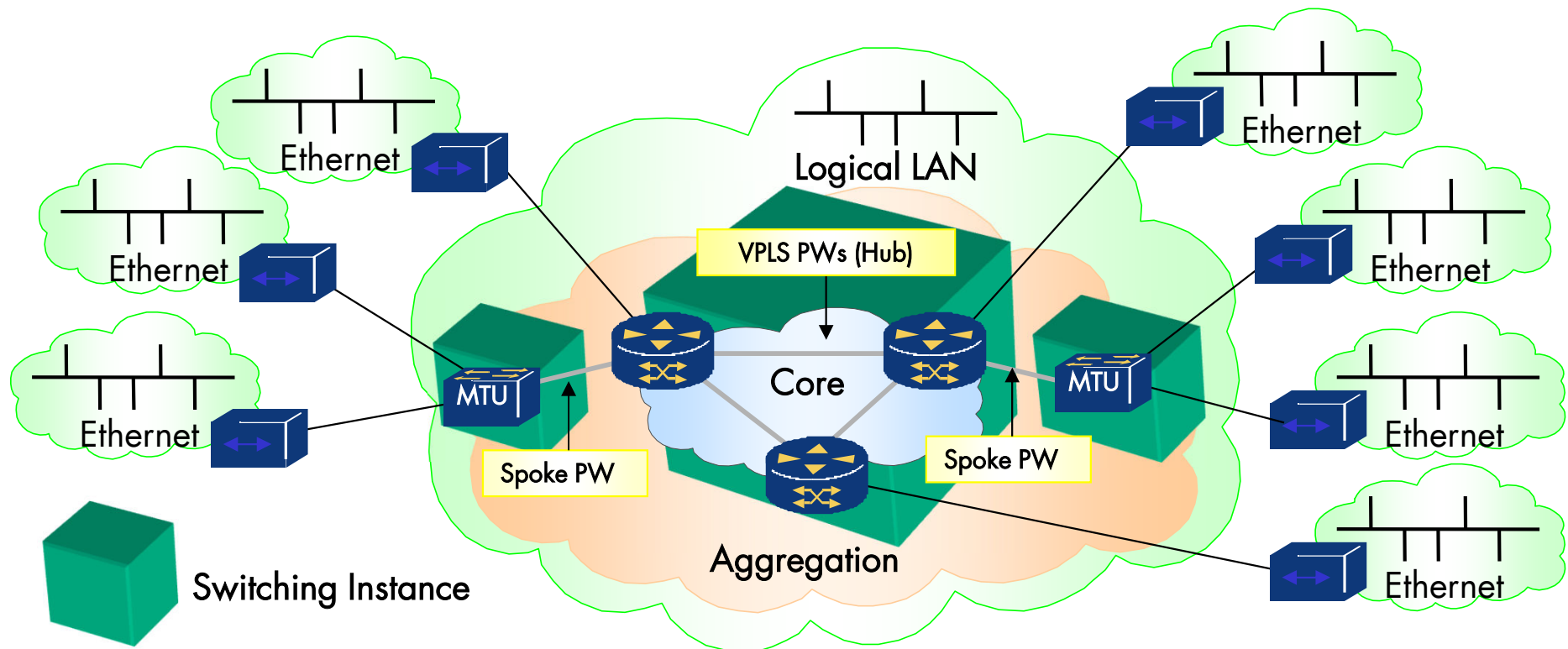
➤ Überwachung durch Mechanismen wie BFD (Bidirectional Forwarding Detection)



- VPLS-Skalierbarkeit
 - Anzahl Pseudowires pro Domain: $N * (N-1) / 2$
 - N: Anzahl der Kundenseiten auf verschiedenen PEs
 - Verschwendung von Bandbreite durch Broadcast Frames
- Hierarchisches Konzept
 - Ein Hub and Spoke Ansatz
 - Anzahl der Pseudowires pro VPLS-Domain reduzieren
 - Mehrere virtuelle Switching-Instanzen innerhalb einer einzelnen VPLS-Domäne
 - Neuer Gerätetyp: Multi-Tenant Unit (MTU-s)
 - Aggregiert viele Kundenports zu einer einzigen „Spoke“ Pseudowire-Verbindung
 - Etabliert „Sprach“ Pseudowire zum nächsten PE
 - Effiziente Replikation

- Erweiterung des traditionellen VPLS
 - In H-VPLS werden PE-Router in zwei Ebenen unterteilt
 - Zentrale PE-Router (Hub)
 - Router agieren als zentrale Punkte für die Verbindung zwischen verschiedenen VPLS-Domänen oder -Instanzen
 - Verteilte PE-Router (Spokes)
 - Router stellen die Verbindung zu den Endbenutzern oder Standorten her und kommunizieren mit den zentralen PE-Router
- Funktionsweise
 - Hierarchische Struktur
 - Datenverkehr wird nicht direkt zwischen allen Standorten (Spokes) übertragen, sondern über die zentralen PE-Router (Hubs).
 - Traffic Management
 - Zentrale Verarbeitung des Verkehrs am Hub -> Replikation reduziert
 - Spoke kann Daten an mehrere Spokes senden über den Hub zur Weiterleitung
 - Verhindert, dass jeder Spoke Datenverkehr an alle anderen Spokes sendet

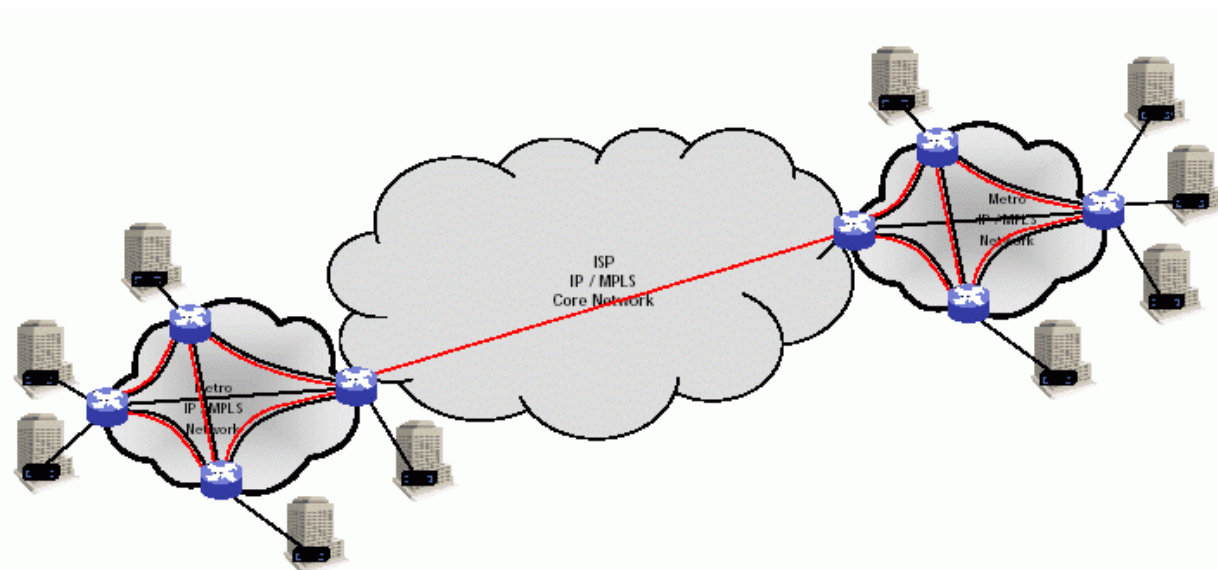
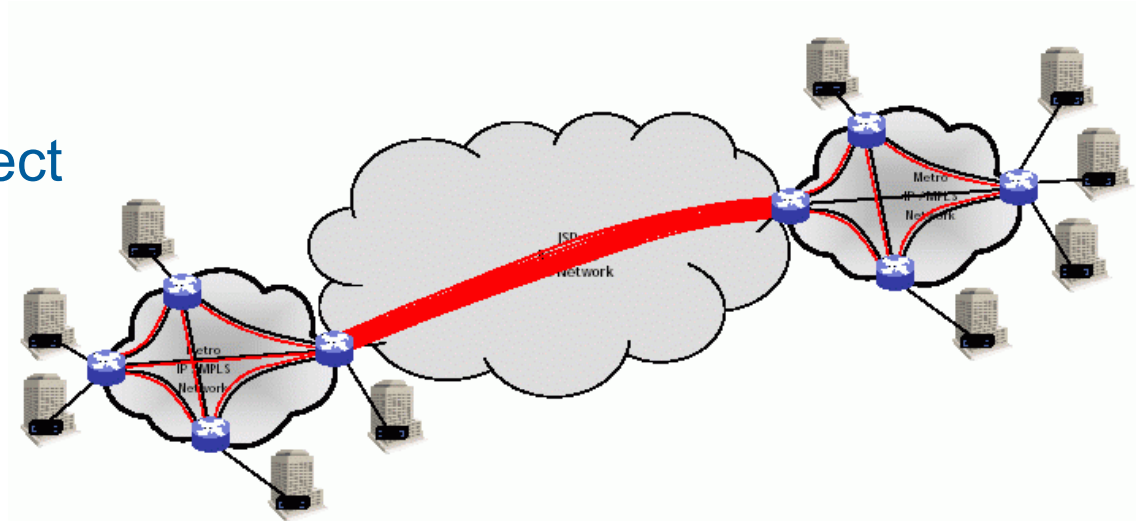
- Verringerung der Bandbreite durch die Aggregation
- Reduzierung der Komplexität durch Vereinfachung der Architektur
 - PE-Router der Standorte kennen nicht den gesamten Verkehr
- Verbesserte Skalierbarkeit da neue Spokes hinzugefügt werden können, ohne die gesamte VPLS-Topologie zu beeinflussen



- Router
 - Verwalten den Datenverkehr zwischen verschiedenen Netzen
 - Ermöglichen Kommunikation zwischen Kunden und dem SP
 - Ein Provider Edge-Router (PE-Router) in einer H-VPLS-Architektur kann als MTU agieren, indem er die Pseudowires für verschiedene Kunden verwaltet und den Datenverkehr steuert
- Switches
 - Layer-2-Switches isoliert den Verkehr innerhalb eines VLAN
 - Ein Ethernet-Switch, der VLANs für verschiedene Kunden bereitstellt, kann als MTU fungieren, indem er sicherstellt, dass der Datenverkehr zwischen den VLANs isoliert bleibt
- Gateways
 - Verbinden von verschiedenen Netzwerken oder Protokollen
 - Verkehr von einem Protokoll (z. B. IP) zu einem anderen (z. B. Ethernet) konvertieren und verwalten
 - Ein Gateway, das MPLS-Dienste für verschiedene Kunden bereitstellt, kann als MTU fungieren, indem es den Verkehr für diese Kunden steuert und an die entsprechenden Endpunkte weiterleitet

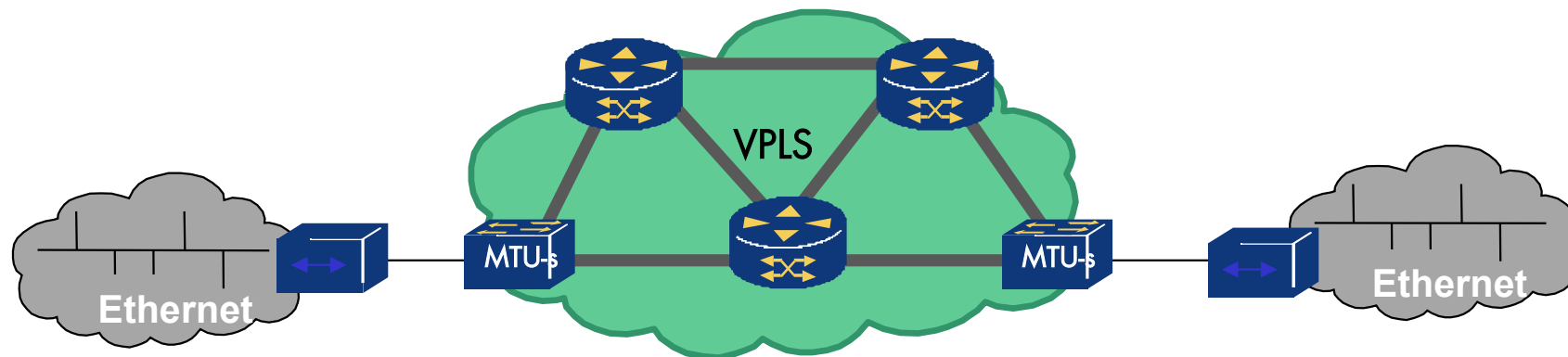
- Reduziert den Konfigurationsaufwand und Konfigurationsfehler
 - **RFC 4761**
 - Virtual Private BGP-Update (VPLS) mit BGP zur automatischen Erkennung und Signalisierung
 - **Automatisch Informationen über andere PE-Router erhalten**
 - Müssen Teil derselben VPLS-Domäne sein
- Vorgesehen durch Erweiterung von BGP als Transportprotokoll
 - **BGP als Transportprotokoll zur Zuordnung des VPLS-Dienstes**
 - PE-Router senden MP-BGP-Nachrichten, die Informationen über die VPLS-Dienste und die zugehörigen Pseudowires enthalten
 - **Neuer PE wird eingefügt**
 - Autodiscovery-Funktion stellt die Informationen über bestehende VPLS-Domänen bereit
 - Austausch von BGP-Update Nachrichten
 - **Verwendung auch mit LDP VPLS, aber nur für Labels!**
 - **Einfache Integration der Multi-AS-Funktionalität von BGP**
 - Wenn verschiedene Service Provider integriert werden müssen

- Begriffe
 - Interconnect Service
 - Metro Ethernet Interconnect
 - VPLS Interconnect
- Realisiert mit VPLS
- Realisiert mit H-VPLS

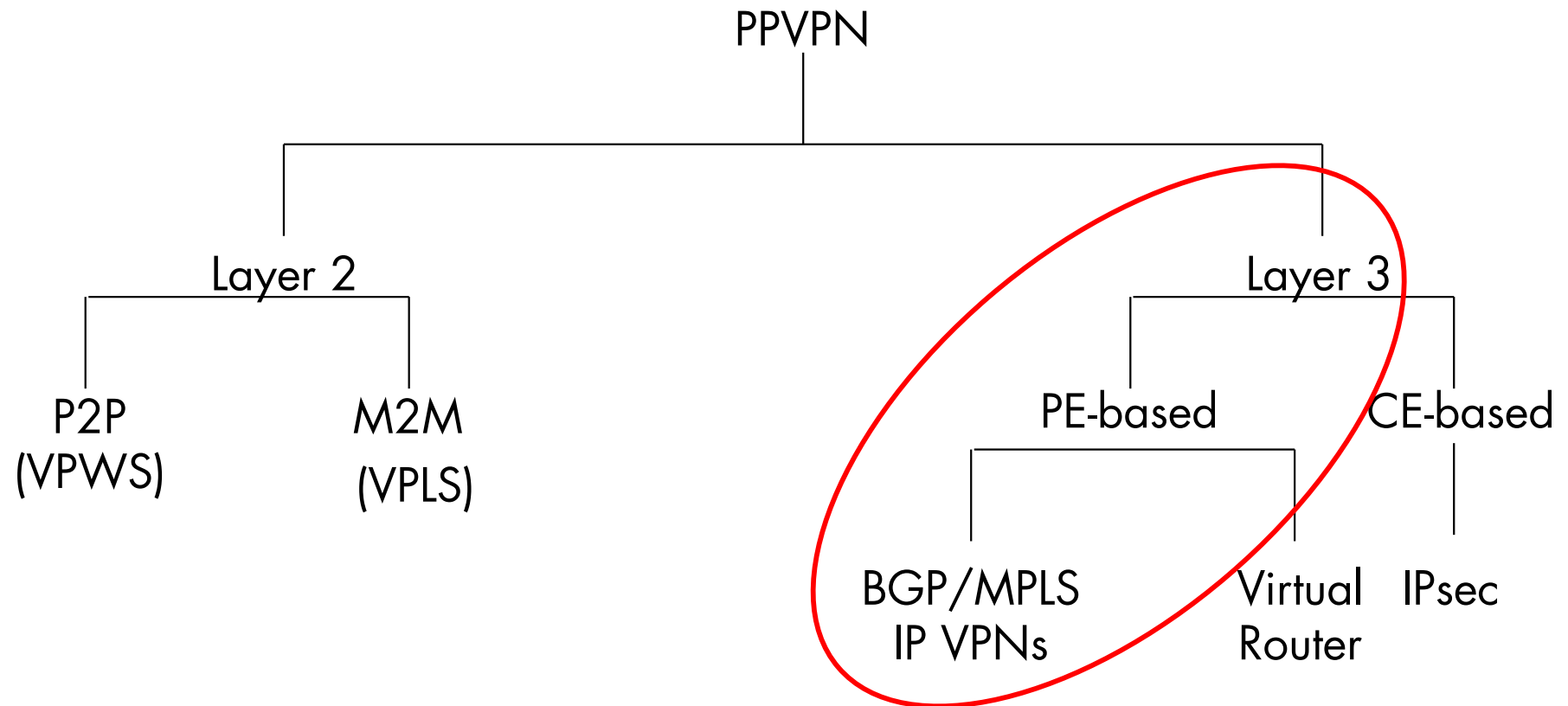


Quelle: IP/MPLS Forum

- VPLS und H-VPLS-Ausfallsicherheit
 - Ausfälle durch einzelne Netzanbindung der MTUs
- Lösung
 - MTUs an zwei PEs anbringen bietet Redundanz



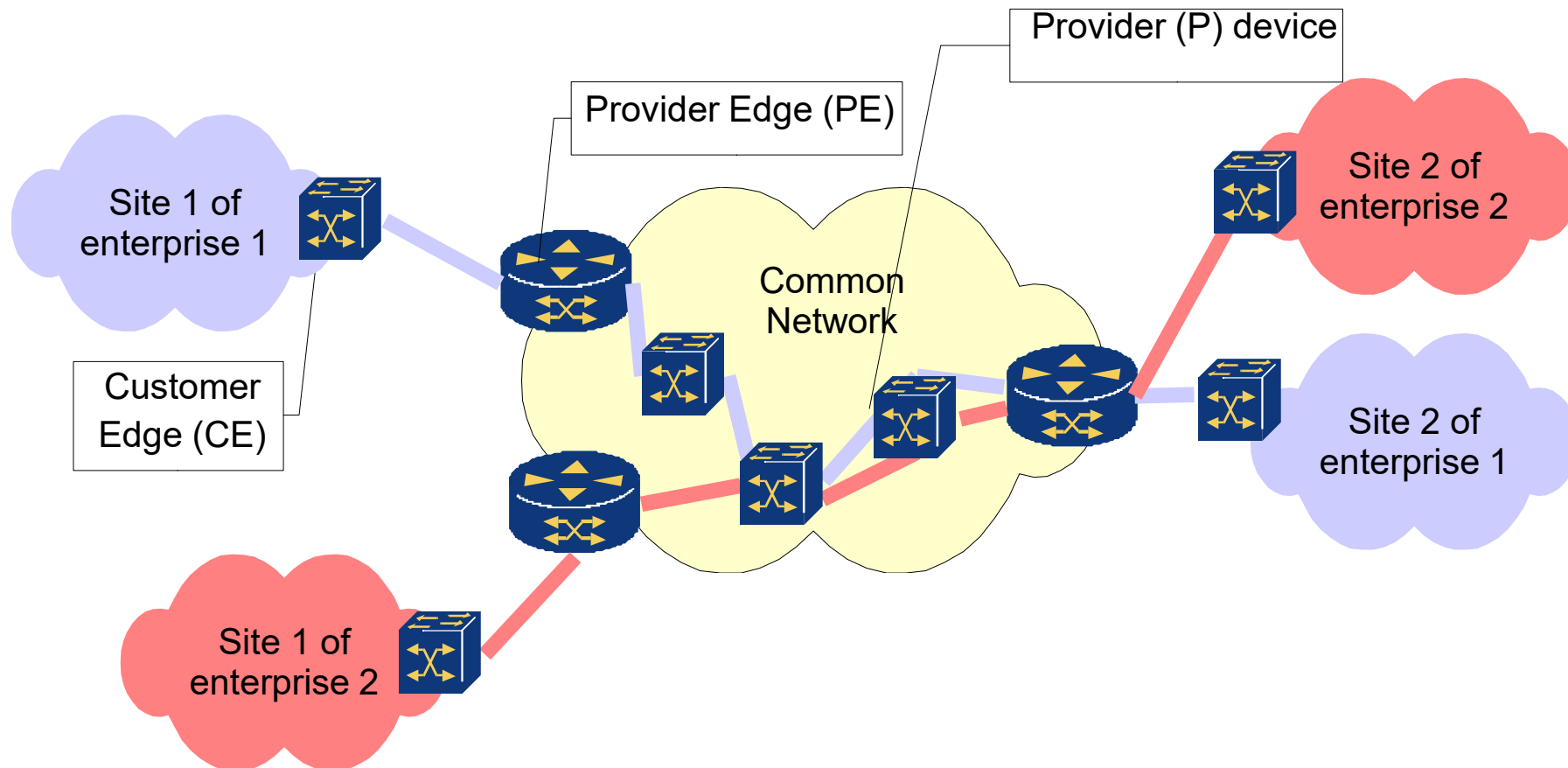
- RFC 4026, Provider Provisioned Virtual Private Network (VPN)



- Unterstützung für privaten Adressraum
 - Kunden nutzen ihren eigenen Adressraum, private IP-Adressen
 - Überlappende Adressräume
- Bereitstellung einer vollständig gerouteten IP-Netzwerklösung
 - VPN-Routen werden vom Backbone-Routing getrennt
- Kunde wird von Routing-Verantwortlichkeiten entlastet
 - Vorteile eines MPLS-Backbones (schnelle Umleitung usw.)
- Pflege nur an Geräten die direkt am Kundenstandort sind
 - MPLS-Backbone ist dem Kunden nicht bewusst
- VPN-Dienst kann mehr als ein SP-Netzwerk überbrücken
- Vereinfachung der IT-Rolle im Unternehmen
 - Neue Verbindung zum VPN durch SP erstellt und verwaltet

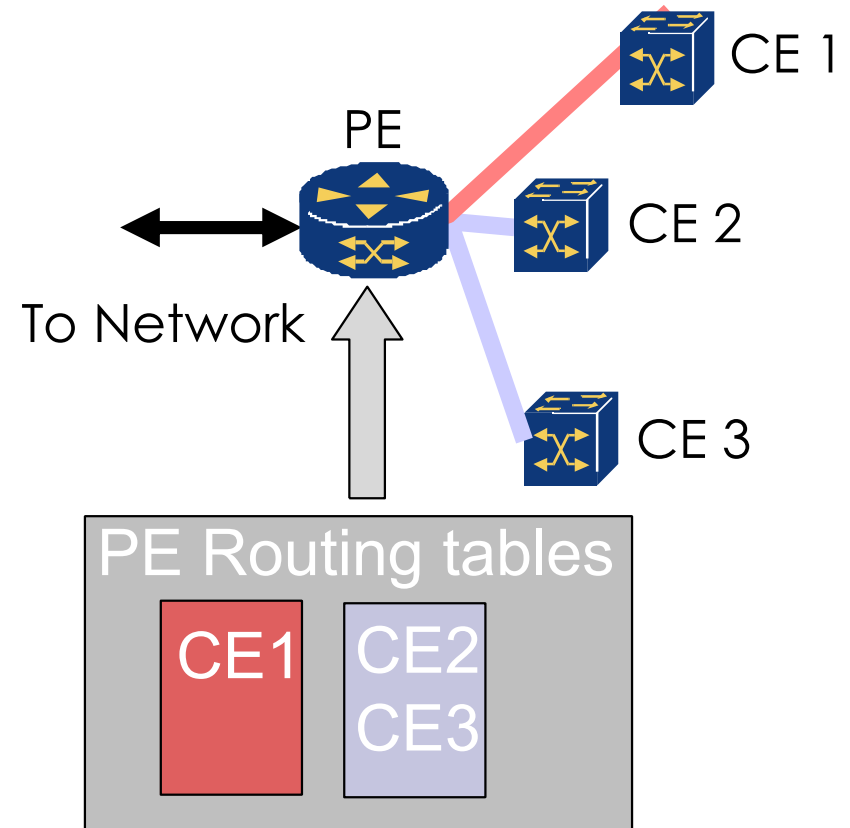
- RFC 4364: BGP/MPLS IP Virtual Private Networks (VPNs)
 - Beschreibt Zusammenarbeit von BGP (Border Gateway Protocol) und MPLS (Multiprotocol Label Switching)
 - Transport von IP-Datenverkehr über ein gemeinsames Netz
 - Logische Trennung verschiedener Kunden oder Netze
- RFC 5519: BGP/MPLS IP VPNs - Address Family Identifier and Subsequent Address Family Identifier
 - Definiert die Address Family Identifiers (AFI) und Subsequent Address Family Identifiers (SAFI)
- RFC 6624: BGP MPLS IP VPNs - Applicability Statement
 - Behandelt die Anwendbarkeit von BGP/MPLS IP VPNs

- CE, PE und P Router
- Policy für den Aufbau der VPNs am PE

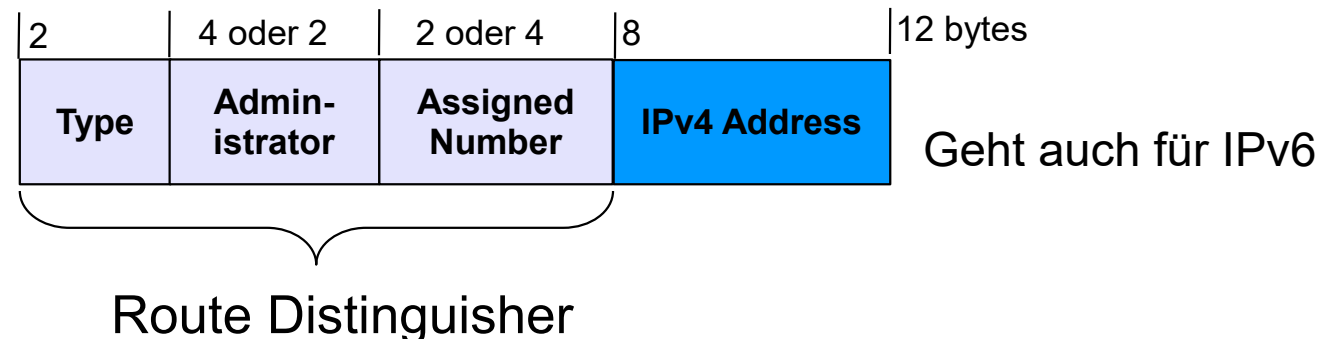


- MPLS Label Edge Router (PE-Gerät)
 - Klassifizierung/Filterung des Kundenverkehrs und Zuordnung zu einem VPN-Dienst
 - Sammeln und Ausfüllen von Kunden-Forwardingtabellen für private Kundennetze
 - Verteilen von privaten Forwardingtabellen des Kunden an andere PEs, die denselben VPN-Dienst bedienen
 - Einrichtung von MPLS-Pfaden über das SP-Netzwerk zu jedem PE, der denselben VPN-Dienst bedient
- MPLS Core Router, oder Label Switch Router (P-Gerät)
 - Keine Kenntnis von Kunden-VPNs; nur Transitknoten für MPLS-Verkehr
 - Genügend Informationen, um Daten durch das Core-Netz zu transportieren

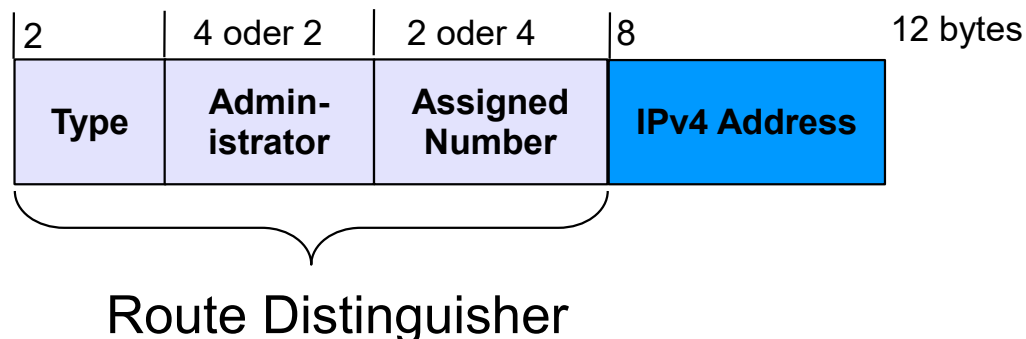
- Wie verwaltet man eine große Anzahl von Kunden-IP-Adressen, die sich möglicherweise überschneiden?
- Routing-Weiterleitungstabellen pro Kunde
- Provider Edge-Router verfügen über
 - mehrere Routing-Tabellen
 - eine für jeden Kunden
 - Propagiert durch BGP-Routing innerhalb des Cores
 - Genannt VPN Routing and Forwarding tables (VRFs) in RFC4364



- Problem:
 - BGP-Instanz kann nur eine Route zu einem bestimmten Adresspräfix installieren und verteilen
 - L3-VPNs können überlappende Adressräume besitzen
- Lösung:
 - Erstellen einer neuen Adressfamilie, Hinzufügen eines Routenunterscheidungsmerkmals zur IP-Adresse
- Route Distinguisher
 - Erlaubt Erstellung einer eindeutigen Route zu IP Address Prefix



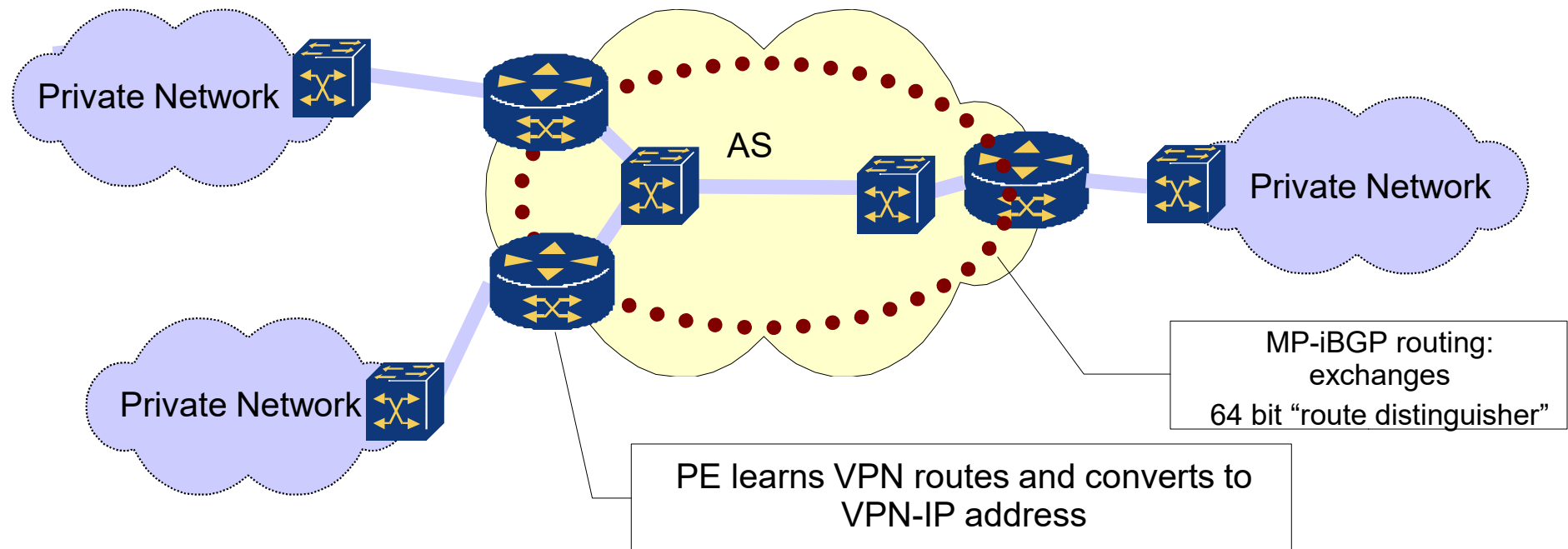
- Typ
 - Bestimmt die Länge der anderen beiden Felder sowie die Semantik des Administratorfelds
- Administrator
 - Identifiziert die Nummernbehörde (z.B. AS-Nummer durch IANA vergeben oder IP-Adresse)
- Zugewiesene Nummer
 - Zusätzliche Informationen, die von der unter „Administrator“ genannten Institution zugewiesen werden



Beispiel:
RD: 65000:101
RD: 10.0.0.1:1001
RD: 1000000:10

- IP-Adressen innerhalb verschiedener VPNs eindeutig
- Wird als Präfix zu einer IP-Adresse hinzugefügt
 - **Dieselbe IP-Adresse für verschiedenen VPNs/Kunden**
 - Ohne, dass es zu Konflikten kommt
- Kombinieren des RD mit der IP-Adresse
 - **Auch für IPv6 Adressen**
 - **Eindeutigkeit der IP-Adresse 192.168.1.10, RD als Präfix**
 - **Ergebnis ist VPNv4-Adresse: 65000:1:192.168.1.10**
 - **VPNv4-Routen:**
 - Adresse 65000:1:192.168.1.10 verwendet, um diese spezifische Route innerhalb des VPNs zu kennzeichnen
 - **Routing-Management:**
 - Wenn der Router diese Adresse empfängt, weiß er, dass es sich um eine virtuelle Route handelt, die zu einem bestimmten Kunden (in diesem Fall, identifiziert durch den RD 65000:1) gehört

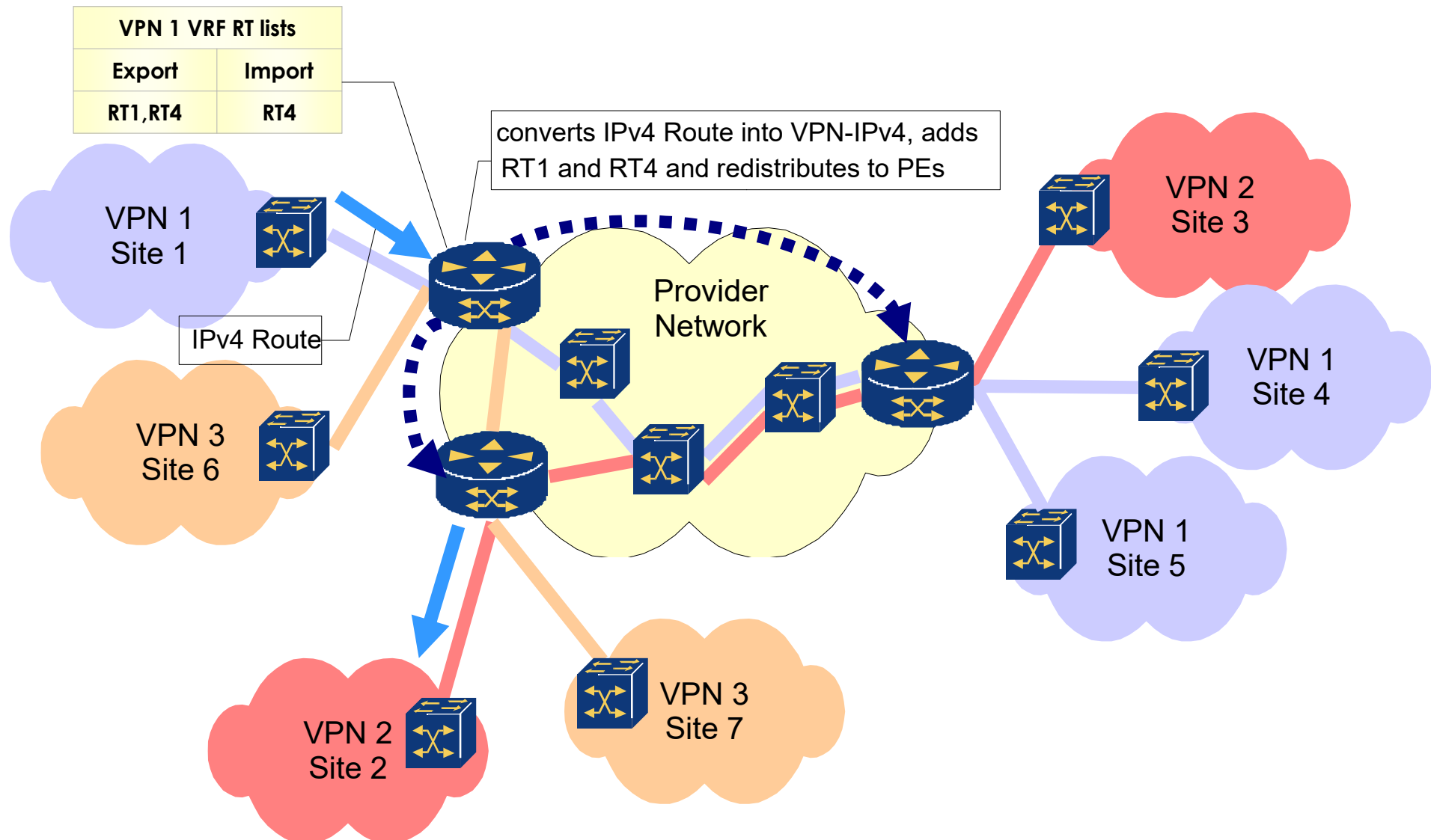
- Standorte eines VPN sind an ein AS angeschlossen
 - VPN-IP Routen können verteilt werden
 - iBGP-Verbindung oder Route Reflector zwischen Standorten

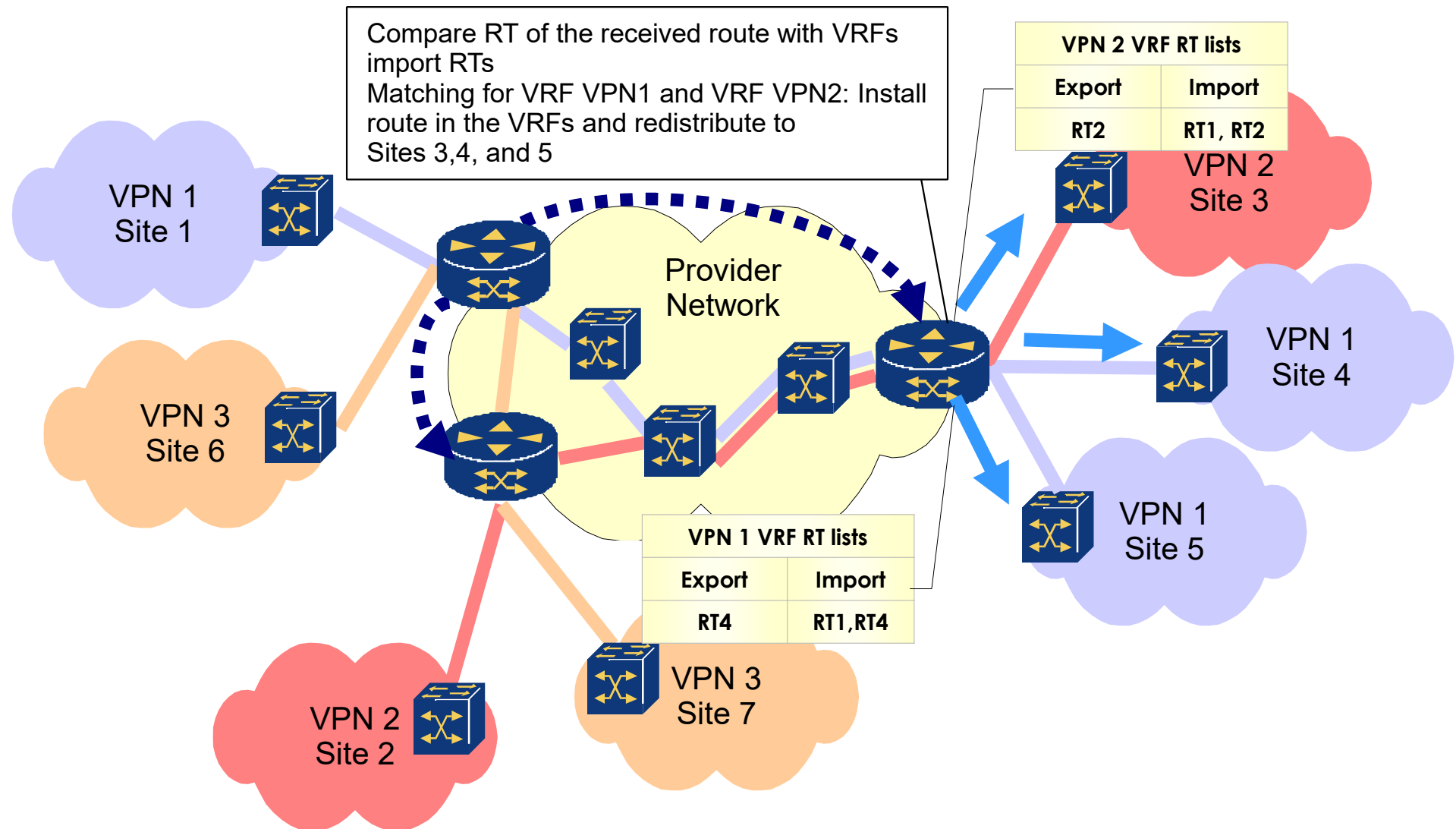


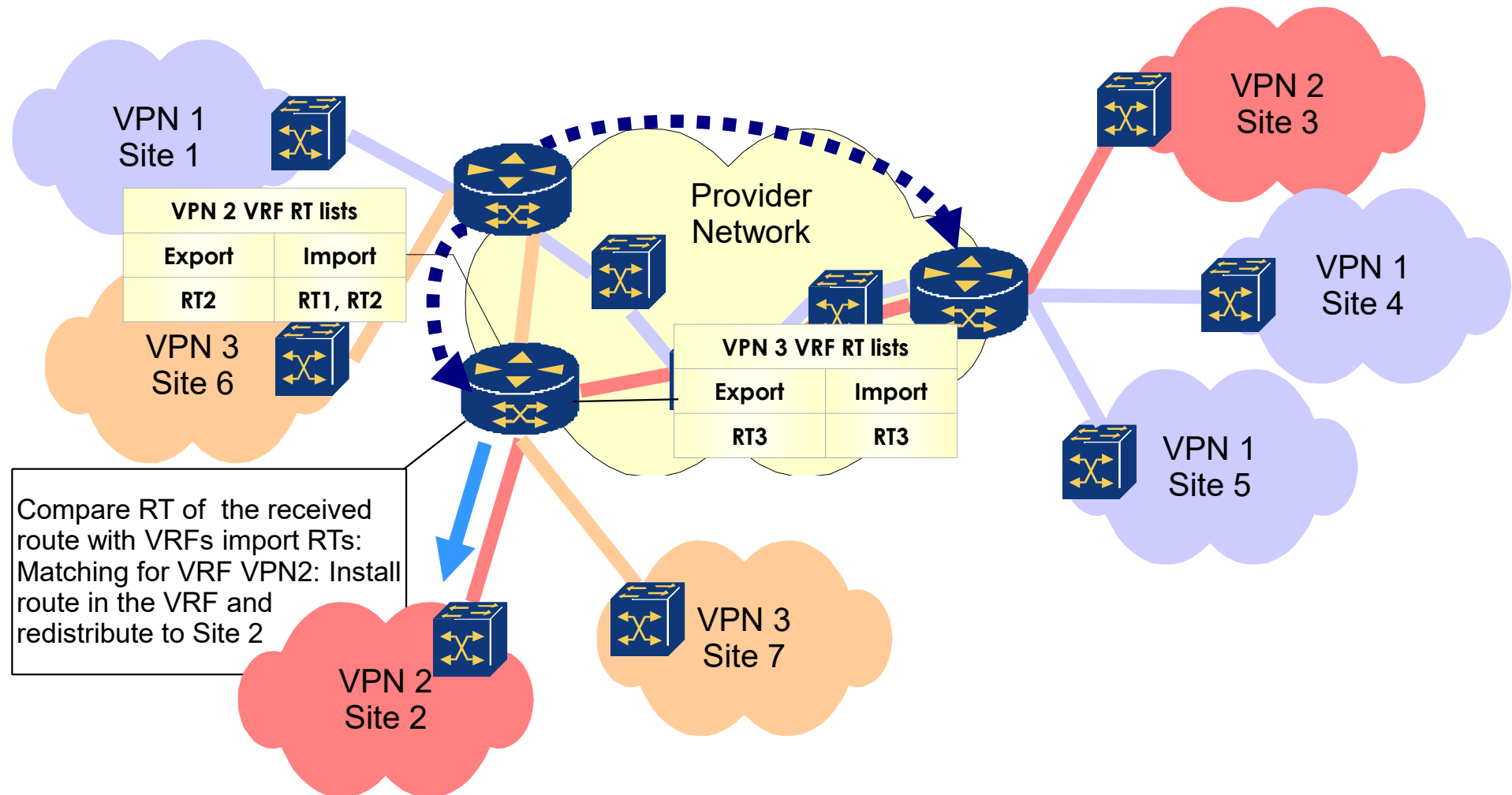
- Obligatorisches Attribut, zugeordnet einer VPN-IP-Route
 - PE lernt Route von CE: ein oder mehrere RTs werden zugewiesen
 - Targetliste exportieren (Import/Export Richtlinien)
 - Wichtig, da mehrere Kunden ggf. dieselben IP-Adressen nutzen
- VPN-IPv4 Routen an die BGP-Peers verteilen
 - BGP-Router, der eine VPN-IPv4 empfängt, vergleicht seine Route Target List mit lokalen VRFs Route Target Lists
 - Jede VRF hat seine eigene Route Target List, auch Import Target genannt
 - Wenn es übereinstimmt, installiert der Router die Route in der VRF
 - Andernfalls ignoriert der Router die empfangene VPN-IP Route
- Definiert als BGP Extended Community Route Targets
 - Spezifiziert in RFC 4360

- Route Target Attribut **nicht gleich** Route Distinguisher
 - RD wird verwendet, um IP-Adressen eindeutig zu machen
 - Dient zur eindeutigen Kennzeichnung von IP-Adressen in verschiedenen VPNs
 - RT-Attribut verwendet zur Steuerung der Verteilung von Routen innerhalb von VPNs
 - Dient zur Steuerung, welche Routen in ein VPN importiert oder exportiert werden
- RD
 - Wird hauptsächlich in der IP-Routeninformation verwendet, um IP-Adressen in einem VPN zu unterscheiden
- RT
 - Wird in BGP-Nachrichten verwendet, um Routen zu identifizieren, die zu einem bestimmten VPN gehören

Beispiel Route Target (Schritt 1)

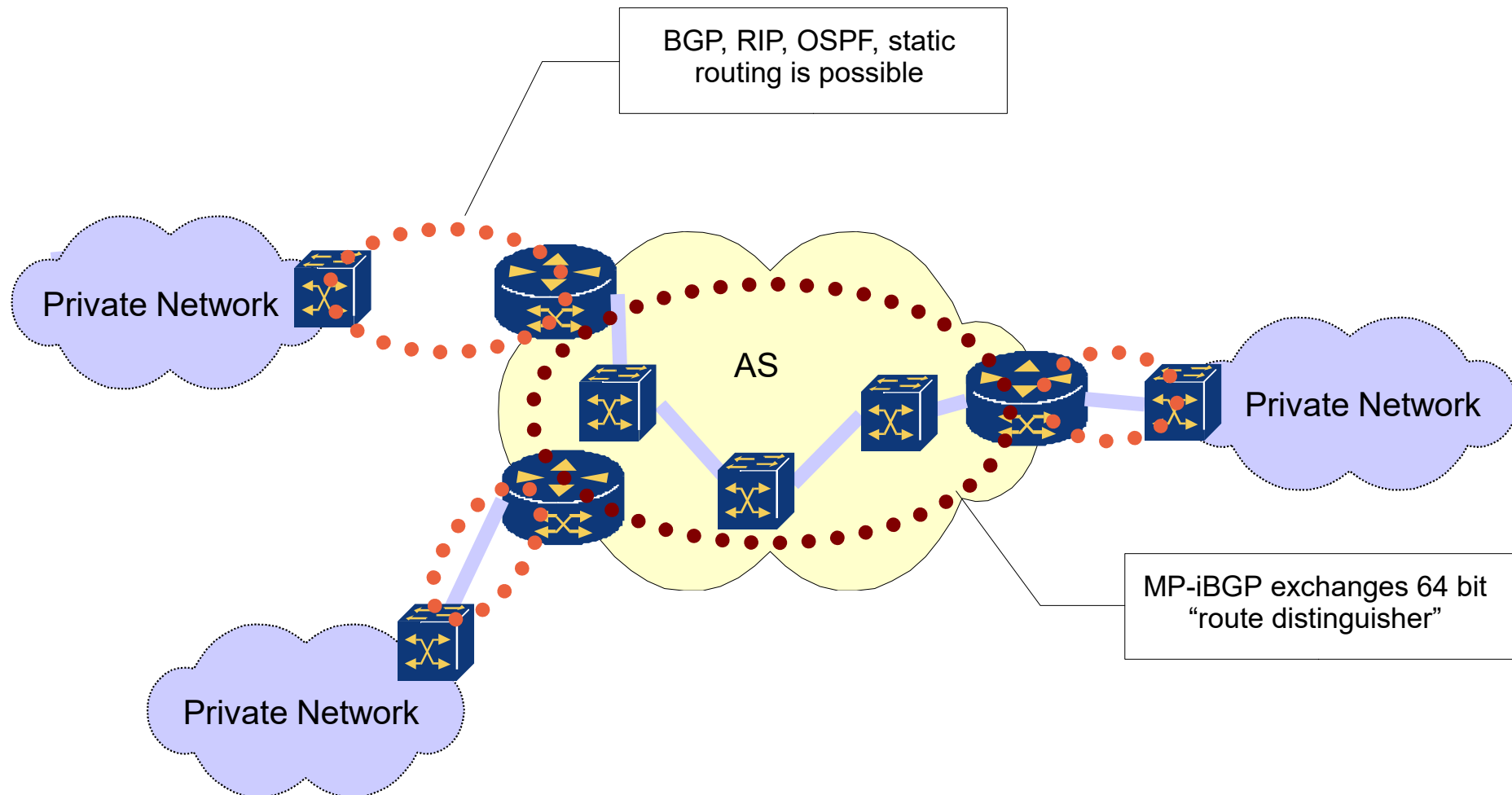




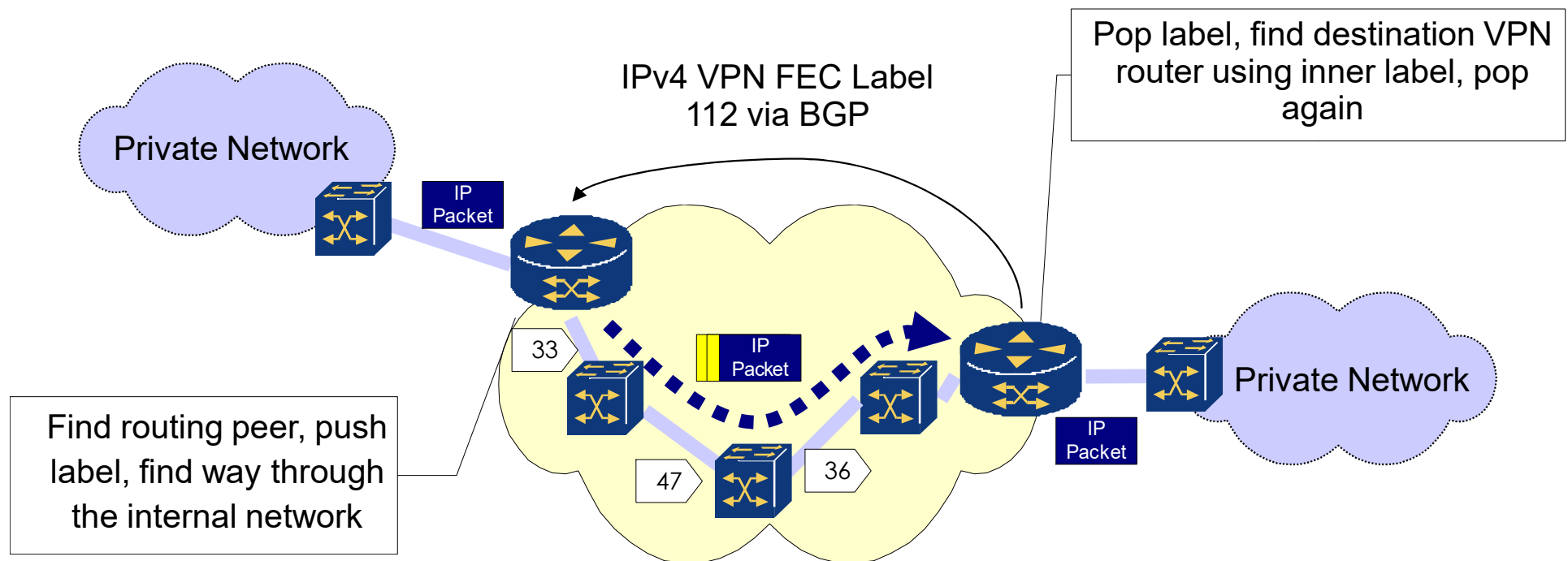


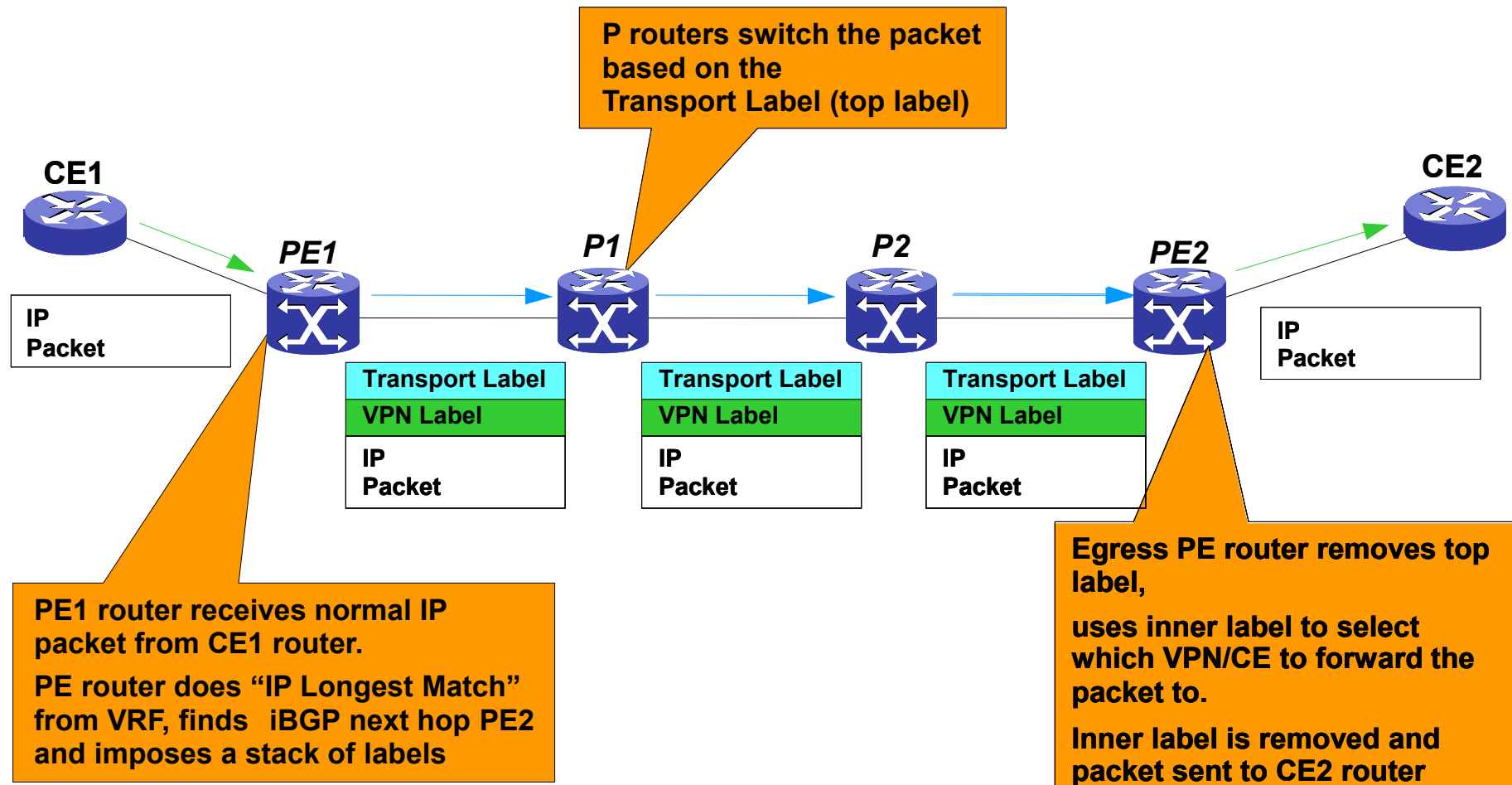
- Ein optionales Attribut, das einer VPN-IP-Route zugeordnet ist
- Zugewiesen, wenn ein PE eine Route von CE lernt
 - Ähnlicher Prozess wie beim Route Target
- Verwendet, um die jeweilige CE-PE-Verbindung zu identifizieren
- Verhindert Routingschleifen
- Ermöglicht Multi-Homed CEs, die mit demselben AS verbunden sind
- Definiert als Route Origin Extended Community
 - Spezifiziert in RFC 4360

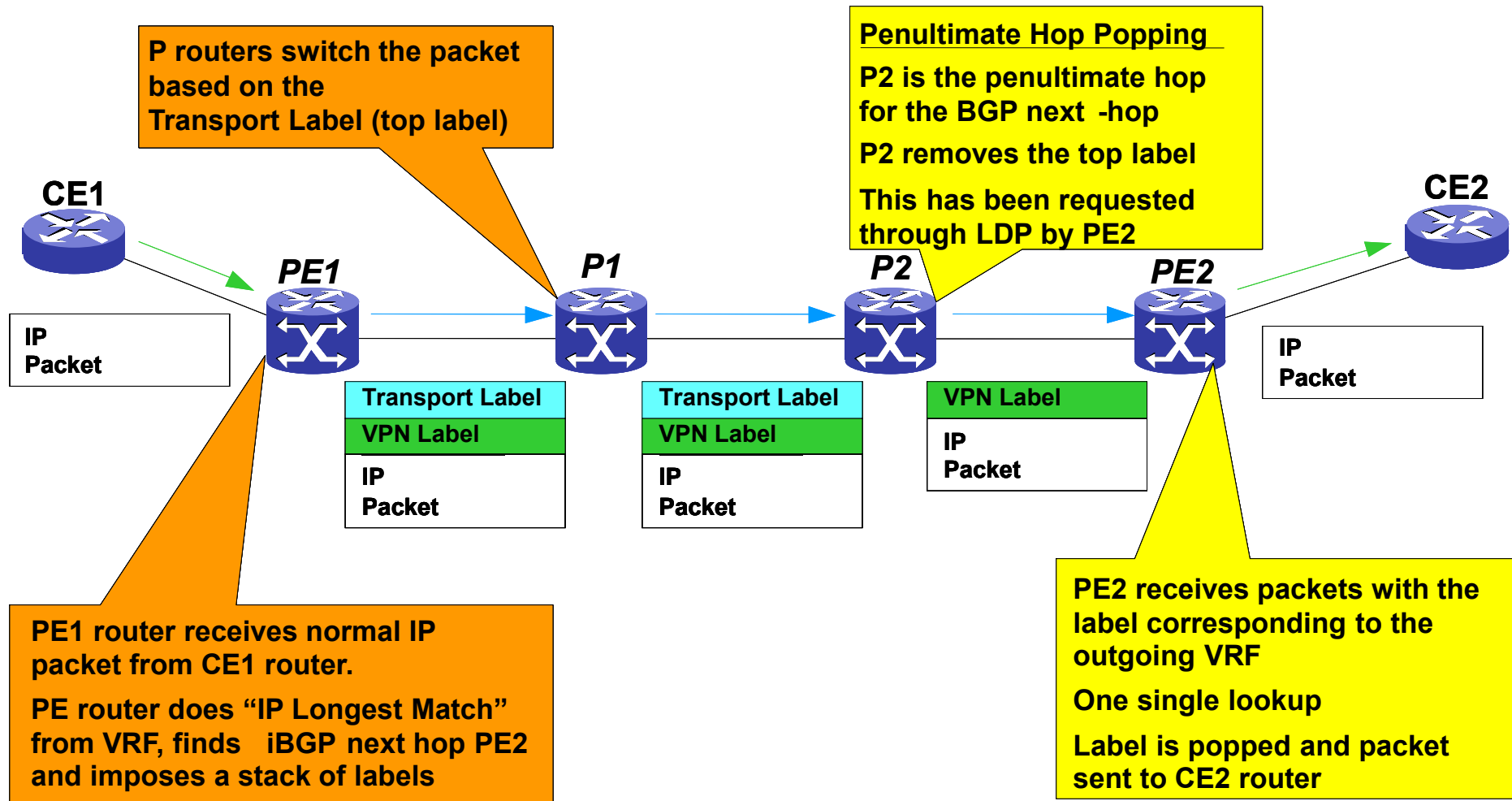
- Mit dem SoO-Attribut können PE-Router gezielt steuern, welche Routen importiert oder exportiert werden sollen



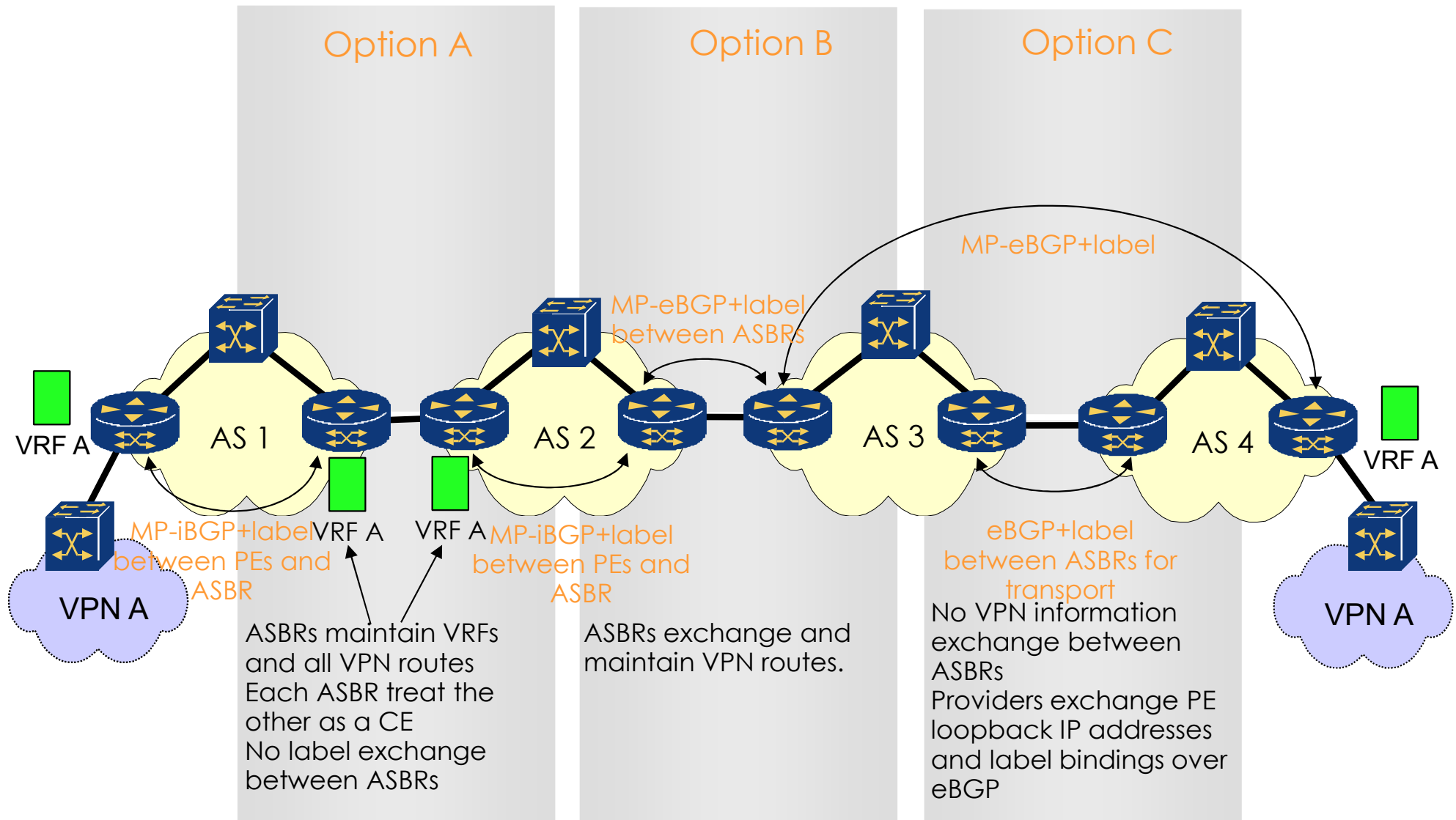
- Verwenden von Labels zur Identifizierung entfernter VRFs
 - Kein Wissen im Core über VPNs
 - Zweites Transportlabel, ähnlich L2VPNs



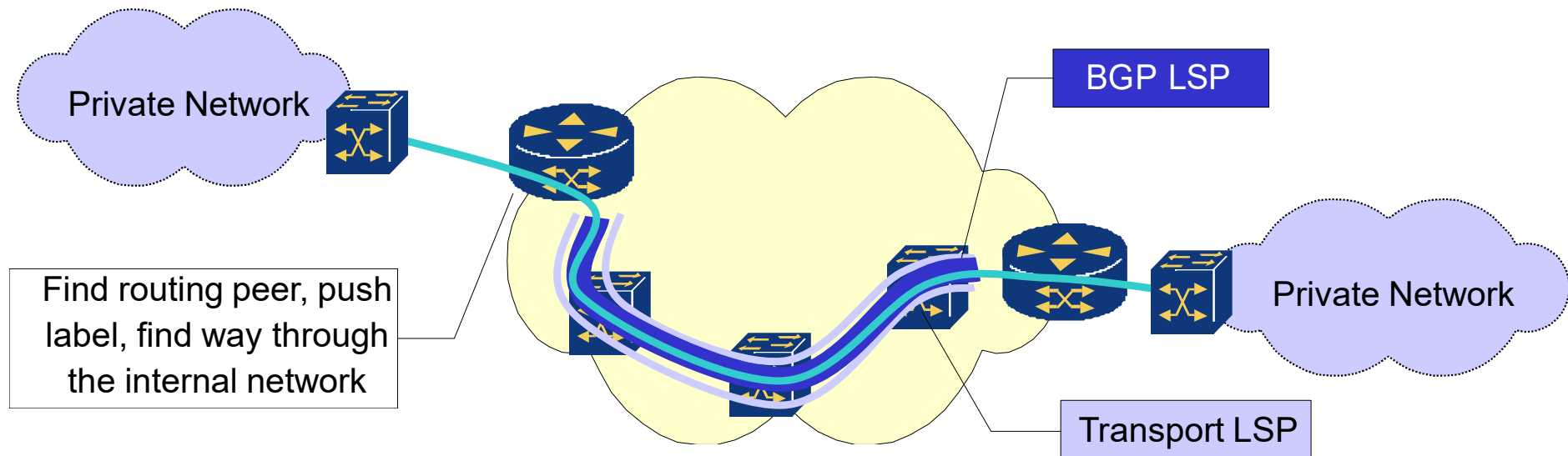




- VPN-Sites sind mit mehr als einem AS verbunden (verschiedene Service Provider)
- PE nutzt iBGP zur Neuverteilung VPN-IPv4 Routen an ASBR
- Verwendet eBGP zwischen Autonomous System Border Router (ASBRs)
 - Vertrauenswürdige Vereinbarung zwischen SPs
 - VPN-IP sollten weder verteilt noch akzeptiert werden aus dem öffentlichen Internet



- Netzwerke, die von einem Carrier bereitgestellt werden, um anderen Anbietern (Carrier) oder großen Unternehmen (Endkunden) Dienste wie MPLS anzubieten
 - Customer Edges (CE) verhandeln Labels mit Provider LERs
 - Provider-LERs bilden das auf Transport LSP ab



Vorteile

Skalierbare VPN-Architektur

Flexibilität: ein Service, der von SP oder Kunden verwaltet wird

Vereinfachtes Kunden-WAN-Routing

SP kann verschiedene SLA pro VPN unterstützen, wenn MPLS TE aktiviert ist

Hohe Verfügbarkeit - MPLS FRR

Nachteile

Komplex für Carrier zu betreiben

Der Kunde hat keine vollständige Kontrolle über sein WAN-Routing

Unterstützt nur IP- oder „IP Encapsulated“-Datenverkehr

Langsame Konvergenz durch BGP, Einsatz von BFD

Network Layer - Vermittlungsschicht

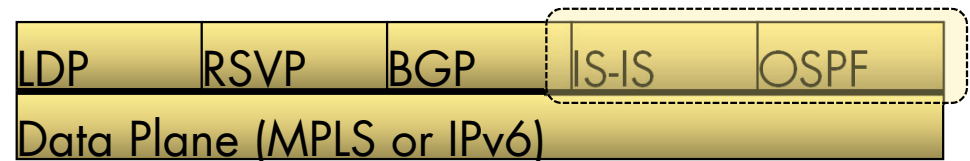
LAYER 3

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

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/>

Classic MPLS

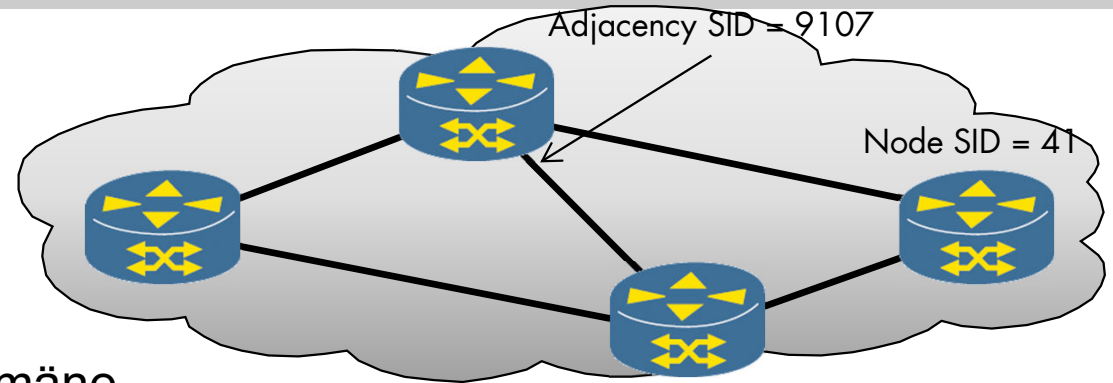
- MPLS verwendet Label-Switched Paths (LSPs), die über Protokolle wie LDP und RSVP-TE signalisiert/aufgebaut werden
- Mehrere Control-Plane-Protokolle (IGP + LDP + RSVP-TE) erhöhen den Betriebsaufwand und erschweren die Fehlersuche
- Eine große Anzahl von LSPs erzeugt viel Zustandsinformation (State)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

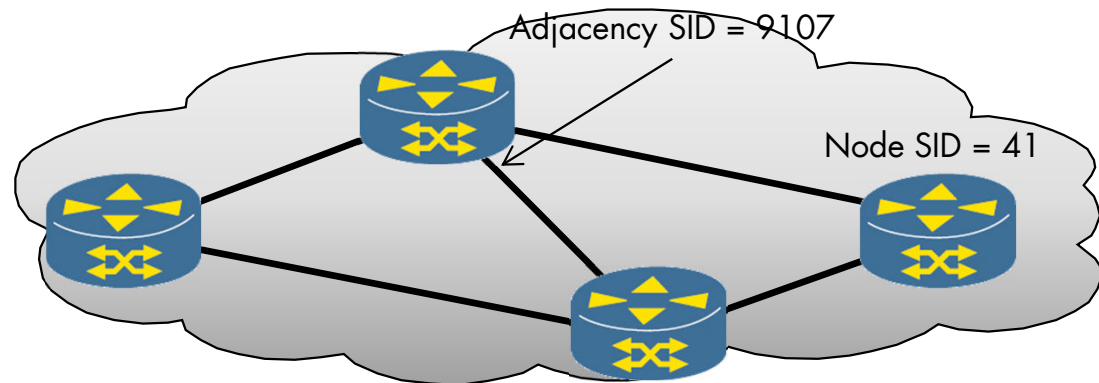
Prefix/Node Segment

- 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 (SR 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



EANTC Interoperability Test Results

Upperside World Congress, March 2026

