

Skalierbare VPNs auf Basis von MPLS

[Zum Starten hier klicken](#)

Inhaltsverzeichnis

Autor: [Axel Clauberg](#)

[Skalierbare VPNs auf Basis von MPLS](#)

[Alphabetsuppe](#)

[Agenda](#)

[Internet Bandbreitenbedarf](#)

[Wachstum des IP Verkehrs](#)

[Erwartungen des Markts](#)

[G-WiN](#)

[Kein ATM mehr - Tränen ?](#)

[Agenda](#)

[IP VPNs](#)

[Was ist ein IP VPN ?](#)

[VPN Modelle - Das Overlay Modell](#)

[VPN Modelle - Das Peer Modell](#)

[VPN Modelle - MPLS-VPN: .Das echte Peer
Modell](#)

[Agenda](#)

[MPLS Konzepte](#)

[MPLS Überblick](#)

[MPLS Betrieb](#)

[MPLS Mehrwertdienste](#)

[MPLS Encapsulations](#)

[Generisches MPLS Headerformat](#)

[Agenda](#)

[MPLS/ VPN Designziele](#)

[“Neue Welt” VPNs](#)

[MPLS VPN .Routing Architektur](#)

[MPLS VPN .VPN-IPv4 Addresses](#)

[MPLS VPN .Per VPN Forwarding
Information Base](#)

[MPLS VPN .Forwarding und Isolierung
Label Stack](#)

[MPLS/VPN Sicherheit](#)

[Agenda](#)

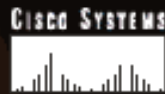
[MPLS Mehrwertdienste](#)

[MPLS Weiterentwicklungen](#)

[Cisco](#)

Skalierbare VPNs auf Basis von MPLS

Axel Clauberg
Consultant IP Services
Axel.Clauberg@cisco.com



AC_041_99

© 1999, Cisco Systems, Inc.

1



Folie 1 von 33

Alphabetsuppe

- **VPN**
Virtuelles Privates Netz
- **MPLS**
Multi Protocol Label Switching



Agenda

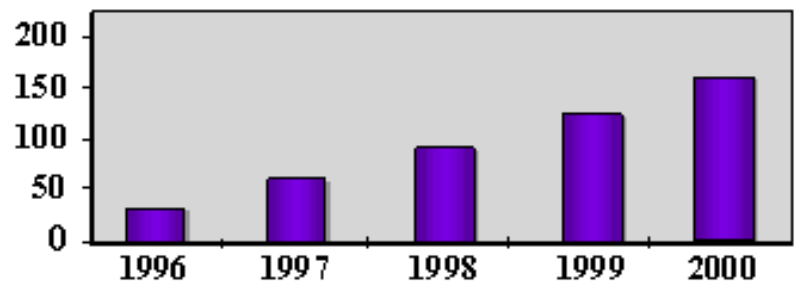
- Aktuelle IP Markttrends
- IP VPNs
- MPLS - Kurzüberblick
- MPLS VPNs
- Ausblick



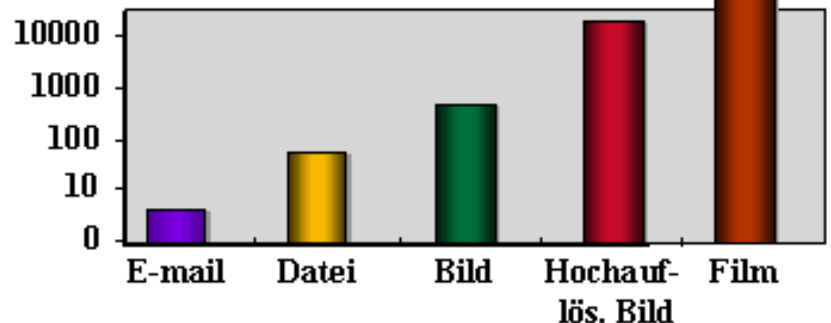
Internet Bandbreitenbedarf

- Anzahl der Endsysteme und Verkehr wächst exponentiell
- Hauptverkehrsanteil: WWW
- Verkehrstypen ändern sich: Multimedia, Echtzeit (Sprache)

World Wide Web Nutzer (Millionen)



Datenumfang (kbytes)



Quelle: IDC

www.cisco.com

AC_041_99

© 1999, Cisco Systems, Inc.

4



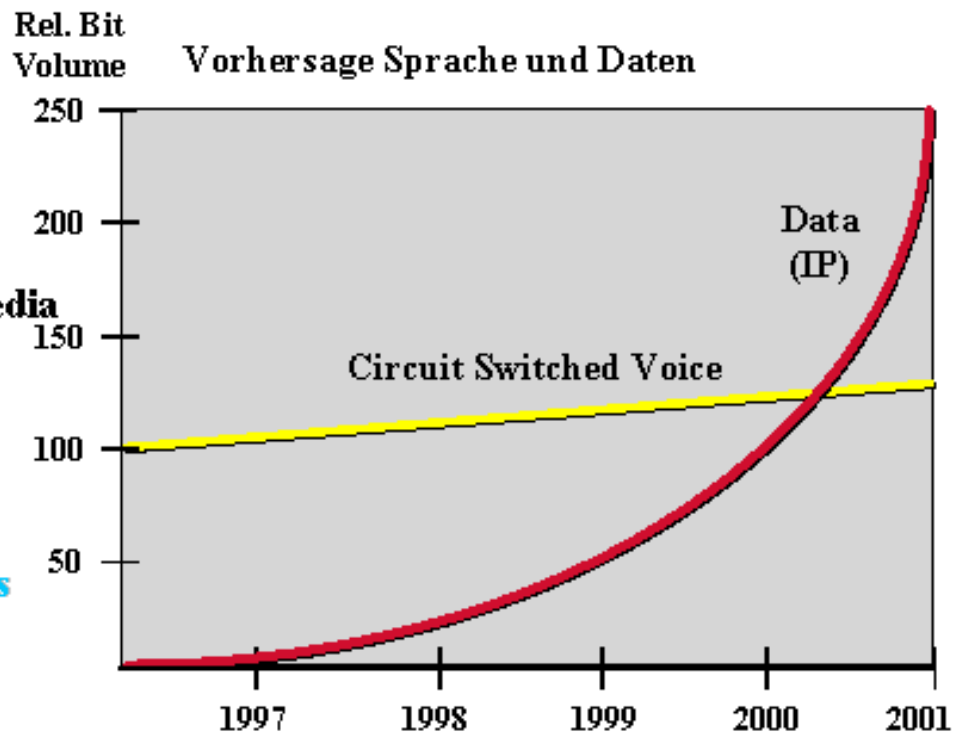
Folie 4 von 33

Wachstum des IP Verkehrs

- **Email**
- **Informations-Suche/Zugriff**
- **Subskriptions-Dienste/“Push”**
- **Konferenzen/ Multimedia**
- **Video/Bildverarbeitung**

“Ab 2000 werden 80% der Service Provider Profite aus IP-basierten Diensten stammen.”

Quelle: CIMI Corp.



Quelle: Mehrere IXC Prognosen



Erwartungen des Markts



Ich sage voraus, daß es in fünf Jahren im Carrierbereich kein getrenntes Netzwerk für Telefonie- und IP-Daten mehr geben wird.

Ein IP Netzwerk mit fortgeschrittenen Dienstmerkmalen im Bereich Sicherheit und Servicequalität — für private und geschäftliche Nutzung — stellt die Basis für alle Dienstangebote dar...



Quelle: InfoWorld Electric July 24, 1997,
Tom Evslin

Ehem als Präsident von AT&T's WorldNet Services



G-WiN

- **IP Optimiert**
- **Punkt-zu-Punkt Dienste mit 2 Mb/s oder 34 Mb/s**
- **Evtl. zusätzlicher ATM Dienst**



Kein ATM mehr - Tränen ?

Nutzung für

- **Videoübertragung, Telemedizin**
Punkt-zu-Punkt Dienst, ATM Service
- **Traffic Engineering für IP Betrieb**
Vertragliche Regelung und/oder MPLS
- **Virtuelle Private IP-Netze**

MPLS

AC_041_99

© 1999, Cisco Systems, Inc.

www.cisco.com

8



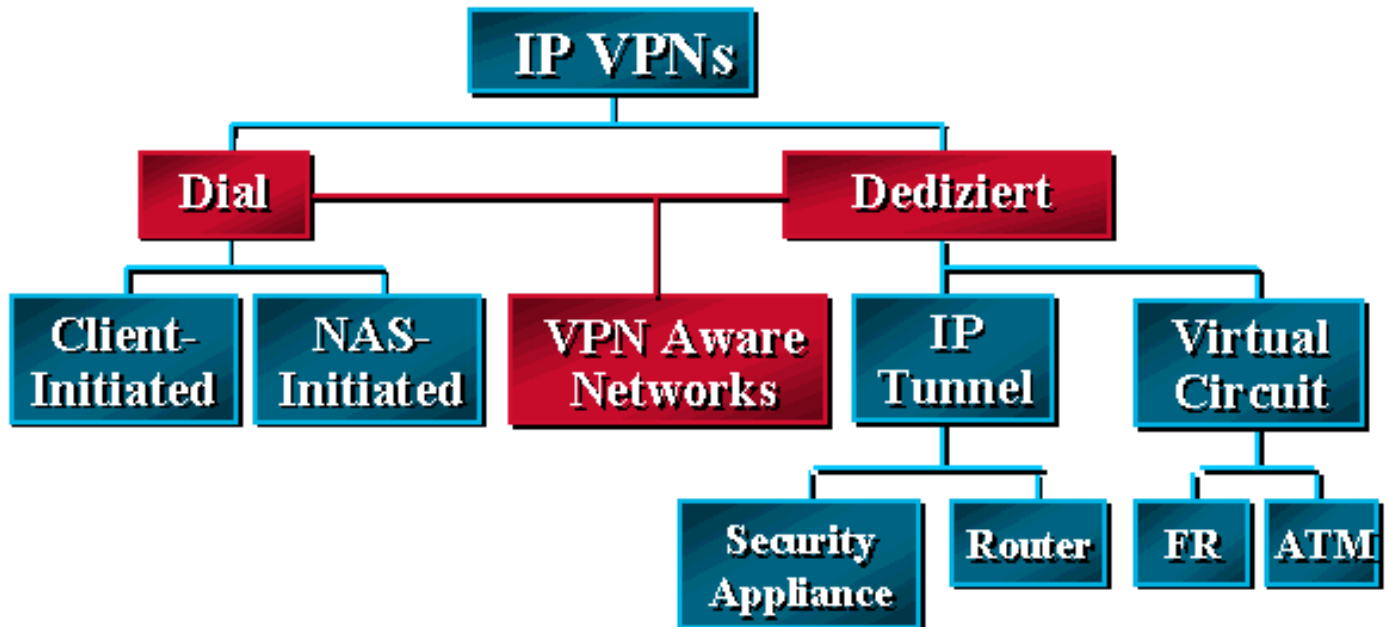
Folie 8 von 33

Agenda

- Aktuelle IP Markttrends
- **IP VPNs**
- MPLS - Kurzüberblick
- MPLS VPNs
- Ausblick



IP VPNs



Was ist ein IP VPN ?

- **Eine IP-basierte Infrastruktur, die private Netzdienste über eine öffentliche Infrastruktur liefert**
- **Wunschliste**
 - Nutzt Layer 3 Backbone**
 - Skalierbar**
 - Einfaches Management (Provider, Kunde)**
 - Globale und private Adressen**
 - QoS**
 - Sicherheit**



VPN Modelle - Das Overlay Modell

- **Private Trunks über eine gemeinsam genutzte Provider-Infrastruktur**
 - Leased/Dialup Lines
 - FR/ATM VCs
 - IP (GRE) Tunnel
- **Transparenz zwischen Provider- und Kundennetz**
- **Optimales Routing erfordert Vollvermaschung über den Backbone**



VPN Modelle - Das Peer Modell

- **Provider und Kunde nutzen dasselbe Netzwerkprotokoll**
- **CE und PE Router tauschen Routen an jeder Site aus**
- **Alle Provider Router führen volle Routinginformation über alle Kundennetze**
- **Private Adressen sind nicht erlaubt**
- **Virtueller Router ?**

Mehrere Kunden = mehrere Routingtabellen



VPN Modelle - MPLS-VPN: Das echte Peer Modell

Wie Peer Modell, aber...

- **Provider Edge Router führen nur Routinginformation über direkt angebundene VPNs**
- **Provider Backbone Router haben keine Informationen über VPNs**
- **MPLS wird genutzt, um VPN-Pakete im Backbone weiterzuleiten**



Agenda

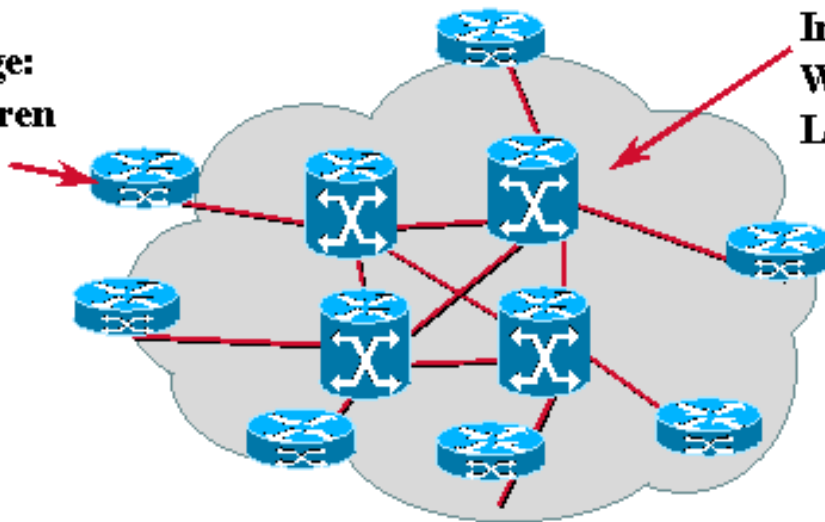
- Aktuelle IP Markttrends
- IP VPNs
- **MPLS - Kurzüberblick**
- MPLS VPNs
- Ausblick



MPLS Konzepte

An der Edge:

- klassifizieren
- labeln



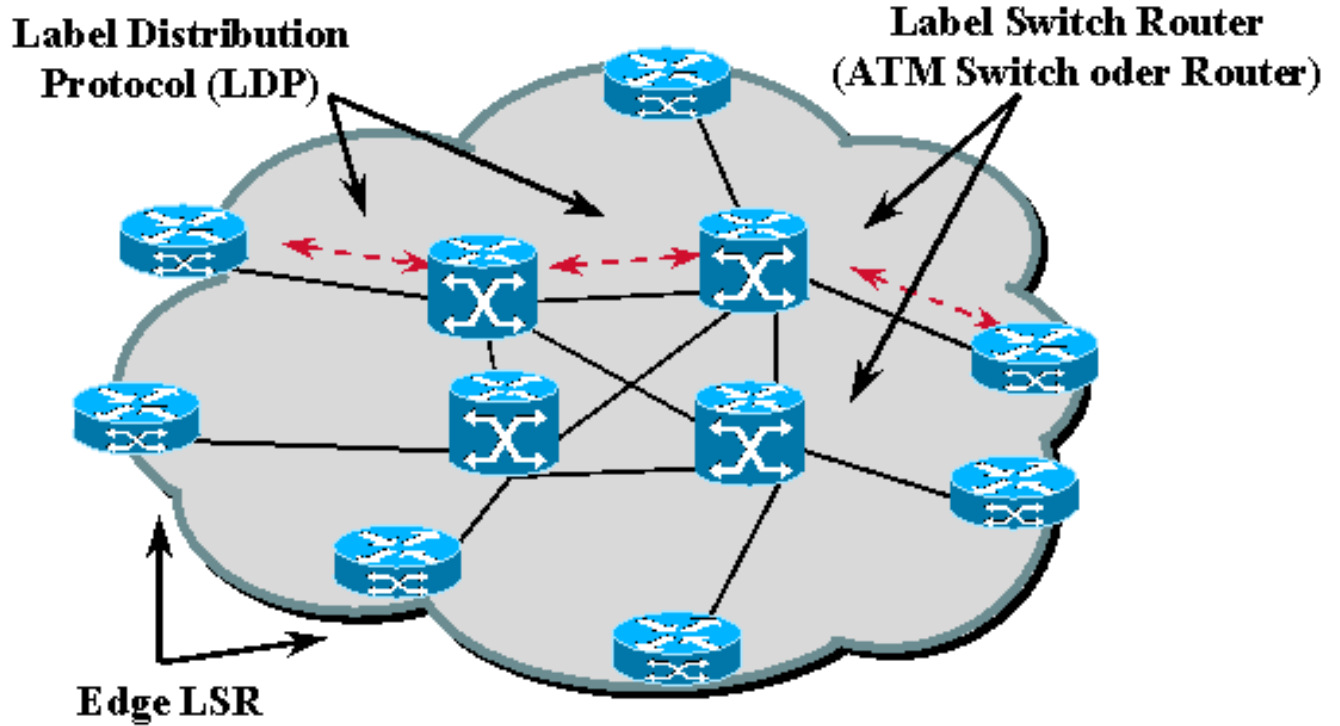
Im Core:

Weiterleitung basierend auf Label anstatt IP Adresse

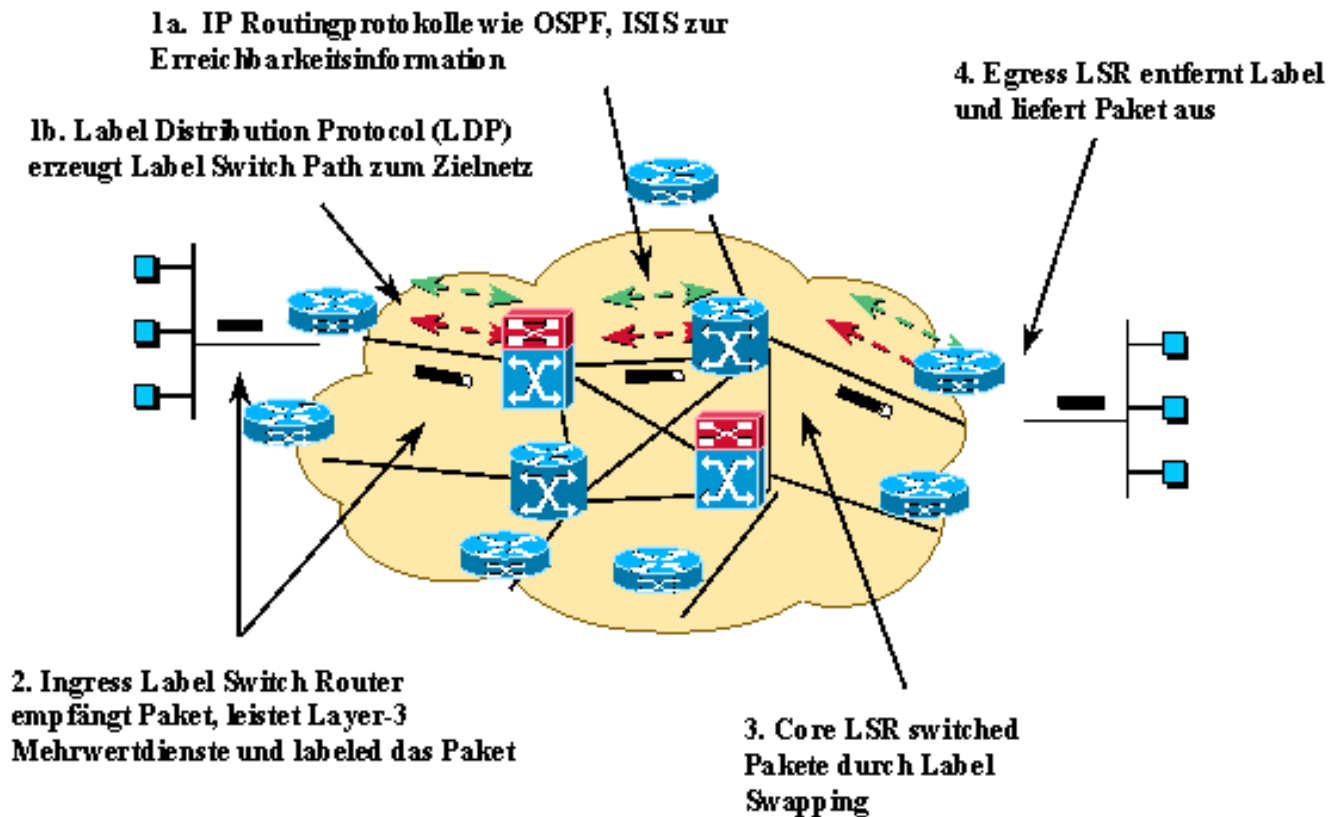
- **ATM Switch als Router nutzbar**
- **Neue IP Dienste durch Trennung von Forwarding und Kontrolle**



MPLS Überblick



MPLS Betrieb



AC_041_99

© 1999, Cisco Systems, Inc.

www.cisco.com

18



Folie 18 von 33

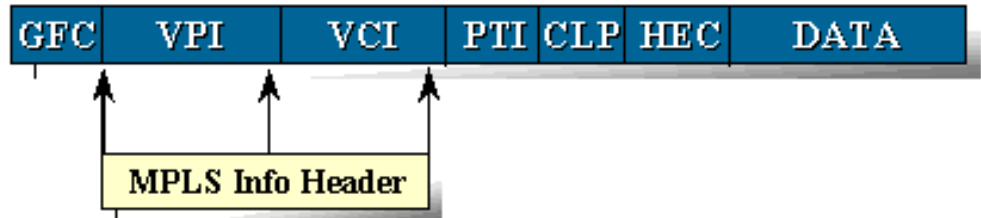
MPLS Mehrwertdienste

- **MPLS Basis: Zielbasiert, Unicast**
- **Viele Optionen zur Erzeugung von Labeln**
- **Kernpunkt: Trennung von Routing und Forwarding**



MPLS Encapsulations

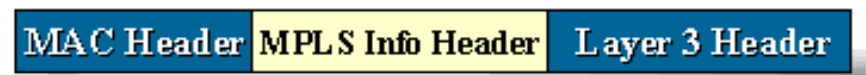
ATM Cell Header



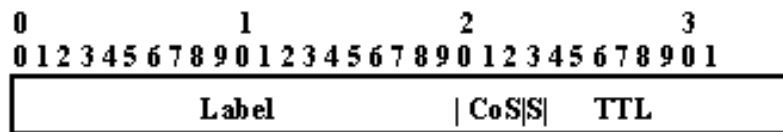
PPP Header (Packet over SONET/SDH)



LAN MAC Tag Header



Generisches MPLS Headerformat



Label = 20 bits

CoS = Class of Service, 3 bits

S = Bottom of stack, 1bit

TTL = Time to live, 8 bits

- **Generisch: Nutzung über Ethernet, 802.3, POS, DPT, PPP Links, Frame Relay, ATM PVCs, etc.**
- **2 neue Ethertypes/PPP PIDs/SNAP/etc. Werte - einer für Unicast, einer für Multicast**
- **4 Oktets (pro MPLS Ebene)**



Agenda

- Aktuelle IP Markttrends
- IP VPNs
- MPLS - Kurzüberblick
- **MPLS VPNs**
- Ausblick

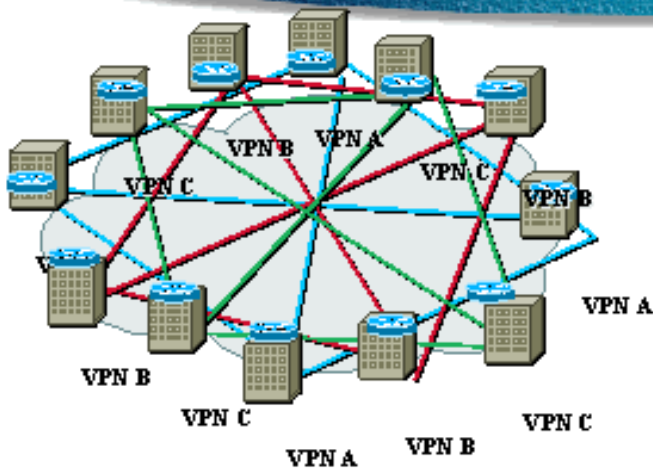


MPLS/ VPN Designziele

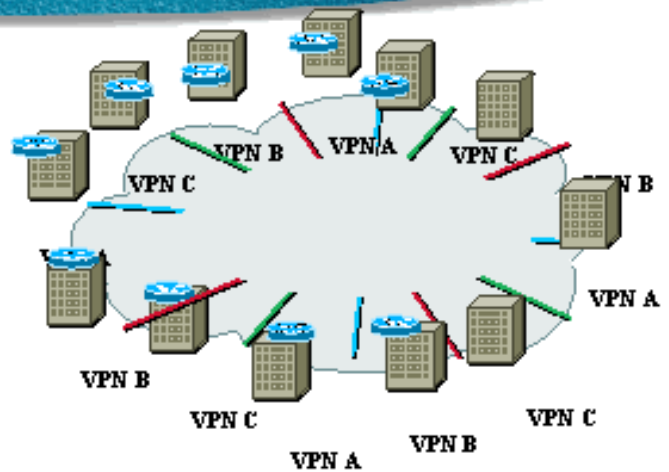
- **Private und isolierte Netze**
- **Sicherheit**
- **Quality of Service & SLA**
- **Leistung**
- **Flexibilität, Medienunabhängig**
- **Private Adressen**
- **Skalierbarkeit**
- **Einfaches Management, Erweiterung**



“Neue Welt” VPNs



**Verbindungsorientiertes
VPN**



**Verbindungsloses
VPN**

**VPN Aware Network :
VPNs sind “eingebaut”
und nicht “aufgesetzt”**



MPLS VPN Routing Architektur

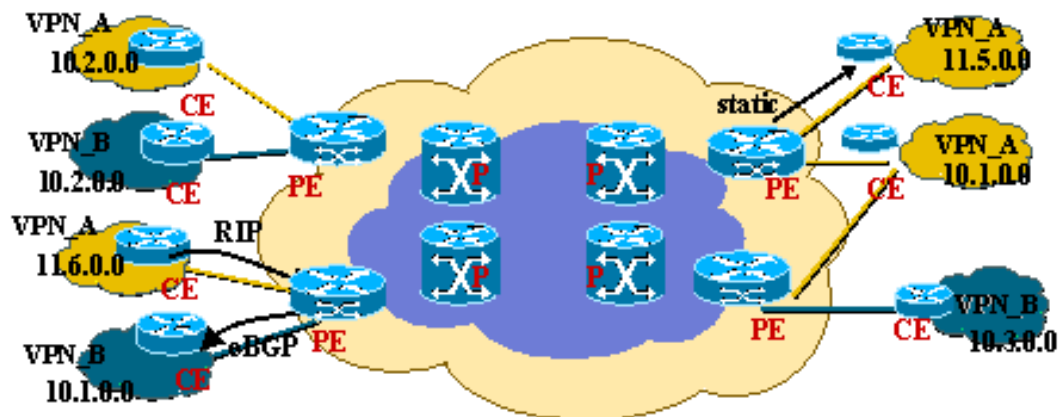


- **P** Router = Provider Router (Core LSR) (ZR, GR)
- **PE** Router = Provider Edge Router (Edge LSR)
kennt VPN-Zuordnung jedes Ces (Interface/Subinterface) (WR, AR, ar)
- **CE** Router = Customer Edge Router (KR)
- 64 Bit Route Distinguisher = eindeutige VPN Identifizierung (AS#,VPN_ID)
- IPv4 Adressen sind innerhalb eines VPN eindeutig
- IPv4 Adressen dürfen in anderen VPN's genutzt werden



MPLS VPN

VPN-IPv4 Addresses

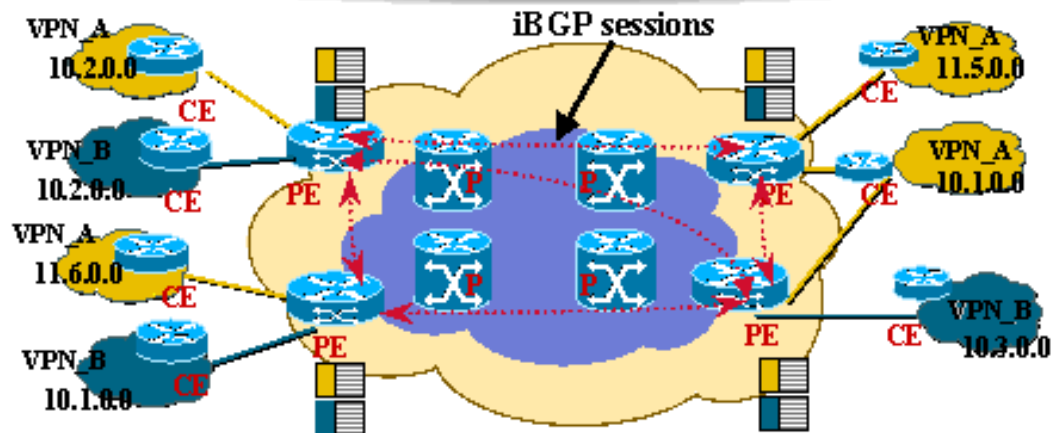


- PE lernt Routen aus VPN durch statische Einträge, RIPv2, eBGP, zukünftig auch OSPF
- PE Router konvertiert IPv4 Adresse zu global eindeutiger VPN-IPv4 Adresse
- 64 bit "**Route Distinguisher**" wird IPv4 Adresse vor gestellt und via MP-iBGP zu anderen PEs kommuniziert (BGP Multiprotocol Extension)



MPLS VPN

Per VPN Forwarding Information Base

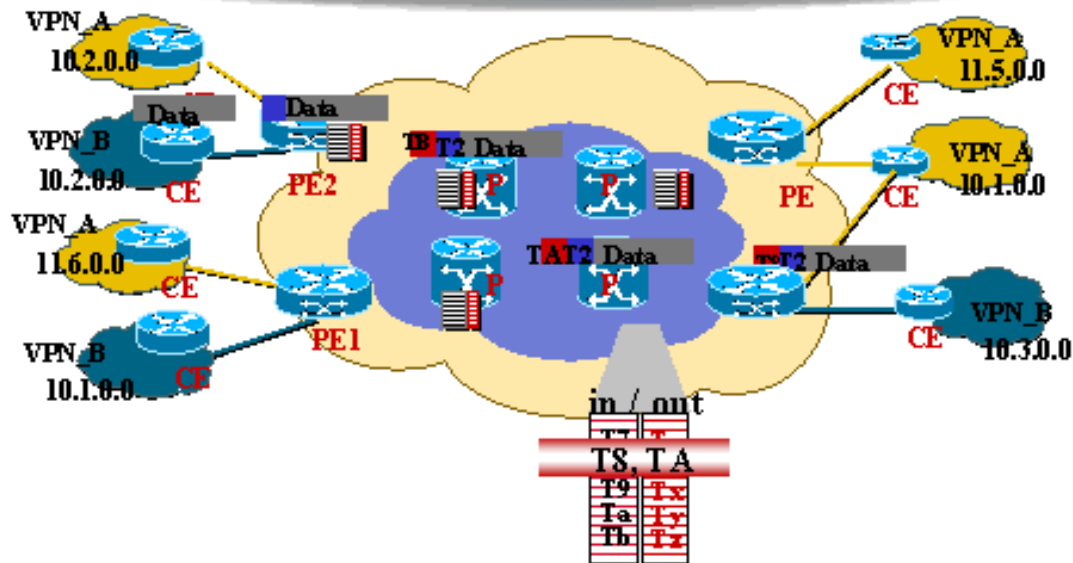


- *VPN-IPv4* Adressen werden zusammen mit dem assoziierten **Label** in "BGP multi-protocol extension" (NLRI field) weitergereicht
- Zusätzliche Community Fields (64 bits Extended Community attribute) sind mit *VPN-IPv4* Adress assoziiert zum Aufbau einer per VPN FIB:
 - **"Target VPN"** (list of), "VPN of Origin", Site of Origin
- **Filter (route-maps) sichern strikte Kontrolle und Intra-/Inter-VPN Kommunikation**



MPLS VPN

Forwarding und Isolierung Label Stack



- Alle P Router switchen das Paket **ausschließlich auf Basis des internen Labels**
- Egress PE Router entfernt **Internes Label**
- Egress PE nutzt **Externes (inneres) Label** zur Selektion des VPNs/CE s
- **Externes Label** wird entfernt und Paket normal zum CE Router geroutet



MPLS/VPN Sicherheit

- **Strikt kontrollierte Routenverteilung**
Äquivalent zu ATM/Frame Relay Netzen
- **VPN Isolierung ist garantiert**
Label Stack mit L2 Switching im Core
- **VPN_ID kann nicht vorgetäuscht werden**
Nicht im Paket enthalten
- **Optional zusätzliche Sicherheit mit IPSec**
- **BGP Authentifikation und Signaturmechanismen (MD5)**



Agenda

- Aktuelle IP Markttrends
- IP VPNs
- MPLS - Kurzüberblick
- MPLS VPNs
- **Ausblick**



MPLS Mehrwertdienste

- **VPNs**
 - **Traffic Engineering**
 - **Grundlage für IP-optimierte Providernetze**
 - **Ablösung von ATM oder Frame-Relay**
- Beispiel: AT&T**



MPLS Weiterentwicklungen

- **Fast Restoration**
- **Konvergenz normaler Routingprotokolle (OSPF, ISIS) ca. 4 - 5 Sekunden**
- **Konvergenz mit MPLS in ca. 50 ms möglich !**





© 1999, Cisco Systems, Inc.

www.cisco.com

33



Folie 33 von 33