# Virtual Private Network / Multi Protocol Label Switching

Elmar Klute[1], Roland Schott[1], Rüdiger Geib[1], und Heinrich Gebehenne[2]

[1] T-Systems Technologiezentrum
[2] T-Systems Nova GmbH

**Zusammenfassung** Viele Unternehmen nutzen inzwischen Intranets zur Steuerung der betrieblichen Abläufe. Die so entstehenden Firmennetze werden in der Regel als Virtuelle Private Netze (VPN) auf öffentlichen Netzen realisiert. Derzeit basieren diese VPNs auf Mietleitungen oder Ebene-2-Netzwerken wie ATM und Frame Relay.

Der Begriff virtuelles privates Netz (VPN) steht allgemein für ein logisches Netz einer geschlossenen Benutzergruppe, das in einem öffentlichen Netz „virtuell" realisiert ist. Bisher werden VPNs im wesentlichen mit Hilfe von Mietleitungen (Leased Lines) oder mit Schicht 2 (Layer 2) Vermittlungsnetzen basierend auf Frame Relay (FR) oder dem Asynchronous Transfer Mode (ATM) realisiert.

Während in der Vergangenheit in Firmennetzen eine Vielzahl unterschiedlicher Ebene 3 Protokolle (SNA, IPX, usw.) eingesetzt wurden, wird in den Firmennetzen heute fast ausschließlich das Internet Protokoll (IP) verwendet. Deshalb benötigen viele Unternehmen inzwischen auch einen hochbitratigen Zugang zum Internet. Wenn zur Abwicklung der Geschäfte ein hochbitratiger Internetzugang erforderlich ist, was liegt da näher, als auch das Unternehmensnetz in Form eines Virtuellen Privaten Netzes (VPN) über das Internet zu realisieren. Die Kosten für diese Lösung sind in der Regel günstiger als „klassische" WAN-Verbindungen, weil das Internet omnipresent ist und Internetzugänge in der Regel flächendeckend zu günstigen Konditionen bereitgestellt werden können.

Inzwischen hat sich die IP-Technologie erheblich weiter entwickelt und ist in der Lage, die für VPNs benötigte Funktionalität bereit zu stellen. So ist inzwischen sichergestellt, dass es keine Vermischung des „Consumer" IP-Verkehrs mit dem VPN-Verkehr gibt. Beide Verkehre werden unabhängig voneinander transportiert.

In einer Multi-Protokollumgebung (z.B. Multi Protocol Label Switching, MPLS) muss der Kunde dem Service Provider ein gewisses Vertrauen entgegenbringen, dass sein Verkehr sicher und unverfälscht über das „shared Network" transportiert wird. Dieses Vertrauen ist aber im Prinzip identisch mit dem Vertrauen, das der Kunde auch einem Betreiber eines ATM- oder FR-Netzes entgegenbringen muss. Wie bei ATM oder FR wird auch bei MPLS der Verkehr unterschiedlicher Nutzer durch ein Label gekennzeichnet und so eindeutig voneinander getrennt. Falls es darüber hinausgehende Sicherheitsanforderungen gibt, sorgen Verschlüsselungsprotokolle wie IPSec für die nötige Sicherheit.

Neben der Datensicherheit sind die Bereitstellung der benötigten Qualität und Zuverlässigkeit weitere Merkmale, die IP-Netze bereitstellen müssen, um als Trägernetz für VPNs Verwendung zu finden. Mit Technologien wie DiffServ (Differentiated Services), sind IP-Netze in der Lage, diese Anforderungen zu erfüllen. Weitere Informationen zu DiffServ sind in Abschnitt 4 zu finden.

Die Realisierung der VPNs in einem IP/MPLS Provider Netz kann entweder Netz oder Endgeräte basierend sein. Außerdem ist zwischen Layer 3 und Layer 2 VPNs

zu unterscheiden. Bei Layer 3 VPNs wird ausschließlich das Internet Protocol unterstützt. In Layer 2 VPNs können auch andere Netzwerkprotokolle übermittelt werden. Layer 3 VPNs können mit Hilfe der Virtual Router (VR) Technologie (siehe Abschnitt 2) oder wie in [5] beschrieben mit Hilfe des Piggybacking-Verfahrens (siehe Abschnitt 3) realisiert werden.

# 1 Realisierung von VPNs mit IPSec

IPSec ist im RFC 2401 [1] und diversen anderen RFCs spezifiziert. Es bietet Sicherungsmechanismen auf der IP-Ebene an. IPSec schützt jedes Datenpaket vor unbefugter Kenntnisnahme und Verfälschung und garantiert somit die Vertraulichkeit, Authentizität und Integrität.

IPSec umfasst folgende Sicherheits- und Managementkomponenten

- den Authentication Header (AH) für die Authentifizierung von IP-Paketen
- die Encapsulating Security Payload (ESP) für die Verschlüsselung von IP-Paketen
- das Internet Key Exchange (IKE) Verfahren für das automatische Aushandeln von Sicherheitsparametern
- die Public Key Infrastructure (PKI) für das Verwalten und Zertifizieren von öffentlichen Schlüsseln.

Während die ersten beiden Komponenten primärer Bestandteil von IPSec sind, sind das IKE-Verfahren und die PKI optionale Elemente, die bei großen VPNs zur notwendigen Skalierbarkeit beitragen.

## 1.1 Transport- und Tunnelmodus

AH und ESP können im Transport- und Tunnelmodus eingesetzt werden (Abb. 1). Der Unterschied zwischen Beiden besteht darin, dass im Transportmodus der original IP-Header erhalten bleibt, während im Tunnelmodus das gesamte IP-Paket (inkl. original IP-Header) durch das Voranstellen eines neuen IP-Headers enkapsuliert wird.

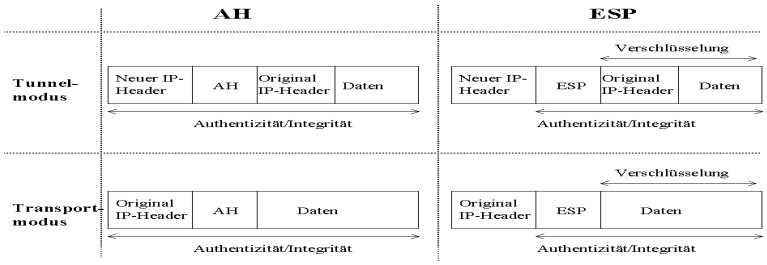


**Abbildung 1:** AH und ESP im Transport- und Tunnelmodus (vereinfachte Darstellung)

Der Transportmodus hat den Vorteil, dass jedem IP-Paket nur wenige Bytes hinzugefügt werden. Demgegenüber bietet der Tunnelmodus eine höhere Sicherheit, weil das gesamte IP-Paket authentifiziert bzw. verschlüsselt wird.

### 1.2 Internet Key Exchange (IKE)

Das Schlüsselaustauschprotokoll IKE ist im RFC 2409 [2] spezifiziert. Bevor eine IPSec-Verbindung zwischen zwei Kommunikationspartnern aufgebaut werden kann, müssen individuelle Sicherheitsparameter festgelegt werden, die die Art der Sicherheitsbeziehung charakterisieren.

Diese Parameter werden in Security Associations (SAs) festgelegt. Die Festlegung der SAs kann manuell oder automatisch mittels IKE erfolgen. Es liegt auf der Hand, dass eine manuelle Vereinbarung der SAs, nur bei kleinen VPNs mit wenigen Nutzern sinnvoll ist.

Die Vereinbarung der IPSec SAs geschieht mit dem Internet Security Association and Key Management Protocol (ISAKMP) in zwei Phasen:

1. Aufbau eines gesicherten Kanals zwischen zwei Partnern (ISAKMP SA Kanal)
2. Vereinbarung der IPSec SAs zwischen den Partnern innerhalb des gesicherten ISAKMP SA Kanals.

Das erste Ergebnis der 1. Phase sind zwei gemeinsame Geheimschlüssel (shared secret keys) zur Authentifizierung und Verschlüsselung der nachfolgenden ISAKMP-Nachrichten. Die Geheimschlüssel werden mit dem Diffie-Hellman (DH) Verfahren berechnet. Hierzu erzeugen beide Partner mit Hilfe eines zuvor vereinbarten mathematischen Basiswertes einen öffentlichen Schlüssel und einen privaten Schlüssel, um anschließend daraus den gemeinsamen Geheimschlüssel zu generieren.

Die wesentliche Aufgabe der 2. Phase ist die Vereinbarung der IPSec SA (z.B. Festlegung des Verschlüsselungsalgorithmuses) für den nachfolgenden Datenverkehr. Die gemeinsamen Geheimschlüssel zur Authentifizierung und Verschlüsselung der späteren IPSec-Verbindung werden entweder aus einem in der 1. Phase mit dem DH-Verfahren speziell generierten Schlüssel (derivation key) abgeleitet (Quick Modus) oder mit Hilfe des DH-Verfahrens völlig neu berechnet (Perfect Forward Secrecy, PFS).

### 1.3 Public Key Infrastructure (PKI)

Wie bereits erwähnt kann die Authentifizierung der Kommunikationspartner mittels fest vereinbarten Geheimschlüsseln (pre-shared secret keys) oder mit Hilfe einer digitalen Signatur geschehen.

Die digitale Signatur basiert auf dem Prinzip, dass ein Sender eine Nachricht mit seinem privaten Schlüssel (private key) – dieser ist nur dem Sender bekannt – signiert und der Empfänger mit dem öffentlichen Schlüssel (public key) des Senders, der allgemein zugänglich ist, die Signatur prüft. Um die Echtheit des öffentlichen Schlüssels zu gewährleisten (Schutz gegen Man-in-the-Middle-Attacks) ist es erforderlich, dass eine unabhängige Partei den öffentlichen Schlüssel zertifiziert. Die Bereitstellung einer entsprechenden Infrastruktur wird als PKI bezeichnet. Eine PKI setzt sich aus den Instanzen Registration Authority (RA) und Certificate Authority (CA) zusammen, die in einem Trust Center angesiedelt sind.

## 2 Virtual Router und IP VPNs

Die Architektur von VPNs basierend auf dem Virtual Router (VR) Konzept ist in [3] und [4] beschrieben. Dabei werden in die Provider Plattform integrierte virtuelle Router verwendet, um den VPN-Service zu realisieren. Bei einem virtuellen Router handelt es sich um die Emulation eines physikalischen Routers. Der emulierte Router unterstützt den vollen Funktionsumfang physikalisch vorhandener Router. Die VR-Technologie unterstützt ausschließlich das Internet Protokoll (IP) .

Die virtuellen Router sind über den Backbone des Providers miteinander verbunden. Innerhalb der Backbone-Plattform werden keine VPN-Funktionen unterstützt. VPN spezifische Mechanismen sind nur am Netzrand (Provider Edge, PE) realisiert.

Die Realisierung von VPNs mit VR-Technologie erfolgt durch die Verbindung der VR über Layer-2-Tunnel oder IP/MPLS-Tunnel. Ob eine Vollvermaschung oder eine hierarchische Struktur der Tunnel gewählt wird hängt von den VPN spezifischen Anforderungen ab.

Die Tunnel werden entweder statisch konfiguriert oder dynamisch aufgebaut. Aus Sicht des VR stellt der Tunnel eine Punkt-zu-Punkt Verbindung dar.

Für jedes VPN können separate Tunnel eingerichtet werden. Die Tunnel sind in der Regel VPN spezifisch; d.h. in einem Tunnel werden nur die Informationen eines VPN übertragen (single Tunnel). Zur Erhöhung der Skalierbarkeit ist aber auch möglich, die Informationen mehrerer VPNs in einem Tunnel zusammen zu fassen (multiple Tunnel). Hierzu eignet sich besonders MPLS, da Label Stacking (siehe Abschnitt 3.1) eine beliebige Anzahl von Hierarchiestufen ermöglicht.

Alle virtuellen Router unterhalten eigenständige Routing- und Forwarding Tabellen. Dies bedeutet, dass sich die VPN-Adressen unterschiedlicher VPNs beliebig überlappen können. Innerhalb eines VPNs muss aber eine eindeutige Adressstruktur bestehen. Die VR unterstützen alle gängigen Routing-Protokolle wie OSPF, RIP, usw. Es können aber auch statische Routen verwendet werden.

Die VR tauschen ihre Routen über die Backbone-Tunnel untereinander aus. Beim VPN-Routing und dem Routing im Backbone handelt es sich um zwei völlig voneinander getrennte Routing-Prozesse, die vollkommen unabhängig voneinander ablaufen und nicht miteinander in Beziehung stehen.

VR-Implementierungen sind vorrangig in der ATM-Welt zu finden. Neben der ATM-Conrol Plane werden zusätzlich VR-Funktionen implementiert. Die VR werden über ATM-VC miteinander vermascht. Dabei gibt es sowohl voll vermaschte als auch „Hub and Spoke“ Lösungen.

## 3 Realisierung von IP-VPNs mit MPLS und MP-BGP

### 3.1 MPLS Grundlagen

Multi Protocol Label Switching (MPLS) ist ein Paradigma zur flexiblen und schnellen Weiterbeförderung von IP-Paketen in einer neuen Generation von Routern, die als Label Switch Router (LSR) (Einsatz im Netzinneren) oder als LER (Einsatz am Netzrand) bezeichnet werden.

MPLS beschreibt sowohl einen schnellen, Hardware gesteuerten Mechanismus zur Beförderung von IP-Paketen, als auch ein Satz von Signalisierungsprotokollen zum Verteilen der Label in einem Netzwerk. Diese Mechanismen wurden von der IETF spezifiziert.

Alle MPLS-Rahmen werden beim Eintritt in das MPLS-Netzwerk mit einem MPLS-Header versehen und anschließend entlang sogenannter MPLS-Pfade (Label Switch Path, LSP) durch das Netzwerk geleitet. Der Aufbau der LSPs geschieht mit Hilfe des Label Distribution Protocol (LDP). Dabei folgen die MPLS-Pfade den vom internen Routing-Protokoll berechneten Erstwegen.

Die Struktur des MPLS-Headers ist im RFC 3036 [6] beschrieben. Im Label Feld steht der Wert des Labels. Die Nutzung der drei Experimental Bits ist nicht weiter spezifiziert. Häufig werden diese Bits zur Kennzeichnung unterschiedlicher Serviceklassen gemäß dem DiffServ-Modell (siehe Abschnitt 4) verwendet. LSPs, bei denen die Experimental Bits zur Kennzeichnung der Serviceklassen verwendet werden, werden als E-LSPs bezeichnet. Daneben gibt es L-LSPs, bei denen der gesamte LSP die Charakteristik einer Serviceklasse aufweist. Das S Bit wird gesetzt, wenn ein Label das letzte Label in einem Labelstack (Verschachteln mehrerer Label) ist. Das TTL Feld (Time to Live) wird einfach aus dem IP Header kopiert. Der Begriff Label wird in der Regel auch als Synonym für den MPLS Header verwendet.

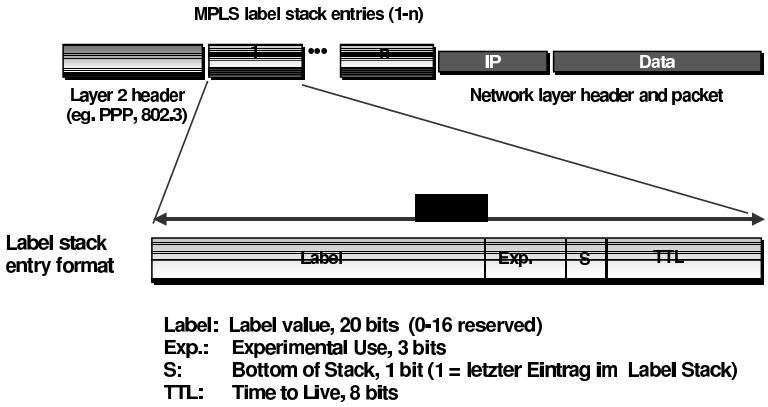


**Abbildung 2:** MPLS-Rahmen

Die Übertragung eines MPLS-Rahmens wird aufgrund der Label-Information im Label Switch Router (LSR) durchgeführt. Die Auswertung des Label, mit dem das IP-Paket versehen ist, basiert auf den Informationen in der Forwarding Information Base (FIB), die zusätzlich zur Routingtabelle in einem LSR unterhalten wird. Eine FIB besteht aus einer mehrspaltigen Tabelle, die neben dem IP-Adresspräfix jeweils einen Eintrag für das ankommende Label und einen Eintrag für das abgehende Label sowie für die ankommende und abgehende Anschlussbaugruppe (Interface) enthält. Der IP-Adresspräfix, für den ein Label zugewiesen wird, wird im MPLS Kontext auch als „Forwarding Equivalence Class“

(FEC) bezeichnet. Üblicherweise handelt es sich bei einer FEC um einen Adresspräfix, der der Routingtabelle des netzinternen Routingprotokolls entstammt.

Sobald ein LSR einen MPLS-Rahmen empfängt, entfernt der LSR den ankommenden Label und vergleicht diesen mit den Einträgen in seiner FIB. Falls für diesen Label ein Eintrag existiert, wird der ankommende Label durch den abgehenden Label entsprechend des Eintrages in der FIB ersetzt. Anschließend wird der Rahmen über das entsprechende Interface an den nachfolgenden LSR weiter geleitet.

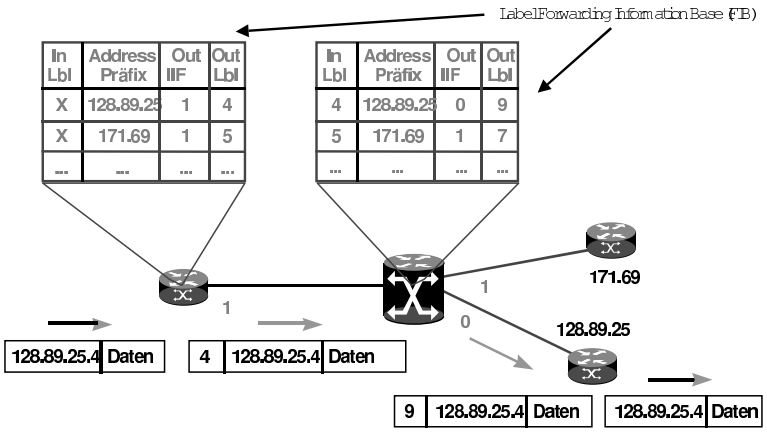


**Abbildung 3:** Weiterbeförderung von MPLS-Rahmen

### 3.2 MPLS und virtuelle private Netze

Der Begriff virtuelles privates Netz (VPN) steht allgemein für ein logisches Netz einer geschlossenen Benutzergruppe, das in einem öffentlichen Netz „virtuell“ realisiert ist. Bezogen auf das IP- und MPLS-Umfeld bedeutet dies, dass ein „öffentliches“ IP/MPLS-Netzwerk genutzt wird, um ein Unternehmensnetz in Form eines privaten Intranets zu realisieren. Die Deutsche Telekom AG kann mit Ihrem IP/MPLS-Netzwerk sowohl den öffentlichen Internet- als auch den VPN-Verkehr abwickeln. Dabei werden die MPLS-Label verwendet, um den „öffentlichen“ Verkehr von dem VPN-Verkehr zu unterscheiden.

Auf dem Markt existieren im wesentlichen zwei Technologien, die MPLS zur Realisierung von VPNs verwenden, u.z. MPLS basierte Layer 3 und Layer 2 Technologien.

#### Layer 3 VPNs

Der RFC 2547bis [5] war einer der ersten Darfts, der die technischen Möglichkeiten von MPLS zur Realisierung von VPNs auf IP-Basis (sog. IP-VPNs) nutzte. Die Technologie wird in der Zwischenzeit von Netzbetreibern – so auch von der Deutschen Telekom AG – auf ihren IP/MPLS-Plattformen eingesetzt.

Zur Realisierung von VPNs innerhalb des IP/MPLS-Netzes sind zwei Label erforderlich. Dieses Verschachteln von MPLS-Label wird als Label Stacking bezeichnet. Die MPLS-Technologie ermöglicht es, beliebig viele Label ineinander zu verschachteln, so dass durch die Einführung von weiteren Label-Hierarchiestufen die Bildung von Sub-VPNs möglich ist.

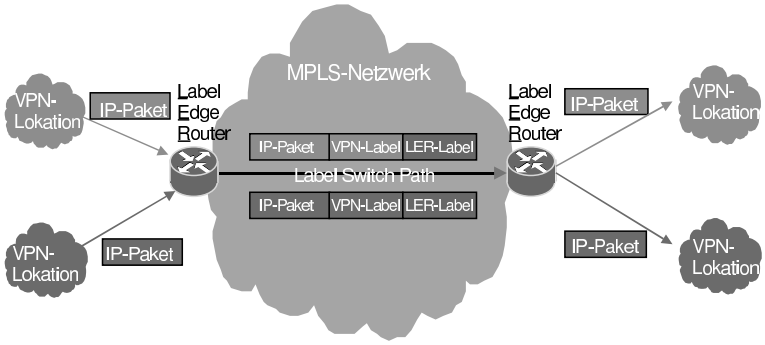


**Abbildung 4:** Nutzung von MPLS Label Stacking bei Layer 3 VPNs

Der äußere Label, der als LER-Label bezeichnet wird, kennzeichnet den LSP zwischen den beteiligten Zugangs-Routern (Label Edge Router, LER). Der innere Label, der als VPN-Label bezeichnet wird, kennzeichnet den Anschlusspunkt der Ziel-VPN-Lokation am Zugangs-Router der Gegenstelle. Der LER-Label kennzeichnet also den Tunnel zwischen den beteiligten Zugangs-Routern, wogegen der VPN-Label genau markiert, zu welchem VPN der gerade übermittelte MPLS-Rahmen gehört.

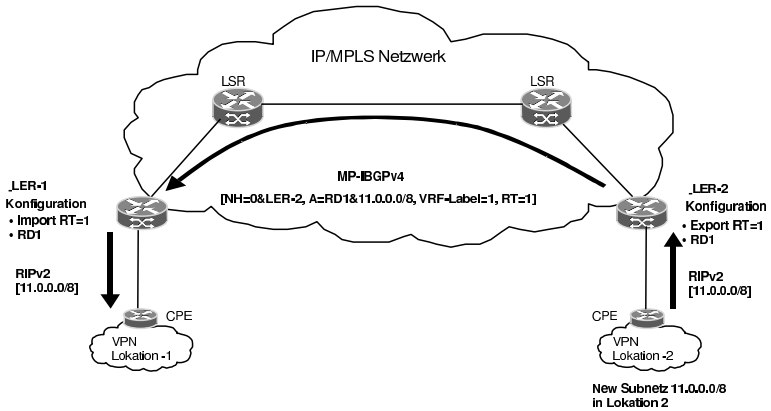


**Abbildung 5:** Nutzung von MP-BGP zur Verteilung von VPN-Routen

Jeder Zugangs-Router verfügt über eine virtuelle Routing- und Forwarding-Funktion (Virtual Routing and Forwarding Function, VRF). Die VRF unterhält für jedes an den Zugangs-Router angeschlossene VPN die entsprechenden Routingtabellen, in der die VPN-IPv4-Routen eingetragen sind. Eine VPN-IPv4-Route besteht aus einem IPv4-Adresspräfix und dem Route Distinguisher (RD). Der Route Distinguisher wird zur Unterscheidung der IPv4-Adresspräfixe benötigt, da identische IPv4-Adressen von unterschiedlichen VPNs genutzt werden können.

Der Austausch der VPN-IPv4-Routen zwischen den LER erfolgt mit Hilfe von Multi Protocol BGP (MP-BGP) [5]. Das Route Traget (RT) gibt an, ob eine Route vom LER importiert werden darf oder nicht. Mit Hilfe des RT sind auch VPN interne Policies realisierbar.

### Inter-Provider MPLS VPNs

Die bislang betrachtete Netzarchitektur beschränkte sich auf das AS eines Netzbetreibers. Im Rahmen der Globalisierung der Märkte wird es notwendig sein, MPLS VPNs auch über Netzbetreibergrenzen hinweg den Kunden anbieten zu können.

Es sind drei Alternativen zur Bildung von Inter-Provider VPNs spezifiziert. (Die internen IGP und LDP Routingprozesse zum Verteilen der LER-Label sind in den folgenden Abbildungen nicht dargestellt.)

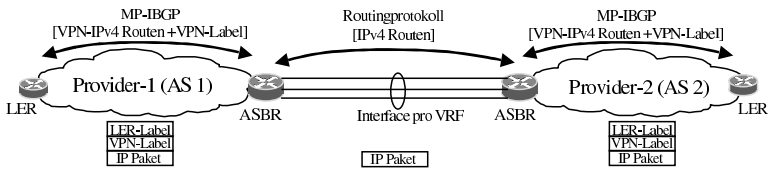


**Abbildung 6:** VRF-VRF Kopplung zwischen Netzen

Bei der ersten Alternative (Abbildung 6) terminieren die Kunden-VPNs an den Netzgrenzen in sog. Autonomous System Border Routern (ASBRs). Die VRF-Tabellen in beiden ASBRs sind über separate Interface miteinander gekoppelt. Zwischen den Tabellen kann ein dynamisches Routingprotokoll zum Einsatz kommen. Es wird kein MPLS zwischen den AS gefahren. Diese Alternative stößt schnell an Skalierungsgrenzen, wenn die Anzahl der im ASBR zu terminierenden VPNs und Kundenrouten zu groß wird.

Die zweite Alternative (Abbildung 7) ist dadurch charakterisiert, dass nur ein Interface für alle VPNs zwischen den ASBRs benötigt wird, gelabelte VPN-IPv4 Routen ausgetauscht werden und MPLS (VPN-Label) zwischen den ASBRs genutzt wird. Nachteil dieser Alternative ist ebenfalls, dass die Speicherkapazität für die VPN-IPv4 Routen die Skalierbarkeit einschränkt.

Die dritte Alternative (siehe Abbildung 8) ist dadurch gekennzeichnet, dass ebenfalls MPLS zwischen den ASBR verwendet wird, die ASBR aber keine VPN-IPv4 Routen

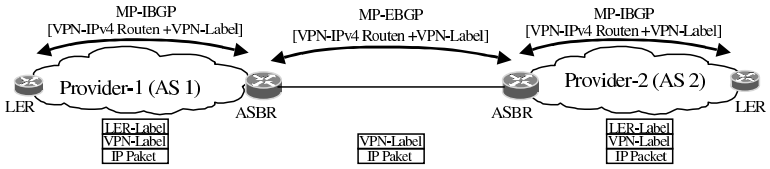


**Abbildung 7:** Verteilung von VPN-IPv4 Routen zwischen Netzen

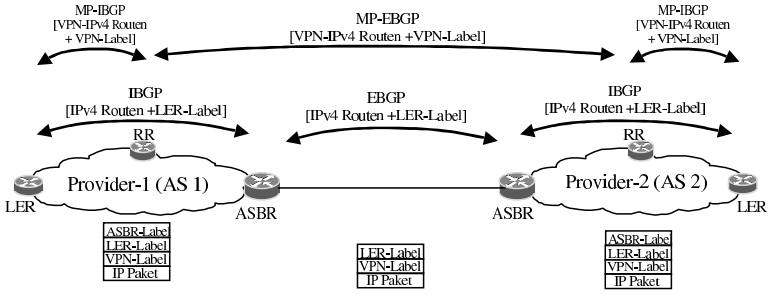


**Abbildung 8:** EBGPv4 und multihop MP-IBGPv4 zwischen Netzen

vorhalten und verteilen müssen. Vielmehr wird ein LSP von einem LER zum anderen aufgebaut. Gelabelte VPN-IPv4 Kundenrouten werden über eine multihop MP-BGPv4 Session zwischen den LERs bzw. zur Verbesserung der Skalierbarkeit zwischen Route Reflektoren (RR) ausgetauscht. Diese Alternative skaliert gegenüber den o.g. am besten.

### Carrier's Carrier

Motivation der Carrier's Carrier Technologie ist es, das IP/MPLS-Netzwerk eines Carriers einem anderen Carrier (VPN-Kunde) als Transportnetz zur Verfügung zu stellen. Die Multiplexfähigkeit von MPLS in Form des MPLS Label Stackings bietet hierfür ideale technische Voraussetzungen. Carrier's Carrier Architekturen werden deshalb auch als hierarchische oder rekursive VPNs bezeichnet.

Darüber hinaus bietet die Carrier's Carrier Technologie zahlreiche Verbesserungen hinsichtlich der Skalierbarkeit gegenüber der bislang betrachteten MPLS VPN Technik.

### Layer 2 VPNs

Ein wesentliches Merkmal von klassischen Layer 2 VPNs ist die Bereitstellung einer transparenten Layer 2 Konnektivität zwischen den Kundenlokationen durch einen Netzbetreiber. Die Kunden können beliebige Layer 3 Protokolle nutzen. Die CPEn fungieren als Router oder Bridges. Häufig werden die CPEn auch selbst vom Kunden gemanaged. Das

Forwarding geschieht anhand von Layer 2 Informationen (z.B. DLCI, MAC). ATM / Frame Relay Netze oder auch Ethernet Leased Lines in Metropolitan Area Networks (MAN) sind klassische Beispiele dafür wie heute Layer 2 VPNs realisiert werden.

Netzbetreiber, die zu einem IP/MPLS-Netz migrieren wollen, benötigen technische Lösungen wie sie weiterhin unterschiedliche Layer 2 Dienste ihren Kunden über ein einziges IP/MPLS-Netz anbieten können. Hierfür bieten MPLS basierte Layer 2 VPNs eine optimale Lösung.

Es können zwei Dienste unterschieden werden, die mit Hilfe von Layer 2 VPNs realisierbar sind

- Virtual Private Wire Service (VPWS)
- Virtual Private LAN Service (VPLS).

Während Virtual Private Wire Services einen Punkt-zu-Punkt Dienst bereitstellen, stellen Virtual Private LAN Services einen Mehrpunkt Dienst auf Basis eines emulierten LANs zur Verfügung.

### Virtual Private Wire Service (VPWS)

Die folgende Abbildung zeigt das VPWS Referenzmodell.

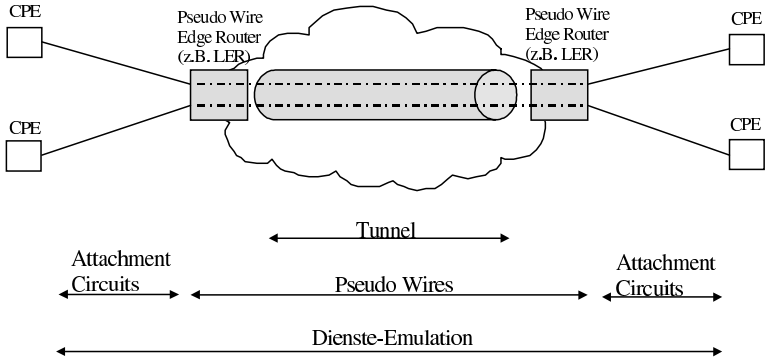


**Abbildung 9:** VPWS Referenzmodell

Die Attachment Circuits (auch Attachment VCs genannt) können Frame Relay DLCIs, ATM VPIs/VCIs, TDM Connections, PPP Connections, Ethernet Ports oder vergleichbare Verbindungen sein. Die Attachment Circuits werden mit Hilfe von Punkt-zu-Punkt Pseudo Wires zwischen den Pseudo Wire Edge Routern (z.B. LERs) über ein Netzwerk verbunden. Ein Pseudo Wire (auch Emulated VC genannt) ist quasi eine Verlängerung und Emulation eines Attachment Circuits über ein IP/MPLS-Netzwerk. Es können mehrere Pseudo Wires innerhalb eines Tunnels transportiert werden. Anzumerken sei, dass neben MPLS als Tunnel und Pseudo Wire Transportmedium zukünftig auch andere Multiplex-Protokolle wie z.B. das Layer 2 Tunneling Protocol (L2TP) über IP-Netzwerke einsetzbar sind.

Für das Forwarding werden zwei MPLS Label verwendet (Abbildung 10).

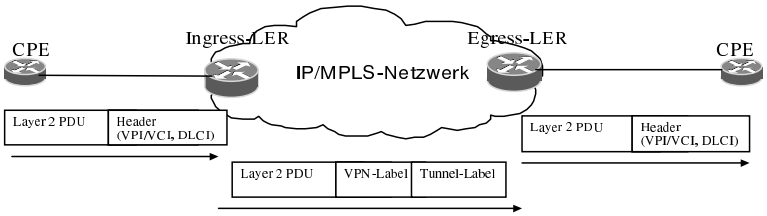


**Abbildung 10:** Transportmechanismus bei VPWSs

Das äußere LER-Label (auch Tunnel-Label genannt) kennzeichnet den LSP vom Ingress-LER zum Egress-LER, während das innere VPN-Label (auch VC-Label genannt) eine Mappinginformation für den jeweiligen Virtual Path Identifier / Virtual Channel Identifier (VPI/VCI) bzw. Data Link Connection Identifier (DLCI) zwischen CPE und LER darstellt. Das VPN-Label repräsentiert den Pseudo Wire. Am Ingress-LER wird einer von der CPE empfangenen Frame Relay Protocol Data Unit (PDU) das DLCI Feld entfernt, in MPLS enkapsuliert und über den Pseudo Wire transportiert. Die Auswertung des VPN-Labels am Egress-LSR gibt im Falle einer ATM AAL5 PDU Aufschluss über das Ausgangsinterface mit dem jeweiligen VPI/VCI und im Frame Relay Fall über den DLCI-Wert.

Die Enkapsulierungsvorschriften von Layer 2 PDUs in MPLS sind in [7] spezifiziert. Für die Enkapsulierung einiger Layer 2 Frames ist ein Steuerungswort notwendig, welches zwischen MPLS Shim Header und dem Layer 2 Frame eingefügt wird (siehe Abbildung 11).

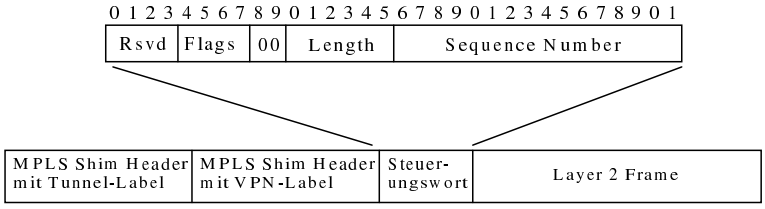


**Abbildung 11:** Steuerungswort

Um einen Mechanismus zur Erkennung der richtigen Paket Sequenzabfolge zu realisieren, wird die Sequenznummer verwendet. Das Flags Feld enthält Layer 2 PDU spezifische Informationen.

Im Fall von Frame Relay entfernt der Ingress-LER den DLCI Header. Das Steuerungswort muss vorhanden sein. Die Nutzung ist jedoch optional. Falls es genutzt wird, enthält es im Flags Feld die BECN (Backward Explicit Congestion Notification), Forward Explicit

Congestion Notification (FECN), Discard Eligible (DE) und Command/Response (C/R) Bits. Das DE Bit kann in eines der Experimental Bits im MPLS Shim Header kopiert werden.

Bei ATM ist sowohl eine Enkapsulierung von AAL5 CPCS PDUs als auch von ATM Zellen vorgesehen. Im Falle von ATM AAL5 CPCS PDUs entfernt der Ingress-LER den AAL5 Trailer, segmentiert die AAL5 PDU in ATM Zellen und fügt das Steuerungswort ein. Die Nutzung des Steuerungswortes ist optional. Falls es genutzt wird enthält es den Transporttyp (hier: AAL5 CPCS PDUs), die Explicit Forward Congestion Indication (EFCI), Cell Loss Priority (CLP) und C/R Bits. Im Fall von ATM Zellen ist das Steuerungswort optional. Es werden ein oder mehrere ATM Zellen in MPLS enkapsuliert. Jede Zelle besteht aus einem 4 Byte ATM Zell Header und 48 Byte ATM Zell Payload. Die EFCI und CLP Bits werden im ATM Zell Header ohne die Header Error Control/Correction (HEC) Information übertragen. Das CLP Bit kann in eines der Experimental Bits im inneren und äußeren MPLS Shim Header kopiert werden. Die Unterstützung von OAM Mechanismen ist optional und sollte gemäß der Spezifikation „Frame Based ATM over SONET/SDH Transport (FAST)“ erfolgen.

Ein wesentliches Merkmal von Layer 2 MPLS VPNs ist der Auto-Discovery Mechanismus. Deshalb ist im Gegensatz zu Layer 3 MPLS VPNs eine strikte Trennung zwischen diesem Mechanismus und dem eigentlichen Kundenrouting zwischen den Lokationen (Austausch von Reachability Informationen) notwendig.

Ein Auto-Discovery Mechanismus dient der Vereinfachung der Konfigurationssprozesse beim Einrichten und Ändern von VPNs, indem die VPNs und VPN-Lokationen automatisch ausfindig gemacht und konfiguriert werden. Die Vorteile eines Auto-Discovery Mechanismuses kommen vor allem in einer any-to-any Topologie zum tragen.

**Virtual Private LAN Service (VPLS)**

VPLS ist ein neuer Service, der es ermöglicht die bisher vorwiegend im Campusbereich vorzufindende VLAN-Architektur gemäß IEEE 802.1Q über ein IP/MPLS-Netzwerk auf geografisch getrennte Lokationen eines Unternehmens auszudehnen. IEEE 802.1Q beschreibt eine Architektur für virtuelle brückengekoppelte LAN. Mit dieser Architektur können innerhalb eines Unternehmens gebäudeübergreifende logische Subnetze aufgebaut werden. Damit ist es möglich, die LANs an die Unternehmensstruktur anzupassen. So können für die einzelnen Unternehmensbereiche separate LANs realisiert werden oder separate campusweite LANs für einen definierten Kreis von Anwendern z.B. mobile PCs oder VoIP-Anwendungen realisiert werden.

VPLS stellt hierzu innerhalb des Provider Edge (PE) eine logische Bridge-Funktion zur Emulation der VLAN-Funktionalität bereit. Alle Kundenlokationen erscheinen im gleichen LAN-Segment unabhängig davon, wo sie sich befinden.

VPLS wird derzeit in der IETF standardisiert. Bei diesem Service handelt es sich um einen reinen Layer 2 Dienst, der unabhängig von den höheren Schichten ist.

Der Anschluss der VLANs an den Provider Edge erfolgt über Attachment Circuits, die auch als Attachment VCs bezeichnet werden. Bei den Attachment VCs kann es sich um

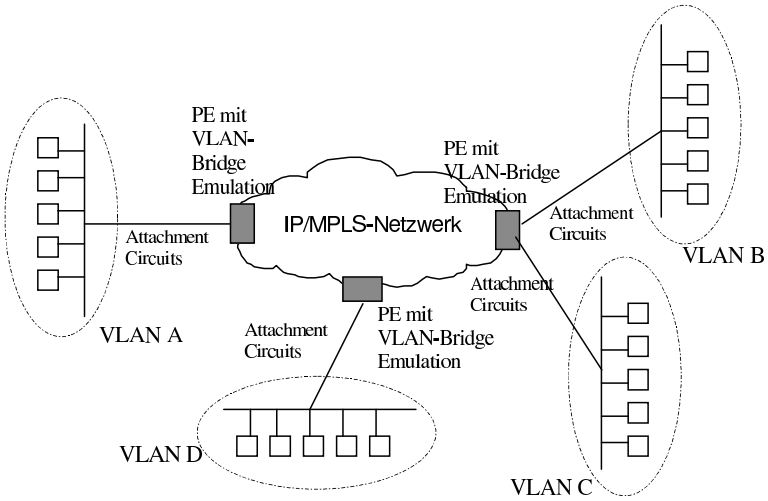


**Abbildung 12:** VPLS Referenz Modell

Frame Relay DLCIs, ATM VPI/VCI, TDM Verbindungen oder PPP Verbindungen handeln.

Im Provider Edge (PE) existiert für jedes VPLS, das von der PE unterstützt wird, eine VPN Forwarding- und Switching-Funktion (VFS). Die VFS ist eine virtuelle VLAN-Bridge, welche die logische Bridge-Funktion für das VPLS bereitstellt.

Zur Vereinfachung der Konfiguration des Overlay_Netzes zwischen den PEn wird beim Einrichten und Ändern von VPLS ein Auto-Discovery Mechanismus verwendet, der die VPLS-Lokationen automatisch ausfindig macht und konfiguriert.

## 4 Qualitätsdifferenzierende Dienste in MPLS gestützten VPNs

In klassischen IP Netzen wir nur eine Dienstklasse verwendet. Diese wird als Best Effort bezeichnet und besagt, dass alle Pakete im Netz mit der selben Priorität behandelt und weitergeleitet werden. Best Effort bedeutet, dass IP eine angemessene Anstrengung unternimmt, jedes Paket unverfälscht an seinem Zielort abzuliefern. Es werden jedoch keine Garantien darüber gegeben, ob das Paket unverfälscht, nicht dupliziert, in der richtigen Reihenfolge oder am richtigen Zielort ankommt. Zusätzlich werden keine Aussagen über die Einhaltung von Delay, Jitter, Paketverlust oder Durchsatz gegeben.

### 4.1 Qualitiy of Service / Class of Service

Im Allgemeinen bedeutet die Definition Quality of Service (QoS), die Möglichkeit, zwischen Verkehrs- oder Diensttypen zu unterscheiden, so dass der Nutzer eine oder mehrere dieser Klassen unterschiedlich zu den anderen behandeln kann. Es ist jedoch so, dass der Begriff QoS und Begriff Class of Service (CoS) in der Literatur unterschieden wird. CoS

bezieht sich auf die Differenzierung von Dienstklassen, so dass man sagen kann, der Begriff bezieht sich auf relative Prioritäten oder Garantien, während der Begriff QoS mehr in Bezug auf absolute Garantien Verwendung findet. Beide Begriffe werden in der Praxis nicht immer scharf getrennt und verschwimmen teilweise miteinander.

Die Unterstützung von multiplen Dienstklassen für spezielle Kundenanwendungen bringt man damit in Verbindung, dass die Behandlung von Paketen, die zu einem Datenstrom gehören anders erfolgt, als die Behandlung von Paketen, die zu einem anderen Datenstrom gehören. Bei der Verwendung unterschiedlicher Dienstklassen werden bestimmte Dienstklassen gegenüber anderen Dienstklassen entsprechend priorisiert oder benachteiligt.

Differenzierte Dienststufen werden durch das Manipulieren von Attributen bestimmter Verkehrsströme erzeugt. Dies führt dazu, dass die Wahrnehmung des Kunden über eine bestimmte Qualitätsstufe des Netzes verändert werden kann. Diese Attribute sind:

- Durchsatz, d.h. die Datenmenge, die in einem bestimmten Zeitraum übertragen werden kann
- Verzögerung (Delay), d.h. die Zeit, welche die Daten benötigen, um von einem Punkt zu einem anderem Punkt im Netz übertragen zu werden
- Jitter, d.h. die Variation des Delays über der Zeit für aufeinanderfolgende Pakete eines Datenflusses
- Paketverlust, d.h. der Prozentsatz an übertragenen Paketen, welche nicht korrekt ihr Ziel erreichen

Die Dienstqualität für eine spezielle Klasse kann nur so gut sein, wie die niedrigste Dienstqualität der schwächsten Verbindung auf dem Ende-zu-Ende Pfad. Das Konzept von multiplen Dienstklassen ist nicht auf klassische TDM Verbindungen anwendbar, da hier, falls die Verbindung hochgefahren ist, Bandbreite, Delay und Jitter konstant sind und keine Paketverluste auftreten [8]. Die Möglichkeit multiple Dienstklassen anzubieten ergibt sich für IP Netze, die auf statistischem Multiplexen beruhen. Die Quality of Service, die der Nutzer wahrnimmt ist eine Funktion, der Umsetzung des statistische Multiplexen an jedem *Hop* (Sprung) und der Leitungscharakteristik der individuellen Verbindungen entlang des Pfades. Durch unterschiedliche Behandlung bestimmter Pakete beim statistischen Multiplexen, können die Router im Netz unterschiedlichen Durchsatz, Verzögerungszeit, Jitter oder Paketverlust für unterschiedliche Paketflüsse erzeugen.

### 4.2 Komponenten von QoS in IP Netzen

Damit Differentiated Services realisiert werden kann, benötigt man eine Reihe von Komponenten. Die Pakete müssen am Eingang des Router klassifiziert werden, d.h. die Pakete werden einer bestimmten Klasse zugeordnet. Nachdem der Ausgangsport bzw. das Ausgangsinterface durch den Router ermittelt wurde, werden die Pakete dort einzelnen Queues zugeordnet. In der Regel assoziiert man eine Klasse oder einer Klassentyp mit einer dieser Queues. Die Verwendung mehrere Queues ist ein wichtiger Unterschied zur Verwendung von nur einer Queue beim klassischen Best Effort Dienst. Ein anschließend folgender Scheduler, liest die Pakete entsprechend der Bandbreite, die einer Queue zugewiesen wurde, aus. Das führt dazu, dass einzelnen Klassen mehr oder weniger Bandbreite zugewiesen werden kann. Ebenso kann die Puffergröße und das RED individuell pro

Queue konfiguriert werden, so dass diese Parameter Einfluss auf Delay, Jitter, Paketverlust bzw. Durchsatz haben. Abbildung 13 zeigt eine mögliche Queue Anordnung an einem Ausgangsport.

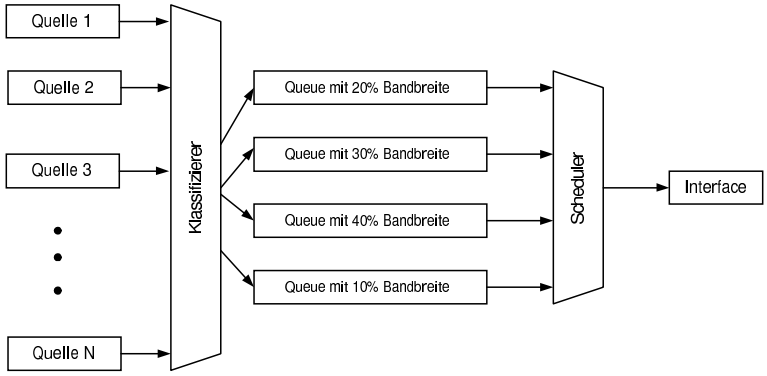


**Abbildung 13:** Queuing und Scheduling

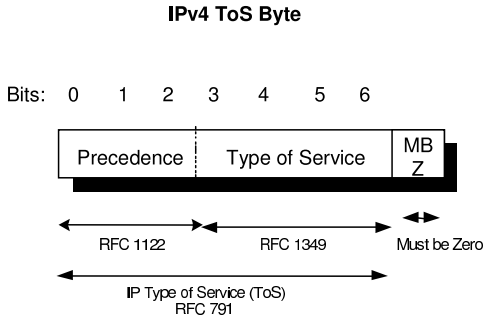


**Abbildung 14:** ToS Feld im IP Header

Die Klassifizierungsinformation ist im IP Header aufgeführt. Der ursprüngliche Ansatz hierzu ist in Abbildung 14 dargestellt. Dabei wurden die ersten drei Bits des ToS Bytes als Precedence Bits definiert. Weiterentwicklungen bzw. Neudefinitionen der IETF haben zu der Definition der DiffServ Codepoints (DSCP) geführt, wie sie in Abbildung 15 dargestellt wird. Das DSCP Schema kann sowohl bei IPv4 als auch IPv6 eingesetzt werden und wird von vielen Routern auch für IPv4 unterstützt.

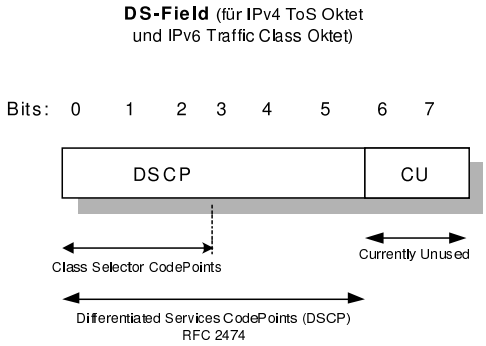


**Abbildung 15:** DiffServ Codepoints im IP Header [23]

### IETF Architektur von Differentiated Services

Die IETF hat sogenannte Per Hop Behaviors definiert. Ein Per Hop Behavior ist eine Beschreibung des nach außen sichtbaren Sendeverhaltens, welches auf ein einzelnes Behavior Aggregate angewendet wird. Der Knoten kann dadurch Ressourcen unterschiedlichen Behavior Aggregates zuweisen. Es ist wichtig festzuhalten, dass DiffServ nicht auf einen individuellen Verkehrsfluss im speziellen angewendet wird, sondern auf dessen Aggregat, also auf den Gesamtfluss einer Verkehrsklasse bzw. eines Verkehrstyps [9]. Dies ist einer der Gründe warum DiffServ sich gegenüber anderen QoS Ansätzen in der IP Welt durchgesetzt hat, da DiffServ dadurch besser skaliert.

Die IETF hat zwei PHB definiert. Das eine PHB ist das Expedited Forwarding (EF), das für Ende-zu-Ende Dienste mit der Anforderung an geringen „Delay, Jitter und gesicherte Bandbreite“ entwickelt wurde. Der empfohlene DSCP für EF ist 101110.

Das Assured Forwarding (AF) PHB, ist eine Gruppe von PHBs, die definiert wurden, um sicherzustellen, dass Pakete mit hoher Wahrscheinlichkeit zugestellt werden, solange der aggregierte Verkehr in einer Klasse nicht die ‚abonnierte‘ Informationsrate übersteigt.

| ***Drop Precedence*** | ***Klasse* 1** | ***Klasse* 2** | ***Klasse* 3** | ***Klasse* 4** |
|---|---|---|---|---|
| **1 (Wenig)** | 001010 | 010010 | 011010 | 100010 |
| **2 (Mittel)** | 001100 | 010100 | 011100 | 100100 |
| **3 (Hoch)** | 001110 | 010110 | 011110 | 100110 |

**Tabelle 1:** : MPLS-Rahmen

RFC 1812 spezifiziert ein default PHB, welche das gewöhnliche Best Effort Sendeverhalten widerspiegelt. Der empfohlene DSCP ist 000000.

### 4.3 Qualitätsdifferenzierende Dienste in MPLS gestützten IP Netzen

Bei MPLS gestützten Netzen wird ein Label vor den IP Header gesetzt. In diesem Label gibt es drei Bits, die sogenannten Experimental Bits (EXP Bits). Diese können für die Realisierung von Differentiated Services verwendet werden. Es bietet sich an, die Precedence Bits aus dem IP Header in diese EXP Bits zu kopieren. Dadurch ist es möglich, bis zu 8 Klassen oder Typen von Klassen in MPLS basierten IP Netzen darzustellen.

### 4.4 CoS aware Layer 3 VPNs

Da bei einem Layer 3 VPN jede Lokation eines VPNs mit einer anderen Loaktion des selben VPN kommunizieren kann, ist es möglich, dass es an gewissen Stellen zu Leistungsengpässen kommt. Das *Hose* Modell beschreibt anschaulich, wie die VPN Lokationen untereinander in Beziehung stehen. Abbildung 15 stellt das *Hose* Modell mit seinen möglichen Performanz Engpässen dar. Im *Hose* Modell sind die Zugangsleitungen dedizierte Leased Lines, d.h. diese Leitungen stehen ausschließlich einem Kunden VPN zur Verfügung. Am Edge des MPLS Netzes sind unter Umständen mehrere dieser Kundenanschlussleitungen angeschaltet. Der Verkehr aus diesen wird in Label Switched Pathes (LSPs) aggregiert und an den Zielort übertragen. Am Ziel LER wird der VPN Verkehr wieder getrennt und über die dedizierten Kundenanschlussleitungen zum Kunden übertragen. Auf der Anschlussleitung zu einer einzelnen VPN Lokation kann es zu Performanzengpässen kommen, falls Verkehr aus verschiedenen Lokationen zu gewissen Zeiten gleichzeitig die Ziellokation erreichen muss. Wenn dies der Fall ist, greifen die qualitätsdifferenzierenden Mechanismen für die unterschiedlichen Dienstklassen eines VPNs.

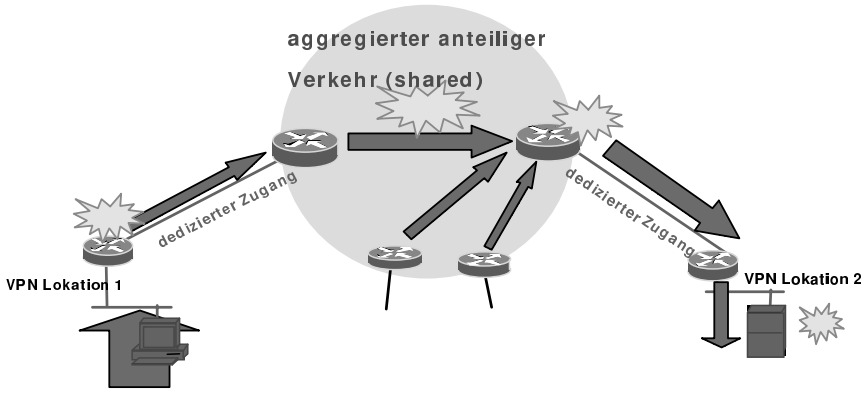


**Abbildung 16:** Mögliche Performanz Engpässe des Hose Modells

Es ist wichtig festzuhalten, das DiffServ keine freie Bandbreite erzeugt. Es ist vielmehr so, dass einzelne Dienste erzeugt werden können, die sich in Bezug auf ihre Eigenschaften unterscheiden. In gut entwickelten IP Netzen werden die Pufferspeicher in den Routern die meiste Zeit nicht gefüllt sein. Es ist aber nicht möglich dies immer sicherzustellen, so

dass DiffServ ein Ansatz ist, bestimmten Verkehr vor anderem Verkehr zu bearbeiten und Congestion in einer Queue bzw. Dienstklasse von den anderen Dienstklassen zu isolieren.

## 5 IP VPN Performanz-Nachweise

Der Nachweis der Qualität einer Nachrichtenübertragung erfordert Messtechnik und eine Datenaufbereitung. Beides bedeutet zusätzlichen Aufwand, der sich in Kosten niederschlägt. Mit der Einführung Qualitäts-differenzierender IP Dienste werden Performanz-Nachweise notwendig. Mit Recht fordert der Kunde den Performanz-Beweis eines Dienstes besserer Qualität, wenn über den selben Anschluss gleichzeitig Information ohne jegliche Qualitäts-Verpflichtung übertragen wird.

### 5.1 Messverfahren

Die Qualität eines IP Netzes kann nur schlecht mit Router-basierten Messungen charakterisiert werden. Zwei Router-externe Methoden ermöglichen eine Ende zu Ende IP Performanz-Messung (siehe Abbildung 16):

- Bei der „aktiven“ Messung werden spezielle Messpakete von einem Ursprungs-Referenz System zu einem Ziel-Referenz System gesendet. Ursprungs- und Ziel-System sind an die jeweiligen Router angebunden, zwischen denen die erzielbare IP Performanz gemessen wird. Mit dieser Methode lassen sich Parameter wie Laufzeit, IPDV und Verlust der speziellen Messpakete erfassen.
- Bei der „passiven“ Messung wird der Verkehr des Ursprungs-Routers auf der Anschlussleitung mit einem Monitor erfasst. Ein gleicher Monitor befindet sich an dem Ziel-Router und erfasst den ankommenden Verkehr.

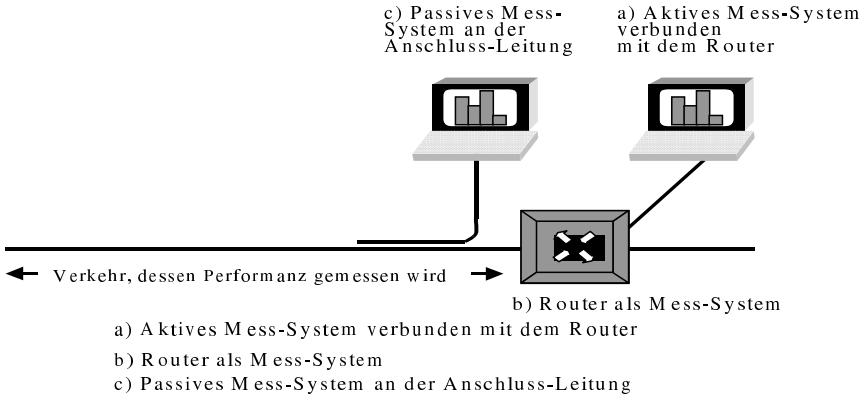


**Abbildung 17:** Architekturen für IPPM Performanz-Messungen

Grundlage aller Messtechnik ist die Forderung, durch die Messung die gemessene Grösse nur minimal zu beeinflussen. Eine aktive Messung ist ganz offensichtlich auf IP Ebene

intrusiv. Je mehr Messpakete eingefügt werden, desto genauer lässt sich die erzielbare Ende zu Ende IP Performanz beschreiben. Und desto weniger Platz bleibt für tatsächlichen Nutzverkehr.

Passive Messungen sind nur auf IP Ebene nicht intrusiv. Mit dem Ziel, zusätzliche Systeme im direkten Pfad der Nutzlast zu vermeiden, werden oft passive Weichen oder Koppler eingesetzt.

Bei passiven Messungen kommt ein wichtiges nicht-technisches Argument zum Tragen: der Datenschutz. Die Kopie eines IP Pakets kann zu mehr genutzt werden als dem Nachweis von Netz-Qualität.

### 5.2 Gestaltung des Global Intranet MPLS Performanz Monitors der Telekom

Im Zuge eines Pilot Versuchs hat die Deutsche Telekom zwei aktive Mess-Systeme miteinander verglichen. PERFAS+ ist eine GPS getaktete Eigenentwicklung der T-Systems Nova. Das zweite System ist Router-basiert. Es ist NTP synchronisiert. Die Zeittakte sind also unterschiedlich genau. PERFAS+ Zeitstempel sind unpräzise erst unter $100\mu$s. NTP Zeitstempel können einen Fehler bis zu 6 ms haben [10]. Das Router-basierte Mess-System ist auch in der zeitlichen Auflösung der Zeitstempel begrenzt: sie beträgt eine Millisekunde.

Vor dem Pilotversuch muss die gewünschte Art der Ergebnis-Ausgabe festgelegt werden. Aus wissenschaftlicher Sicht optimal wären einzelne Messwerte. Doch schon bei 10 Pilot-Standorten ergeben sich wegen der vier IP Verkehrsklassen des Telekom Netzes 360 Verkehrsbeziehungen. Wenn jede Minute ein Paket gesendet wird, ergeben sich am Tag 518.400 Messwerte. Reduziert man die weitergegebene Information auf einen Mittelwert, der alle 15 Minuten berechnet wird, ergeben sich 34.560 Datenpunkte zum Nachweis der an einem Tag erzielten Netz-Performanz. Ein einfacher Kompromiss aus Genauigkeit und Begrenzung der Nachverarbeitungslast ist erreicht.

Gemessen werden Laufzeit, Laufzeit-Schwankungen (Jitter) und Verluste. Geht von 15 Paketen eines verloren, entspricht dies im 15 Minuten-Intervall einer Verlustrate von etwa 7%. Generell gilt, dass je niedriger die anvisierten Fehlerraten sind umso problematischer die Betrachtung kurzer Mess-Intervalle bei Aussagen zu Fehlerraten. Eine statistisch zuverlässige Aussage erfordert ein Mehrfaches des Kehrwerts der Fehlerrate als Grundgesamtheit der Messungen. Bei der gewählten aktiven Messung erfordert eine Aussage zu einer Fehlerrate ein langes Mess-Intervall. Die Alternative, eine hohe Anzahl von Messpaketen in einem kurzen Intervall zu senden, ist wenig sinnvoll. Die Messpakete sollen nicht selbst die Last darstellen, die zu Verlusten führt. Damit sind Real-Zeit Messungen der Verlustrate nur möglich, indem eine Verlustrate auf der Basis bereits länger zurückliegender Messungen kontinuierlich neu berechnet wird.

Die Erfassung von Laufzeit und Jitter scheint einfacher. Aber auch hier hat ein begrenzter Umfang an Messwerten seinen Einfluss. Unter der Annahme, für einen abgegrenzten Zeitraum einen bestimmte Performanz erreichen zu wollen, können einzelne Extremwerte eine Aussage verfälschen. Deshalb macht auch [11] den Vorschlag, einen Schwellwert zu definieren, ab dem ein Paket mit einer hohen Laufzeit als Verlust gewertet wird. Die genaue Definition eines Schwellwerts für eine zu hohe Laufzeit ist Service- und Betreiber-individuell.

Der Laufzeit-Schwellwert ist nicht nur relevant für Pakete, die lange unterwegs sind. Jedes Mess-System benötigt eine interne Überprüfung auf die Korrektheit seiner Zeitstempel. Neben den ohnehin auftretenden Abweichungen bei der Synchronisation entfernter System-Zeiten, dürfen keine weiteren Fehler auftreten. Zu schnell wird der Mittelwert einer kompletten Stichprobe von Mess-Werten verfälscht.

Pakete, die von später gesendeten Paketen überholt werden, werden solange sie innerhalb des Zeitlimits ankommen, als korrekt empfangen gezählt. Eine spezielle Re-Ordering Metrik ist bei der IETF IPPM Arbeitsgruppe in Diskussion.

Der Pilotversuch der Telekom zeigt, dass das in den Router integrierte Mess-System wegen seiner NTP Synchronisation kombiniert mit einer Auflösung im Bereich von +/- 1 ms Probleme hat, bei niedriger Last die aktivierte Qualitäts-Differenzierung nachzuweisen. Die verschiedenen Verkehrsklassen werden auch unterschiedlich tarifiert. Der Untergang der Qualitäts-Differenzierung im „Zeitstempel-Rauschen“ des Messgeräts ist dem Kunden nicht notwendigerweise vermittelbar.

Ein weiteres Problem bei dem Router-basierten System sind gelegentliche Ausfälle von Messwerten. Eine Ausgabe von 0,0 ms als mittlere Laufzeit von 50 Mess-Paketen deutet auf Abwesenheit von Ergebnissen hin. Dieses Ergebnis tritt in einer geringen, aber sichtbaren Anzahl von Fällen auf. Bei Jitter und Verlusten stellt die Ausgabe 0,0 ein sinnvolles Ergebnis dar. Die seltenen Fälle fehlender Daten müsste von den Laufzeit-Messungen hergelitten werden. Eine Korrelation von Messungen macht ohnehin Sinn. Trotzdem ist diese notwendige Korrektur etwas unschön.

Daraus zu schließen, dass Router-basierte Mess-System sei völlig unbrauchbar, ist unzulässig. Es hat den Vorteil, leicht vor Ort installierbar zu sein und kann bei der Fehlerbehebung eingesetzt werden. Für den Nachweis einer Qualitäts-Differenzierung eignet sich ein GPS synchronisiertes Mess-Systems besser. Die Deutsche Telekom weist die Qualitäts-Differenzierung in ihrem Netz deshalb mit einem aktiven GPS synchronisierten Mess-System nach.

## Literatur

[1] Kent, S.et al „Security Architecture for the Internet Protocol“ RFC 2401
[2] D. Harkins et al „The Internet Key Exchange“ RFC 2409
[3] draft-ietf-ppvpn-ppv-vr-02.txt „Network based VPN Architecture using virtual Router“
[4] B. Gleeson, RFC 2764 „A Framework for IP Based Virtual Private Networks“
[5] Rosen, C. et al „BGP/MPLS VPNs“ draft-ietf-ppvpn-rfc2547bis-01.txt
[6] Anderson, P.et al „LDP Specification“ RFC 3036
[7] Martini, L. et al „Encapsulation Methods for Transport of Layer 2 Frames Over IP and MPLS Networks“ draft-martini-l2circuit-encap-mpls-04.txt
[8] Semeria, C., et al., Supporting Differentiated Services in Large IP Networks, White Paper Juniper Networks, Dezember 2001
[9] Blake S., et al., An Architecture for Differentiated Services, RFC 2475
[10] Pásztor, A., Veitch, D.: “A Precision Infrastructure for Active Probing“. Proceedings PAM 2001 (2001), S.33-44.
[11] Almes, G., Kalidindi, S. et al.: “A One-way Delay Metric for IPPM“ RFC. 2679 IETF (1999).

# A Abkürzungsverzeichnis

| | |
|---|---|
| AAL | ATM-Adaptation-Layer (ATM-Anpassungsschicht) |
| AF | Assured Forwarding |
| AH | Authentication Header |
| AS | Autonomous System |
| ASBR | Autonomous System Border Router |
| ATM | Asynchronous Transfer Mode |
| BECN | Backward Explicit Congestion Notification |
| BGP | Border Gateway Protocol |
| CA | Certificate Authority |
| CE | Customer Edge |
| CLP | Cell Loss Priority |
| CoS | Class of Service |
| CPCS | Common Part Convergence Sublayer |
| CPE | Customer Premise Equipment |
| DE | Discard Eligible |
| DH | Diffie-Hellman |
| DiffServ | Differentiated Services |
| DLCI | Data Link Connection Identifier |
| DSCP | DiffServ Code Point |
| EF | Expedited Forwarding |
| EFCI | Explicit Forward Congestion Indication |
| FAST | Frame Based ATM over SONET/SDH Transport |
| FEC | Forwarding Equivalence Class |
| FECN | Forward Explicit Congestion Notification |
| FIB | Forward Information Base |
| FR | Frame Relay |
| GPS | Global Positioning System |
| HEC | Header Error Control/Correction |
| HMAC | Hashed Message Authentication Code |
| IBGP | Interior BGP |
| IEEE | The Institute of Electrical and Electronic Engineers |
| IETF | Internet Engineering Task Force |
| IGP | Interior Gateway Protocol |
| IKE | Internet Key Exchange |
| IP | Internet Protocol |
| IPDV | Instantaneous Packet Delay Variation |
| IPPM | IP Performance Metrics |
| IPv4 | Internet Protocol Version 4 |
| IPX | Internetworking Public Exchange Protocol |

| | |
|---|---|
| ISAKMP | Internet Security Association and Key Management Protocol |
| ISP | Internet Service Provider |
| L2TP | Layer 2 Tunnelling Protocol |
| LAN | Local Area Network |
| LDP | Label Distribution Protocol |
| LER | Label Edge Router |
| LSP | Label Switched Path |
| LSR | Label Switch Router |
| MAC | Media Access Control |
| MAN | Metropolitan Area Network |
| MP-BGP | Multi Protocol BGP |
| MPLS | Multi Protocol Label Switching |
| MTU | Maximum Transfer Unit |
| NTP | Network Time Protocol |
| OAM | Operation and Maintenance |
| OSPF | Open Shortest Path First |
| PDU | Protocol Data Unit |
| PE | Provider Edge |
| PFS | Perfect Forward Secrecy |
| PHB | Per Hop Behaviour |
| PKI | Public Key Infrastructure |
| PPP | Point to Point Protocol |
| QoS | Quality of Service |
| RA | Registration Authority |
| RD | Route Distinguisher |
| RFC | Request for Comments |
| RIP | Routing Information Protocol |
| RR | Route Refelctor |
| RSVP | Resource Reservation Protocol |
| RT | Route Target |
| RTT | Round Trip Time |
| TCP | Transmission Control Protocol |
| TDM | Time Division Multiplex |
| TTL | Time to Live |
| VC | Virtual Channel |
| VCI | Virtual Channel Identifier |
| VFS | VPN Forwarding and Switching |
| VFS | VPM Forwarding and Switching |
| VLAN | Virtual LAN |
| VoIP | Voice over IP |

| | |
|---|---|
| VPI | Virtual Path Identifier |
| VPLS | Virtual Private LAN Service |
| VPN | Virtual Private Network |
| VPN-ID | VPN-Identifier |
| VPWS | Virtual Private Wire Service |
| VR | Virtual Router |
| VRF | VPN Routing and Forwarding |
| WAN | Wide Area Network |