Zeitschrift: Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

Herausgeber: Swisscom

Band: 80 (2002)

Heft: 5

Artikel: Kundenanforderungen bedingen unterschiedlicher Lösungen

Autor: Kirchberger, Wolfgang

DOI: https://doi.org/10.5169/seals-877199

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Siehe Rechtliche Hinweise.

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. Voir Informations légales.

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. See Legal notice.

Download PDF: 26.04.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

MPLS-basierte VPN-Lösungen

Kundenanforderungen bedingen unterschiedliche Lösungen

Internet-Serviceprovider müssen heute in der Lage sein, den Kunden differenzierte VPN-Services anzubieten. Jeder Kunde hat unterschiedliche Sicherheits- und Routinganforderungen, Verkehrsmuster und -volumen, Applikationen, Outsourcingkriterien, ein unterschiedliches IT-Know-how sowie eine verschiedene Anzahl von Lokationen und Benutzern. Die Hersteller von Netzwerkequipments versuchen diesen heterogenen Kundenanforderungen mit verschiedenen VPN-Modellen gerecht zu werden. Von den vielen möglichen VPN-Lösungen wird in diesem Artikel auf die Klasse der Provider Provisioned VPNs (PP-VPNs) eingegangen.

Provider Provisioned VPNs werden ausschliesslich im Netzwerk des Providers konfiguriert und verwaltet. Die Systeme des Kunden sind in die Konstruktion des VPN nicht miteinbezogen. Für die Kunden stellt sich das VPN als Netzwerk mit bestimmten definierten Eigenschaften dar.

WOLFGANG KIRCHBERGER

Festverbindungen, Frame-Relay und ATM-Services können als erste Generation von Provider Provisioned VPNs (PP-VPNs) auf Layer-2-Basis interpretiert werden. Moderne Ansätze basieren auf den MPLS/IP-Infrastrukturen von IP-Serviceprovidern und definieren Verfahren und Modelle zur Bildung von PP-VPNs unter Benutzung der Technologien IP und MPLS.
Dieser Beitrag diskutiert zwei derzeit stark beachtete Entwicklungen in diesem Bereich:
- Layer-3-VPNs nach RFC 2547bis basierend auf BGP4 und MPLS
- MPLS-basierende Layer-2-VPNs

Es werden Motivation sowie Vor- und Nachteile der verschiedenen Ansätze beleuchtet und die technische Funktionalität erläutert. Gute Kenntnisse über MPLS, IP und IP-Routing sind Voraussetzung für das Verständnis des Beitrags.

VPN-Modell nach RFC 2547bis

Das VPN-Modell nach RFC 2547bis (draft-ietf-ppvpn-rfc2547bis-00) beschreibt einen Mechanismus, der es einem Serviceprovider erlaubt, seinen Kunden VPN-Services im Sinne eines privaten IP-Netzes (Intranet, Extranet) über den eigenen IP/MPLS-Backbone zu liefern.
Die primären Ziele dieses VPN-Modells sind:
- Realisierung eines VPN-Services, der es ermöglicht, viele Kunden mit überlappenden Adressräumen und/oder privaten Adressen gleichzeitig zu bedienen.
- Übernahme des IP-WAN-Routings für den Kunden und dadurch Realisierung eines VPN-Services, der auch von Kunden ohne grosse Erfahrung im IP-Routing genutzt werden kann (WAN-Backbone-Outsourcing).
- Definition eines vom Link Layer (Layer 2) unabhängigen IP-VPN-Services, das heisst, die Lokationen des Kunden können über unterschiedliche Layer-2-Technologien angeschlossen sein.

Modellbausteine

Im Kontext von RFC 2547bis ist ein VPN eine Sammlung von Policies, welche die möglichen Verbindungen zwischen einer Gruppe von Kundenlokationen beschreiben. Eine Kundenlokation ist über ein oder mehrere Provider Edge Router an das Netzwerk des Serviceproviders angeschlossen.

Bild 1 zeigt die fundamentalen Bauteile eines BGP/MPLS VPN nach RFC 2547bis.

Customer-Edge-Systeme (CE-System)
Das CE-System ermöglicht dem Kunden, über eine Data Link Layer Verbindung (Ethernet, Frame Relay, ATM usw.), einen Zugang zum PE-Router im Netzwerk des Serviceproviders. Das CE-System ist typischerweise ein Router; möglich sind aber auch Layer-2-Switches oder Endgeräte. Das CE-System wird im Regelfall vom Kunden selbst verwaltet.

Provider Edge Router (PE-Router)
Der PE-Router terminiert die Link-Layer-Verbindungen zu den angeschlossenen CE-Systemen der Kunden. Dem PE-Router obliegt die Aufgabe, mehrere Forwarding-Tabellen getrennt zu verwalten, um die Separierung der Routinginformationen per VPN zu ermöglichen. Darüberhinaus ist er für die Verteilung der VPN-Informationen im Providernetzwerk und für das Setup der MPLS-Datenwege verantwortlich. Die Verwaltung des PE-Routers obliegt ausschliesslich dem Provider.

Provider Router (P-Router)
Ein P-Router ist jeder Router im Providernetzwerk, der nicht direkt mit CE-Systemen verbunden ist. P-Router fungieren als MPLS Transit Label Switch Router, wenn sie VPN-Daten zwischen PE-Routern transportieren. Für P-Router ist der VPN-Service nach RFC 2547bis eine transparente MPLS-Applikation – sie benötigen keine spezielle VPN-Konfiguration.

Funktionsweise des Modells

Das VPN-Modell nach RFC 2547bis trennt strikt nach Controlplane und Forwardingplane.
Auf der Controlplane werden VPN-Routinginformationen zwischen PE-Routern

sowie zwischen CE- und PE-Routern ausgetauscht und die entsprechenden Label Switch Paths (LSPs) für den Datentransport über MPLS eingerichtet.
Auf der Forwardingplane wird MPLS als protokollunabhängiger Mechanismus für den Transport der Daten zwischen den VPN-Lokationen eingesetzt.

Adressierung
Wenn Kunden beispielsweise private IP-Adressen aus dem nach RFC 1918 definierten Adressraum benutzen, können Überlappungen von Adressräumen zwischen Kundennetzen auftreten. Routingprotokolle setzen die Eindeutigkeit von IPv4-Adressen voraus. Es muss daher ein Verfahren definiert werden, das es gestattet, die Adressen eindeutig zu gestalten.
Da BGP4 als Protokoll für die Übertragung der Adressinformationen eingesetzt wird, muss also explizit für BGP4 ein Mechanismus definiert werden, der es dem Protokoll erlaubt, gleiche IPv4-Adressen aus unterschiedlichen VPNs zu unterscheiden.
Dieses Problem wird durch die Definition der VPN-IPv4-Adressfamilie gelöst.
Eine VPN-IPv4-Adresse umfasst 12 Bytes, bestehend aus einem 8 Byte Route Distinguisher (RD) und dem 4 Byte IPv4 Adress-Prefix. Bild 2 zeigt die Struktur einer VPN-IPv4-Adresse.
Der RD wird vom Serviceprovider festgelegt. RFC 2547bis fordert explizit, dass der RD global eindeutig gewählt wird, sodass eine Unterscheidung auch über Providergrenzen hinweg möglich ist. Für die Wahl des RD wird eine der folgende Optionen durch das Type Field selektiert:

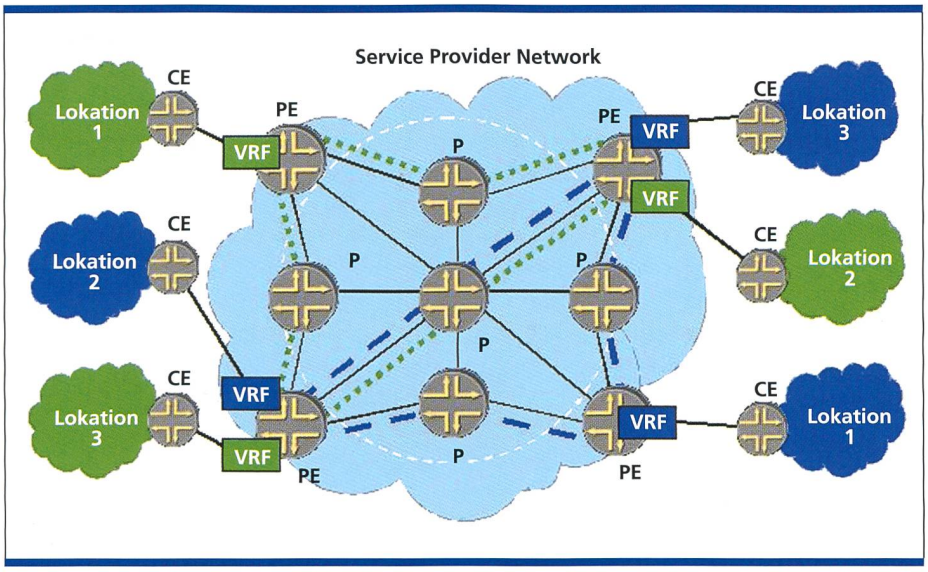


Bild 1. Fundamentale Bauteile eines BGP/MPLS-VPN nach RFC 2547bis (CE: Customer Edge, P: Provider Router, PE: Provider Edge).

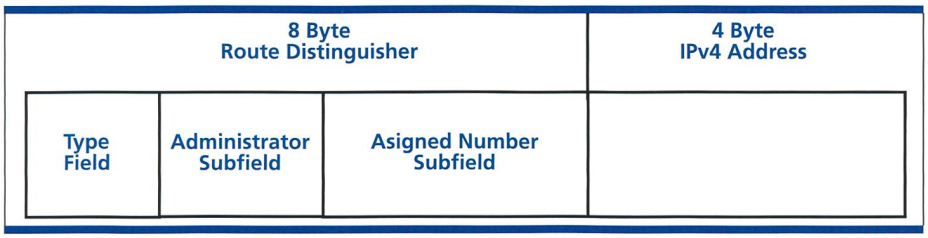


Bild 2. VPN-IPv4-Adressfelder.

- Die global eindeutige Autonomous System Number (ASN) des Providers (Administrator Subfield) mit einer ergänzenden Ziffer zur Unterscheidung der einzelnen VPNs bzw. VRF (Assigned Number Subfield).
- Eine IPv4-Adresse aus dem global eindeutigen Adressraum des Serviceproviders (Administrator Subfield) in Verbindung mit einer ergänzenden Ziffer zur Unterscheidung der einzelnen VPNs bzw. VRFs (Assigned Number Subfield).

VPN-IPv4-Adressen sind für die Kundennetze unsichtbar, sie werden nur auf der Controlplane im Providernetzwerk eingesetzt.
Für die Unterstützung der VPN-IPv4-Adressen wird BGP4 mit Erweiterungen für Multiprotokollunterstützung – MP-BGP extensions – benötigt. PE-Router müssen daher MP-BGP extensions verstehen.

Austausch von Routing-Informationen

CE-PE
Für den Austausch von IPv4-Routinginformationen zwischen PE- und CE-Routern wird dynamisches (OSPF, BGP4/EBGP, RIP) oder statisches Routing eingesetzt. Der CE-Router sendet die Routes der Adressprefixes der eigenen Lokation an den PE-Router und lernt vom PE-Router die Routen zu den Adressprefixes der Remote-VPN-Lokationen.
Für den CE-Router stellt sich die Routingsituation sehr einfach dar; er sieht nur einen Neighbour-Router, den PE-Router, mit dem er über ein festgelegtes Routingprotokoll oder statisch kommuniziert.
Am PE-Router ist jedes Interface oder Subinterface einem Kundennetzwerk (z. B. Frame Relay DLCI, ATM PVC, VLAN) einer bestimmten «virtual routing and forwarding table» (VRF) zugeordnet.

PE-PE
Die lokal gelernten VPN-Routinginformationen (VPN-IPv4) tauschen die PE-Router untereinander mittels IBGP aus. Der Serviceprovider muss zwischen den PE-Routern entweder eine IBGP-Vollvermaschung implementieren, oder BGP-Route-Reflektoren zur Skalierung einsetzen.
Als Routinginformation sendet der PE-Router mit dem Adressprefix eines Kundennetzes die BGP-Next-Hop-Adresse (seine eigene Loopback-Adresse) und ein zugeordnetes MPLS-Label.
RFC 2547bis kontrolliert die Verteilung von VPN-Routinginformationen zwischen PE-Routern durch den Einsatz von Filterung auf Basis von BGP Extended Community Attributes. Durch die Zuordnung von BGP-Community-Attributen zu VPN-IPv4 Adressprefixes erhält der Serviceprovider ein äusserst mächtiges und flexibles Werkzeug, um die Verteilung von VPN-Routinginformationen zu gestalten. Die PE-Router entscheiden über entspre-

chend gestaltete Import-Policies, welche Routes sie in die jeweiligen VRFs importieren wollen und über Export-Policies, welche Routes sie mit welchen Attributen versehen.
Damit ist es dem Serviceprovider beispielsweise möglich, unterschiedliche VPN-Topologien für Kunden zu konstruieren (z. B. Full Mesh, Partial Mesh, Hub & Spoke).

Setup von LSPs
Für das Forwarding von VPN-Daten über das Providernetz müssen LSPs zwischen den PE-Routern aufgesetzt werden. Für das Setup und die Verwaltung von LSPs wird das Label Distribution Protocol LDP oder ein anderes LSP-Setup-Protokoll (z. B. RSVP mit Traffic Engineering Extensions) eingesetzt. Um die Herstellerinteroperabilität zu garantieren, wird vorausgesetzt, dass alle PE-Router und P-Router zumindest LDP unterstützen.
LDP baut eine Full Mesh von LSPs zwischen den PE-Routern auf. Die LSPs folgen dabei den durch das interne IP-Routingprotokoll des Providers vorgegebenen «besten» Wegen.
Ein denkbares Mixed-Szenario ist der Einsatz von RSVP in einem Traffic-Engineered Core und von LDP am Edge zwischen PE-Router und dem ersten P-Router.

Data Forwarding
Die Kundendaten werden zwischen den PE-Routern mittels MPLS übertragen, wobei jedem Datenpaket zwei MPLS-Labels zugeordnet sind:
– Das äussere Label wird für die Übertragung entlang des definierten LSP zwischen den PE-Routern benutzt; das innere Label identifiziert das Ziel-CE-System.
– Der Prozess der Datenübertragung wird anhand des Beispielnetzwerks gemäss Bild 3 erläutert:
- Host 10.2.3.4 sendet Datenpakete zu Server 10.1.3.8. CE2 führt einen «longest-match route-lookup» durch und sendet das Datenpaket zu PE2.
- PE2 empfängt das Paket und führt einen Route-Lookup in der VRF RED durch, da das Interface zu CE2 dem VPN RED zugeordnet ist. PE2 erhält dadurch das MPLS Label und die BGP-Next-Hop-Adresse (die Loopback-Adresse von PE1), die von PE1 mit dem Adressprefix 10.1/16 verteilt wurden.
- PE2 stellt dann fest, über welchen der bereits existierenden LSPs die BGP-Next-Hop-Adresse erreichbar ist und bestimmt das Outgoing Interface sowie das erste MPLS-Label für den LSP.
- PE2 hängt nun das MPLS-Label für das Zieladressprefix und das MPLS-Label für den ausgewählten LSP an das Datenpaket und sendet es über den selektierten LSP zum ersten P-Router im LSP von PE2 nach PE1. Die P-Router senden das Datenpaket anhand der Informationen im äusseren Label durch das Netzwerk zum Router PE1. Der letzte P-Router vor PE1 entfernt das äussere MPLS-Label und sendet das Datenpaket an PE1.
- PE1 identifiziert die direkt angeschlossene CE1 über das verbliebene innere MPLS-Label als «next hop» zum Zielnetzwerk, entfernt das MPLS-Label und sendet ein IPv4-Paket an CE1. CE1 sendet das Paket zum Server 10.1.3.8.

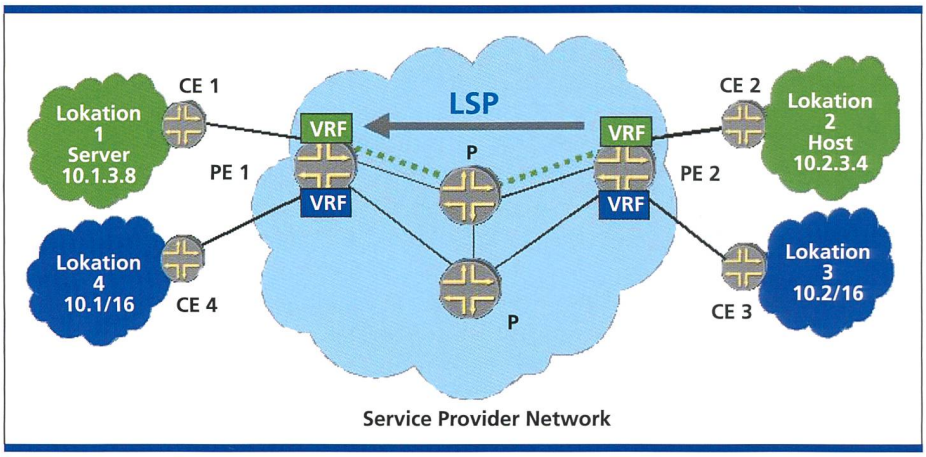


Bild 3. Datenfluss von Lokation 2 nach Lokation 1.

Diskussion und Bewertung des VPN-Modells nach RFC 2547bis

Servicegestaltung
Der VPN-Ansatz nach RFC 2547bis ermöglicht dem Serviceprovider, sehr hochwertige Intranet- und Extranet-Services, beispielsweise Outsourcing des WAN-IP-Backbone, anzubieten.

Limitierungen
Das VPN-Modell ist sehr gut für einfach zu formulierende Kommunikations-Policies geeignet, beispielsweise viele gleichrangige Lokationen – jeder darf mit jedem kommunizieren. Komplexe Routingsituationen wie beispielsweise die zusätzliche Verbindung von zwei VPN-Lokationen ausserhalb des VPN (Backdoor-Routing) können zu Problemen führen.
IP-Multicasting wird im Basismodell nicht adressiert, es existieren aber bereits konkrete Lösungsvorschläge (draft-rosen-vpn-mcast-02), und möglicherweise werden in Zukunft entsprechende Implementierungen verfügbar sein.
Kunden können das eigene Routingprotokoll möglicherweise nicht End-to-End einsetzen, sondern werden am PE-Router terminiert. So kann beispielsweise im RFC 2547bis-Basismodell ein Single-Area-Konzept für OSPF, das alle Lokationen umfasst, nicht realisiert werden.
Erste Drafts (draft-rosen-vpns-ospf-bpg-mpls-03) beschreiben hier Lösungsmöglichkeiten, erfordern aber zusätzlichen Implementierungsaufwand.

Skalierbarkeit der Implementierung
In grossen Providernetzen sind möglicherweise Hunderte von Routingtabellen zu verwalten. BGP-Route-Reflektoren (möglicherweise mehrere) sind erforderlich, um die Verteilung der VPN-Informationen skalierbar zu gestalten. Besondere Beachtung ist den PE-Routern zu widmen, die Speicher- und Verarbeitungskapazität dieser Systeme begrenzt die Anzahl und Grösse der VPNs.
Folgende primären Einflussfaktoren sind hierbei zu beachten:
– Die Anzahl der Routes/Prefixes pro VPN
– Die Anzahl der VPNs/Lokationen
– Die Art der Routingprotokolle zwischen CE-PE

Administration
Adds, Moves & Changes von Kundenlokationen werden durch die implementierten Verteilmechanismen sehr gut unterstützt.
Der hohen Flexibilität bezüglich des Aufbaus von spezifischen Netzwerktopologien steht eine zunehmende Komplexität in Bezug auf Policygestaltung gegenüber,

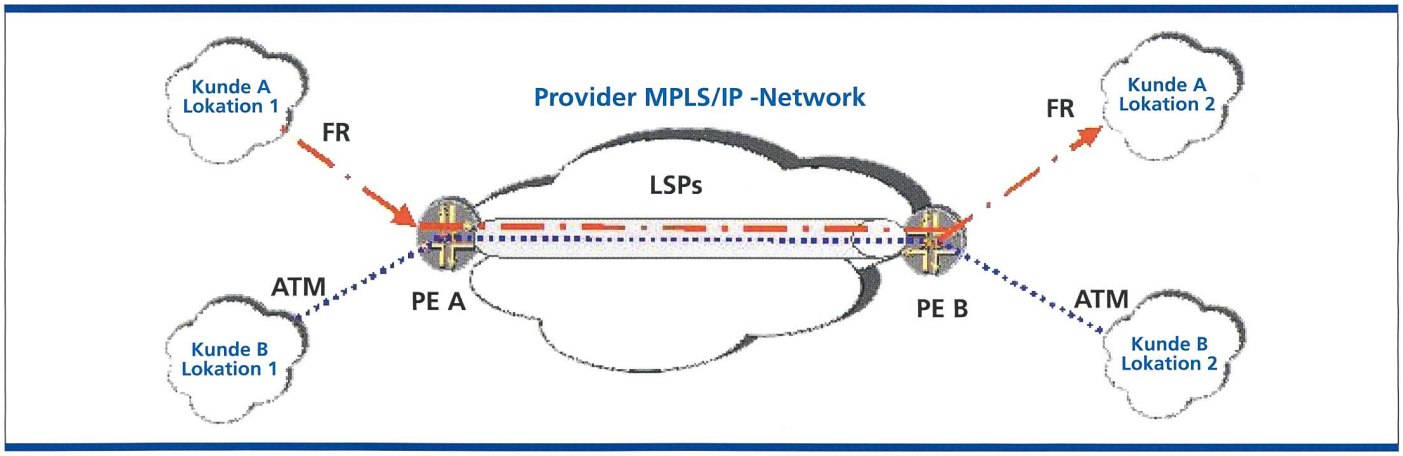


Bild 4. MPLS-Layer-2-VPN-Ansatz.

sodass wohl die einfach zu beschreibende Vollvermaschung als Netzwerktopologie und einfache Hub & Spoke-Topologien bevorzugt realisiert werden.

Sicherheit
Die Sicherheit dieses Layer-3-VPN-Services ist vergleichbar mit der von ATM- oder Frame-Relay-Netzen. Weder Daten noch Routinginformationen werden zwischen den VPNs ausgetauscht. Die Verschlüsselung des Datenstroms (z. B. IPSEC) wird im Rahmen dieses VPN-Ansatzes nicht adressiert und bleibt den teilnehmenden CE-Systemen vorbehalten.

MPLS-Layer-2-VPNs
MPLS-Layer-2-VPNs verfolgen den Ansatz, dem Kunden eine logische Layer 2-Verbindung durch das Netzwerk des Providers zu bieten. Dazu eignet sich natürlich besonders MPLS als universeller Transportmechanismus.
MPLS-Layer-2-VPNs ermöglichen es, Frame Relay-DLCI, ATM-VCI/VPI, Ethernet, Ethernet-VLANs, PPP- und HDLC-Verbindungen über einen MPLS/IP-Backbone zu schalten.

Funktionsweise
Bild 4 beschreibt das MPLS-Layer-2-VPN-Modell. Der Provider konfiguriert an seinen PE-Routern die korrespondierenden Incoming- und Outgoing-Interfaces, bzw. Subinterfaces und definiert das verwendete Layer-2-Protokoll.
Die PE-Router erfüllen in diesem Modell eine Layer-2-Forwarding-Funktion. Sie lesen die von den angeschlossenen Kundennetzwerken ankommenden Layer 2 Frames, ordnen ein entsprechendes MPLS-Label dem Layer 2 Frame zu und selektieren den LSP zum Ziel-PE-Router. Die LSPs zwischen den PE-Routern werden als Tunnels für den Transport der Layer 2 Frames eingesetzt.
Mit Hilfe des Label-Stackings können mehrere Layer-2-Verbindungen zwischen zwei PE-Routern über einen LSP übertragen werden.
Neben bereits vorhandenen proprietären Ansätzen existieren unterschiedliche Drafts (draft-martini-l2circuit-trans-mpls-08, draft-martini-l2circuit-encap-mpls-04, draft-kompella-ppvpn-l2vpn-01) für die Implementierung von Layer-2-VPNs. Erste Implementierungen dieser Drafts sind von verschiedenen Herstellern bereits verfügbar.

Diskussion und Bewertung

Servicegestaltung
Mit einem Layer-2-VPN werden dem Endkunden Punkt-zu-Punkt-Verbindungen zur Verfügung gestellt. Der Serviceprovider nimmt nicht am IP-Routing des Kunden teil. Der Kunde ist selbst verantwortlich für den Betrieb seines Routernetzes (Layer-3-Ebene). Der VPN-Service ist auf die Zurverfügungstellung der Layer-2-Verbindung beschränkt; es kann kein hochwertiger WAN-IP-Backbone-Outsourcing-Service realisiert werden.
Der MPLS-Layer-2VPN-Service gibt dem Kunden jedoch eine erhöhte Gestaltungsfreiheit gegenüber dem Layer-3-VPN-Service. Kunden können beliebige Vermaschungen ihres Netzwerkes bilden, ohne dass auf Seiten des Providers Massnahmen getroffen oder Konfigurationsänderungen durchgeführt werden müssen. Kunden sind vollkommen unabhängig in der Wahl des Layer-3-Protokolls (IP, IPX, AppleTalk etc.), in der Gestaltung des Routings und in der Wahl ihrer Routingprotokolle. IP-Multicasting wird ebenfalls transparent unterstützt.

Limitierungen
Die Anbindungen der Kundenlokationen sind auf eine Layer-2-Technologie pro VPN festgelegt und nicht unabhängig wählbar.
Entsprechende Limitierungen wie beim Layer-3-VPN-Ansatz bestehen nicht, jedoch ist die Skalierungsfähigkeit definitiv eingeschränkt. MPLS-Layer-2-VPNs skalieren nicht, wenn eine dichte Vermaschung einer grossen Anzahl von Lokationen erforderlich ist.
Auf Kundenseite besteht das Problem, dass bei n Lokationen jeder CE-Router n andere CE-Router als Neighbour hat. Hier wird die Verarbeitungskapazität der CE-Router und die Konvergenzfähigkeit der auf Kundenseite eingesetzten IP-Routingprotokolle zu einer limitierenden Grösse.
Layer-2-VPNs sind daher tendenziell für Kundennetze mit einer geringen Zahl an Lokationen oder mit einem strikt hierarchischen Routingmodell (z.B. Hub & Spoke) geeignet.

Skalierbarkeit der Implementierung
Im Gegensatz zu Layer-3-VPNs besitzen MPLS-Layer-2-VPN eine relativ geringe Grundkomplexität. Die PE-Router müssen sich nicht mit VPN-Routingtabellen und IP-Routingprotokollen der angeschlossenen Kundennetze befassen.

Administration
Adds, Moves & Changes von Kundenlokationen sind gegenüber dem Layer-3-VPN-Modell, abhängig von der gewählten Netzwerktopologie, mit relativ ho-

hem Konfigurationsaufwand verbunden. So muss bei einer Vollvermaschung beim Hinzufügen einer neuen Lokation jeder am VPN teilnehmende PE-Router zusätzlich konfiguriert werden. Der Konfigurationsaufwand steigt bei einer Vollvermaschung daher nicht linear, sondern quadratisch mit der Anzahl der Lokationen. So sind bei n Lokationen n x (n–1) Layer-2-Verbindungen zu konfigurieren. Aktuelle Drafts adressieren jedoch bereits diesen Konfigurationsaspekt, so dass in zukünftigen standardbasierenden Implementierungen diese Problematik nur noch eine untergeordnete Rolle spielen wird.

Sicherheit
Analog Layer-3-VPN nach RFC 2547bis.

Schlussbemerkung
Layer-3-VPNs nach RFC 2547bis und MPLS-Layer-2-VPNs erfüllen unterschiedliche Kundenanforderungen. Sie lassen sich in modernen IP/MPLS Backbones parallel zu Standard-IP-Services implementieren. Beide VPN-Modelle werden daher, idealerweise als wählbare Alternativen, neben dem Standard-Internetzugang in den Serviceportfolios der Provider zu finden sein. [5]

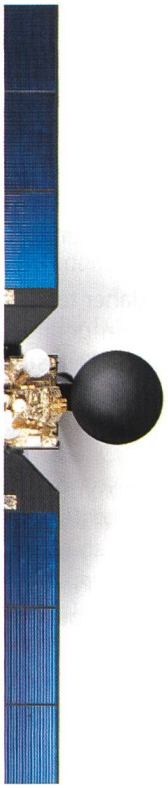
Wolfgang Kirchberger,
SE Central EMEA, Juniper Networks

Info:
Juniper Networks Switzerland
Urs Nussbaumer
Leutschenbachstrasse 95
CH-8050 Zürich
Tel. 01 308 38 13

Summary

MPLS-based VPN Solutions

These days, Internet Service Providers need to be able to offer a variety of VPN models that meet different customer requirements. Each customer has different security and routing requirements, types and volumes of traffic, applications, outsourcing criteria, a varying degree of IT know-how and a different number of locations and users. From the many possible VPN solutions this article investigates the class of Provider Provisioned VPNs (PP-VPNs).



YOUR SUCCESS - OUR BUSINESS

Executive MBA - Management in Telecommunications

You need an EMBA to move forward, but you can't afford to interrupt your career? The unique design of the **iimt EMBA** allows you to earn a full time EMBA without putting your career on hold. From here, the iimt path leads you to almost anywhere.

Come to one of our **Information Evenings**

Fribourg, 17.06 ***Zürich, 19.06***

Genève, 25.06 ***Bern, 27.06***

For further details, please visit
www.iimt.ch
or send an e-mail to
marketing@iimt.ch

international institute of management in telecommunications
Avenue de Tivoli 3
CH - 1700 Fribourg
Tel. +41 (0)26 300 84 30
Fax. +41 (0)26 300 97 94
Université de Fribourg - Universität Freiburg

iimt