Ethernet erweitert

Virtuelle private LAN-Dienste helfen Providern beim Übergang von lokalen zu Metro- und Weitverkehrsnetzen

Wolfgang Schulte

Unternehmen der IT- und Telekommunikationsindustrie arbeiten seit Jahren an dem Thema der Virtual Private Networks (VPN). Es ist anzunehmen, daß nach Verabschiedung entsprechender IETF-Standards die Service Provider ihren Kunden auch Schicht-2-Dienste – Virtual Private LAN-Services (VPLS) – anbieten werden.
Gegenwärtig arbeitet z.B. Alcatel an der Standardisierung mit und bietet Produkte an, die diese Dienste unterstützen sollen; von Cisco gibt es ein Statement of Direction über die aktive Mitarbeit u.a. an den IETF-Standards und die Bereitstellung entsprechender Produkte mit der Cisco 7600-Serie. Andere große Unternehmen wie die Deutsche Telekom, AT&T oder Siemens halten sich dagegen mit Aussagen zu VPLS noch zurück.

Wolfgang Schulte ist Dozent für Kommunikations- und Netztechnik an der Berufsakademie Stuttgart

Die Arbeitsgruppe Layer 2 Virtual Private Networks (l2vpn) bei der IETF Internet Area unterscheidet drei Typen von virtuellen privaten Netzen der Schicht 2 (L2VPN). In *Bild 1* ist deren strukturelle Einordnung dargestellt. Die VPWS und die Point to Multipoint IP-only LAN-like Services (IPLS) werden hier nicht beschrieben.

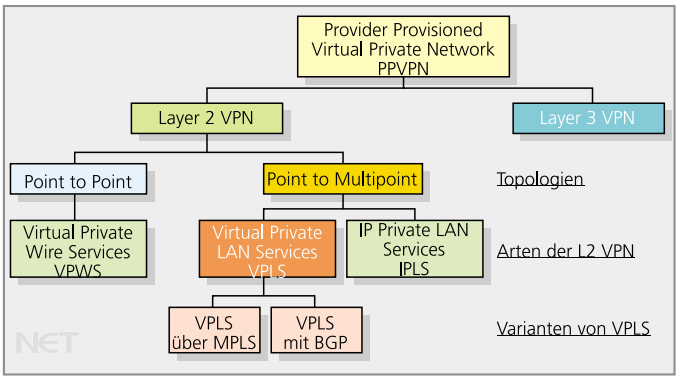

Bild 1: Die Taxonomie der Provider Provisioned Virtual Private Networks

Virtuelle private LAN-Dienste (VPLS), auch bekannt als Transparent LAN Service (TLS) oder Virtual Private Switched Network Service, werden die neuen VPN-Dienste der Schicht 2 bei den Service Providern. VPLS verbindet verteilte LAN-Segmente so, daß sie über Metro-Netze oder Wide Area Networks (WAN) wie ein einziges größeres LAN arbeiten.
Schicht-2-VPNs sind üblicherweise Punkt zu Punkt verbunden, etwa die VPWS. VPLS hingegen nutzt die Vorteile der Multipoint-Topologie, um mehrere LANs über paketorientierte Netze zu verbinden.
Der neue Internet Draft – Virtual Private LAN-Services – vom Januar 2004 steht bis Juli 2004 zur Kommentierung bereit. Der zweite, konkurrierende Standard vom November 2003 beschreibt den Virtual Private LAN-Service (VPLS) über Multiprotocol Label Switching (MPLS im RFC 3031) und wird u.a. von Cisco unterstützt.
Beide Entwürfe unterscheiden sich im wesentlichen durch die Empfehlungen für das Autodiscovery, also die Art, wie die Router der Service Provider, die am VPLS teilnehmen, sich finden und in der spezifizierten Signalisierung zwischen den Routern der Service Provider.

In Ergänzung dazu stehen weitere neue, ergänzende Internet-Entwürfe wie das Framework for Layer 2 Virtual Private Network, Service Requirements for Layer 2 Provider Provisioned Virtual Private Networks und die PPVPN Terminology seit Februar bzw. März dieses Jahres ebenfalls zur Kommentierung an.
In den Service Requirements wird das Interworking, d.h. die Notwendigkeit zur Zusammenarbeit zwischen den unterschiedlichen Lösungen für die Schicht-2-VPN-Dienste, gefordert.
Firmen wie Cisco und Alcatel bestätigen die Bedürfnisse nach der Verfügbarkeit von Ethernet-basierenden

Das Thema in Kürze

Ethernet-, also CSMA/CD-Protokolle werden neben ihrem Einsatz in den LANs durch die neu entstehenden Virtual Private LAN-Services (VPLS) über die lokalen Netze hinaus auch in den Weitverkehrsnetzen einzusetzen sein. Der Beitrag zeigt, daß mit Hilfe der VPLS der Einsatz von LANs für Service Provider in einem voll vermaschten, paketorientierten Multipoint WAN oder Metro-Netz ermöglicht werden kann.

Multipoint-Diensten im WAN und bieten ihren Kunden entsprechende Produkte an.

Architektur von VPLS

Bild 2 zeigt die Architektur einer typischen VPLS-Umgebung mit ihren spezifizierten Komponenten. Die Einheiten Provider Edge (PE) und L2PE sind VPLS-unterstützt, das heißt, sie wissen, daß ein VPLS-Dienst angeboten wird. Diese Einheiten, auch VPLS Edge (VE) genannt, bilden mit den Tunnels das Zentralnetz (Backbone) des Service Providers.

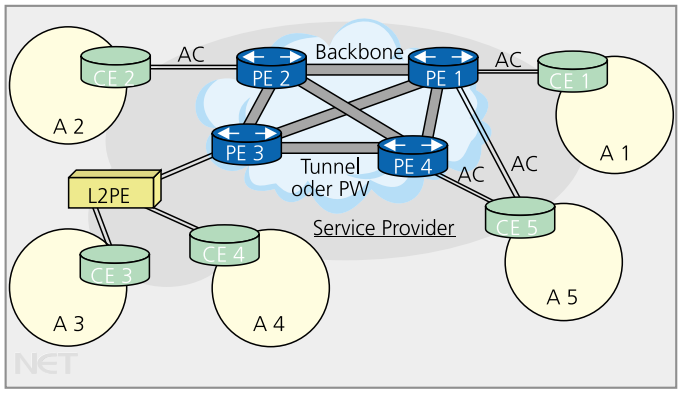

Bild 2: Darstellung eines VPLS-Systems
A – Area, LAN-Segment mit Shared- oder Switched-Ethernet;
AC – Attachment Circuits, die Verbindung von CE nach PE;
CE – Customer-Edge-Einheit, die vom Kunden oder vom Service Provider beim Kunden bereitgestellt wird, um auf den Dienst der Schicht 2 zuzugreifen;
L2PE – eine Einheit vom Service Provider auf Schicht 2 zur Zusammenfassung mehrerer Kunden-LANs und zur Unterstützung von VPLS;
PE – Provider-Edge-Einheiten sind VPLS-Router im Netz des Service Providers;
PW – Pseudo Wire, die Punkt-zu-Punkt-Verbindung zwischen den PEs (im Entwurf für die VPWS so bezeichnet)

Das Service-Provider-Netz ist paketorientiert, mit PEs, die untereinander voll vermascht verbunden sind. Die Verbindung zwischen den PEs bilden IP-Tunnel, die durch Generic Routing Encapsulation (GRE im RFC 2784) oder durch MPLS mittels RSVP-TE oder mit dem Label Distribution Protocol (LDP im RFC 3036) eingerichtet wurden. Mit Tunnel wird hier eine Verbindung im paketorientierten Netz zwischen den PEs bezeichnet, die die Pakete durch das Netz transportieren.

Funktionen von VPLS

Der virtuelle private LAN-Dienst ist nur in einem Netz, nicht über mehrere VPLS-Netze hinweg, vorgesehen. CE-Einheiten an unterschiedlichen Netzen können nicht ohne weiteres miteinander kommunizieren.
Es werden zwei Ebenen der VPLS beschrieben: die Control Plane mit der Aufgabe der Steuerung der beteiligten Einheiten wie PE oder L2PE und die Data Plane mit der Aufgabe der Erstellung und Weiterleitung der Pakete durch das Netz. Die Control Plane nutzt zwei Hauptfunktionen, das Autodiscovery der PEs und das Signalling mit Set-up and Teardown der Verbindungen zwischen den PEs. Mit Autodiscovery wird der automatisierte Prozeß bezeichnet, um alle am VPLS teilnehmenden PEs zu finden. Eine manuelle Konfiguration der PEs wäre bei Störungen, Ausfällen oder bei Neukonfigurationen im Netz zu anfällig gegen Fehler. Die automatische Identifizierung der PEs wird u.a. mittels Border Gateway Protocol (BGP) geplant, das um die Funktion der Extended Communities erweitert wurde. PEs melden sich via I-BGP an, um ihre Zugehörigkeit in einem VPLS-Dienst anzuzeigen. Andere Vorschläge für das Autodiscovery sind Domain Name System (DNS) oder Remote Authentication Dial-in User Services (RADIUS). Wenn die teilnehmenden PEs bekannt sind, muß ein Prozeß zum Verbindungsauf- und -abbau, die Signalisierung, spezifiziert werden. Die Standards, speziell für die Point-to-Point-Topologie, sprechen hier auch von der Schaltung von „Pseudo Wires“ von einem Router zum anderen. Für den Verbindungsaufbau und -abbau wird die Multiprotocol Extension für BGP-4 (RFC 2858) eingesetzt. Mit der Network Layer Reachability Information (NLRI) zur Kennung, welche Route verfügbar ist und mit dem neuem Address Family Identifier (AFI), in dem das Network Layer Protocol und seine Adresse aufgeführt sind, wird diese Aufgabe erledigt.
Eine wichtige Aufgabe der Data Plane ist die Encapsulation, d.h. das Einpacken des Schicht-2-Ethernet-Rahmens vom CE in ein Schicht-3-Paket, das über das paketorientierte Netz zu versenden ist. Die zweite Aufgabe besteht in der Weiterleitung des neu zusammengesetzten Pakets durch das Netz des Service Providers.
Beim Lernen der MAC-Adresse kann man sich das Netz des Service Providers als eine einzige logische lernende Brücke vorstellen. Wie eine Brücke die MAC-Adressen von den aktiven Einheiten im angeschlossenen LAN-Segment an ihren Ports lernt, so lernt das Service-Provider-Netz mit den PEs die MAC-Adressen der aktiven Stationen im Netz und schreibt die Adressen in eine Forwarding Information Base (FIB). Zwei Methoden des Lernens von MAC-Adressen sind vorgesehen: Ein qualifiziertes Lernen, bei dem die PEs die MAC-Adresse aus dem Ethernet-Teil des Packets und dem VLAN-Tag lernen. Das nichtqualifizierte Lernen umfaßt nur die MAC-Adresse aus dem Ethernet-Teil des Packets.
Wenn eine Brücke einen Rahmen mit einer ihr unbekannten MAC- oder mit einer Broadcast-Adresse erhält, leitet

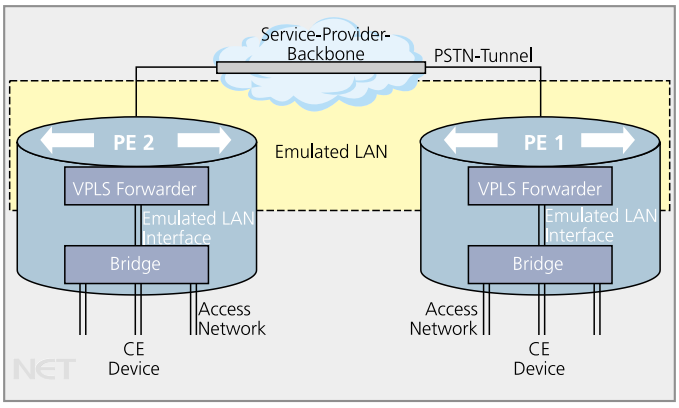

Bild 3: VPLS-Referenzmodell

Nach Redaktionsschluß:

Swisscom verkauft Debitel

In der Sache war es keine große Überraschung, als am 30. April die Nachricht die Runde machte: „Swisscom verkauft ihre Beteiligung an der netzunabhängigen Mobilfunkgesellschaft Debitel." Schon lange hielten sich Informationen zur Verkaufsabsicht des schweizer Betreibers. Allenfalls Zeitpunkt, Preis und Käufer schienen lange Zeit unklar. Doch auch das hat seine Logik. Debitel hatte für 2003 das nach eigenen Angaben „beste Jahr in ihrer Unternehmensgeschichte" hingelegt und so die Braut hübsch gemacht. Einigermaßen jedenfalls. Denn ein guter Deal ist der Verkauf – gemessen an dem, was die Schweizer reingesteckt haben – nicht: Für 640 Mio. € gehen die 95 % der von Swisscom an Debitel gehaltenen Aktien an von der Private Equity Gesellschaft Permira beratene Fonds. Zum Vergleich: Anfang 2001 hatte Swisscom den im Sommer 1999 mit festem Blick auf UMTS erworbenen Anteil von 74 % auf 84 % erhöht. Und für den Zukauf der 10 % der von DaimlerChrysler Services gehaltenen Aktien 470 Mio. CHF hingelegt. Auch für die wenigen freien Aktionäre ist es – unterstellt, daß sie die Anteile seit dem Gang an die Börse halten – kein gutes Geschäft. Zwar haben sie von der Telco Holding S.a.r.l., Luxemburg, ein Übernahmeangebot von 11 €/Aktie erhalten, immerhin ca. einen Euro mehr, als der Markt zuletzt notierte. Aber vom ursprünglichen Kapitaleinsatz ist nur ein Drittel übriggeblieben. „Auf Grund unterschiedlicher Geschäftsmodelle von Swisscom und Debitel und der Entwicklung der Mobilfunkmärkte in Europa nach den UMTS-Auktionen blieben die erwarteten Synergien aus", kommentiert die Verkäuferin die eigene Fehlspekulation. In dieser Situation hat sich die Swisscom lieber für den Spatz in der Hand als die Taube auf dem Dach entschieden. Die Übernahme steht noch unter dem Vorbehalt kartellrechtlicher Genehmigungen. *bac*

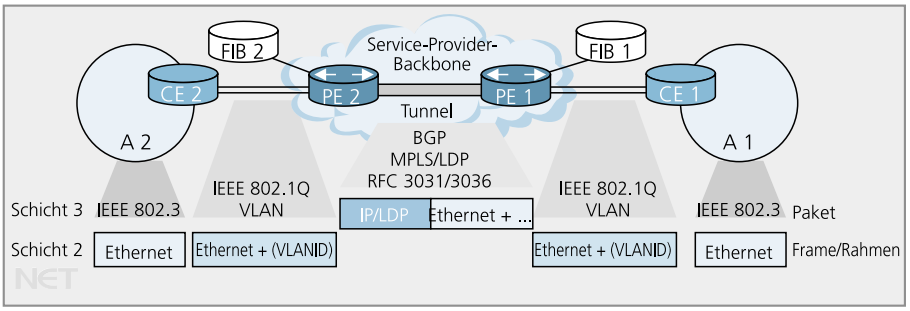

Bild 4: Rahmen und Pakete im Netz

sie den Frame an ihre aktiven Ports weiter, dies nennt man Flooding. Das gleiche gilt bei VPLS: Falls kein Eintrag für die Unicast-MAC-Adresse in der FIB existiert, leiten die PEs die Information von ihrer CE an alle ihr bekannten PEs weiter. Der Empfang eines Pakets in einer PE von einer anderen PE darf

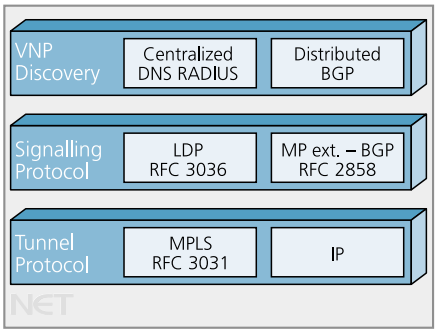

Bild 5: Die Bausteine für ein VPLS-System

nur an die angeschlossenen CEs weitergeleitet werden und nicht an andere PEs. Dieser Mechanismus wird als Split Horizon Flooding bezeichnet, um logische Schleifen in der Topologie zu vermeiden, die zu Broadcast-Stürmen führen würden. Der gleiche Mechanismus wird auch bei den Routing-Protokollen eingesetzt.

Mit Multihoming ist die Konfiguration einer CE bezeichnet, die an mehr als einer PE angeschaltet wird (siehe CE 5 in Bild 2).

Bild 3 zeigt das Referenzmodell für VPLS aus dem Framework-Dokument, wonach die CE-Einheiten über Zugangsnetze und Brücken an verbundene LAN-Segmente angeschlossen erscheinen. Die Brückenmodule sind mittels Emulated LAN Interfaces über das Emulated LAN verbunden. Die VPLS-Forwarder-Funktion leitet die Pakete von der sendenden PE über die Public Switched Network Tunnels (PSN) an die empfangende Provider-Edge-Einheit weiter.

Rahmen- bzw. Paketaustausch

Bild 4 stellt den Rahmenaustausch auf Schicht 2 zwischen CE und PE und die Übertragung der Pakete auf Schicht 3 zwischen den PEs dar. Auf Schicht 2 wird die MAC-Adresse verwendet. Für die Schicht 3 braucht man die IP-Adresse.

In den Netzsegmenten A1 und A2 wird entweder das Ethernet-Protokoll oder bereits nach IEEE 802.1Q ein Virtual-LAN-Protokoll (VLAN) eingesetzt. Zwischen den CEs und den PEs ist ein VLAN oder nach dem IEEE 802.1ad-Standard (Provider Bridges, eine Erweiterung von 802.1Q) zu konfigurieren. Die Verbindungen zwischen CE und PE werden im Framework-Dokument auch mit Attachment Circuits (AC), die Verbindungen zwischen den PEs als Tunnel oder Pseudo Wires (PW) bezeichnet.

Bild 5 zeigt die alternativen Bausteine für ein VPLS-System. Als Tunnelprotokoll scheint sich das MPLS durchzusetzen. Beim Signalling-Protokoll prüft man das LDP oder die Multiprotokollerweiterung (MP) für das BGP-4. Ob sich BGP für Autodiscovery durchsetzen wird oder andere Lösungen, ist zur Zeit noch offen.

Man erwartet, daß die konkurrierenden VPN-Standards nicht vor Ende 2004 zum Abschluß kommen. Für die Netzbetreiber ist es notwendig, daß die beiden vorliegenden Standards zusammengeführt werden.

Neben dem neuen L2-VPN-Multipoint-Service werden die L2-Point-to-Point- und die L3-VPN-Dienste (MPLS L3 VPN) bei den Service Providern eine Weile nebeneinander bestehen.

Unabhängige Testlabors wie Isocore (www.isocore.com) haben bereits verschiedene Interoperabilitätstests für VPLS durchgeführt. *(we)*