Virtuell aber real

Virtuelle Private Netze und deren Basistechnologien

Torsten Braun,
Manuel Günter

Die Absicht der Unternehmen und Einrichtungen, vertrauenswürdige und vertrauliche Kommunikation immer kostengünstiger gestalten zu wollen, hat Virtuelle Private Netze auf den Plan gerufen.
Sie sind dabei, den mietleitungsbasierten Corporate Networks Marktanteile wegzunehmen.
Um die Informationsübertragung unverfälscht und unzugänglich für Nichtautorisierte gestalten zu können, sind teils noch im Standardisierungsprozeß befindliche Basistechnologien erforderlich, die hier vorgestellt werden.

Prof. Dr. Torsten Braun ist Leiter, Dipl.-Inf. Manuel Günter Assistent der Forschungsgruppe Rechnernetze und Verteilte Systeme am Institut für Informatik und angewandte Mathematik der Universität Bern

Was ist ein VPN?

Der Begriff Virtuelles Privates Netz (VPN) wird oft in sehr unterschiedlichen Bedeutungen verwendet und mit einer Vielzahl verschiedenartiger Produkte in Verbindung gebracht. Ein privates Netz besteht aus einer Vielzahl von Netzgeräten und -mitteln, auf die nur ein eingeschränkter Benutzerkreis (eine geschlossene Benutzergruppe) Zugriff hat. Nun ist es nicht unbedingt sinnvoll oder auch möglich, daß jede geschlossene Benutzergruppe ihr eigenes privates Netz auf der Basis einer eigenen Infrastruktur aufbaut. Vielmehr bietet es sich an, vorhandene öffentliche Kommunikationsnetze als Grundlage zu verwenden und darüber ein privates Netz zu simulieren. Im Idealfall sollten die Nutzer dabei nicht bemerken, daß das private Netz auf einem öffentlichen Netz basiert, das gleichzeitig auch von anderen Benutzergruppen benutzt wird. D.h. das private Netz ist nicht wirklich privat, sondern es erscheint lediglich privat. Man spricht in diesem Fall von Virtuellen Privaten Netzen (Virtual Private Networks, VPNs). Der Ausdruck privat bedeutet dabei, daß die Kommunikation über ein VPN in sicherer Art und Weise, d.h. vertrauenswürdig und vertraulich, erfolgt. Vertrauenswürdig heißt, daß der Empfänger von Daten davon ausgehen kann, daß die empfangenen Daten wirklich vom angegebenen Sender stammen und daß die Daten nicht durch Dritte erzeugt oder verändert wurden. Von vertraulicher Kommunikation spricht man, wenn Dritte auf die ausgetauschten Daten nicht zugreifen können oder diese nur in unkenntlicher Form sehen können. Falls das verwendete öffentliche Netz solche private Kommunikation nicht unterstützt (wie das Internet), müssen Verschlüsselungstechniken eingesetzt werden.

Vorläufer von VPNs sind sogenannte Corporate Networks, d.h. Unternehmensnetze, bei denen Netzkomponenten (z.B. Router) über öffentliche Mietleitungen verbunden werden. Heute sind firmeninterne private Datennetze meist IP-basiert. Diese werden auch Intranets genannt. IP-VPN-Technologie verbindet nun geografisch verstreute Intranets über das Internet, ohne dabei den privaten Charakter der Netze preiszugeben. Immer häufiger werden auch firmenübergreifende IP-Netze benötigt, um eine Netzinfrastruktur für firmenübergreifende geschlossene Benutzergruppen zur Verfügung stellen zu können. Solche Netze werden häufig Extranets genannt.

Anforderungen an VPNs

Angebot und Nachfrage für VPN-Lösungen sind groß. Es gilt, hard- oder softwaregestützte Ansätze oder auch ausgelagerte Dienste zu unterscheiden. Dieser Artikel beleuchtet die zugrundeliegenden Basistechnologien. Folgende Faktoren charakterisieren eine VPN-Technologie: Sicherheit, Trans-

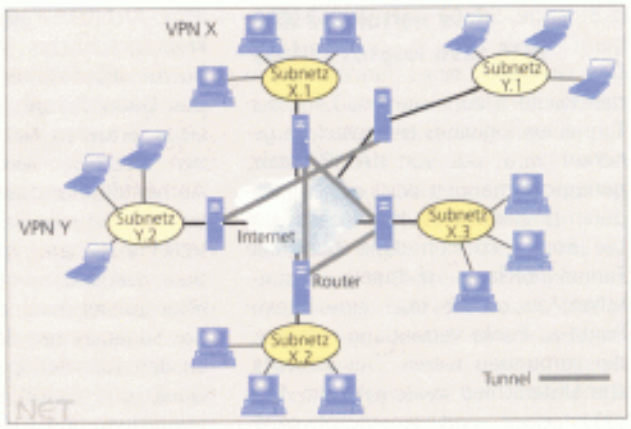
Das Thema in Kürze

Nach einer Definition Virtueller Privater Netze werden die VPN-Typen vorgestellt und der Trend zum Network-Layer-VPN (IP-VPN) herausgearbeitet. Das Tunneln von Paketen und die Bedeutung von IPSec (DES zur Verschleierung, MD5 zur Authentifizierung) werden beschrieben, auf Entstehen und Perspektive von L2TP wird eingegangen. IEEE 802.1Q und LANE werden als Technologien für Link-Layer-VPNs ebenso vorgestellt wie das zur Standardisierung anstehende MPLS.

parenz, Kosten, Granularität, Flexibilität und Dienstgüte.

Die Sicherheit eines VPNs hängt in erster Linie von der Angriffsfläche ab, die das verwendete öffentliche Netz exponiert und der Stärke der Gegenmaßnahmen der VPN-Technologie. Die Gegenmaßnahmen erstrecken sich meist auf die Zugangskontrolle und Datenverschleierung mit kryptographischen Algorithmen unterschiedlicher Stärke. Eine transparente VPN-Technologie schützt VPN-Teilnehmer (und deren Applikationen), ohne daß diese davon Kenntnis haben oder etwas dazu beitragen müssen. VPNs erlauben daher, im Gegensatz zu Sicherheitsmechanismen auf der Anwendungsebene (z.B. shttp) einen flächendeckenden Schutz. Jede ernstzunehmende VPN-Technologie muß ein Mindestmaß an transparenter Sicherheit bieten.

Die Kosten einer VPN-Technologie sind abhängig vom verwendeten öffentlichen Netz. Allerdings beinhalten sie auch den zusätzlichen Verwaltungsaufwand. Dieser wird wiederum von der Flexibilität und Granularität der Technologie beeinflußt. Ein flexibles VPN läßt den Nutzer beispielsweise auch auf die öffentlichen Dienste des verwendeten Datennetzes zugreifen. Eine solche Lösung integriert meistens bestehende Firewall-Funktionalitäten und muß auf diese abgestimmt werden. Unterstützt das VPN nur stationäre Teilnehmer und keine Mobilität, so ist das VPN zwar leichter aufzusetzen, aber es verkleinern sich die möglichen Anwendungsgebiete. Die Flexibilität der verwendeten Technologie kann auch durch die Reichweite des öffentlichen Netzes beschränkt sein. Extranets sollen es Teilnehmern von verschiedenen Firmen ermöglichen, für eine gewisse Zeit an einem gemeinsamen Projekt zu arbeiten. Wenn die beteiligten Firmen nicht ihr privates Netz komplett dem Partner öffnen wollen, so muß das verwendete VPN differenzieren können, es muß eine feine Granularität erlauben. So kann es erwünscht sein, daß einzelnen VPN-Teilnehmern nur eingeschränkte Dienste (z.B. Zugriff auf bestimmte Datenbanken oder Web-Server) zur Verfügung stehen.



Struktur eines VPNs

Selbstverständlich erhöht eine feine Granularität auch den Verwaltungsaufwand.

Ein weiteres Merkmal einer VPN-Technologie ist die Dienstgüte des Transportmediums. Das bedeutet, daß auch in einem VPN, ähnlich wie in einem lokalen Netz oder einem Corporate Network eine garantierte minimale Bandbreite für die Mitglieder des Netzes zur Verfügung stehen sollte. Nur in diesem Fall wird ein Unternehmen bereit sein, ihr Corporate Network durch ein VPN zu ersetzen.

Typen von VPNs

Als öffentliche Netze zur Realisierung von VPNs können verschiedene Netztechnologien dienen, z.B. X.25, ISDN, Frame Relay oder auch ATM-Netze, d.h. Technologien, die oft in die Schicht 2 des ISO/OSI-Basisreferenzmodells oder unterhalb von IP in der Internet-Protokollarchitektur eingeordnet werden. Ein auf Frame Relay oder ATM beruhendes VPN wird daher oft als *Link-Layer-VPN* bezeichnet. Die Realisierung eines Link-Layer-VPNs erfordert, daß durch den Netzbetreiber ein Link-Layer-Dienst, z.B. ein Frame-Relay- oder ein ATM-Dienst bereitgestellt wird. Bei Link-Layer-VPNs werden dann die Netzkomponenten (Router, Switches) über ein und dieselbe Link-Layer-Technologie miteinander verbunden, wobei sehr oft zwischen den Netzkomponenten virtuelle Verbindungen (virtual circuits) etabliert werden. Diese virtuellen Verbindungen ersetzen bei VPNs die bei Corporate Networks verwendeten Mietleitungen.

Ein Link-Layer-VPN erfordert demnach, daß die grundlegende Link-Layer-Technologie des VPNs flächendeckend zur Verfügung steht. Das ist nicht immer der Fall, speziell dann, wenn ein VPN über mehrere Staaten oder mehrere Netzbetreiber mit unterschiedlichen Link-Layer-Technologien hinweg realisiert werden soll. Um dieses Problem zu umgehen, ist als Basis zum Aufbau eines VPNs alternativ ein IP-Dienst vorzusehen. Sämtliche Daten eines VPNs werden dann über IP transportiert. Ein solches VPN heißt *Network-Layer-VPN* oder– da auf der Netzschicht IP eingesetzt wird – auch IP-VPN. Verschiedene Möglichkeiten zum Aufbau von Link-Layer- und Network-Layer-VPNs werden nachfolgend vorgestellt.

Tunneln als Basistechnik für Network-Layer-VPNs

Ein einfaches, aber wenig flexibles Konzept zur Realisierung von Network-Layer-VPNs besteht im Einrichten von sogenannten Tunneln zwischen Routern. Beispielsweise können zwei IP-Subnetze über zwei Router miteinander verbunden werden, indem zwischen den jeweiligen Routern der beiden Subnetze ein sogenannter Tunnel eingerichtet wird. Das Einrichten eines Tunnels erfolgt dabei in der Regel manuell oder über ein Netzmanagementsystem. Sollen mehrere Subnetze miteinander verbunden werden, muß sich der Betreiber des VPNs überlegen, welche Subnetze direkt über Tunnels miteinander verbunden werden sollen. Die Tunnel können dann verschiedene Strukturen bilden

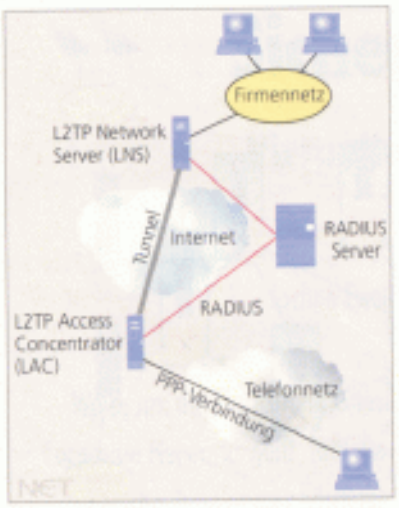
(z.B. Ringe, Sterne oder Vermaschungen).
Das Einrichten eines Tunnels hat in den Routern zur Folge, daß für den Tunnel ein logisches Netzinterface generiert wird, das von der IP-Instanz genauso behandelt wird wie alle anderen physikalischen Interfaces auch. Die Router können dann über ihre Tunnel-Interfaces IP-Pakete austauschen, als ob sie über eine direkte Punkt-zu-Punkt-Verbindung miteinander verbunden wären. Der wesentliche Unterschied zwischen dem Tunnel-Interface und einem physikalischen Interface besteht darin, daß durch das Tunnel-Interface IP-Pakete nochmals in IP-Pakete eingekapselt werden, d.h. ein über einen IP-Tunnel übertragenes Paket hat zwei IP-Header. Dadurch kann ein mit privaten Adressen adressiertes Paket (wie sie in einem Intranet auftreten) mit einer öffentlichen Adresse versehen und so über das öffentliche Netz übertragen werden.
GRE (Generic Routing Encapsulation) spezifiziert einen allgemeinen Mechanismus, um ein beliebiges Protokoll (z.B. IP, XNS, SNA, Appletalk usw.) über IP zu tunneln. Zwischen den zu übertragenden Daten und dem IP-Tunnel-Header wird dabei ein GRE-Header eingefügt, der neben Kontrollflags eine Kennung des eingekapselten Protokolls enthält.

IPSec

Um den immer stärker werdenden Wunsch nach sicherer Internet-Kommunikation zu erfüllen, wurde in der Internet Engineering Task Force (IETF) der IP Security Standard (IPSec) definiert. IPSec standardisiert die Anwendung von kryptographischen Algorithmen zur Verschleierung und Authentifizierung. IPSec bearbeitet jedes einzelne IP Paket separat. Damit ermöglicht IPSec den geforderten flächendeckenden und transparenten Schutz eines VPNs. Um Interoperabilität zu gewährleisten verlangt IPSec die Unterstützung von weitverbreiteten Algorithmen wie dem Data Encryption Standard (DES) zur Verschleierung und dem Message-Digest-5-Algorithmus (MD5) zur Authentifizierung. Die IPSec-Architektur kann aber beliebige kryptographische Algorithmen benutzen. IPSec kennt einen Tunnel-Modus. Dadurch kann IPSec zum Aufbau eines virtuellen Netzes benutzt werden. Die IPSec-Verschleierungs- und Authentifizierungsmethoden erweitern das virtuelle Netz dann zu einem VPN. In einem typischen Anwendungsszenario verbindet ein IPSec-Tunnel zwei private Subnetze. Die sogenannten Security Gateways an den Tunnelendpunkten verbergen Quell- und Zielort sowie den Inhalt sämtlicher über das Internet verschickter Pakete. Die Security Gateways müssen dafür über einen gemeinsamen Geheimschlüssel verfügen. Im öffentlichen Internet agierende Angreifer sind ohne Kenntnis dieses Schlüssels nicht in der Lage, den Inhalt der Pakete zu entziffern oder unbemerkt zu manipulieren. Protokolle zum sicheren und automatischen Austausch oder zum Erneuern der Schlüssel werden zur Zeit definiert. IPSec ist in den heute verfügbaren IP-Routern der meistbenutzte Sicherheitsstandard. Beim Einrichten von IP-Tunnels kann dabei konfiguriert werden, ob und wie die über den Tunnel gesendeten IP-Pakete verschlüsselt oder mit Authentifizierungsdaten versehen werden.

Point-to-Point Protocol und Layer-2 Tunneling Protocol

Oft, z.B. wenn Mitarbeiter einer Firma reisen müssen, besteht die Notwendigkeit von einem beliebigen Ort auf das VPN der Firma zugreifen zu können. Um ein solches Szenario unterstützen zu können, muß es auch möglich sein, Tunnel von den Endsystemen zu einem Router des VPN aufzubauen. Eine Möglichkeit, ein solches Szenario zu unterstützen, besteht darin, zwischen einem Router eines VPNs und einem Endsystem, das auf das VPN zugreifen will, eine PPP-Verbindung (PPP – Point-to-Point Protocol) aufzubauen und die PPP-Pakete über das Internet zu tunneln.
Das PPP unterstützt die Übertragung von beliebigen Schicht-3-Protokollen über Punkt-zu-Punkt-Verbindungen, z.B. Telefonverbindungen, serielle Verbindungen, ISDN-Verbindungen oder SONET-Links. Allerdings ist es oft nicht wünschenswert, daß ein mobiler Nutzer eine PPP-Verbindung über eine Wählverbindung zu einem Router (PPP-Server) etabliert, speziell dann, wenn sich das Endsystem sehr weit vom Router entfernt befindet.
Kostengünstiger läßt sich das Szenario realisieren, indem sich das Endsystem in einen Zugangsknoten im Nahbereich einwählt und die PPP-Pakete zwischen dem Zugangsknoten und dem VPN-Router über das Internet getunnelt werden. Zum Tunneln von PPP-Paketen eignet sich das Layer-2 Tunneling Protocol (L2TP), das sich in der Standardisierungsphase befindet. L2TP erlaubt das Tunneln von PPP-Paketen zwischen Zugangsknoten (L2TP Access Concentrator, LAC) und dem VPN-Router, der den Tunnel terminiert. Dieser VPN-Router wird auch als L2TP Network Server (LNS) bezeichnet. L2TP entwickelte sich aus zwei zunächst konkurrierenden Protokollvorschlägen der Firmen Microsoft (PPTP – Point-to-Point Tunneling Protocol) und Cisco (L2F – Layer 2 Forwarding). PPTP ist derzeit noch weiter verbreitet als L2TP. Die Verbreitung von L2TP nimmt aber stetig zu.
In einem auf L2TP basierenden VPN wählen sich die Endsysteme über PPP beim nächsten LAC ein. Der LAC bildet dabei den Zugang zum Internet für Endsysteme, die über Punkt-zu-Punkt-Verbindungen (entweder direkt oder über Wählverbindungen) verbunden sind. Ein LAC hat einerseits eine Punkt-zu-Punkt-Verbindung zum Endsystem, andererseits ist der LAC mit einem Interface zum Internet verbunden. Ein Endsystem etabliert zunächst zum LAC eine Punkt-zu-Punkt-Verbindung. In Abhängigkeit des Nutzers wählt der LAC einen L2TP Network Server (LNS) aus, zu dem die empfangenen PPP-Pakete weitergeleitet werden. Zu diesem Zweck etabliert der LAC zum LNS durch den Austausch entsprechender L2TP-Kontrollnachrichten zwischen LAC und LNS einen IP-Tunnel. Ein LAC wird typischerweise durch einen Netz-Provider betrieben, während ein LNS eher von der Firma, der ein VPN gehört, verwaltet wird. Es ist aber auch möglich, daß



Layer-2 Tunneling Protocol (L2TP)

ein Netz-Provider das Betreiben eines LNS übernimmt. Nach dem Etablieren des Tunnels zum LNS werden die am LAC ankommenden PPP-Pakete in L2TP-Datenpakete eingekapselt und über IP an den LNS gesendet. Durch den Tunnel entsteht für das Endsystem der Eindruck, daß eine PPP-Verbindung zum LNS aufgebaut wurde. Der LNS packt das Paket wieder aus und leitet es über ein anderes Interface weiter. Ein wichtiger Vorteil von L2TP gegenüber PPTP besteht darin, daß jedes mobile Endsystem nur mit einer PPP-Protokollimplementierung ausgestattet sein muß, um auf ein VPN zugreifen zu können. Lediglich zwischen LAC und LNS muß das L2TP-Protokoll abgehandelt werden.

Ein wichtiger Aspekt bei VPNs ist die Zugriffskontrolle auf ein solches VPN. Das bedeutet, nur ausgewählte Nutzer sollen auf ein bestimmtes VPN zugreifen können. Um die Sicherheit der Kommunikation zu erhöhen, können durch PPP unterstützte Sicherheits- und Authentifizierungsmechanismen wie RADIUS eingesetzt werden. In PPP/L2TP-Szenarien kann eine erforderliche Authentifizierung beim Etablieren der PPP-Links im LAC oder LNS erfolgen. LAC und LNS können über das RADIUS-Protokoll mit einem zentralen RADIUS-Authentifizierungs-Server Authentifizierungsdaten oder auch Accounting-Information austauschen. Um die Vertraulichkeit der Übertragung mit L2TP zu gewährleisten, können die in PPP eingekapselten IP Pakete mit IPSec gesichert werden.

Link-Layer-VPNs

Bei Network-Layer-VPNs macht sich bezüglich der Durchsatzleistung nachteilig bemerkbar, wenn auf dem Datenpfad zwischen Sender und Empfänger Router-Instanzen die Datenpakete verarbeiten. Ein weiteres Problem von Network-Layer-VPNs besteht darin, daß zwischen den zu einem VPN zusammengeschlossenen Subnetzen viele Router liegen können und damit keine Dienstgüten (Bandbreite, Verzögerungen) garantiert werden können. Das kann für viele Firmen ein entscheidender Grund sein, keine Umstellung des Intranets von einem mietleitungsbasierenden Corporate Network auf ein VPN durchzuführen.

Da im Network-Layer jeder Router für jedes Paket eine Wegwahl trifft, ist es im allgemeinen für einen Angreifer leichter, Pakete abzufangen oder einen falschen Paketabsender vorzutäuschen. Hingegen werden viele Link-Layer-Technologien auch ohne Verschlüsselung als genügend sicher betrachtet, um für VPNs geeignet zu sein. Ein Nachteil der Technologien ist jedoch die größere Abhängigkeit von einem Link-Layer-Dienstanbieter sowie eine allenfalls beschränkte Reichweite des Dienstes.

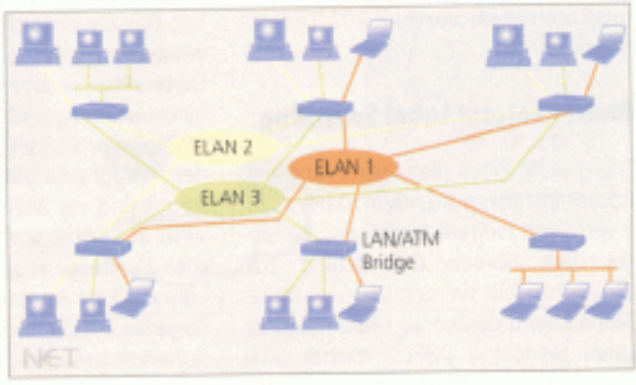
Als Technologien zur Etablierung von Link-Layer-VPNs dienen die Standards IEEE 802.1Q sowie die im ATM Forum entwickelte LAN Emulation (LANE), die nachfolgend vorgestellt werden. Mit diesen beiden Techniken lassen sich virtuelle LANs (VLANs) realisieren, die aus Sicht des Endsystems die gleichen Eigenschaften wie LANs haben, zusätzlich aber eine Virtualisierung unterstützen.

LAN Emulation und Multi-Protocol over ATM

LANE ist eine geeignete Technologie zum Aufbau protokollunabhängiger virtueller LANs. Das Bild zeigt eine Beispielkonfiguration, bestehend aus verschiedenen virtuellen LANs. Ein virtuelles LAN besteht in diesem Fall aus den darin enthaltenen Endsystemen, verschiedenen LAN-Ports der LAN/ATM-Bridges, den jeweils einem virtuellen LAN (VLAN) zugeordneten emulierten LANs (ELANs) sowie den virtuellen LANE-Interfaces (LANE Clients, LECs) der an den ELANs angeschlossenen LAN/ATM-Bridges.

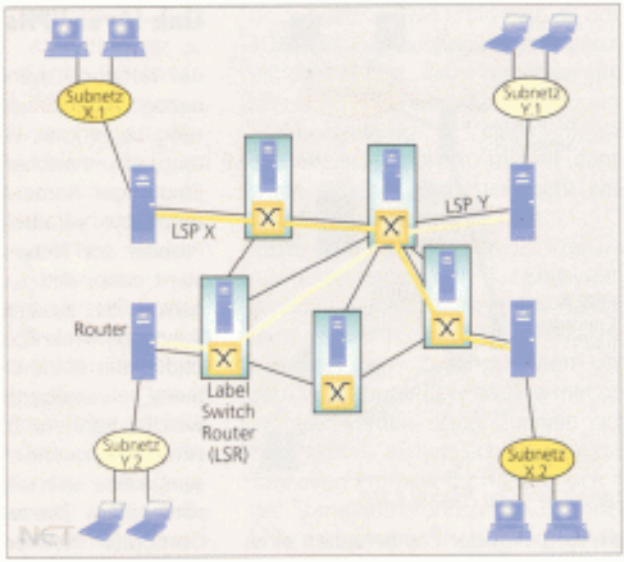
Ein weiterer Vorteil der ATM-basierten Architektur besteht in der einfachen Erweiterung der virtuellen LANs über öffentliche ATM-Netze hinweg. Während in einer lokalen VLAN-Implementierung Campus-ATM-Switches miteinander verbunden sind, können in einer Weitverkehrs-Implementierung die Campus-ATM-Switches mit permanenten VPs (PVPs) über ein öffentliches ATM-WAN miteinander verbunden werden. Über diese PVPs können transparent für das öffentliche Netz zwischen den Proxy-LECs VCs für LANE etabliert werden. Eine solche Architektur erlaubt beispielsweise, daß sich Endsysteme an weit entfernt liegenden Lokationen trotz der großen räumlichen Distanz im selben virtuellen LAN und damit im Fall von IP im gleichen IP-Subnetz befinden können. Auch kann diese ATM-basierte Technik Dienstgüten garantieren, wenn die ATM-Verbindungen mit entsprechenden Dienstgüten aufgebaut werden.

Virtuelle LANs können in der gleichen Art wie reale LANs über Router mit-



Virtuelle LANs mit LAN Emulation

einander verbunden werden. In diesem Fall kann es aber vorkommen, daß zwischen zwei VLANs mehrere Router liegen, die jeweils wieder über VLANs miteinander verbunden sind. Als Erweiterung der LANE hinsichtlich der Kopplung virtueller Netze ist der im ATM Forum entwickelte Standard Multi-Protocol over ATM (MPOA) aufzufassen. Dieser erlaubt auf LANE basierende logische IP-Subnetze zu koppeln und hierbei weitestgehend die Router-Instanzen aus dem Datenpfad zu entfernen. MPOA basiert dabei im wesentlichen auf LANE und dem innerhalb der IETF entwickelten Protokoll NHRP.



VPNs mit Multi-Protocol Label Switching

IEEE 802.1Q

Die IEEE-Organisation hat zur Definition virtueller LANs verschiedene Standardisierungsaktivitäten lanciert. Der Standard 802.1Q legt dabei ein Paketformat fest, das verwendet wird, um Pakete unterschiedlicher virtueller LANs (VLANs) zu kennzeichnen, d.h., Pakete unterschiedlicher VLANs sind mit unterschiedlichen Tags markiert. Dieser Tagging-Mechanismus ermöglicht es, daß zwei Switches über eine beliebige Netztechnologie (ggf. über ein WAN) miteinander verbunden werden können und daß der empfangende Switch die VLAN-Zugehörigkeit des Pakets anhand des Tags erkennen und das Weiterleiten des Pakets auf bestimmte LAN-Ports begrenzen kann. Zusammen mit den VLAN-Tags wurden auch Paketfelder in MAC-Paketen definiert, die zur Anzeige von Verarbeitungsprioritäten verwendet werden. Dies erlaubt Nutzern, verschiedenen MAC-Paketen unterschiedliche Prioritätsstufen zuzuordnen. Die Bedeutung dieser Prioritätsstufen ist im Standard 802.1p festgelegt.

Multi-Protocol Label Switching

Das gleiche Ziel – die Eliminierung der Router-Instanzen aus dem Datenpfad – verfolgen weitere Techniken, die unter dem Namen IP-Switching zusammengefaßt werden können. Diese Technik wird derzeit als Multi-Protocol Label Switching (MPLS) in der IETF standardisiert. MPLS dient dazu, IP-Router direkt über sogenannte Switching-Pfade (LSP – Label Switching Path) zu verbinden, falls es die zugrundeliegende Netztechnologie (z.B. ATM) zuläßt. So ist es beispielsweise möglich, anstatt zwei Router über einen IP-in-IP-Tunnel zu verbinden, einen LSP aufzusetzen.

Zusammenfassung und Ausblick

Es wurden zwei grundlegende Arten VPNs vorgestellt: Link-Layer-VPNs und Network-Layer-VPNs. Beide Arten haben ihre Vor- und Nachteile. Im Zuge der allgemeinen Popularität der Internet-Technologien ist eindeutig ein Trend zu den Network-Layer-VPNs, speziell zu IP-VPNs, zu erkennen.
Heutigen VPNs gemeinsam sind einige Schwachstellen. Meist ist deren Management sehr aufwendig. Einheitliche, plattformunabhängige VPN-Managementsysteme sind kaum verfügbar. Das erweist sich – sowohl für Network-Layer-VPNs als auch für Link-Layer-VPNs – speziell dann als Problem, wenn Netzkomponenten unterschiedlicher Hersteller eingesetzt werden. Integrierte VPN-Managementsysteme sind vor allem erforderlich, um VPNs aus Komponenten unterschiedlicher Hersteller effizient verwalten zu können. Eine Alternative, um den Management-Aufwand eines VPNs zu reduzieren, besteht im Outsourcing des VPN-Managements vom Anwender zum Netzbetreiber.
Ein weiteres – vor allem für IP-VPNs signifikantes – Problem ist die mangelnde Dienstgütenunterstützung in der IP-Protokollarchitektur. Zur Beseitigung dieses Nachteils befindet sich mit dem Differentiated-Services-Ansatz eine vielversprechende Technolgie in der Entwicklung, wobei deren Standardisierung erst seit kurzer Zeit verfolgt wird.
Die Themen VPN-Management und VPN-Dienstgüten mit Differentiated Services sind daher auch Gegenstand von Forschungsarbeiten, die auch am Institut der Autoren intensiv verfolgt werden. Im von den Schweizerischen Nationalfonds (SNF) geförderten Kooperationsprojekt CATI (Charging and Accounting Technologies for the Internet) werden die aufgezeigten Probleme untersucht und Lösungsansätze evaluiert (www.iam.unibe.ch/~rvs/cati).

(bac)

Universität Bern
Institut für Informatik und angewandte Mathematik
Tel: +41 31 631-86 81
Fax: +41 31 631-39 65
mguenter@iam.unibe.ch
braun@iam.unibe.ch
www.iam.unibe.ch/~rvs