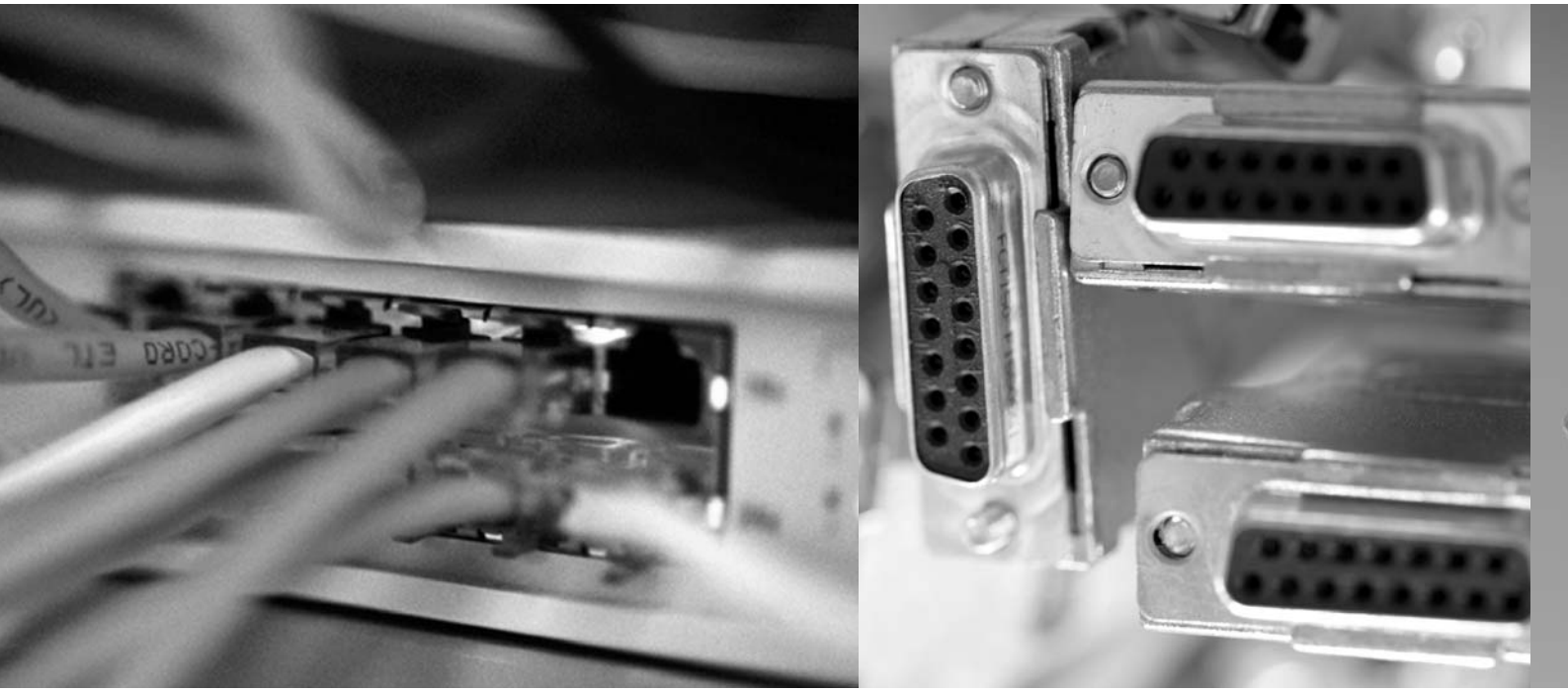
WissenHeute Jg. 58 12/2005



Virtuelle Private Netze – ein Überblick

In den meisten größeren Unternehmen ist es heute üblich, ein eigenes privates Netzwerk, ein so genanntes Virtual Private Network (VPN), zu betreiben. Der vorliegende Beitrag behandelt die Grundlagen, die unterschiedlichen Techniken und die Auswahlkriterien bei der Einrichtung eines VPN sowie deren Einsatzfelder. Ausgehend von einer allgemeinen Begriffsdefinition werden zunächst die Klassen und Einsatzgebiete von VPNs eingeführt. Anschließend werden die wichtigsten Techniken mit deren Vor- und Nachteilen analysiert und gegenüber gestellt sowie grundlegende Konzepte näher erläutert. Der Beitrag schließt mit einem Auszug aus dem aktuellen Lösungsportfolio von T-Systems und T-Com.

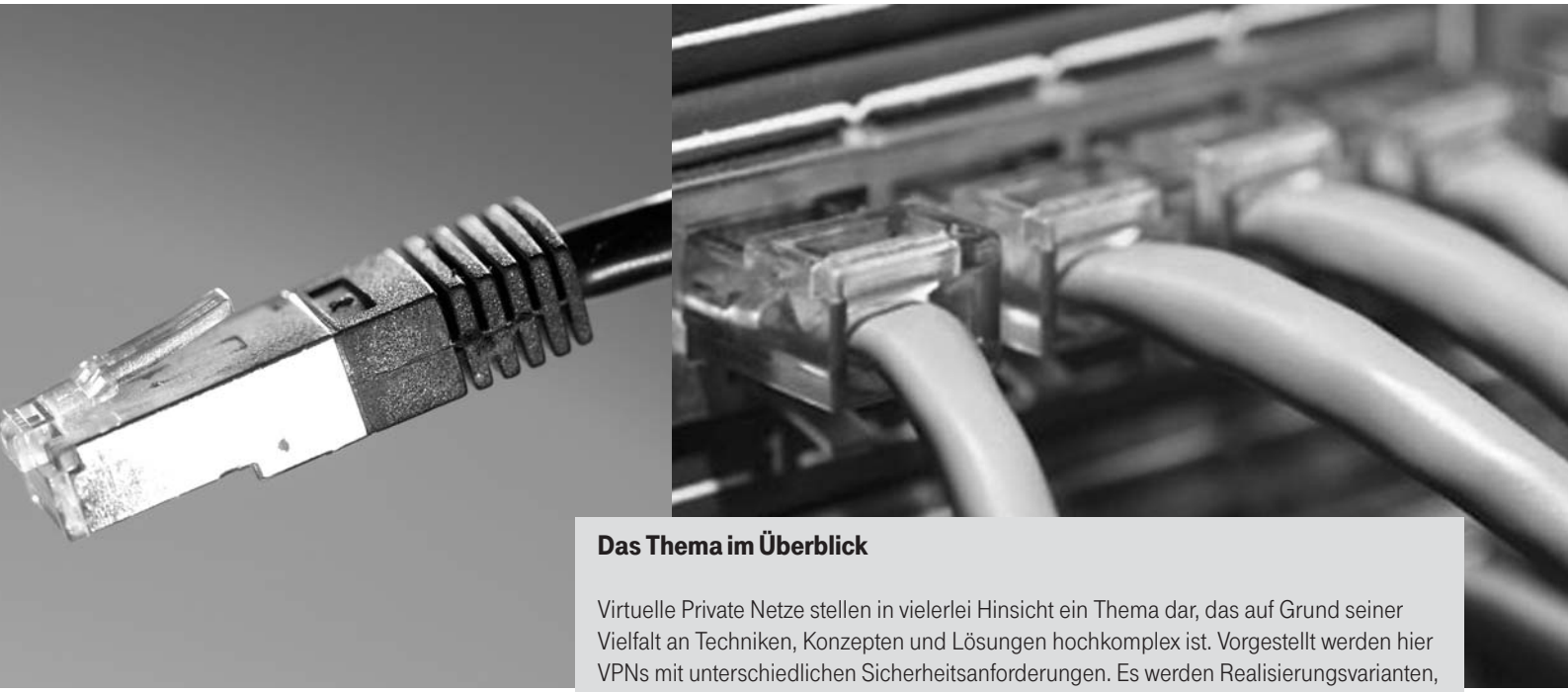
Der Autor

Dipl.-Ing. Stefanus Römer arbeitet als Produktmanager bei T-Mobile, wo er insbesondere für das Produkt Mobile IP VPN und für mobile Intranet-Access-Lösungen zuständig ist.

Einführung

Virtuelle Private Netze werden einerseits eingesetzt, um geographisch verteilte Unternehmensstandorte oder Organisationseinheiten miteinander zu verbinden oder andererseits, um den Mitarbeitern eine kontrollierte Einwahl in das interne Unternehmensnetz (Intranet) zu ermöglichen. Im ersten Anwendungsfall spricht man von Branch-Office-VPN. Einwahllösungen werden dagegen mit Dial-In-VPN bezeichnet. Ein weiterer Spezialfall sind so genannte Extranet-VPNs, die im Gegensatz zu Branch-Office-VPNs dazu genutzt werden, Standorte unterschiedlicher Firmen, wie beispielsweise von Geschäftspartnern oder Kunden, miteinander zu vernetzen (Bild 1). Solche Netze sind „privat“, weil sie nur von dem jeweiligen Unternehmen oder der jeweiligen Organisation selber genutzt werden können bzw. sollen. Sie bieten einen Schutz vor unbefugtem Zugriff, wodurch ein Mitlesen, Manipulieren, Einschleusen von fremden Daten oder ein Angriff durch Attacken verhindert werden soll. Virtuelle Private Netze sind daher durch ein Sicherheitsregelwerk (Policy) definiert, das genau festlegt, wer in welcher Form und unter welchen Bedingungen Zugang zu welchen Ressourcen im jeweiligen Unternehmensnetz haben soll.

Der praktische Nutzen eines VPN liegt darin, dass die genannten Sicherheitsanforderungen bereits auf der unteren Netzebene umgesetzt werden, so dass weder in den Anwendungen noch bei den einzelnen Nutzern derartige Sicherheitsfragen berücksichtigt werden müssen. Ein praktisches Beispiel ist der Ver-



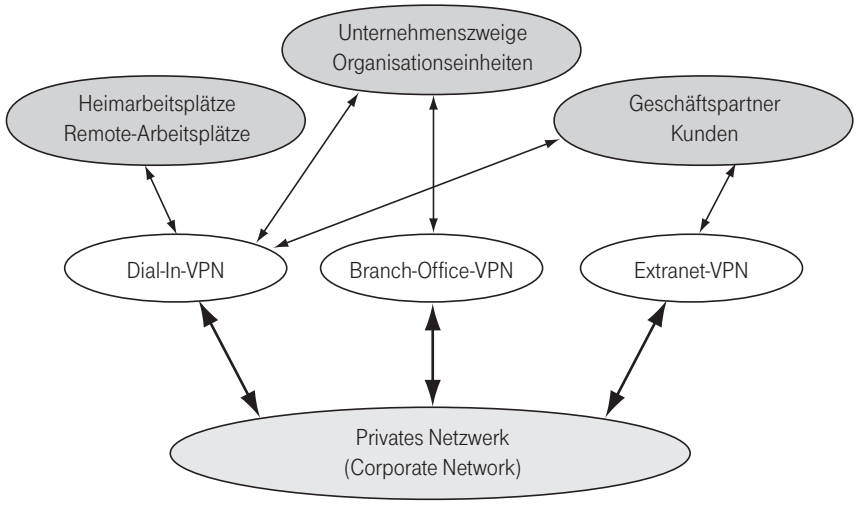
Das Thema im Überblick

Virtuelle Private Netze stellen in vielerlei Hinsicht ein Thema dar, das auf Grund seiner Vielfalt an Techniken, Konzepten und Lösungen hochkomplex ist. Vorgestellt werden hier VPNs mit unterschiedlichen Sicherheitsanforderungen. Es werden Realisierungsvarianten, wie das Overlay- und das Peer-Modell betrachtet und die Techniken ATM, Frame Relay und MPLS sowie Tunnelverfahren erläutert. Der Beitrag vermittelt einen kompakten und verständlichen Zugang zu diesem Themenfeld und bietet somit einen Einstieg zu einer weiteren Vertiefung.

sand vertraulicher Informationen per E-Mail zwischen zwei Unternehmensstandorten. Sofern die Verbindung zwischen diesen Standorten über ein VPN realisiert ist, muss der jeweilige Anwender keine besonderen Verfahrensweisen beachten. Er verschickt die E-Mail, als befände sich der Empfänger im gleichen lokalen Netz. Sind die beiden Standorte jedoch ohne VPN nur über das öffentliche Internet mit einander verbunden, so müssen die Informationen vor dem Versand durch eine aktive Handlung des Benutzers z. B. mit Pretty Good Privacy (PGP)[1] verschlüsselt und signiert werden, um den nötigen Schutz zu gewährleisten.

Ursprünglich wurden standortübergreifende Unternehmensnetze (Corporate Networks = CNs) mit Hilfe von Mietleitungen aufgebaut. Dies hatte zur Folge, dass teure Übertragungskapazitäten ausschließlich für das jeweilige CN vorgehalten wurden, ohne dass sie auch zu jeder Zeit maximal ausgelastet werden konnten. Daher kamen in der Folge vermittelte Datennetze zunächst auf der Basis von X.25, später dann basierend auf Frame Relay (FR) oder Asynchronous Transfer Mode (ATM) zum Einsatz. An Stelle von physikalischen Mietleitungen zwischen den einzelnen Standorten wurden hier virtuelle Kanäle auf der Datenvermittlungsplattform eines Dienstleisters (VPN Service Provider) konfiguriert. Derartige vermittelte Unternehmensnetze sind „virtuell", weil Einrichtungen und Übertragungskapazitäten, die zum Aufbau und zum Betrieb dieser Netze notwendig sind, für

Bild 1 **VPNs in verschiedenen Einsatzfeldern**



VPN Virtual Private Network

[1] **Pretty Good Privacy:** PGP ist ein frei verfügbares Verfahren (Anwendungsprogramm) zur Verschlüsselung von Daten, das sich besonders in der Mailkommunikation durchgesetzt hat. Es handelt sich um ein Public-Key-Verfahren, das mit zwei Schlüsseln arbeitet: einem privaten Schlüssel (Private Key) und einem öffentlichen Schlüssel (Public Key), die beide einmalig gemeinsam generiert werden.

Bild 2 VPN-Protokolle im OSI-Modell

OSI-Schicht	VPN-Protokoll
Transport (Schicht 4)	■ Secure Socket Layer (SSL)
Netzwerk (Schicht 3)	■ IP Security (IPSec) ■ Generic Route Encapsulation (GRE) ■ Multi Protocol Label Switching (MPLS)
Verbindung (Schicht 2)	■ Frame Relay (FR) ■ Asynchronous Transfer Mode (ATM) ■ Layer-2-Tunneling-Protocol (L2TP) ■ Point-to-Point-Tunneling-Protocol (PPTP)
Physik (Schicht 1)	■ Mietleitungen

VPN Virtual Private Network
OSI Open Systems Interconnection
IP Internet Protocol

mehrere VPNs gleichzeitig genutzt werden, ohne die Trennung oder die grundlegende Sicherheit dieser Netze aufzuheben. Mit der Verbreitung des Internets kamen in der Folge zunehmend Internet Protokoll basierte VPNs (IP-VPNs) zum Einsatz, bei denen an Stelle virtueller Verbindungen auf Schicht 2 des OSI-Modells[2] so genannte Tunnelverbindungen eingerichtet werden. Häufig werden hierfür die Tunnelprotokolle Generic Route Encapsulation (GRE)[3] oder Internet Protocol Security (IPSec, Schicht 3 = Layer 3) bzw. Layer-2-Tunneling-Protocol (L2TP) oder Point-to-Point-Tunneling-Protocol (PPTP, Schicht 2) eingesetzt. Sowohl PPTP als auch L2TP werden in der Regel für Dial-In-VPNs eingesetzt. Als Transportplattform wird das Internet oder eine spezielle IP-Plattform eines VPN-Providers genutzt. Darüber hinaus haben sich z. B. mit Secure Sockets Layer (SSL) auf Schicht 4 des OSI-Modells im Internet noch weitere Protokolle etabliert, mit denen sich ein gesicherter Datenaustausch realisieren lässt. Diese Lösungen können jedoch nur für bestimmte Anwendungen (z. B. Browsing) genutzt werden. Bild 2 zeigt eine Übersicht verschiedener VPN-Protokolle und deren Einordnung im OSI-Modell.

Während die verschiedenen Standorte eines Unternehmens oder einer Organisation mit Hilfe von Branch-Office-VPNs miteinander verbunden werden, können mit Hilfe von Dial-In-VPNs für die einzelnen Mitarbeiter eines Unternehmens gesicherte Einwahlmöglichkeiten über verschiedene Zugangswege realisiert werden wie beispielsweise über Modem, ISDN, Digital Subscriber Line (DSL), General Packet Radio Service (GPRS), Wireless Local Area Network (WLAN) oder Universal Mobile Telecommunications System (UMTS). Auch hier wird eine gemeinsame Einwahlplattform eines Providers (z. B. die eines Internet Service Providers) an Stelle einer eigenen Ende-zu-Ende-Einwahllösung über das Telefonnetz genutzt. Die Einwahl wird ebenfalls unter Beachtung eines Sicherheitsregelwerkes überwacht, das festlegt, wie sich die Nutzer authentisieren müssen und welche Vorkehrungen zum Schutz der Authentizität und der Vertraulichkeit der übertragenen Daten zu treffen sind. Häufig kommen hierzu die Übertragungsprotokolle Point-to-Point-Protocol (PPP), PPTP, L2TP und/oder IPSec zum Einsatz. Der Zugang zum Unternehmensnetz wird in der Regel durch die Abfrage von Benutzername und Passwort von einem RADIUS[4]-System oder einem VPN-Gateway kontrolliert. Zunehmend kommen jedoch auch Authentisierungsverfahren wie z. B. Einmalpasswort oder Zertifikate zum Einsatz.

Allgemein lässt sich somit festhalten, dass VPNs durch zwei wesentliche Merkmale gekennzeichnet sind:

- Sie sind durch eine Regelwerk definiert, das genau festlegt, wer in welcher Form und unter welchen Bedingungen Zugang zu dem jeweiligen Unternehmensnetz haben soll und
- sie werden auf einer öffentlichen Datenvermittlungsplattform aufgebaut und teilen sich gemeinsame Einrichtungen und Übertragungswege eines Providers untereinander.

VPN-Klassen

Auf Grund der Vielzahl an unterschiedlichen VPN-Lösungen ist es hilfreich zunächst verschiedene Klassifizierungen vorzunehmen, um einen ersten Überblick zu gewinnen.

Neben der grundlegenden Einteilung nach Branch-Office-VPN und Dial-In-VPN (s. Bild 1) lassen sich weitere Einteilungen treffen:

- Layer-2-VPN gegenüber Layer-3-VPN (nach OSI-Modell)
- Secure VPN gegenüber Trusted VPN
- CPE[5] basierte VPN gegenüber Netzwerk basierte VPN
- Best-Effort-VPN gegenüber QoS[6]-VPN
- Overlay-Modell gegenüber Peer-Modell

Die Unterscheidung in Layer-2-VPNs (L2VPNs) oder Layer-3-VPNs (L3VPNs) hängt davon ab, in welcher Schicht des OSI-Referenzmodells das VPN realisiert wird. Eine Einteilung wichtiger VPN-Protokolle wurde bereits weiter oben vorgenommen (s. Bild 2). Die L2VPNs auf der Basis von Frame Relay oder ATM sind noch immer am weitesten verbreitet. Weil jedoch viele Diensteanbieter neben den klassischen Frame-Relay- oder ATM-Plattformen inzwischen auch IP-basierte Plattformen betreiben, gibt es Bestrebungen, L2VPN-Dienste zukünftig auf einer gemeinsamen Layer-3-Plattform zu realisieren. Bei

[2] **OSI-Modell:** Abk. für Open Systems Interconnection.

[3] **Generic Route Encapsulation:** GRE ist ein von Cisco entwickeltes, weit verbreitetes Tunnelverfahren.

[4] **RADIUS:** Abk. für Remote Authentication Dial-In User Service.

[5] **CPE** steht für Customer Premises Equipment und bezeichnet in der Regel einen Router oder ein VPN-Gateway am Kundenstandort als Übergang zwischen dem internen Netz des Kunden und dem Weitverkehrsnetz des Providers.

[6] **QoS** steht für Quality of Service und bezeichnet die Eigenschaft bestimmter Übertragungsverfahren, wie z. B. ATM, zwischen zwei Endstellen Verbindungen mit einer fest definierten und garantierten Übertragungsqualität (z. B. Mindestbandbreite, maximale Übertragungsverzögerung) bereitzustellen.

den L3VPNs unterscheidet man im Wesentlichen drei Techniken:

- Tunneling (z. B. IPSec, GRE)
- Virtuelle Router
- Multi Protocol Label Switching (MPLS)

Die Klassifizierung nach Secure VPN und Trusted VPN ist eine Einteilung, die vom VPN-Consortium eingeführt wurde[7]. Demnach bezeichnet ein Secure VPN eine VPN-Lösung, die zwischen den jeweiligen Endstellen eine starke Verschlüsselung einsetzt, die es einem „Angreifer", der an irgendeiner Stelle des Übertragungsweges den Datenverkehr aufzeichnet, praktisch unmöglich macht, die Daten zu entschlüsseln und im Klartext zu lesen. Die Sicherheit eines Secure VPN stützt sich einzig auf die eingesetzte Ende-zu-Ende-Verschlüsselung, die von den Endstellen vorgenommen wird. Beispiele für Secure VPNs sind VPN-Lösungen auf der Grundlage von IPSec über das Internet. Demgegenüber hängt bei der Klasse der Trusted VPNs die Sicherheit von der Vertrauenswürdigkeit der Übertragungsplattform des jeweiligen Service Providers ab. Der Kunde verlässt sich hierbei darauf, dass niemand anderes als der Service Provider selbst die Übertragungspfade konfigurieren oder ändern kann und dass niemand anderes auf dem Übertragungsweg Zugang zu den übertragenen Daten hat und somit Daten verändern, löschen oder manipulieren kann. Beispiele für Trusted VPNs sind VPN-Lösungen der Deutschen Telekom auf der Grundlage von ATM, Frame Relay oder MPLS (Tabelle 1).

Tabelle 1 **VPNs der Deutschen Telekom**

Produkt	Klasse	Kurzbeschreibung
Secure IP	Secure VPN	Die Secure IP Solution ist eine umfassende, modular aufgebaute und somit erweiterbare VPN-Systemlösung für mittlere und große Netzwerke. IPSec basierte VPN-Lösung einschließlich Projektierung, Management und Service; Branch-Office-VPN und Dial-In-VPN.
Business LAN	Secure VPN VPN	IPSec basierte VPN-Lösung inklusive CPE-Management und -Service für mittelständische Unternehmen zur Standortvernetzung mit T-DSL Anschlüssen; Unterstützung von dynamischen IP-Adressen mit Hilfe von Dynamic VPN[8]; Branch-Office-VPN; Dial-In mit GPRS und UMTS über Mobile IP VPN Basic (siehe unten).
Secure VPN	Secure VPN	IPSec-basierte VPN-Lösung von T-Online einschließlich Projektierung, Management und Service; Branch-Office-VPN und Dial-In-VPN.
directVPN	Secure VPN	Einfache VPN-Lösung für kleine Unternehmen. Mit Hilfe eines speziellen Client können über jeden beliebigen Internet-Zugang verschiedene Rechner zeitweise miteinander verbunden werden. Vor einer Datenübertragung meldet sich der Benutzer/der Client an einem Kommunikationsserver von T-Online an. Anschließend kann der Benutzer durch einfaches Anklicken eines anderen aktiven Benutzers eine gesicherte Verbindung aufbauen. Die Daten werden verschlüsselt und über das Internet getunnelt.
IntraSelect Familie	Trusted VPN	Lösungsportfolio auf der Basis von Frame Relay, ATM, IP-Tunneling und MPLS inklusive CPE-Management und -Service. **Varianten:** ■ Variante Classic[9]: FR, ATM ■ Variante ATM: ATM ■ Variante MPLS: MPLS Besonderheit: garantierte Übertragungsklassen und Zuordnung zu anwendungsspezifischen Qualitätsklassen; Branch-Office-VPN sowie Dial-In-VPN mit weltweiter Einwahl und mobilen Zugängen über GPRS/UMTS (s. Mobile IP VPN).
Mobile IP VPN	Trusted VPN	Sichere mobile Einwahl über GPRS und UMTS in Unternehmensnetze in Kombination mit der IntraSelect-Familie bzw. Business-LAN-Lösungen; Geschlossene Benutzergruppe im Mobilfunknetz[10]; private Netzkennung mit direktem Übergang zu IntraSelect.

Bei der Differenzierung nach CPE basierten VPNs oder Netzwerk basierten VPNs geht es um die Frage, in welcher Komponente des Netzes die VPN-Policy hinterlegt und umgesetzt wird (Bild 3). Man spricht in diesem Zusammenhang vom Service Creation Point. Grundsätzlich gibt es hier zwei Möglichkeiten:

- Entweder ist die Konfiguration der VPN-Zugehörigkeit in der CPE, z. B. einem Anschlussrouter in den Räumen des Kunden zu finden oder
- sie wird am Provider Edge, dem jeweiligen Zugangsrouter zur VPN-Plattform des Providers, vorgenommen.

Im ersten Fall spricht man vom CPE basierten VPN, im zweiten Fall wird die Lösung Netzwerk basiertes VPN genannt. Virtuelle Private Netze, die auf CPE basieren, können ohne besondere Mitwirkung des Service Providers vom Kunden selbst realisiert werden. Bei Netzwerk basierten VPNs hingegen muss die CPE lediglich IP-Routing-Funktionen unterstützen.

Die Klassifizierung nach Best-Effort-VPN gegenüber QoS-VPN betrifft die Übertragungs-

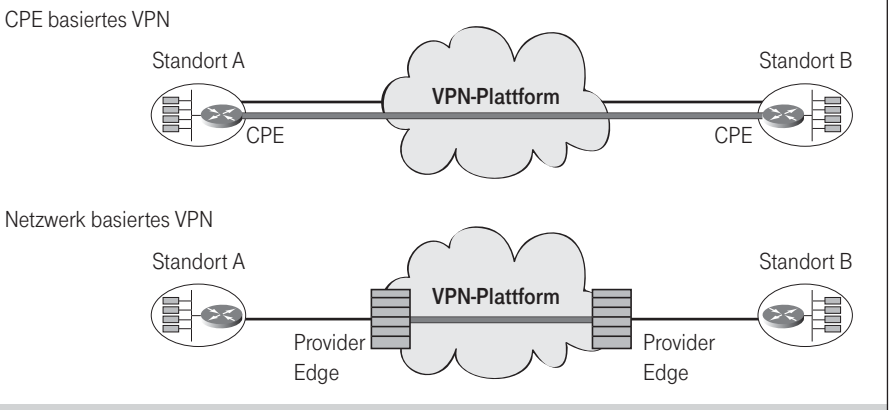
[7] Die Definitionen der unterschiedlichen VPN-Technologien lehnen sich an den im Juli 2004 formulierten Vorschlag des inzwischen entstandenen VPN-Consortium an (http://www.vpnc.org/).

[8] Siehe hierzu den Beitrag „Fernzugriff auf Computernetze mit DSL-Anschluss", WissenHeute 5/2004, S. 256 ff.

[9] **Variante Classic:** Das Vorgängerprodukt hatte den Produktnamen LAN to LAN. Siehe hierzu den Beitrag „Das Produkt LAN to LAN", Unterrichtsblätter 2/2000, S. 82 ff.

[10] Siehe hierzu den Beitrag „Mit GPRS ins Intranet – Das Produkt LAN to LAN GPRS Access", Unterrichtsblätter 3/2001, S. 168 ff.

Bild 3 CPE basiertes VPN und Netzwerk basiertes VPN



CPE Customer Premises Equipment VPN Virtual Private Network

qualität zwischen den einzelnen Standorten eines VPN. Unterschiedliche Anwendungen haben verschiedene Anforderungen an ein Übertragungsnetz. So stellt z. B. ein File Transfer hohe Anforderungen in Bezug auf die Bandbreite und die Netzstabilität. Die Übertragungsverzögerung ist dabei eher unkritisch. Echtzeitanwendungen wie Video-Conferencing oder Voice over Internet Protocol (VoIP) erfordern demgegenüber eine geringe und stabile Verzögerung (Delay[11]). Um diesen unterschiedlichen Anforderungen Rechnung zu tragen, kommen bei der Realisierung von VPNs Übertragungstechniken wie z. B. ATM, Frame Relay oder MPLS zum Einsatz, die die geforderten Qualitäten z. B. Mindestbandbreite, konstantes Delay oder Jitter[12] zwischen zwei Standorten Ende-zu-Ende einhalten können. Zudem müssen die jeweiligen Endstellen und Abschlussrouter so konfiguriert werden, dass diese unterschiedlichen Übertragungsklassen abhängig von der jeweils genutzten Anwendung bereitgestellt werden und somit jede Anwendung die Behandlung erfährt, die sie für eine einwandfreie Funktionsweise benötigt (s. Tabelle 1).

Von einem Best-Effort-VPN ist hingegen dann die Rede, wenn sich auf Grund der gewählten Übertragungstechnik oder der genutzten Datenplattform (z. B. dem Internet) keine Ende-zu-Ende-Qualitätszusagen machen lassen und die Übertragungsressourcen nicht fest für eine Verbindung reserviert werden können.

Von grundlegender Bedeutung ist die Unterscheidung nach Overlay- und Peer-Modell, welche im nachfolgenden Abschnitt daher ausführlich behandelt wird.

Overlay-Modell und Peer-Modell

Die meisten VPNs sind noch immer nach dem so genannten Overlay-Modell (Bild 4 und 5) aufgebaut. Dieses Modell bezeichnet eine Realisierungsvariante, bei der die einzelnen Anschlussrouter in den verschiedenen Standorten eines Unternehmens mit Punkt-zu-Punkt-Verbindungen miteinander vernetzt werden. Hierzu können entweder Mietleitungen oder virtuelle Verbindungen auf der Grundlage von ATM oder Frame Relay als Übertragungsmedium genutzt werden. Virtuelle Verbindungen werden auf Schicht 2 (Layer 2) des OSI-Modells realisiert. Sie werden eingesetzt, um IP-Verkehr zwischen den Anschlussroutern der einzelnen Standorte zu übertragen.

Das Overlay-Modell erfordert besondere Kenntnisse für die Planung, Konzeption und den Betrieb von Router-Netzen sowie die Konfiguration von virtuellen Kanälen auf Basis von ATM- oder Frame Relay. Diese Kenntnisse sind jedoch in vielen Unternehmen nicht vorhanden. Daher bieten fast alle Service Provider so genannte Managed Services an, bei denen die einzelnen Anschlussrouter des VPN zentral vom jeweiligen Service Provider konfiguriert und überwacht werden.

Ein Nachteil des Overlay-Modells ist die schlechte Skalierbarkeit. Hierunter versteht man, dass der Aufwand für die Anschaltung zusätzlicher Standorte überproportional mit der Anzahl bereits angeschalteter Standorte zunimmt. Dies gilt insbesondere für VPNs mit einem hohen Vermaschungsgrad[13]. Bei vollvermaschten Netzen gibt es beispielsweise insgesamt

$$n \cdot \frac{n-1}{2}$$

Verbindungen. Die Zahl der direkten Verbindungen steigt demnach quadratisch mit der Anzahl n der Standorte. Bei Hinzunahme eines weiteren Standorts muss in diesem Beispiel die Konfiguration aller anderen Anschlussrouter angepasst werden, zu denen eine direkte Verbindung bestehen soll. Nicht nur der Aufwand für die Konfiguration und somit die Fehleranfälligkeit solcher Netze steigt überproportional, sondern auch die betrieblichen Kosten sowie die durchschnitt-

[11] **Delay:** Verzögerungs- oder Wartezeit. Zeitspanne, um die ein Ereignis verzerrt oder verzögert wird, beispielsweise die Zeit, die vergeht, bis eine abgesandte Information vom Zielsystem empfangen wird.

[12] **Jitter:** Weitgehend zufallsbestimmte Schwankungen der Flanken eines realen Datensignals um die Sollzeit des Nulldurchganges.

[13] Der **Vermaschungsgrad** gibt an, mit wie vielen Gegenstellen die einzelnen Standorte durchschnittlich verbunden sind. Bei sternförmigen Netzen, bei denen die Unternehmenszentrale jeweils nur mit den einzelnen Außenstellen verbunden ist, beträgt der Vermaschungsgrad 1. Bei vollvermaschten Netzen mit n Standorten, wo zwischen allen Standorten jeweils paarweise eine direkte Verbindung besteht, entspricht der Vermaschungsgrad $(n-1)$.

Bild 4 Overlay-Modell: sternförmiges Netz

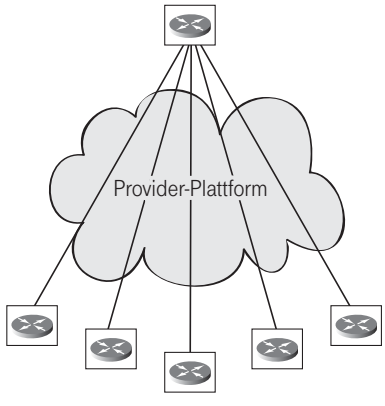
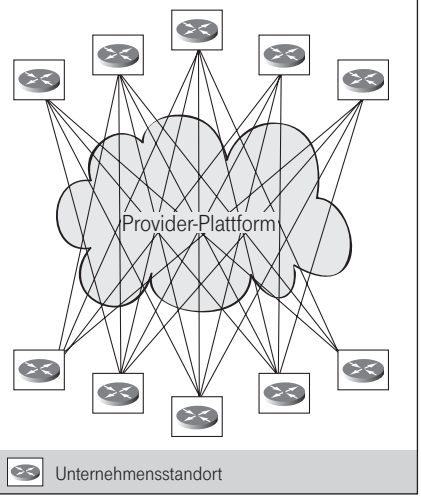


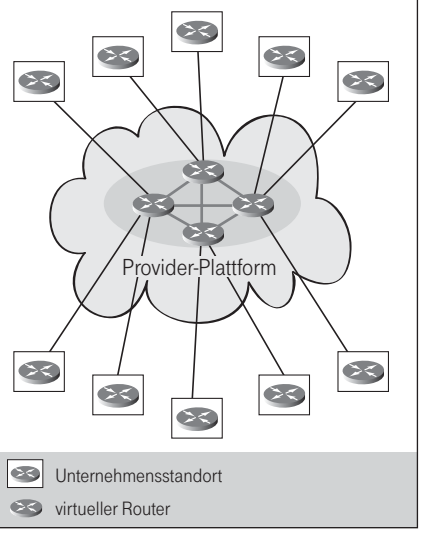
Bild 5 **Overlay-Modell: Netz mit hohem Vermaschungsgrad**



liche Entstörzeit im Fehlerfalle. Sehr große Netze sind somit nur schwer zu verwalten.

Um die Zahl der direkten Verbindungen und den betrieblichen Aufwand sowie die Fehleranfälligkeit zu reduzieren, betreiben manche Service Provider auf ihrer Plattform kundenspezifische Aggregationsrouter[14] oder virtuelle Router[15] (Bild 6). Hiermit wird die Zahl der Verbindungen von $n \cdot \frac{n-1}{2}$ auf n reduziert. Die Komplexität verringert sich dabei im gleichen Maße. Ein weiterer Vorteil dieses Konzeptes ist es, dass gerade bei den häufig zu findenden sternförmigen Netzen, bei denen die Außenstellen jeweils nur mit der Zentrale verbunden sind, nicht der gesamte

Bild 6 **Vollvermaschtes Any-to-Any Netz mit virtuellen Routern**



Datenverkehr zwischen den Außenstellen über die Zentrale geführt werden muss. Dies verringert den Bandbreitenbedarf am zentralen Anschluss und erhöht zudem die Ausfallsicherheit.

Alternativ zur Verwendung von virtuellen Verbindungen auf der Grundlage von FR oder ATM können auch Tunnelverbindungen, z. B. mit IPSec oder GRE genutzt werden. Mit diesen Tunnelverfahren werden wie im Falle von FR oder ATM ebenfalls Punkt-zu-Punkt-Verbindungen realisiert. Der Unterschied liegt darin, dass die Verbindungen hierbei auf Schicht 3 des OSI-Modells über eine IP-Plattform (z. B. das Internet) realisiert werden. An dem zu Grunde liegenden Overlay-Modell und der oben beschriebenen Einschränkung ändert sich jedoch nichts. Vielmehr ergeben sich hierdurch weitere Besonderheiten: Zum einen erhöhen sich die Komplexität und die Kosten, wenn z. B. ein aufwendiges Schlüsselmanagement genutzt wird. Zum anderen bietet dieses Übertragungsverfahren keine definierten Übertragungsqualitäten (QoS). Die Übertragung geschieht nach dem so genannten Best-Effort-Prinzip. Feste Übertragungsbandbreiten oder konstante Übertragungsverzögerungen (Delay), wie sie beispielsweise für die Sprachübertragung (VoIP) benötigt werden, können hiermit nicht garantiert werden. Demgegenüber besteht der Vorteil, dass sich z. B. mit Hilfe von IPSec sehr leicht weltweite Verbindungen über das Internet realisieren lassen.

Die Nutzung des Internets als Datenplattform wirft jedoch zusätzliche Sicherheitsfragen auf. Die Zahl der Angriffe aus dem Internet nimmt weiterhin zu. Für die Unternehmen ist es erforderlich, in immer kürzeren Zeitabständen auf neue Bedrohungen (z. B. Würmer oder Viren) zu reagieren und neue Softwarestände (Patches) in ihre Systeme einzuspielen, wodurch entsprechend der Betreuungsaufwand zunimmt. Hinzu kommt, dass zum

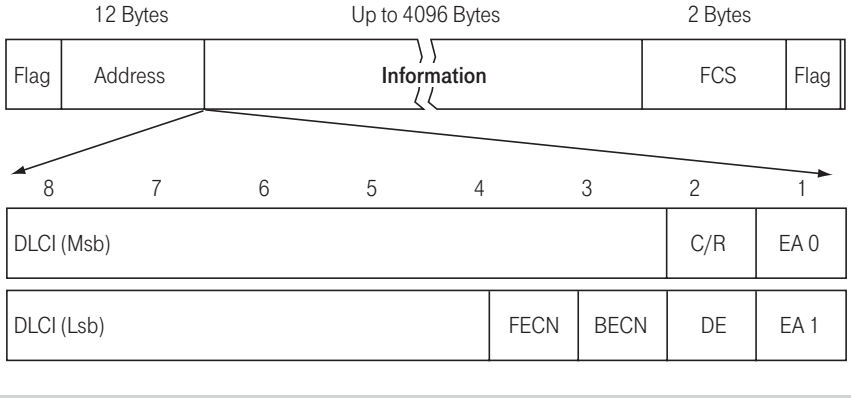
[14] Ein **Aggregationsrouter** ist ein Routertyp, der in den Netzknoten des Internets den Netzzugangspunkt für die Kunden eines Internet Service Providers darstellt. Mit den privaten Netzen dieser Kunden (Kundenroutern) ist der Aggregationsrouter auf der physikalischen Ebene über digitale Mietleitungen oder über leitungsvermittelte Verbindungen permanent oder fallweise verbunden.

[15] Ein **virtueller Router** verhält sich wie ein physikalisch vorhandener Router. Der einzige Unterschied besteht darin, dass er sich die Hardware-Ressourcen, also den Speicher, die CPU und die Übertragungskapazitäten mit anderen virtuellen Routern teilt.

Verwendete Abkürzungen

3DES	Triple Data Encryption Standard
AAL	ATM Adaption Layer
AES	Advanced Encryption Standard
ATM	Asynchronous Transfer Mode
BECN	Backward Explicit Congestion Notification
CE	Customer Edge
CPE	Customer Premises Equipment
CN	Corporate Network
DE	Data Event Block
DES	Data Encryption Standard
DLCI	Data Link Connection Identifier
DSL	Digital Subscriber Line
EA	Extended Address
FCS	Frame Checking Sequence
FECN	Forward Explicit Congestion Notification
FR	Frame Relay
GPRS	General Packet Radio Service
GRE	Generic Route Encapsulation
IP	Internet Protocol
IPSec	IP Security
LAN	Local Area Network
L2TP	Layer-2-Tunneling-Protocol
L2VPN	Layer-2-VPN
L3VPN	Layer-3-VPN
LER	Label Edge Router
LSP	Label Switched Path
LSR	Label Switch Router
MD5	Message Digest 5
MPLS	Multi Protocol Label Switching
MBS	Maximum Burst Size
OSI	Open Systems Interconnection
PAD	Padding-Byte (vom engl. padding = Füllung)
PCR	Peak Cell Rate
PE	Provider Edge
PGP	Pretty Good Privacy
PPP	Point-to-Point-Protocol
PPTP	Point-to-Point-Tunnelling-Protocol
QoS	Quality of Service
RADIUS	Remote Access Dial-In User Service
RFC	Request for Comments
SCR	Sustainable Cell Rate
SHA1	Secure Hash Algorithm 1
SSL	Secure Sockets Layer
UMTS	Universal Mobile Telecommunications System
VPN	Virtual Private Network
VRF	VPN Routing and Forwarding
WLAN	Wireless Local Area Network

Bild 7 Frame Relay Rahmenformat



BECN	Backward Explicit Congestion Notification	FCS	Frame Checking Sequence
C/R	Command Response Identification	FECN	Forward Explicit Congestion Notification
DLCI	Data Link Connection Indentifier	Lsb	Least Significant Byte
DE	Data Event Block	Msb	Most Significant Byte
EA	Extended Address		

Schutz des eigenen Netzes immer mehr Spezialsysteme wie Firewalls, Intrusion Detection Systeme (IDS)[16] oder Virenscanner eingesetzt werden müssen.

Der entscheidende Nachteil des Overlay-Modells ist seine eingeschränkte Skalierbarkeit für große Netze mit einem hohen Vermaschungsgrad. Durch die Nutzung von virtuellen Routern auf der Provider-Plattform kann dieser Nachteil teilweise kompensiert werden, wenngleich das grundlegende Modell erhalten bleibt und das Problem der Skalierbarkeit hiermit nicht grundsätzlich gelöst werden kann.

Eine weitere Möglichkeit ist das **Peer-Modell**. Die Bezeichnung Peer-Modell bringt zum Ausdruck, dass die IP-Gegenstelle des Kundenrouters (Customer Edge = CE) nicht wie im Falle des Overlay-Modells ein Kundenrouter an einem anderen Unternehmensstandort ist, sondern ein Zugangsrouter (Provider Edge = PE) des Service Providers auf der VPN-Plattform selbst. Mit Hilfe des Peer-Modells kann ein Service Provider eine weit größere Anzahl von verschiedenen VPNs unterschiedlicher Größe und Komplexität mit geringen Kosten betreiben.

VPN-Basistechniken

Neben den unterschiedlichen VPN-Klassen und Konzepten sind auch die VPN-Techniken wichtig. Von besonderer Bedeutung sind hierbei die Übertragungstechniken MPLS und IPSec. Diese Techniken werden zukünftig eine immer wichtigere Rolle im Bereich der Branch-Office-VPNs einnehmen, wobei MPLS vermutlich die etablierten Übertragungstechniken wie Frame Relay oder ATM im Bereich der VPN-Lösungen schrittweise ablösen wird. Bereits heute ist IPSec im Bereich der Internet-VPNs und Secure VPNs die am häufigsten genutzte Technik.

Frame Relay

Frame Relay (ITU-T Q.022) ist ein paket- und verbindungsorientiertes Datenübertragungsverfahren und gilt als Weiterentwicklung von X.25 (Datex-P). Durch den Verzicht auf Übertragungssicherungsverfahren auf Schicht 3 des OSI-Modells können deutlich höhere Durchsatzraten und Bandbreiten realisiert werden als mit der Vorgängertechnik.

Genauso wie X.25 arbeitet Frame Relay ebenfalls verbindungsorientiert. Zwischen den einzelnen Anschlüssen werden feste virtuelle Verbindungen eingerichtet, die festlegen, über welchen Weg die einzelnen Datenpakete durch die Plattform zum jeweiligen Ziel gelangen. Die Nutzdaten (z. B. einzelne IP-Pakete) werden dabei in einen Rahmen (Frame) verpackt. Ein Frame hat eine variable Länge und besteht aus vorangestellten Informationselementen zur Verbindungssteuerung (Header) sowie aus angehängten Informationselementen (Trailer), die das jeweilige Rahmenende markieren. Bild 7 zeigt den Rahmen des Frame-Relay-Protokolls. Jeder einzelnen Frame enthält im Header eine Kanalnummer, den so genannten Data Link Connection Identifier (DLCI), anhand dessen er entlang eines „virtuellen Pfades" durch die Datenplattform vermittelt wird. Die einzelnen Rahmen einer virtuellen Verbindung nehmen dabei stets den gleichen Übertragungsweg durch die Datenplattform. Die Verbindung ist insofern wie bei einer Mietleitung durch den Provider fest vorgegeben, wenngleich sie auf Grund der Kanalnummer nur virtuell besteht. Eine wesentliche Eigenschaft von Frame Relay ist es, dass sich mit dieser Technik für jede Verbindung eine garantierte Übertragungsbandbreite (Commited Information Rate = CIR) fest vergeben lässt. Diese Eigenschaft macht Frame Relay zu einer QoS-Technik, mit deren Hilfe sich QoS-VPNs realisieren lassen.

ATM

Asynchronous Transfer Mode[17] (ITU-T I.361 bis ITU-T I.366) ist wie Frame Relay ein paket- und verbindungsorientiertes Übertragungsverfahren. Die einzelnen Pakete werden ATM-Zellen genannt. Im Gegensatz zu Frame Relay haben sie eine feste Größe von nur 53 Byte und bestehen aus einem Header von insgesamt 5 Byte und einem Nutzdatenfeld von 48 Byte. Ein Trailer wie bei Frame Relay ist auf Grund der festen Größe nicht notwendig. Wegen der verbindungsorientierten Datenübertragung besteht zwischen zwei Endstellen jeweils eine feste virtuelle Verbindung oder eine virtuelle Wählverbindung. Der Asynchronous Transfer Mode zeichnet sich gegenüber Frame Relay im Wesentlichen durch höhere Übertragungsraten sowie weiter differenzierte Übertragungsqualitäten in

[16] **Intrusion Detection Systeme:** vom lat. intrusio (Einschließung). Im Bereich der IT-Sicherheit die Gesamtheit von Werkzeugen (Tools), die den vollständigen Prozess der Intrusion Detection (ID) von der Ereigniserkennung über die Auswertung bis hin zur Eskalation und Dokumentation von Ereignissen unterstützen. Unter Intrusion Detection (auf deutsch etwa „Einbruchssicherung") versteht man in diesem Zusammenhang die aktive Überwachung von Computersystemen und/oder -netzen mit dem Ziel der Erkennung von Angriffen und Missbrauch.

[17] Siehe hierzu den Beitrag „ATM – Kommunikationstechnologie der Zukunft", Unterrichtsblätter 10/1998, S. 492 ff. oder http://www.atmforum.com.

Tabelle 2 Verkehrskategorien bei ATM

Verkehrskategorie	Beschreibung
Constant Bit Rate (CBR)	Die Verkehrskategorie CBR wird im Allgemeinen zur Übertragung von isochronem, zeitsensitiven Verkehr wie von Sprache oder Video genutzt. Bei CBR werden die einzelnen Zellen mit höchster Priorität und minimaler Übertragungsverzögerung übertragen.
non-real-time Variable Bit Rate (nrt-VBR)	Die Verkehrskategorie nrt-VBR ist definiert durch eine Spitzenzellrate (Peak Cell Rate = PCR; Maximum Burst Size = MBS) sowie einer garantierten durchschnittlichen Zellrate (Sustainable Cell Rate = SCR) für nicht-synchronen Verkehr konzipiert wie z. B. für Anwendungen mit variablem oder burstartigen Verkehrsverhalten. Sie eignet sich daher für die Übertragung von paketorientierten Daten, d. h. für Anwendungen, für die keine Bitsynchronität erforderlich ist. In der Regel wird der nrt-VBR-Service genutzt, um Informationen zwischen LANs über ATM zu transportieren.
Unspecified Bitrate (UBR)	Die Verkehrskategorie UBR ist definiert durch eine Spitzenzellrate PCR in Sende- und Empfangsrichtung und speziell für Anwendungen mit stark burstartigem, nicht-synchronen Verhalten geeignet, bei denen keine oder nur geringe Anforderungen hinsichtlich der Zellenverzögerung und der Zellverzögerungsschwankungen bestehen. Diese Verkehrskategorie eignet sich besonders für Anwendungen, deren Verkehrsverhalten nicht oder nur sehr ungenau vorhersagbar ist (z. B. Internet-Anwendungen). Für die Verkehrskategorie UBR werden dem Anwender keine Güteparameter garantiert.

Bezug auf die Bandbreite, die Übertragungsverzögerung und den Zellverlust aus. Auf Grund der zur Verfügung stehenden Übertragungsqualitäten und Verkehrskategorien ist ATM universell sowohl für isochronen[18] (z. B. Sprache) als auch burstartigen Verkehr (z. B. Local Area Network-[LAN-]Kopplung) einsetzbar. Die zur Verfügung stehenden Verkehrskategorien sind in Tabelle 2 aufgeführt.

Um die Nutzdaten an die Größe der ATM-Zellen anzupassen, ist innerhalb des OSI-Layers 2 eine zusätzliche Umsetzungsfunktion erforderlich, die als ATM Adaption Layer (AAL) bezeichnet wird. Je nach gewählter Verkehrskategorie und Anwendung stehen hier fünf verschiedene AALs zur Wahl. Der wichtigste Adaptionslayer ist AAL5 (Bild 8), der für typischen LAN-Verkehr eingesetzt wird und somit im Bereich der Branch-Office-VPN am häufigsten genutzt wird.

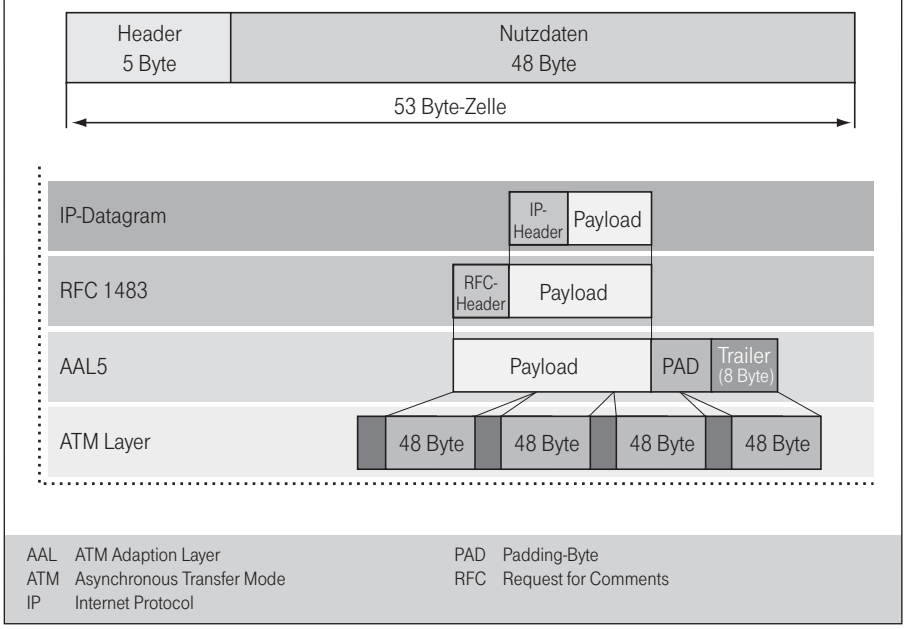
MPLS

Im Gegensatz zu ATM und FR ist MPLS[19] eine Technik, mit deren Hilfe VPNs nach dem bekannten Peer-Modell realisiert werden. Das Multi Protocol Label Switching (RFC 2547) vereint die Vorteile der schnellen ATM-Vermittlungstechnik mit der Flexibilität von IP-Routing. Es bietet die Möglichkeit viele VPNs mit identischen privaten IP-Adressbereichen ohne Adressvermischung transparent über eine MPLS-Plattform zu vermitteln. Die Einrichtung eines VPN wird vollständig im Zugangsrouter zur MPLS-Plattform, dem so genannten Label Edge Router (LER), und nicht wie bei ATM- oder Frame Relay basierten VPNs im Kundenrouter (CPE), vorgenommen. Die Vermittlung über die MPLS-Plattform erfolgt durch Label Switch Router (LSR), die für den VPN-Verkehr vollkommen transparent sind. Dies bedeutet, dass die LSR keine Unterscheidung der einzelnen VPNs treffen und jeglichen Verkehr in gleicher Weise bearbeiten. Dadurch ist eine gute Skalierbarkeit zur Unterstützung vieler VPNs auf der MPLS-Plattform gewährleistet. Routing-Funktionalitäten werden lediglich in den Zugangsknoten der MPLS-Plattform, den LER, vorkommen. Der Verkehr wird innerhalb der Plattform ähnlich wie bei Frame Relay anhand einer Pfadkennung, dem so genannten Label, vermittelt oder „geswitcht". Das Label ist daher vergleichbar mit der Kanalkennung DLCI im

[18] **Isochrone Anwendungen:** Diese Anwendungsklasse erfordert ein sehr geringes Delay sowie eine sehr geringe Delay-Varianz (Jitter).

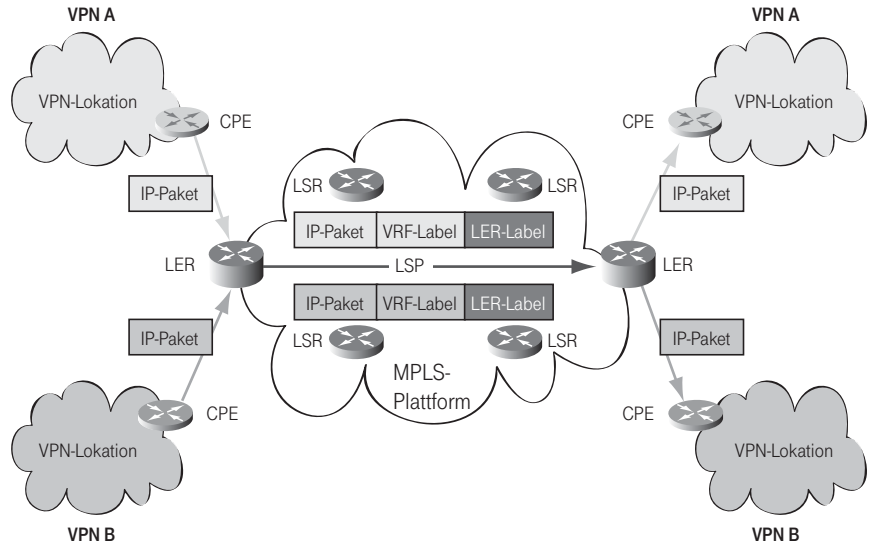
[19] Siehe hierzu den Beitrag „ Multimediaverbindungen über Internet Protokolle – Teil 5", Unterrichtsblätter 6/2002, S. 292 ff.

Bild 8 ATM Adaption Layer (AAL5)



AAL ATM Adaption Layer
ATM Asynchronous Transfer Mode
IP Internet Protocol
PAD Padding-Byte
RFC Request for Comments

Bild 9 Multi Protocol Label Switching (MPLS)



CPE Customer Premises Equipment
IP Internet Protocol
LER Label Edge Router
LSP Label Switched Path
LSR Label Switching Router
VPN Virtual Private Network
VRF VPN Rooting and Forwarding

Falle von Frame Relay mit dem einzigen Unterschied, dass dieses Label nicht fest vorkonfiguriert ist, sondern sich dynamisch mit Hilfe der Routing-Funktionalität der LER ergibt. Somit lässt sich die Flexibilität des IP-Routing mit der Übertragungseffizienz des Layer-2-Switching kombinieren (Bild 9).

Getunnelte Übertragungsverfahren (Tunneling)

Tunnelverfahren werden eingesetzt, um VPNs über IP-Netze zu realisieren. In diesem Falle spricht man von einem IP-Tunnel. Ein IP-Tunnel wird dadurch realisiert, dass die Protokolldaten von Layer-2- (z. B. PPP) und Layer-3-Protokollen (z. B. IP) in IP-Pakete eingepackt, an eine feste Zieladresse oder den Tunnelendpunkt übertragen und dort entsprechend wieder ausgepackt werden (Bild 10). Mit diesem Verfahren können beispielsweise lokale Netze mit privaten IP-Adressräumen über das öffentliche Internet miteinander vernetzt werden, ohne dass es zu Adresskonflikten kommt. Die ursprünglichen IP-Pakete mit dem originalen IP-Header enthalten private IP-Adressen aus den lokalen Netzen. Diese werden in ein neues „äußeres" IP-Paket mit offiziellen IP-Adressen aus dem Adressraum der VPN-Plattform des Service Providers eingepackt und am Zielort wieder ausgepackt. Dabei sind im Internet nur die offiziellen IP-Adressen, nicht aber die privaten Adressen, sichtbar. Ein häufig genutztes Verfahren, das im Bereich der Branch-Office-VPNs Anwendung findet, ist das im RFC 2784 spezifizierte Tunnelprotokoll GRE. Generic Route Encapsulation ist ein einfaches Tunnelverfahren, bei dem den ursprünglichen IP-Paketen aus dem internen Unternehmensnetz ein GRE-Header von 8 Byte und ein neuer IP-Header mit einer externen IP-Adresse vorangestellt wird. Mit Hilfe von GRE werden die inneren IP-Pakete lediglich getunnelt. Eine Verschlüsselung wird nicht durchgeführt.

Ebenfalls weit verbreitet sind die Layer-2-Tunneling-Verfahren PPTP und L2TP, mit deren Hilfe sich Dial-In-VPN realisieren lassen. Im Gegensatz zu dem Layer-3-Tunneling-Verfahren IPSec (RFC 2401) werden die Nutzdaten bei der Übertragung mit PPTP oder L2TP ebenfalls unverschlüsselt und ohne Manipulationsschutz übertragen. Das PPTP ist eine Erweiterung von PPP und wird häufig verwendet, weil es fester Bestandteil von Windows ist. Das L2TP erlaubt gegenüber PPTP zudem den Aufbau und den gleichzeitigen Betrieb paralleler Tunnelsitzungen (Sessions) zu unterschiedlichen Gegenstellen.

Auf Grund des unzureichenden Schutzes bei PPTP und L2TP wurden mit IPSec verschiedene Verfahren entwickelt, um die Unversehrtheit (Integrität) und die Vertraulichkeit (Privacy) der Nutzdaten sowie die Echtheit (Authentizität) von Absender und Empfänger zu gewährleisten. Hierzu können wahlweise verschiedene Sicherheitsverfahren wie die Hash-Algorithmen Message Digest 5 (MD5)[20] oder Secure Hash Algorithm 1 (SHA1)[21] zur Gewährleistung der Datenintegrität und bewährte Verschlüsselungsverfahren wie Data Encryption Standard (DES)[22], Triple DES (3DES) oder Advanced Encryption Standard (AES)[23] eingesetzt werden. Internet Protocol Security besteht somit nicht aus einem einzigen Protokoll, sondern stellt vielmehr eine Sammlung verschiedener Protokolle und Verfahren bereit, die in unterschiedlichster Kombination eingesetzt werden können. Trotz dieser Vielfalt haben sich dennoch bestimmte Standardkonfigurationen bewährt, die in den meisten Fällen zur Anwendung kommen. IPSec ist inzwischen neben MPLS die wichtigste VPN-Technik und hat sich im Bereich der Internet-VPNs zum beherrschenden Standard entwickelt.

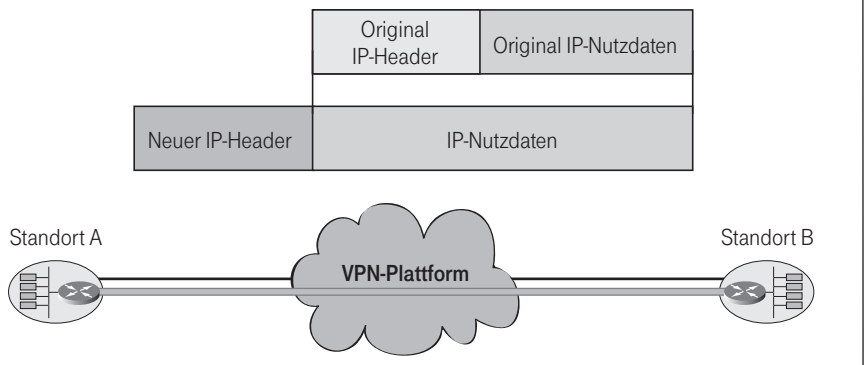
[20] **MD5:** Abk. für Message Digest 5 Challenge (MD5, RFC 1321), auch als Extensible Authentication Protocol-(EAP-)MD5 bezeichnet. Im Jahre 1998 vorgestelltes Optionsprotokoll EAP für die Authentifizierung in Remote-Access-Anwendungen eine von derzeit sechs angebotenen Optionen. Bei dieser Option entspricht der Ablauf des Aushandelns des Authentifizierungsverfahrens weitgehend den vom Challenge Handshake Authentication Protocol (CHAP) bekannten Mechanismen, wenn CHAP für den Betrieb mit dem Algorithmus MD5 konfiguriert wurde. Die Anforderung (Request) wird in diesem Fall wie bei CHAP als Aufforderung (Challenge) interpretiert. Als Antwort darauf wird ein so genanntes Success/Failure-Paket erwartet. Die EAP-Spezifikation sieht vor, dass jede EAP-Implementation MD5 unterstützen muss.

[21] **SHA1:** Abk. für Secure Hash Algorithm. Im Jahr 1993 vom US-amerikanischen National Institute of Standards and Technology (NIST) veröffentlichter Sicherheitsstandard (FIPS PUB 180-1), der im Juli 1994 modifiziert wurde. Der Standard basiert auf Ideen des Message Digest Algorithm 4 (MD4). Die Länge des Inputs ist auf höchstens 264 Bit beschränkt, der Output beträgt 160 Bit.

[22] **Data Encryption Standard:** Von IBM im Auftrag der US-Regierung entwickeltes Blockverschlüsselungsverfahren (Blockchiffre), das 1978 in den USA standardisiert wurde (ANSI X3.92) und sich in vielen Bereichen weltweit durchgesetzt hat. Der DES zählt zu den symmetrischen Verfahren, weil der Sender und der Empfänger über den gleichen Schlüssel verfügen müssen.

[23] **Advanced Encryption Standard:** Vom US-amerikanischen NIST (National Institute of Standards and Technology) vorgestellter offizieller Kryptostandard für die USA. Der AES ist der Folgestandard von DES.

Bild 10 **IP-Tunnelverfahren**



IP Internet Protocol VPN Virtual Private Network

Das aktuelle VPN-Lösungsportfolio der Deutschen Telekom

Die Deutsche Telekom verfügt über ein Angebotsportfolio unterschiedlicher VPN-Lösungen. Diese Lösungen umfassen beispielsweise die Layer-2-Basistechniken ATM und Frame Relay, die als sogenannte Native Services ohne CPE-Management und -Service angeboten werden, Komplettlösungen wie IntraSelect auf der Basis von ATM, Frame Relay oder MPLS einschließlich CPE-Management und -Service und verschiedene Secure-VPN-Angebote. Dies bietet Wahlmöglichkeiten hinsichtlich besonderer Anforderungen, Preis, Qualität, Service und Flexibilität. Tabelle 1 bietet eine Übersicht über das VPN-Angebot der T-Systems und der T-Com. (Auf Grund der schnellen Veränderungen in diesem Bereich stellt die Tabelle einen momentanen Auszug dar).

(Br)