Wolfgang Böhmer

Skriptum: VPN
Virtual Private Networks

TU-Darmstadt / Vorlesung LV 200096

vertrauliche Kommunikation in trusted-, secure- und hybrid-VPN

sowie über GPRS und WLAN

Draftversion 2.1.01

WS-2010/11

this page is initially blank

Inhaltsverzeichnis

1 Einleitung **1**

1.1 Traditioneller Datenaustausch 1
1.2 VPN-Definition der ersten Generation 5
1.3 VPN-Terminologie 6
1.4 Überblick der VPN-Varianten 9
1.5 VPN-Leistungsspektrum 12

2 Netz- und Kommunikationsgrundlagen für VPN **17**

2.1 Verfahren der Kommunikationstechnik für ein VPN 18
2.2 Offene Kommunikation in Datennetzen 20
2.2.1 Die Architektur des OSI-Referenzmodells 21
2.2.2 Die sieben OSI-Funktionen 22
2.2.3 Die OSI-Dienste 24
2.2.4 Die OSI-Protokolle 25
2.3 Das Internet-Protokoll in der Version IPv4 und IPv6 28
2.3.1 BOOTP/DHCP und Mobile-IP 32
2.3.2 Ende-zu-Ende-Flusskontrolle mittels TCP 38
2.3.3 Dienstgüte CoS und QoS in IP-Netzen 42
2.3.4 Integrierte und differenzierte Dienste 47
2.4 Übungen 56

3 Informations- und Kommunikationssicherheit **59**

3.1 Definition IuK-Sicherheit 60
3.2 Verfahren zur Erlangung der IuK-Sicherheit 65
3.2.1 Risikoanalysen 66

3.2.2 ITSEC und Common Criteria 72
3.2.3 Vergleich zwischen CC und ITSEC 73
3.2.4 Kurzüberblick Common Criteria 74
3.2.5 Sicherheitsarchitektur offener Systeme 76
3.2.6 Sicherheitsparadigma und Sicherheitspyramide 81
3.2.7 Evaluierung der Gesamtunternehmenssicherheit 83
3.2.8 IT-Security Capability Maturity Model (IT-SecCMM) 85
3.3 Übungen 87

4 Verschlüsselung **89**
4.1 Verschlüsselungstechniken 90
4.1.1 Substitutionstechniken 90
4.1.2 Transpositionstechniken 97
4.2 Symmetrische Kryptosysteme 99
4.2.1 Blockchiffre und Stromchiffre 100
4.2.2 DES, Triple DES, IDEA und AES 109
4.2.3 Triple DES 114
4.2.4 IDEA 115
4.2.5 AES 116
4.2.6 RIJNDAEL 117
4.3 Asymmetrische Kryptosysteme 119
4.4 Schlüsselaustausch-Verfahren 120
4.4.1 Diffie-Hellman, RSA, ELGamal, DSA 120
4.5 Kryptographische Hash-Funktionen 128
4.6 Elektronische Signatur 130
4.6.1 Mechanismen einer elektronischen Signatur 131
4.6.2 Bedeutung der digitalen und der elektronischen Signatur . 133
4.7 PKI und Trust Center 134
4.7.1 X.500 und X.509 v3 136
4.7.2 Zertifizierung und Validierung 140
4.7.3 PKI-Unterscheidungsmerkmale 141
4.7.4 Einsatz von elektronischen Zertifikaten 142
4.8 Übungen 143

5 Verfahren zur Authentifizierung 145
5.1 Einfache Authentifizierungsverfahren . . . 147
5.2 Starke Authentifizierungsverfahren . . . 152
5.2.1 Ein-Wege-Authentifizierung . . . 153
5.2.2 Zwei-Wege-Authentifizierung . . . 154
5.2.3 Drei-Wege-Authentifizierung . . . 155
5.3 Zwei-Faktoren-Authentifizierung in der Praxis . . . 156
5.3.1 Zeitsynchrone Authentifizierung mittels Token-Cards . . . 156
5.3.2 Speicherkarten und Smart Cards . . . 159
5.4 Authentifizierungsverfahren in der Anwendung . . . 162
5.4.1 Die PPP-Verbindung als Voraussetzung für PAP und CHAP 162
5.4.2 Password Authentication Protocol (PAP) . . . 164
5.4.3 Challenge Handshake Authentication Protocol (CHAP) . . . 164
5.4.4 Die AAA-Sicherheitsarchitektur . . . 166
5.4.5 Remote Authentication Dial-In User Service (RADIUS) . . . 168
5.4.6 Terminal Access Controller Access Control System . . . 170
5.4.7 Vergleich zwischen RADIUS und TACACS+ . . . 171
5.4.8 DIAMETER . . . 172
5.4.9 Kerberos . . . 174
5.5 Übungen . . . 179

6 Varianz der VPN-Typen 181
6.1 VPN-Einsatzmöglichkeiten . . . 182
6.1.1 Intranet-VPN (Site-to-Site) . . . 186
6.1.2 Extranet-VPN (End-to-End) . . . 188
6.1.3 Remote-Access-VPN (End-to-Site) . . . 190
6.2 Eckpunkte für den Einsatz eines VPN . . . 192
6.2.1 VPN-Sicherheitspolitik . . . 192
6.2.2 VPN und Firewall . . . 193
6.2.3 VPN und Router . . . 198
6.2.4 Quality of Service in VPN . . . 198
6.2.5 Diffserv in VPN . . . 198
6.2.6 Beispiel einer komplexen VPN-Architektur . . . 199
6.2.7 Ausblick . . . 201
6.3 Übungen . . . 202

7 Secure VPN im Internet, 3G-Netzen und WLAN 205
7.1 Tunneling . . . 206
7.2 Layer-2-Techniken . . . 208
7.2.1 L2F . . . 210
7.2.2 PPTP . . . 211
7.2.3 L2TP . . . 217
7.2.4 SSL over L2TP oder L2Sec . . . 225
7.3 Layer-3-Techniken . . . 226
7.4 Sicherheitsstandard für das Internet (IPSec) . . . 227
7.4.1 Das Ziel von IPSec . . . 229
7.4.2 Die IPSec-Sicherheitsvereinbarungen (SA) . . . 232
7.4.3 IPSec-Authentifizierung mittels AH-Header . . . 234
7.4.4 IPSec-Vertraulichkeit mittels ESP-Header . . . 236
7.4.5 Transport- und Tunnelmodus . . . 238
7.4.6 Kombinationen von Security Associations . . . 241
7.4.7 Initiierung einer Security Association . . . 243
7.4.8 IPSec und Remote Access . . . 245
7.4.9 Schlüsselaustausch für IPSec (IKE) . . . 248
7.4.10 IKEv1-Phase-1 . . . 251
7.4.11 IKEv1-Phase-2 oder der Quick Mode . . . 256
7.4.12 Das Internet Security Association and Key Management Protocol (ISAKMP) . . . 257
7.4.13 Das Oakley-Schlüssel-Protokoll (Oakley) . . . 260
7.4.14 IKEv2 - Schlüsselaustausch der nächsten Generation . . . 262
7.4.15 IPSec, IKEv2 und Roaming-Verfahren . . . 269
7.4.16 Zertifikatsbasierte PKI-Authentifizierung für IPSec . . . 273
7.4.17 Secure VPN im Wireless LAN (WLAN) . . . 278
7.4.18 Das Simple Key Management for Internet Protocol (SKIP) . . . 281
7.4.19 Layer-2- und Layer-3-Vergleich . . . 282
7.5 Layer-4-Techniken . . . 282
7.5.1 Secure Socket Layer (SSL) und Transport Layer-Sicherheit (TLS) . . . 282
7.5.2 Vergleich zwischen IPSec und SSL/TLS . . . 292
7.6 Layer-5-Techniken . . . 294
7.6.1 SOCKS v5 . . . 294
7.7 Übungen . . . 295

8 Trusted VPN in Weitverkehrsnetzen (WAN) 297

8.1 VPN und Multiprotocol Label Switching 298
8.1.1 MPLS und Switching-Eigenschaften 300
8.1.2 MPLS und das $n(n-1)/2$ Problem 300
8.1.3 MPLS als Königsweg für Quality of Service in VPN 302
8.1.4 Gemeinsamkeiten und Unterschiede von RSVP-TE und CR-LDP 306
8.1.5 IP-MPLS und Multiprotocol Lambda Switching ($MP\lambda S$) . 311
8.2 Fast-Packet-Switching (FPS) 314
8.3 Frame Relay 315
8.3.1 MPLS über Frame Relay 320
8.4 Asynchroner Transfer Modus (ATM) 320
8.4.1 Dienstgüten und -klassen in ATM-Netzen 325
8.4.2 Verkehrs- und Überlaststeuerung 327
8.4.3 ATM-Referenzmodell 329
8.4.4 MPLS über ATM-Verbindungen 333
8.5 Übungen 335

9 Hybrid VPN – Sichere Kommunikation über fremde Netze 337

9.1 Provider-Netze und Netzstrukturen 338
9.1.1 Struktur der globalen Netze 339
9.1.2 IP-VPN über Wählverbindungen 344
9.1.3 VPN über fremde Netze 345
9.1.4 Referenzmodell für ein verwaltetes CE-basiertes VPN . . . 348
9.1.5 Referenzmodell für ein NB-basiertes VPN 350
9.2 Netzwerk-Performance und Management 352
9.2.1 ITIL als Defacto-Standard für IT-Service-Management . . . 355
9.2.2 Sicherheitsaspekte 358
9.2.3 Servicevereinbarungen (SLA) 358
9.3 VPN-Klassifizierungen 360
9.3.1 Vergleichsverfahren und Anforderungen 366
9.4 Übungen 367

10 Einsatz von Virtual Private Networks 369
10.1 VPN-Marktbetrachtungen 369
10.2 VPN der zweiten Generation 379
10.2.1 IPSec und Performance-Aspekte 381
10.3 Planungsaspekte 386
10.4 Vier-Phasen-Plan eines VPN-Projekts 387
10.4.1 Analyse 389
10.4.2 Konzeption 404
10.4.3 Realisierung 406
10.4.4 Betrieb 407
10.5 Schlussbemerkung 408
10.6 Übungen 409

Literaturverzeichnis 411

Glossar 421

Stichwortverzeichnis 421

Vorwort

Das Wort „virtuell“ *(lat. virtus, Tugend, Tapferkeit)* tauchte in den 50er Jahren zunächst als Begriff in der Computerwissenschaft auf. Virtuelle Computer spiegeln den Benutzern vor, dass sie allein Zugriff auf die Systemressourcen hätten, gleichwohl mehrere Benutzer sequentiell mit hoher Rechengeschwindigkeit an einem System arbeiten. Mittlerweile zu einem Modewort geworden, werden mit dem Ausdruck „virtuell“ Anpassungsfähigkeit und Interaktion, losgelöst von zeitlichen und örtlichen Beschränkungen, verknüpft. Sogar das Wort „virtuelle Unternehmen“ ist davon geprägt. Virtuelle Unternehmen zeichnen sich durch geschäftsorientierte zeitlich limitierte Partnerschaften aus, bei denen Lieferanten, Kunden und Produzenten aktiv und synergetisch einen Bedarf zum gemeinsamen Vorteil aller Beteiligten abdecken [Füser 1997].

Doch was ist unter „virtuell“ im Zeitalter der Informationsgesellschaft zu verstehen? Wie ist der Begriff des Nicht-Wirklichen, des Nicht-Realen, auf die Computerwelt bzw. auf das „Netz der Netze“ zu übertragen? Bei Scott et al. 1998 heißt es: „A virtual private network is a way to simulate a private network over a public network, such as the Internet“. Doch trifft diese Definition nicht den Kern. Besser ist es, ein Virtuelles Privates Netzwerk (VPN) allein durch logische Größen zu definieren und nicht durch physikalische. Die Grundidee ist, dass die Plattform, die physikalische Größe in erster Linie eine öffentliche Plattform sein muss. Dies können neben dem Internet auch andere Plattformen sein, wie z.B. die Sprachplattform Integrated Service Digital Network (ISDN), Weitverkehrsnetze (WAN) auf Basis eines Asynchronen Transfermodus (ATM) und Frame Relay (FR) oder auch Multi Protokol Label Switching (MPLS). Netzbetreiber (NSP) bieten ihren Kunden vielfach ein VPN auf dieser Basis an. Die Benutzung eines VPN wiederum kann man sich mit einer einfachen Metapher vorstellen: Das VPN-Gateway arbeitet wie ein Pförtner, der einen Verbindungskorridor zweier Gebäude bewacht und der nur jene Personen in den Korridor und damit in das andere Gebäude lässt die dazu berechtigt sind. Ein VPN ermöglicht einer bestimmten Anzahl von Teilnehmern einer öffentlichen Plattform, bei gleichzeitigem Ausschluss der Öffentlichkeit, miteinander zu kommunizieren resp. einen bestimmten Verbindungskorridor zu betreten. Eine anderes Analogon vergleicht ein VPN mit einem elektronisches Rohrpostsystem.

Dieses Buch gibt dem versierten Leser wie dem interessierten Laien einen umfassenden Einblick in die Technologie der VPN. Zunächst werden die Hintergründe und die Motivation zur Entwicklung der VPN-Technologie diskutiert. An zwei Beispielen wird die Spannbreite der unterschiedlichen Entwicklungsformen aufgezeigt. Dies wirft die Frage nach einer allgemeingültigen VPN-Definition auf; dieser ist ein eigener Abschnitt gewidmet. Anschließend werden die Netzwerk- und Kommunikationstechnologien für die VPN-Technologie diskutiert. Es werden die sieben Schichten des OSI-Referenzmodells vorgestellt, deren Kenntnis eine Unterscheidung zwischen einem Layer-2-VPN einem Layer-3- oder auch ei-

nem Layer-7-VPN erst ermöglicht.

Erläutert wird außerdem das Internetprotokoll IPv4 und die Version 6 (IPv6) sowie deren Unterschiede. Die Möglichkeiten des Internetprotokolls in Hinblick auf die Dienstgüten *(Quality of Service, QoS)*, die zwischen den Kommunikationspartnern realisierbar sind, werden ebenso betrachtet. Auch auf MPLS-VPN, als zukunftsweisende Technologie für ein VPN im Weitverkehrsnetz wird eingegangen. Da ein VPN häufig firmenübergreifend eingesetzt und mit einem Netzwerkanbieter realisiert wird, werden die Netztechnologien eines Weitverkehrsnetzes (WAN) diskutiert. Speziell die paketorientierten Vermittlungsverfahren, Frame Relay und ATM, welche auf Basis von Multiplexing-Verfahren arbeiten, werden skizziert. VPN auf dieser Basis werden als *trusted VPN* bezeichnet.

Secure VPN, die mittels Verschlüsselung gebildet werden, sind ein weiterer Bestandteil des Buches. Neben kryptographischen Verfahren nehmen die Themen Verschlüsselungsverfahren, Schlüsselmanagement und Schlüsselinfrastruktur einen breiten Raum ein. Im Sinne einer Zugriffsicherung werden sie zum Nachweis der Identität herangezogen. Außerdem werden sie eingesetzt, um die Integrität der Urheberschaft von elektronischen Dokumenten zu garantieren. Bei den Secuure VPN wird die Privatsphäre durch Nachrichtenverschlüsselung verwirklicht. Sie verhindert, dass unbefugte Dritte Nachrichten lesen oder manipulieren können.

Auf die unterschiedlichen Möglichkeiten verschiedener VPN-Varianten Intranet, Extranet- und Remote-Access-VPN wird anschließend eingegangen. Es wird ausführlich der bedeutsame Tunnelmechanismus und eine VPN-Realisierung auf verschiedenen OSI-Schichten erläutert. Der Quasi-VPN-Standard (IPSec) wird detailliert vorgestellt und es wird deutlich, wieviel Interoperabilitätsschwierigkeiten, trotz Spezifikationen der Internet Engineering Task Force (IETF), noch existieren.

Die sichere Kommunikation über fremde Netze, den Providernetzen, bildet einen weiteren Schwerpunkt des Buches. Seit kurzem existieren Referenzmodelle, auf die speziell eingegangen wird. Themen, wie z.B. Serviceleistungen eines Providers und deren Einhaltung, werden einer eigenen Betrachtung unterzogen. Abschließend wird die nicht triviale Planung eines VPN durch einen Vierphasenplan diskutiert.

Ziel des Buches ist es, die VPN-Technologie umfassend zu beschreiben. Kommentare, Anregungen oder auch Verbesserungsvorschläge sind jederzeit willkommen.

Frankfurt, im Frühjahr 2002

Wolfgang Böhmer
wjboehmer@t-online.de

Vorwort zur Draftversion

Ich möchte mich an dieser Stelle für die zahlreichen Anregungen und Rezensionen bedanken, die inzwischen bei mir in den letzten Jahren eingegangen sind. Entstanden ist das Skript zum großen Teil durch die Vorlesungen, die ich seit dem Sommersemester 2002 halte. Etliche Anregungen und Änderungswünsche, z.B. das Glossar und die Übungsaufgaben, die jetzt am Ende eines jeden Kapitels eingeflossen sind, rühren daher. Ebenso möchte ich den Studenten danken, die mir in den letzten Semestern durch zahlreiche Fragen und Diskussionen hilfreiche Anregungen und Verbesserungsvorschläge gaben.

Eine der gravierendsten Änderungen ist durch die Neustrukturierung hervorgerufen worden. Es werden jetzt zuerst alle Grundlagen vermittelt und anschließend die VPN-Technologien *secure VPN, trusted VPN* und *hybrid VPN* diskutiert. Marktbetrachtungen und das 4-Phasenmodell schließen das Buch ab. Die Definitionen der unterschiedlichen VPN-Technologien lehnen sich an den im Juli 2004 formulierten Vorschlag des inzwischen entstandenen VPN-Consortiums an. Dies hat die Begriffe *trusted VPN*, *secure VPN* und *hybrid VPN* eingeführt. Im Abschnitt 1.3 des Kapitel 1 werden diese richtungsweisenden Begriffe detailliert erklärt.

Im Vergleich zur ersten Auflage wurden folgende Änderungen vorgenommen:

- Im Kapitel 1 wurde das zweite Beispiel durch ein Szenario aus dem Bereich Server Based Computing ersetzt. Damit wird der aufkommende mobile VPN-Bereich berücksichtigt.
- Im neu strukturierten Kapitel 2 wurden zahlreiche Ergänzungen und Korrekturen vorgenommen. Das Kapitel wurde aufgeteilt. Es vermittelt nun die notwendigen Grundlagen der VPN-Technologie. Die Diskussion der ATM, Frame Relay und MPLS Netze ist in das neu entstandene Kapitel 8 verschoben. Diese Art der VPN werden zukünftig als trusted VPN bezeichnet.
- Im Kapitel 3 wurden die Betrachtungen zur Unternehmensevaluierung erweitert und ergänzt. Einen Ausblick auf Reifegradmodelle wird außerdem gegeben.
- Im Kapitel 4 wurden die Ausführungen zur Hashfunktion überarbeitet. Ebenso wurde die Diskussion über AES – nachdem das Auswahlverfahren abgeschlossen ist – dem heutigen Sachstand angepasst.
- Im Kapitel 5 wurde das gegenüber RADIUS verbesserte Authentifizierungsverfahren DIAMETER aufgenommen.
- Das Kapitel 6 wurde gestrafft.
- Im Kapitel 7 werden die secure VPN diskutiert. Es werden u.a. ergänzende Betrachtungen zu IPSec aufgenommen. Die SSL-VPN sind nun stärker betont. In diesem Kapitel sind die Betrachtungen zum WLAN und Mobilität in Verbindung mit der secure VPN-Technologie neu hinzugekommen.

- Das neu entstandene Kapitel 8 widmet sich den trusted VPN. Hier sind Teile vom Kapitel 2 eingeflossen.
- Im Kapitel 9 sind die Referenzmodelle überarbeitet und ausführlicher beschrieben.
- Im Kapitel 10 wurden die VPN-Marktbetrachtungen auf den aktuellen Stand gebracht. Ebenso wurden die Performance-Messungen überarbeitet und es wir ein überarbeiteter Vorschlag zur IPSec-Throughput-Messung vorgestellt.

Durch die zahlreichen Verbesserungen und zusätzlichen Erläuterungen, die in das Buch eingeflossen sind, ist die zweite Auflage substanziell verbessert worden.
Doch ist das vorliegende Werk nicht als technische Anleitung zur Konfiguration (HowTo) von VPN zu verstehen. Zum einen gibt es für diesen Zweck bereits Literatur z.B. von [Spengenberg 2004], zum anderen ändern sich die technischen Implementierungen erfahrungsgemäß recht schnell. Begleitend zur Vorlesung im WS 2010 werden weitere Themen, die im Umfeld eines VPN angesiedelt sind, berücksichtigt. So kann z.B. obwohl ein IPsec-VPN die Vertraulichkeit einer Verbindung garantiert, immer noch auf den Traffic - also mittels einer Verkehrsanalyse - geschlossen werden und somit herausgefunden werden, das zwei bestimmte IP-Adressen kommuniziert haben. Oftmals ist selbst diese Information geheim zuhalten.

Ihre Kritik, weitere Ideen und Verbesserungsvorschläge nehme ich gerne per E-Mail entgegen.

Darmstadt, im Okt. 2010

Wolfgang Böhmer
wboehmer@cdc.informatik.tu-darmstadt.de

1 Einleitung

Durch die Informationstechnologie und den sich ändernden Kommunikationsmöglichkeiten sehen sich die Unternehmen mit einer rasanten Entwicklung konfrontiert. Internationale Märkte und die zunehmende Verflechtung der Unternehmen haben zur Folge, dass der Datenaustausch zwischen den Beteiligten stark zunimmt. Der gezielte Einsatz von Informations- und Kommunikationstechnologien ist der Dreh- und Angelpunkt im heutigen Wirtschaftsleben. Immer größere Datenmengen müssen in immer kürzeren Zeiträumen verarbeitet werden. Dadurch steigen die Anforderungen an die Unternehmensnetze hinsichtlich der bereitzustellenden Übertragungsbandbreiten. Die lokalen Netzsegmente an neuen Standorten oder mobile Einzelplatzsysteme müssen schnell, flexibel und kostengünstig angebunden werden – und das zunehmend weltweit.

Die Unternehmen müssen inzwischen ihre Marktpositionen in immer kürzeren Produktzyklen behaupten. Dies wirkt sich auf die eingesetzten IT-Anwendungen und -Systeme und ihre Vernetzung aus. Neue Applikationen erlauben ein effizienteres Abwickeln bestehender geschäftlicher Vorgänge oder zwingen zu deren Veränderung. Die traditionellen Verfahren zum Datenaustausch, z.B. Briefpost oder Fax-Kommunikation, werden den neuen Anforderungen nicht mehr gerecht, da sie zeitaufwändig und verwaltungsintensiv sind (vgl. Abb. 1.1) und der verkürzten Time-to-Market-Spanne nicht mehr gerecht werden. Die Übertragung von Daten auf elektronischem Weg hingegen führt zu Vereinfachungen, beschleunigt Arbeitsabläufe und ermöglicht eine nahezu medienbruchlose Weiterverarbeitung von Informationen (vgl. Abb. 1.2). Voraussetzung für den Einsatz elektronischer Datenübertragung ist ein Konsens über die Formate der zu übermittelnden Daten. Der Empfänger eines geschäftlichen Vorfalles muss in der Lage sein, diese korrekt zu interpretieren.

1.1 Traditioneller Datenaustausch

Zu Beginn der IT-Nutzung bestimmten Einzelplatzsysteme den Einsatz von Rechnern in Unternehmen. Dann trat die lokale Vernetzung der Rechnersysteme an den einzelnen Unternehmensstandorten in den Vordergrund. Ziel war die Nutzung zentraler Ressourcen wie z.B. Plattenspeicher, Drucker oder Applikationen auf leistungsstarken Servern. Eine Zusammenarbeit fand im Wesentlichen in lokalen Arbeitsgruppen statt. Heute spielt der Standort eines Unternehmens innerhalb der Unternehmenskommunikation keine Rolle mehr. Die Unternehmen verfügen über eigene Netze, die die einzelnen Filialen verbinden. Die lokalen Netzsegmente sind über Weitverkehrsnetze miteinander verbunden.

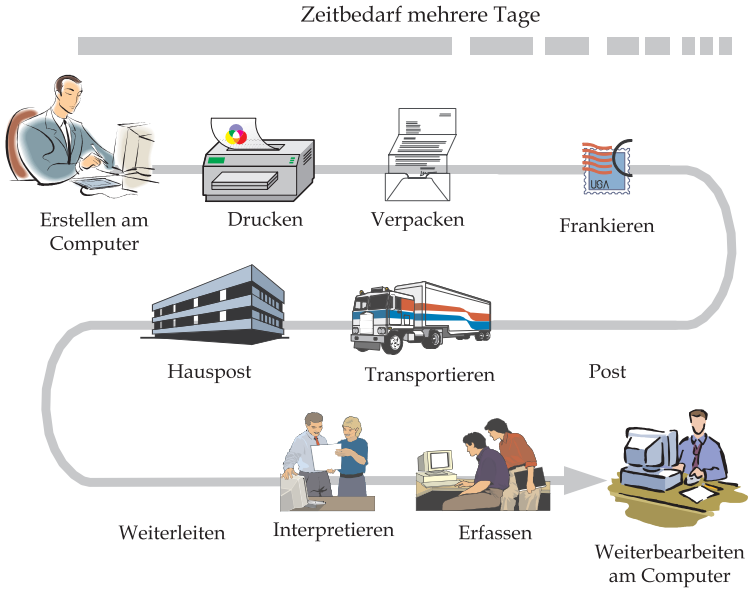


Abb. 1.1: Herkömmlicher zeitraubender Informationsaustausch

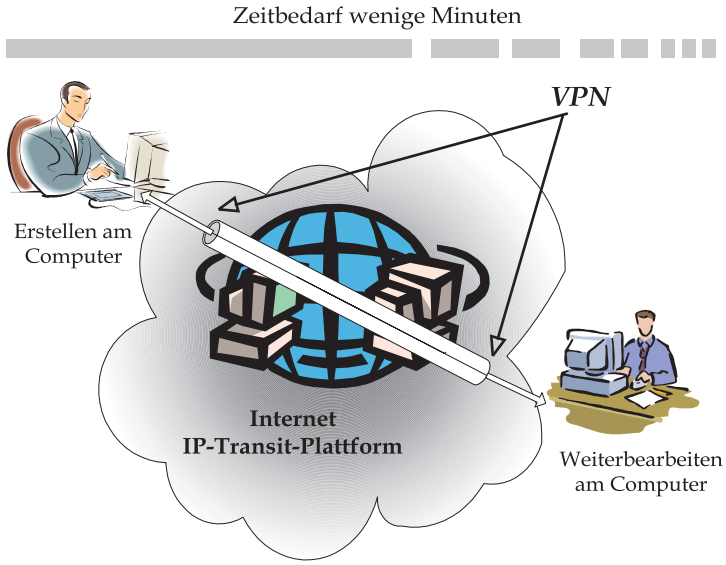


Abb. 1.2: Moderner Informationsaustausch mittels VPN zur direkten Kommunikation zwischen zwei Standorten

Wird ein Vergleich gezogen zwischen dem herkömmlichen Austausch von Informationen, der einige Tage in Anspruch nehmen kann, und modernen Verfahren, angefangen von E-Mails bis hin zur gleichzeitigen Bearbeitung eines Dokumentes an unterschiedlichen Standorten, so wird deutlich, welche Zeitersparnisse die neuen Verfahren mit sich bringen (vgl. Abb. 1.2 mit Abb. 1.1).

Ein VPN erfordert eine Menge Technologieanpassung und Prozessveränderungen. Eine oberflächliche Betrachtung von VPN-Produkten reicht deshalb nicht aus, um ein VPN zu planen und zu realisieren. Mittlerweile gibt es zu viele Varianten hinsichtlich einer Realisierung und des Zugriffs.

Gerade im Zuge des aufkommenden E-Business (B-to-B) wird die Sicherheit der Kommunikation über das Internet immer wichtiger. Eine Schlüsselrolle wird hierbei die VPN-Technologie einnehmen. Neben reinen Sicherheitsfunktionen sind allerdings noch weitere Kenngrößen gefragt, wie z.B. Interoperabilität, Kosten und Performance. Dabei hängt die Performance nicht unwesentlich von den eingesetzten Verschlüsselungsverfahren ab – falls überhaupt verschlüsselt werden soll.

Grundlage der Planung eines VPN ist die Kenntnis der einzusetzenden Technik bzw. der unterschiedlichen Technologien. Zum Beispiel werfen die Übertragung in der OSI-Schicht 2 bzw. -Schicht 3 oder die möglichen Verschlüsselungsverfahren eine Reihe von Fragen auf. Unter Umständen beeinflusst ein schlecht geplantes VPN die Performance im ganzen Netz.

Somit können mehrere Problemfelder – von der Grundlagentechnologie abgesehen – identifiziert werden, die in dem vorliegendem Buch diskutiert werden:

- **Identifizierung und Berechtigung:** Ein VPN muss wissen, wer am anderen Ende die Kommunikation aufnehmen will.
- **Verschlüsselung:** Daten bleiben privat (vertraulich), auch wenn der Datenverkehr unterwegs belauscht wird.
- **Zugriffsberechtigung:** Aktionen und Zugriffe Berechtigter dürfen keine anderen als die vorgesehenen Datenbestände umfassen.
- **Datenintegrität:** Es muss sichergestellt werden, dass die dem VPN anvertrauten Daten unverfälscht übertragen werden.
- **Zugriffskosten:** Es muss festgehalten werden können, wer eine Transaktion verursacht hat (angehängte Rechnungsprüfung).
- **Transaktionsverweigerung:** Es muss sichergestellt werden, dass eine gewünschte Transaktion zu den vereinbarten Rahmenbedingungen möglich ist.
- **Benutzerfreundlichkeit:** Eine entsprechend einfache und klar verständliche Benutzerführung ist erforderlich.

Neben diesen Problemfeldern müssen jedoch auch praktische Anforderungen an ein VPN in Erwägung gezogen werden:

- Integration des Netzwerkes mit der Benutzerumgebung

- Adäquater Zugriff für Endbenutzer
- Einfache Administrierbarkeit des VPN
- Investitionsschutz und Weiterentwicklungsmöglichkeiten
- Leistungsfähigkeit und Skalierbarkeit sowie
- Einfachheit im Gebrauch

Die aufgezählten Punkte umreißen technische, organisatorische und logistische Anforderungen an ein VPN. Um diesen Anforderungen in Teilen oder vollständig gerecht zu werden, werden für ein VPN spezielle Kommunikationsplattformen eingesetzt. Neben dem Internet als beliebter Kommunikationsplattform kommen im Weitverkehrsbereich jedoch auch Plattformen wie z.B. ATM oder Frame Relay zum Einsatz. Der Begriff „Plattform “ wird dabei oftmals benutzt, um über eine Kommunikationsinfrastruktur zu sprechen, auf der bestimmte Dienste oder Anwendungen aufsetzen. Im Vordergrund des Interesses stehen für den Anwender allerdings nur die Dienste und Anwendungen; die technischen Details zu ihrer Realisierung spielen für ihn eine untergeordnete bzw. gar keine Rolle. Die Entscheidung, welche der oben genannten Plattform gewählt wird, richtet sich nach dem zu transportierenden Verkehrsvolumen und den daraus resultierenden Kosten. Ist das Unternehmen über mehrere Standorte verteilt, die eine gemeinsame Plattform nutzen, erfüllt die Plattform und die darauf aufsetzende Kommunikation die Eigenschaft eines privaten Netzes. Deshalb wird in diesem Zusammenhang oft von *Enterprise Network* gesprochen. „Privat“ bedeutet in diesem Kontext, dass einerseits der Zugang nur einem begrenzten und namentlich bekannten Personenkreis möglich ist, andererseits ist die Vertraulichkeit – und dies ist eine Forderung, die erst neuerdings hinzugekommen ist – der elektronisch ausgetauschten Informationen gewährleistet.

Noch zu Beginn der 90er Jahre wurden üblicherweise die Filialen eines Unternehmens über Weitverkehrsstrecken verbunden, die entweder permanent oder nach Bedarf aufgebaut wurden. Im ersten Fall mieteten die Unternehmen sich von öffentlichen Anbietern Standardfestverbindungen (SSV) oder Datendirektverbindungen (DDV). Die geschalteten Leitungen standen dem Unternehmen exklusiv zur Verfügung. Im letzteren Fall dienten ISDN- und X.25-Netze dem Verbindungsaufbau zwischen den Standorten. Neuerdings ist ein Rückgang dieser Vernetzungsform zu verzeichnen. Die Unternehmen gehen vermehrt dazu über, die erforderlichen Verbindungskapazitäten einzelner Lokationen z.B. über Frame-Relay- oder ATM-Netze von öffentlichen Anbietern zu beziehen. Diese Plattformen ermöglichen Verbindungen zwischen Unternehmensstandorten, bei denen lediglich der Weg der Daten in der Kommunikationsplattform hinterlegt ist. Es findet *keine* permanente Reservierung physikalischer Netzressourcen statt. Erst wenn die Daten zur Übertragung anstehen, werden erforderliche Bandbreiten zugewiesen und die Informationen entlang des festgelegten Weges weitergeleitet. Es wird also nur der Anschein erweckt, als seien die Standorte physikalisch miteinander verbunden. Derartige Verbindungen werden als *virtuell* bezeichnet; synonym wird von *logischen* Verbindungen gesprochen. Der Vorteil dieser Art der

Vernetzung liegt in der größeren Flexibilität, auf steigenden Bandbreitenbedarf zu reagieren, und sie erlaubt in der Regel höhere Übertragungsbandbreiten. Die Grenzen dieser Unternehmensnetze bestehen darin, dass ein Anschluss nur dann möglich ist, wenn am jeweiligen Nutzungsort ein Zugang zur Kommunikationsplattform existiert.

Die Privatsphäre der Kommunikation bleibt dadurch gewahrt, dass die virtuellen Verbindungen zwischen den Unternehmensstandorten innerhalb einer geschlossenen Benutzergruppe als *Closed User Group (CUG)* verwaltet werden. Das bedeutet, dass die Zugangspunkte innerhalb der Kommunikationsplattform nur über eindeutige Adressen erreichbar sind. Somit sind alle Anschlusspunkte der verschiedenen Standorte eines Unternehmens durch eine begrenzte Menge von eindeutigen Adressen vertreten. Die Adressen sind dem Unternehmen exklusiv zugeordnet. Innerhalb der Kommunikationsplattform sorgt das Netzwerkmanagement dafür, dass nur Wege zwischen jenen Adressen möglich sind, die dem Unternehmen vorbehalten sind. Die Kommunikation zu einem Anschlusspunkt außerhalb einer in sich geschlossenen Menge (CUG) wird unterbunden.

1.2 VPN-Definition der ersten Generation

Die oben beschriebene Form eines Unternehmensnetzes stellt bereits ein Virtuelles Privates Netz dar: Die öffentliche Kommunikationsplattform, die von mehr als nur einem Unternehmen genutzt wird, erlaubt durch das Einrichten von logischen Verbindungen die exklusive private Kommunikation zwischen Gruppen von Zugangspunkten. Wird der Begriff des VPN allerdings einer genaueren Betrachtung unterzogen, so eröffnet sich ein beträchtliches Spektrum an Interpretationsmöglichkeiten und Unterscheidungsmerkmalen. Historisch betrachtet haben sich VPN zunächst im Sprachbereich zu Beginn der Deregulierung des Telekommunikationsmarktes entwickelt. Firmen konnten so genannte Corporate Networks (CN) als Unternehmensnetzwerke aufbauen. Firmenseitig gemietete E1-Leitungen, die bis zu 2 Mbit/s transportieren können, wurden in Kanäle zu je 64 Kbit aufgeteilt und zur Sprachanbindung entfernter Standorte eingesetzt. Gerade über die teuren Fernverbindungsstrecken zwischen entlegenen Firmenstandorten machten sich die Corporate Networks bezahlt. Daten wurden in den wenig genutzten Auslastungszeiten, z.B. in den späten Abendstunden, transportiert. Durch den einsetzenden Preisverfall der Verbindungsminuten im Sprachbereich in der zweiten Hälfte der 90er Jahre wäre die Wirtschaftlichkeit vieler CN sicherlich in Frage gestellt worden, hätte nicht zeitgleich der Datenverkehr rapide zugenommen. Hierdurch etablierten sich Netzwerktechnologien wie Frame Relay als Erweiterung und letztendlich als Nachfolge für X.25 und ATM für den Einsatz von Corporate Networks. Gerade Frame Relay erlangte in den späten 90er Jahren große Popularität. An den Endpunkten wird wenig Equipment benötigt – lediglich ein Router an jedem Verbindungspunkt. Aus dieser Kopplung resultiert die Vorstellung einer *Wolke*, die erst dann durchgeschaltet wird, wenn Frame-Relay-Verbindungen aktiv benötigt werden.

Vor allem die bedarfsweise geschalteten Frame Relay-Verbindungen könnten als eine der ersten modernen Virtuellen Privaten Netze bezeichnet werden. Streng genommen müsste auch die X.25-Technologie berücksichtigt werden, die ebenso mittels Virtueller Circuits (VC) und geschlossener Benutzergruppen (CUG) ein Virtuelles Privates Netz einrichten kann.

Aus der oben geführten Diskussion, die den Begriff *virtuell* betrachtet, sowie aus dem vom englischen Sprachgebrauch abgeleiteten Adjektiv *private* wird im vorliegenden Kontext folgende VPN-Definition der ersten Generation eingeführt:

Ein Virtuelles Privates Netz (VPN) ist ein Netz von logischen Verbindungen zur Übermittlung von privaten Daten/Informationen bzw. Datenverkehr. Eine logische Verbindung ist eine Netzverbindung zwischen einem Sender und einem Empfänger, bei der der Weg der Information und die Bandbreite dynamisch zugewiesen werden.[1]

Hierbei bedeutet privater Datenaustausch, dass die übertragenen Daten hinsichtlich ihrer Integrität und ihrer Vertraulichkeit[2] nicht kompromittiert werden können. Zwar spielt die Zugriffskontrolle und die Authentifizierung eine wesentliche Rolle, um einen Zugang ins private Netzwerk zu bekommen. Sie werden aber als systemimmanent angesehen und sind kein Bestandteil der Definition.

Für die technische Umsetzung der Privatsphäre des Datenaustausches gibt es zwei Möglichkeiten: Die einfachste ist, die Datenverbindung zu privatisieren, so dass niemand Zugang oder einen physikalischen Zugriff auf die Leitung bekommt (CUG). Bei der zweiten Möglichkeit werden die Methoden der Kryptographie benutzt, um eine Datenübertragung bei unsicheren Verbindungen abzusichern. Die zu übertragenden Daten werden verschlüsselt und sind so für unbefugte Dritte nutzlos.

Neuerdings wird auch Sprache über VPN übertragen. Neue Protokolle und Verschlüsselungsmechanismen sorgen für den nötigen Durchsatz mit entsprechender Qualität und garantieren die gleiche Privatsphäre wie im herkömmlichen Telefonnetz.

1.3 VPN-Terminologie

Aufgrund der unterschiedlichen Ausrichtungen und Technologien, die mit dem Begriff VPN heutzutage verbunden sind, hat sich ein Konsortium mit Sitz in Santa Cruz, USA im Jahre 1999 zusammengefunden, um eine Klärung und Transparenz herbeizuführen. Das Konsortium, das unter der Bezeichnung VPN Consortium[3]

---

[1] Vergleiche auch [Kosiur 1998] Anzumerken ist, dass im engl. Sprachgebrauch das Adjektiv *private* nur die Vertraulichkeit ausdrückt und nicht die Integrität. Datenintegrität ist ebenfalls eine notwendige Eigenschaft heutiger VPN.

[2] Auf die Begriffe Integrität und Vertraulichkeit sowie Verbindlichkeit, die ebenfalls in engem Kontext mit dem privaten Datenaustausch stehen, wird in Abschn. 3.1 näher eingegangen.

[3] Das Consortium VPNC ist in Santa Cruz, CA 95060 USA am 127 Segre Place beheimatet. Im Internet ist das VPNC unter http://www.vpnc.org zu finden.

(VPNC) agiert, hat sich folgende Aufgaben gestellt:

- Veröffentlichungen und Unterstützung bei Interoperabilitätstests
- Unterstützung seiner Mitglieder und deren Produkte bzgl. Produktinteroperabilität
- Einrichtung eines weltweiten Forums zum Informationsaustausch zwischen Herstellern und Providern
- Pressearbeit zur Verbreitung der unterschiedlichen VPN-Technologien

Die Arbeit des VPNC ist z.T. in enger Anlehnung an die Arbeiten der Internet Society zu verstehen, die mit den bekannten IETF-Arbeitsgruppen, ein bestimmendes Instrument der Internet-Technologie inne haben. Auf den Internetseiten des VPNC sind neben eigenen Arbeitspapieren auch die wesentlichen Entwicklungen im Bereich der VPN-Technologie der IETF in Form von RFCs und Internet Drafts zu finden. Das VPNC hat eine allgemeine Beschreibung der VPN-Terminologie[4] erarbeitet, die hier im Originaltext wiedergegeben werden soll:

A virtual private network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of tunneling protocol and security procedures. A virtual private network can be contrasted with a system of owned or leased lines that can only used by one company. The main purpose of a VPN is to give the company the same capabilities as private leased lines at much lower cost by using the shared infrastructure. Phone companies have provided private shared resources for voice message for over a decade. A virtual private network makes it possible to have the same protected sharing of public resources for data. Companies today are looking at using a private virtual network for both extranets and wide-area intranets.

Diese Terminologie – stammend aus dem Jahre 2004 – ist umfassender als die VPN-Definition der ersten Generation im Abschn. 1.2. Weiterhin hat das Konsortium unterschiedliche VPN-Begriffe eingeführt: Secure VPN, Trusted VPN und Hybrid VPN.[5] Dabei ist zu bemerken, dass die Secure VPN und Trusted VPN nicht notwendigerweise in Beziehung stehen müssen. Es ist durchaus möglich, dass diese in einem Serviceangebot koexistieren, aber auch getrennt eingesetzt werden können.

Bevor das Internet populär wurde, bestand ein VPN aus einem oder mehreren Virtual Circuits (VC), die von einem Provider vermietet wurden. Jede vermietete VC agierte wie eine einzelne Kanalverbindung in einem Netzwerk, das von dem nutzendem Unternehmen kontrolliert wird. Manchmal unterstützt der Provider

[4] Auf den Internetseiten des VPNC ist ein Whitepaper vom Juli 2004 zu finden, das unter dem Titel „VPN Technologies: Definitions and Requirements “diese Beschreibung beinhaltet.

[5] Die nachfolgenden Beschreibungen der Begriffe Trusted VPN, Secure VPN und Hybrid VPN sind für dieses Buch elementar. Denn hierauf ist zum großen Teil die Neustrukturierung des Buches zurückzuführen.

das Unternehmen, um das Netzwerk zu betreiben und zu warten. Die Grundidee besteht darin, dass das Unternehmen die gemietete Verbindung (VC) in der gleichen Weise nutzt und beherrscht wie ein physikalisches Kabel im eigenen Netzwerk. Daraus ergibt sich folgende Definition:

Trusted VPN: In einem Virtual Circuit wird die Privatsphäre der Verbindung dadurch erreicht, dass der Provider dem Kunden versichert, dass nur dieser und kein anderer die ihm zugewiesene Verbindung nutzt. Dies erlaubt dem Kunden, sein eigenes IP-Adress-Schema und seine eigene IT-Sicherheitspolitik auf die Verbindung anzuwenden. Dabei kann sich die Verbindung durchaus über mehrere Kommunikationsknoten erstrecken, die theoretisch von einem unbefugten Dritten kompromittiert werden können, der den Netzwerkverkehr beobachtet. Der VPN-Kunde vertraut dem Provider, dass dieser die Integrität der Daten wahrt, dass er die beste für den Geschäftsvorfall vorgesehene Verfügbarkeit bereitstellt und Vorkehrungen getroffen hat, so dass niemand den Netzwerkverkehr belauschen kann.

Im Zuge der aufkommenden Popularität des Internets als ein allgemeines Kommunikationsmittel wurde gleichzeitig Druck auf die Provider und auf die Unternehmen hinsichtlich der IT-Sicherheit ausgeübt. Es wurde erkannt, dass die Trusted VPN in dieser Form keine reale Sicherheit bieten können. Somit entstand eine zweite Art von VPN; die entsprechende Definition lautet wie folgt:

Secure VPN: In einem solchen VPN wird der Netzwerkverkehr verschlüsselt. Ausgehend vom Rand des Netzwerkes (*edge of one network*) oder direkt vom Computer selbst werden die VPN-Daten wie andere Daten – allerdings in verschlüsselter Weise – über das Internet transportiert. Am Ziel, d.h. am Computer oder im Unternehmensnetzwerk angelangt, werden die Daten entschlüsselt. Der verschlüsselte Netzwerkverkehr wird mittels einem Tunnel zwischen den zu überbrückenden Internetknoten eingerichtet. Ein unbefugter Dritter kann dabei lediglich erkennen, dass eine Kommunikation stattfindet. Diese ist aber für ihn unlesbar, und jede Änderung an dem Verkehrsstrom des Tunnels kann von den Kommunikationspartnern erkannt werden.

In diesem Zusammenhang haben die Provider begonnen, ihren Kunden einen neuen Typ von Trusted VPN anzubieten. Dieser neue Typ bietet nach wie vor keine reale Sicherheit, er ermöglicht allerdings den Unternehmen in sehr einfacher Weise, ein Netzwerksegment für das Weitverkehrsnetz (WAN) einzurichten und dieses von einem einzigen Punkt aus zu kontrollieren. Oftmals wird vom Provider dabei eine garantierte Dienstgüte (Quality of Service, QoS) bereit gestellt. Vor diesem Hintergrund hat sich eine weitere VPN-Definition durchgesetzt:

Hybrid VPN: Ein Hybrid VPN kann z.B. aus einem Secure VPN und einem Trusted VPN bestehen. Dabei wird i.d.R. das Secure VPN vom Unternehmen kontrolliert und beherrscht – entsprechend der Secure VPN-Definition. Außerdem besteht grundsätzlich die Möglichkeit, dass der Provider, der das Trusted VPN zur Verfügung stellt, ebenso das Secure VPN betreibt.

Unternehmen, die ein Trusted VPN bevorzugen, wollen i.d.R., dass ihre Daten über einen spezifischen Verkehrsweg vom Provider transportiert werden. Das Unternehmen vertraut dem Provider, dass der Verkehrsweg des VPN speziellen, zugesicherten Eigenschaften genügt, sie jedoch die Vertraulichkeit bestimmen können.

Es ist offensichtlich, dass die Secure VPN und Trusted VPN unterschiedliche Eigenschaften besitzen. Secure VPN haben zwar ein hohes Maß an Vertraulichkeit, jedoch keine Zusicherung über die Güte des Verkehrsweges, wie z.B. zeitliche Verzögerungen der IP-Pakete auf dem Transportweg oder Rate der Paktverluste. Trusted VPN dagegen besitzen Qualitätseigenschaften hinsichtlich des Verkehrsweges, jedoch keine oder eine geringe Vertraulichkeit. Beide haben Stärken und Schwächen. Allerdings gibt auch eine Anforderung, die für die Secure VPN, Trusted VPN und Hybrid VPN gleichermaßen gilt: Dem VPN-Administrator muss die Existenz des VPN bekannt sein und er muss zu jeder Zeit wissen, welche Daten ins VPN gelangen dürfen und welche nicht.

1.4 Überblick der VPN-Varianten

Virtuelle Private Netze haben ihren Ursprung in der Datenkommunikation, wenn man von der Sprachübertragung und der Deregulierung der Telekommunikation einmal absieht. Die für die Datenkommunikation eingesetzten Paketübermittlungsverfahren (Kapitel 2) schaffen *die* Voraussetzungen zum Aufbau logischer Verbindungen.

Der Wunsch nach gleichzeitiger Nutzung vorhandener Netzressourcen durch mehrere Nutzer lässt im Zeitmultiplex[6] keine feste Reservierung von Übertragungskapazitäten und damit keinen Aufbau physikalischer Verbindungen für einen Nutzer mehr zu. Lediglich der Weg, den die Informationen durch das Netz nehmen, wird festgelegt. Ressourcen und Bandbreiten werden nach Bedarf zugewiesen. Diese Eigenschaft wird in der Trennung der physikalischen Plattform von den darüber geführten Verbindungen erreicht. Das hinzugekommene Verbindungsnetz wird durch diese zusätzliche Verbindungsebene vollkommen von den Einrichtungen zum physikalischen Transport der Informationen entkoppelt. Der Begriff *Overlay-Netz* drückt diesen Zusammenhang aus.

Diese Form der Datenübermittlung, die mit Frame Relay- oder ATM-Netzen realisiert wird, ist in zweierlei Hinsicht sehr flexibel: Zum einen erlaubt sie eine hohe Granularität der Informationsbitraten der angeschalteten Informationsquellen. Das bedeutet, dass die Übertragungsbitraten beim Zugang zur Kommunikationsplattform variabel gestaltet werden können. Technische Veränderungen oder Anpassungen an der Kommunikationsplattform sind in der Regel nicht notwendig. Zum anderen lassen sich die logischen Verbindungen einfach festlegen.

[6] Unter Zeitmultiplex wird die feste Ressourcenzuordnung im Zeitscheibenverfahren verstanden.

Sie können permanent oder vermittelt eingerichtet werden. Bei den permanenten Einrichtungen werden die Netzelemente über das Netzmanagement entsprechend fest konfiguriert. Im zweiten Fall erlauben Verbindungsauf- und -abbauprozeduren das benutzergesteuerte Verwalten der Verbindungen. Beide Varianten führen zu wesentlich geringeren Betriebskosten dieser Plattformen im Vergleich zu den starren Netzen aus den herkömmlich festgeschalteten physikalischen Leitungen, wie z.B. die oben angesprochenen X.25-Leitungen. Der Aufbau eines VPN mittels Frame Relay oder ATM ist technisch auf das jeweilige Übermittlungsverfahren festgelegt. Plattformübergreifende VPN sind damit allerdings *nicht* zu realisieren. Für den Nutzer bedeutet dies, dass alle zu vernetzenden Lokationen einen einheitlichen Anschluss an die jeweilige Kommunikationsplattform erhalten müssen. Diese Notwendigkeit kann die räumliche Ausdehnung dieser Form der Virtuellen Privaten Netze, z.B. auf Landesebene, einengen. Unternehmen im Internationalisierungsprozess stoßen damit auf technologisch begründete Grenzen.

Eine global verfügbare Kommunikationsplattform stellt das Internet dar. „Internet“ ist der Sammelbegriff für eine Vielzahl unterschiedlicher lokaler Rechnernetzwerke und einzelner Rechner, die zur gegenseitigen Verständigung das Internet-Protokoll einsetzen. Es spielt keine Rolle, ob die Rechner oder die lokalen Netzwerke temporär über Wählnetze oder permanent über Festverbindungen, Frame Relay oder ATM angeschlossen sind. Auch die Hard- und Softwareausstattung ist unwichtig. Die Systeme können Daten austauschen und miteinander kommunizieren, solange das Internet-Protokoll verwendet wird. Das Internet bietet eine attraktive Kommunikationsplattform zum Aufbau internationaler oder weltweiter Unternehmensnetze. Neben der globalen Verbreitung können Zugangsmöglichkeiten bedarfsgerecht gestaltet werden. Standorte mit großen lokalen Netzsegmenten können hochbitratig angebunden werden. Einzelplatzsysteme wie Laptops oder Fest-PCs (Telearbeit) können im Bedarfsfall mittels Einwahl über öffentliche Wählnetze Verbindungen zum Internet herstellen. Die entstehenden Kosten sind dabei nutzungsabhängig abrechenbar.

Wie aber lässt sich das Internet zum Aufbau eines VPN nutzen? Zwei Dinge müssen erreicht werden: Erstens muss die Menge der Anschlusspunkte eines Unternehmens innerhalb einer geschlossenen Gruppe verwaltet werden. Zweitens muss die Privatsphäre im Sinne der VPN-Definition der ausgetauschten Daten gewährleistet sein. Die erste Forderung kann erreicht werden durch Abweisen aller IP-Pakete am Anschlusspunkt des Unternehmensstandortes zum Internet, die nicht von anderen zugelassenen Unternehmensstandorten stammen. Diese Selektion von IP-Paketen wird in diesem Zusammenhang als IP-Filterung bezeichnet.

Die Privatsphäre (Vertraulichkeit) wird im einfachsten Fall durch den Kunstgriff der *Tunnelbildung* gewährleistet. Im Internet wird jegliche Information in Form von Internet-Protokoll-Dateneinheiten ausgetauscht, die als IP-Datagramme bezeichnet werden. IP-Datagramme enthalten neben der eigentlichen Nutzinformation auch Informationen, von welcher Quelle das IP-Datagramm stammt und für welches Ziel es bestimmt ist. Anhand dieser Adressinformationen wird der Weg

im Internet bestimmt. Soll nun die Privatsphäre der Informationen bewahrt werden, müssen sowohl die Nutzdaten als auch die Adressdaten verschlüsselt werden, damit kein unbefugten Dritter (andere Internetnutzer, Vermittlungsknoten etc.) die Informationen im Klartext mitlesen können. Nach dem Verschlüsseln liegen jedoch auch die Adressen in keiner für die Vermittlungselemente des Internets lesbaren Form vor. Aus diesem Grund werden die verschlüsselten IP-Datagramme als Nutzdaten in andere IP-Datagramme gekapselt, deren Adressinformationen aus den Adressinformationen der zuvor unverschlüsselten IP-Datagrammen abgeleitet werden. Dieses Einpacken von Dateneinheiten eines Protokolls in Dateneinheiten desselben Protokolls wird als *Tunneln*[7] bezeichnet. Außer der Tunneltechnik gibt es noch weitere Verfahren, wie z.B. das *Label-Switching-Verfahren MPLS* (vgl. Abschn. 8.1), mit dem eine Verbindungsprivatisierung eingerichtet werden kann.

Die skizzierten Grundprinzipien erlauben den Aufbau von Unternehmensnetzen, und zwar sowohl mit dem Internet als globale Kommunikationsplattform als auch ohne Internet mit modernen Frame-Relay- und ATM-Verbindungen. Somit ist es schwierig, eine Varianteneinteilung vorzunehmen. Als eine mögliche Einteilung bietet sich ein technologisch unabhängiges Unterscheidungsmerkmal an:

Compulsory Mode: Mit dem Compulsory Mode[8] wird die Inanspruchnahme der Dienstleistung eines ISP bzw. NSP bezeichnet, der eine standortübergreifende Netzkopplung vornimmt. Erreicht werden kann dies z.B. durch ein *Virtual Private Trunking* (VPT) im Rahmen der Providereigenen ATM- oder Frame-Relay-Infrastruktur, indem *Permanent Virtual Circuits* (PVC) für die entsprechende Bandbreite reserviert werden. Der Benutzer nimmt diese wie eine normale Standleitung wahr. Da jedoch in der Regel keinerlei Sicherung der Inhalte stattfindet, ist ein VPT relativ leicht angreifbar, wenn der Zugriff auf die Infrastruktur eines Providers erfolgt ist. Oftmals versuchen Provider diese „Achillesferse“ mit einem *Virtual IP-Routing* (VIPR) zu unterbinden. Dabei sorgen feste private Routing-Tabellen für die korrekte Weiterleitung der IP-Pakete. Jedes IP-Paket nimmt dabei einen vorgegebenen Weg durch das Netz des Providers. Für einen Nutzer erscheint dagegen das Netz des Providers völlig transparent; selbst private IP-Adressen können gemäß [RFC 1918] zum Einsatz kommen. Dennoch schützt auch ein VIPR nicht vollständig vor fremdem Mitlesen der IP-Pakete. Deshalb setzen Provider vermehrt effektive Verschlüsselungsmechanismen ein.

Voluntary Mode: Der Voluntary Mode[9] benutzt zwar ebenso die Infrastruktur eines ISP oder auch NSP, doch die Kopplung wird von dem jeweiligen Unternehmen selbst realisiert. Dabei kommen zur Verbindungsabsicherung kryptographische Verfahren zum Einsatz. Diese haben zwei Aufgaben zu erfüllen:

---

[7] Der Begriff des Tunnels wird im Allgemeinen etwas weiter gefasst, siehe Abschn. 7.1.

[8] Dabei kann *Compulsory* mit dem Begriff „Verpflichtung“bzw. „obligatorisch “interpretiert werden.

[9] Dieser Begriff kann treffend mit „freiwillig “übersetzt werden.

Sie gewähren zum einen eine eindeutige Authentifizierung der Kommunikationspartner und sichern zum anderen die Integrität und die Vertraulichkeit der übermittelten Daten durch geeignete Verschlüsselungsverfahren. Diese Aufgabenteilung spiegelt sich in den eingesetzten kryptographischen Protokollen und Verfahren wider. Solche kryptographisch abgesicherten VPN arbeiten vorwiegend auf der Netzwerkebene (Layer-3) und unabhängig von der benutzten Infrastruktur. Allerdings haben sich VPN auch auf höheren Ebenen etabliert, wie z.B. mit dem SSL-Protokoll deutlich wird. Das SSL-Protokoll wird häufig bei Bestellungen bzw. beim Online-Banking im Internet eingesetzt.

Sollen externe Rechner oder Netze mittels eines VPN an das firmeneigene Netz gekoppelt werden, steht zunächst die grundsätzliche Entscheidung zwischen folgenden Konzepten an: Soll selbst eine entsprechende Infrastruktur aufgebaut werden oder soll auf die Dienste eines Internet Service Providers zurück gegriffen werden? An zwei Fallbeispielen werden nachfolgend die Anforderungen und unterschiedliche VPN-Konzepte diskutiert.

1.5 VPN-Leistungsspektrum

Werden heute Anforderungen an ein Virtuelles Privates Netzwerk gestellt, so sind die in Abb. 1.3 dargestellten Größen zu nennen. Angefangen von der Anbindung der Telearbeiter über die Bildung von virtuellen Teams bis hin zum unkomplizierten Datenverkehr mit zeitlich befristeten Geschäftspartnern gruppieren sich die VPN um das tägliche Geschäftsleben eines Unternehmens. Natürlich zeich-

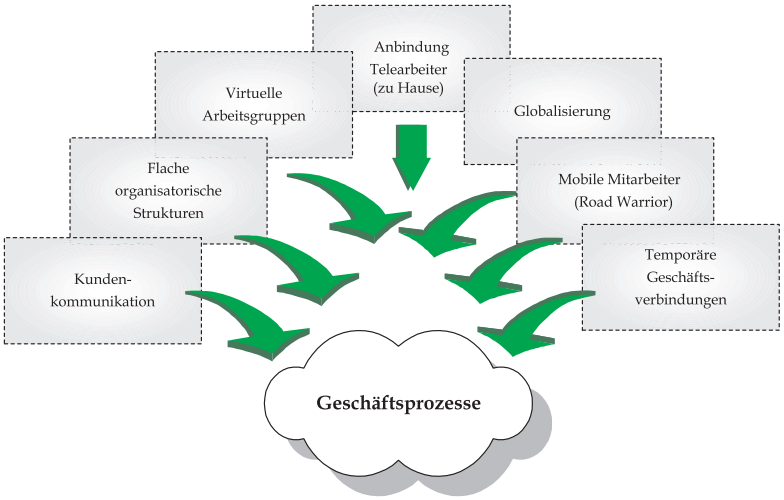


Abb. 1.3: Typische Geschäftsverflechtungen im heutigen Markt

nete sich dieser Trend zur Flexibilität und zum Umgang mit Geschäftspartnern nicht erst in den 90er Jahren ab. So wurde z.B. mit dem Produkt EDIFACT[10] ebenfalls versucht, unter Geschäftspartnern verbindlich zu kommunizieren. EDIFACT setzte *den* Kommunikationsstandard in der Automobilbranche der 70er Jahre. Die Kosten, die Dauer der Weiterentwicklung und die technischen Grenzen ließen EDIFACT jedoch gegenüber anderen Anwendungen zurückfallen.

Der Verband der Automobilindustrie hat in den späten 90ern ein Branchennetz, das *European Automotive Network* Exchange (ENX) realisiert. Es stellt ein VPN auf Basis des IP-Protokolls dar und zwar mit folgenden Anforderungen:

- Kopplung unternehmensübergreifender Geschäftsprozesse
- Frei wählbare Kommunikationsbeziehungen unter den Geschäftspartnern
- Höchste Sicherheitsanforderungen
- Integration altbewährter Kommunikationsdienste (z.B. OFTP oder E-Mail)
- Electronic-Business-Dienste aus der Steckdose

Bei der Entwicklung des ENX wurde konsequent das Ziel verfolgt, einen flächendeckenden einheitlichen (Daten-)Kommunikationsdienst zur optimalen Unterstützung der gesamten Wertschöpfungskette *Automobil* – zwischen den Handelspartnern mit unterschiedlichen Geschäftszwecken, beliebigen Unternehmensgrößen und Standorten – zu realisieren (Abb. 1.4).

Als Plattform wurde ein IP-Netz gewählt, das sich je nach Ausprägung auf ein ATM bzw. Frame-Relay-Weitverkehrsnetz stützt. Einzelne Handelspartner erlangen über einen lokalen Zugriffspunkt (PoP) mittels einer mit IPSec gesicherten Kommunikationsverbindung einen geschützten Datenaustausch mit einem anderen Handelspartner. Ein vertraulicher Datenaustausch zu den jeweiligen Kommunikationspartnern ist damit sichergestellt. Konkret bedeutet dies, dass der Zulieferer gemeinsam mit dem Hersteller auf der gleichen Datenbasis arbeitet und interaktive Zugriffe auf den gleichen Datenbestand möglich sind. Wird z.B. bei der Weiterentwicklung oder Veränderung eines Fahrzeugteils auch die Veränderung eines Bauteils eines Zulieferers notwendig, so kann mittels interaktivem Zugriff (CAD-Web) ein digitaler *Mock-up*[11] erstellt werden. Damit ist es dem Zulieferer möglich, nahezu zeitgleich seine Bauteile der Fahrzeugentwicklung anzupassen. Dieser sehr fortschrittliche Einsatz eines VPN zeigt durch seine hohe Flexibilität, wie wichtig es für die Automobilbranche geworden ist, eine moderne Kommunikationsinfrastruktur einzusetzen.

---

[10] EDIFACT ist die international eingeführte EDI-Sprache für Verwaltung, Wirtschaft und Verkehr der so genannten *Electronic Data Interchange For Administration, Commerce And Transport*. Mit EDIFACT (ISO 9735) ist ein internationaler Standard geschaffen worden, der branchenübergreifende Anforderungen erfüllt. Für den Versand der Daten steht der internationale Standard X.400 zur Verfügung.

[11] Unter dem Begriff *digitaler Mock-up* werden digitale Prototypen verstanden, die im Entwicklungsprozess gerade in der Automobilherstellung eine Reduzierung der physikalischen Prototypen bewirken und somit Einsparungen in Höhe von etwa 30% der Entwicklungszeit und -kosten erzielen.

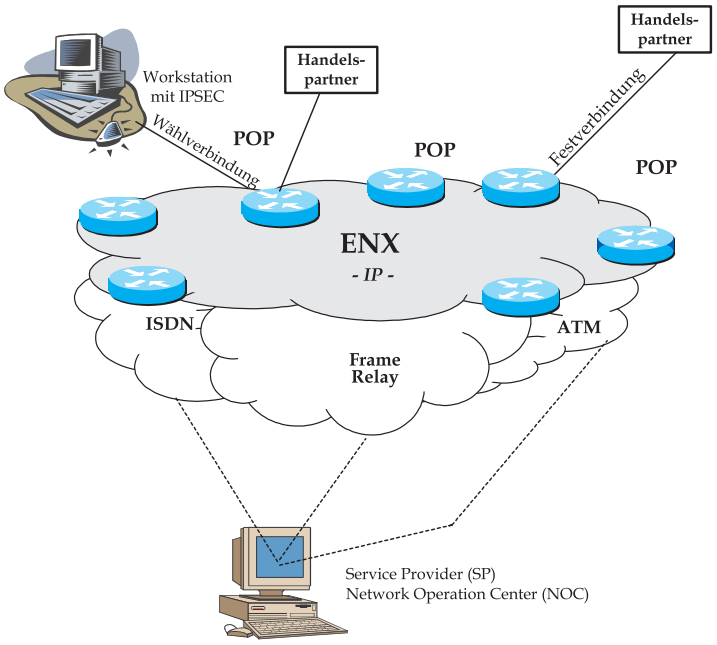


Abb. 1.4: Das europäische Extranet der Automobilindustrie mit seinen Zulieferern

Ein völlig anders gelagertes Beispiel für ein VPN (Abb. 1.5) ist aus dem Bereich des mobilen Datenzugriffs (Online-Verarbeitung) auf Unternehmensdaten. Mittels Kopplung von verschiedenen VPN-Technologien (IPSec, SSl) gepaart mit dem Server-based-Computing-Ansatz, besteht die elegante und gleichzeitig sichere Möglichkeit auf Daten zuzugreifen, die im Unternehmen lagern und die nur dort vorgehalten werden. Der Zugriff erfolgt mit einem PDA bzw. Tablet-PC über die Luftschnittstelle auf einen UMTS/GPRS-Sendemast. Die Verbindungsanfrage wird dann nach Authorisierung (PIN-Eingabe am Gerät) ins Internet zu einem Relay-Server weitergeleitet. Der Relay-Server gilt gleichzeitig als VPN-Gateway für das SSL-Protokoll. Die Datenübertragung innerhalb des SSL-VPN erfolgt mit einem speziellen Protokoll, das auch in der Lage ist, über schmale Bandbreiten genügend graphische Informationen zu transportieren. Anschließend baut der Relay-Server seinerseits ein IPSec-VPN auf, um über das Internet einen gesicherten Tunnel zu dem Eingangsrouter des Unternehmens aufzubauen. Transportiert wird innerhalb des IPSec-VPN das *Remote Desktop Protocol* (RDP). RDP erlaubt es von externer Seite auf Applikationen, die im Terminal-Server-Mode auf einem Windows-Server (z.B. Windows 2003-Server) installiert sind, zuzugreifen.

Wie in beiden Beispielen deutlich wird, können unterschiedliche Architekturen und Netzphilosophien eines VPN herangezogen werden. Auch die Vorstellung dessen, was ein VPN leisten muss, hat sich mittlerweile weiterentwickelt. Eine

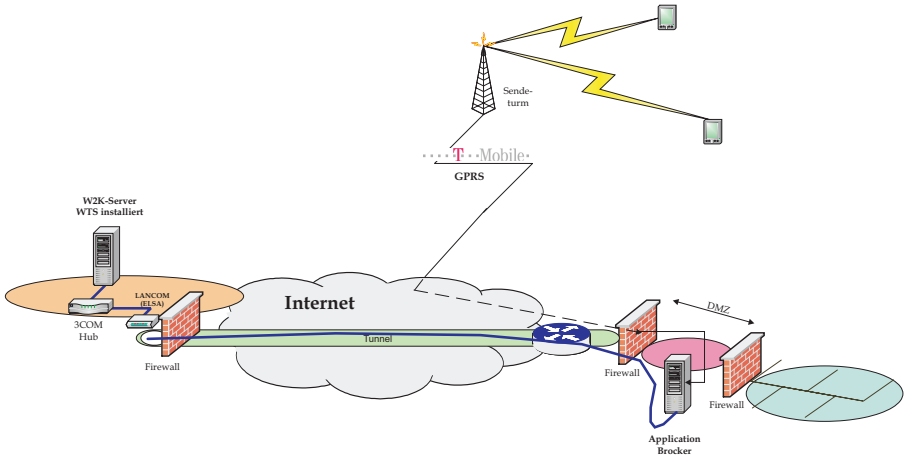


Abb. 1.5: Mobilität im Handwerk am Beispiel gekoppelter VPN-Technologien

Reihe von Attributen, wie z.B. Dienstgüten und Skalierbarkeit, sind hinzugekommen, so dass von einem VPN der ersten und zweiten Generation gesprochen werden kann. Um diese unterschiedlichen Architekturen und Netzphilosophien zu verstehen und ihre Ideen im Kern kennen zu lernen, wird über die vertikal orientierte OSI-Schicht – ausgehend von der physikalischen Leitung bis hin zur Applikation – im nächsten Kapitel eingegangen.

2 Grundlagen für VPN

In diesem Kapitel werden die erforderlichen Grundlagen zum Verständnis für die unterschiedlichen VPN-Technologien vermittelt. Es wird jedoch nur so weit auf die unterschiedlichen Technologien eingegangen, wie es aus der Sicht der unterschiedlichen VPN-Technologien nötig erscheint. In den Abschnitten 2.1 und 2.2.1 wird auf die Kommunikationstechniken in offenen Rechnernetzen sowie die Grundprinzipien der Kommunikation eingegangen. Anschließend wird der Begriff der Kommunikationstechnik, das Internet, welches in vielen Fällen eine der Plattformen für ein VPN darstellt, detaillierter erläutert.

Der Begriff wird heute synonym für eine Vielzahl von unterschiedlichen Rechnern verwendet. Typischerweise sind die beteiligten Rechnersysteme, Workstations, Router und Switches durch die herrschende Produktvielfalt bezüglich der Hardware-, Software- und Betriebssystemausstattung höchst verschieden. Dies gilt ebenso für die Ausstattung der lokalen Netzwerke (LAN), die z.B. im Fall eines Extranet-VPN untereinander über eine Internetverbindung Daten austauschen wollen.

Verbindendes Element ist das *Internet-Protokoll* oder kurz IP. Abschn. 2.3 beschreibt das IP-Protokoll und seine derzeit gebräuchlichsten Versionen IPv4 und IPv6 näher. Das IP-Protokoll wird nahezu durchgängig eingesetzt, um lokale Netzsegmente mit anderen Systemen zu vernetzen oder Einzelplatzsysteme über einen Internet Service Provider (ISP) an das Internet anzubinden. Dabei bestehen die Hauptnetzelemente des Internets aus Routern und den verbindenden Leitungen. Die Router stellen die Schaltstellen des Internets dar. Ihre Aufgabe besteht darin, Informationen schnellstmöglich weiterzuleiten und die dafür am besten geeigneten Wege zwischen den Kommunikationspartnern zu finden.

Dabei kommunizieren die Router untereinander mit eigenen Protokollen, wie z.B mit OSPF[1] in einem autonomen System. Aber auch aneinander grenzende Netze (autonome Systeme) kommunizieren mit grenzüberschreitenden Protokollen. Das *Border-Gateway-Protokoll* (BGP-4) ist das wohl älteste und gängiste. Weitere Ausführungen hierzu sind bei [Tanenbaum 2000] zu finden.

Zur Übertragung des IP-Protokolls zwischen den Routern werden unterschiedliche Verbindungstechnologien wie z.B. ATM und Frame Relay eingesetzt. Diese sind mittlerweile in der Lage IP direkt zu interpretieren, wie mit IP-over-ATM (IP-o-ATM) und IP-over-Frame-Relay (IP-o-FR) dargestellt werden soll. Beide Paketübermittlungsverfahren werden in den Abschnitten 8.3 und 8.4 diskutiert.

---

[1] OSPF bezeichnet ein von der IETF entwickeltes Link-Sate Routing-Protokoll und basiert auf einen von Dijkstra entwickelten Algorithmus. Es ist ein dynamisches Routing-Protokoll innerhalb eines autonomen Systems. Es hat mittlerweile das *Routing Information Protocol* (RIP) als Standard *Interior Gateway Protocol* (IGP) abgelöst.

Einzelplatzsysteme werden meistens über einen ISP mittels ISDN (*Integrated Services Digital Network*) an das Unternehmensnetzwerk (LAN) angebunden. Allerdings werden häufig auch digitale Fernsprechnetze mit analogen Zugängen, Funknetze gemäß GSM-Funkstandard und zukünftig wohl auch vermehrt GPRS/UMTS-Funknetze eingesetzt.

2.1 Verfahren der Kommunikationstechnik für ein VPN

Die elektronische Informations- und Nachrichtenübermittlung teilt sich in die beiden großen Kategorien *Nachrichtenvermittlung* und *Nachrichtenübertragung* auf. Beide sind erforderlich für den Austausch von Informationen – gleich welcher Art – zwischen den beteiligten Kommunikationspartnern und haben ihren festen Platz im OSI-Referenzmodell (Abb. 2.2), das später diskutiert wird.

Die reine Nachrichtenübertragung, die im Wesentlichen die Signalübertragung nach verschiedenen Methoden und Konzepten beinhaltet wie z.B. die *Puls-Code-Modulation-Technik* (PCM), die *Synchrone Digitale Hierarchie* (SDH) oder die *Wave Length Division Multiplex* (WDM), wird hier nicht weiter verfolgt. Abb. 2.1 zeigt die Nachrichtenübertragung im linken Teil der Abbildung in Form von Ellipsen.

Die Nachrichtenvermittlung dagegen nimmt einen breiten Raum des Buches ein und ist für das Verständnis der Virtuellen Netze unerlässlich. Sie unterteilt sich in die Gruppe Leitungsvermittlung[2] auch als Durchschaltevermittlung oder oftmals als *Circuit Switching* bezeichnet und Speichervermittlung[3] (*Message Switching*). Als dritte bedeutsame Vermittlungsvariante ist die Datenvermittlung zur Übertragung von Zeichenfolgen zu nennen. Abb. 2.1 zeigt die Nachrichtenübermittlung als Verzweigungsbaum.

Bei genauerer Betrachtung der Grundstruktur eines Weitverkehrsnetzes (WAN) fällt auf, dass dieses entweder auf einer Leitungsvermittlung oder auf einer Datenpaketvermittlung basiert (siehe auch Abschn. 8). Bei der leitungsvermittelten Struktur wird eine hierarchische Gliederung der Vermittlungsstellen

---

[2] Merkmal der Leitungsvermittlung ist, dass für die gesamte Dauer der Verbindung eine permanente Reservierung von Kanälen (Bandbreiten) zwischen Sender und Empfänger aufrechterhalten wird. Diese Verbindung ist den Kommunikationspartnern fest zugewiesen und bleibt auch dann bestehen, wenn in Sendepausen (z.B. Sprechpausen) die Leitung eigentlich nicht benötigt wird. Die herkömmlichen Fernsprechnetze (z.B. ISDN oder GSM) arbeiten nach diesem Vermittlungsverfahren.

[3] Kennzeichnend für eine Speichervermittlung ist, dass die Nachricht als Ganzes von Zwischenknoten zu Zwischenknoten übertragen wird *(Store-and-Forward-Switching)*. Jeder Zwischenknoten empfängt die vollständige Nachricht, trifft anhand der mitgeführten Adressinformation die weitere Wegewahl und sendet die Nachricht zum nächsten Zwischenknoten bzw. zum Endgerät. Aufgrund des zeitintensiven Zwischenspeicherns hat sich die spezielle Variante *Cut-Through-Switching* herausgebildet, in der die Adressauswertung und Nachrichtenweiterleitung vor ihrem vollständigen Empfang ausgeführt wird.

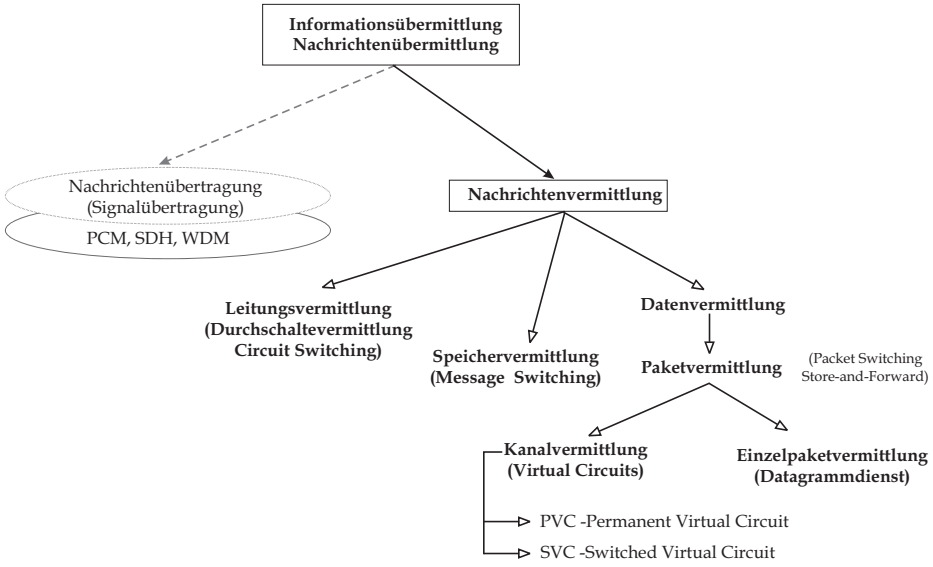


Abb. 2.1: Aufgliederung der Nachrichtenübermittlung

verfolgt. Die Vermittlungsstellen einer niederen Hierarchie sind linienförmig mit den Vermittlungsstellen der höheren Hierarchie verbunden.

Zum Bereich der Datenvermittlung wiederum gehört die Paketvermittlung (*Packet Switching*), die eine deutlich andere Netzstruktur aufweist als die Leitungsvermittlung. Es handelt sich hierbei um vermaschte Teilstreckennetze, deren Vermittlungsrechner, auch Knotenrechner genannt, mit mehreren anderen Knotenrechnern verbunden sind. Bei dieser Netzstruktur werden die Daten in Form von Datenpaketen von einem Knotenrechner zum nächsten durch das Netzwerk weitergereicht.

Bei der Paketvermittlung handelt es sich um ein asynchrones Zeitmultiplexing. Hier werden Nachrichten paketweise im Store-and-Forward-Verfahren über Teilstrecken von einem Netzknoten zum nächsten vermittelt. Dabei kann die Länge der Pakete bis zu einer Obergrenze variabel oder für alle Pakete konstant sein. Zu lange Nachrichten, die entweder die Obergrenze der Paketlänge oder die festgelegte konstante Länge der Pakete überschreiten, werden segmentiert und in mehreren Paketen sequentiell übermittelt.

Weiterhin werden die zu übertragenden Informationen bzw. Nachrichten als Daten – oder spezieller als Dateneinheiten – in einer Paketstruktur bei der Paketvermittlung transportiert. Informationen sind demzufolge Inhalte der übermittelten Dateneinheiten.

Die Datenpaketvermittlung bildet die Basis für Datenpaketnetze. Die Paketvermittlung hat zwei alternative Betriebs- bzw. Dienstarten. Dies sind zum einen

die *Einzelpaketvermittlung*, der Datagrammdienst, zum anderen die *virtuellen Verbindungen* (Virtual Circuits, VC), oft auch als Kanalvermittlung bezeichnet. Bei der Einzelpaketvermittlung bzw. *Kanaltechnik* wird jedes Paket mit einem Header ausgestattet, der die gesamten vermittlungsrelevanten Informationen enthält. Dies sind Adressinformationen von Empfänger und Absender, Hinweise zur Versendung, Routing-Informationen und Hinweise an den Empfänger. Die zu übertragenden Nachrichten werden in mehrere Datenpakete aufgeteilt. Bei diesem Verfahren wird jedes Datenpaket einzeln in loser Reihenfolge übertragen und von der empfangenen Station wieder zu einer vollständigen Nachricht zusammengesetzt. Dabei kann es vorkommen, dass die empfangenen Datenpakete – bedingt durch Datenpaketverluste, Überholung von Datenpaketen und ungewollte Duplizierung – unvollständig und durcheinander geraten sind. Dies macht es erforderlich, dass beim Empfänger Vorkehrungen getroffen werden, die die richtige Reihenfolge der Pakete wiederherstellen. Die Wiederherstellung der korrekten Reihenfolge wird als *Resequencing* bezeichnet und bei IP-Datagrammen von dem *Transmission Control Protocol* (TCP) vorgenommen.

Die zweite Vermittlungsart ist die Kanaltechnik (Abb. 2.1). Dabei werden virtuelle Verbindungen mittels logischer Kanäle gebildet. Bei diesem Verfahren gibt es eine Paketkarte mit allen Adressen, besonderen Leistungsmerkmalen, Informationen zum Routing usw., die im CALL-Paket übermittelt werden. Bei der Datenpaketvermittlung werden im Unterschied zur Leitungsvermittlung die Übertragungswege nicht exklusiv genutzt; daher die Bezeichnung virtuelle Verbindung.

Das Datenpaketvermittlungsprinzip unterscheidet zwei Arten von virtuellen Verbindungen: die feste virtuelle Verbindung (*Permanent Virtual Circuit*, PVC) und die gewählte virtuelle Verbindung (*Switched Virtual Circuit*, SVC). Bei der Datenpaketvermittlung wird die Übertragungsbandbreite bedarfsorientiert angefordert und kann gleichzeitig mehreren logischen Verbindungen zur Verfügung gestellt werden.

Beim Aufbau der virtuellen Verbindung wird in jedem Zwischenknoten eine Routing-Tabelle erzeugt, in der eingetragen wird, zu welcher Ausgangsleitung und zu welchem geeigneten Zwischenknoten die ankommenden Pakete einer Kommunikationsbeziehung weitergeleitet werden sollen. In den Abschnitten 8.3 und 8.4 werden mit Frame Relay und mit dem Asynchronen Transfer Modus zwei Hochgeschwindigkeitsübermittlungsverfahren, die Pakete in virtuellen Verbindungen übermitteln, eingehend diskutiert. Dabei verwendet Frame Relay, im Gegensatz zu ATM, Pakete variabler Länge, wenngleich es sich bei ATM nicht direkt um Pakete handelt, sondern um Zellen mit einer festen Länge.

2.2 Offene Kommunikation in Datennetzen

Ein offenes Kommunikationssystem ist ein System, das sich zum einen durch seine Schnittstellen eindeutig abgrenzen lässt, zum anderen die Fähigkeit besitzt, mit anderen Systemen in Form eines Nachrichtenaustausches zu kommunizieren und

zu kooperieren. Ein System kann gebildet werden durch Terminals, Computer, Computernetze und ganze LANs. Auch ein VPN, das weit auseinander liegende LANs einer Firma koppelt, stellt ein System dar. Dabei dient der Nachrichtenaustausch allein dazu, eine bestimmte Aufgabe gemeinsam zu erledigen. Abstrakt betrachtet bedeutet dies, dass eine herstellerübergreifende freizügige Kommunikation ermöglicht wird, indem standardisierte Prozeduren in offenen Systemen für den Informationsaustausch genutzt werden. Die standardisierten Prozeduren beinhalten genormte Regeln und Protokolle, die das Systemverhalten bestimmen. Die Protokolle legen dabei nicht die interne Struktur des offenen Systems fest, sondern speziell sein äußeres Verhalten. Die genormten Regeln beschreiben Funktionen, die in Protokolle münden und angewandt werden. Die einzelnen Funktionen werden in einem allgemeinen Referenzmodell hierarchisch definiert und in Schichten bzw. Layer des Referenzmodells vertikal gegliedert. Beispielsweise setzt der Datenaustausch zwischen zwei räumlich weit voneinander entfernten Rechnern (Systemen) wie z.B. in einem VPN voraus, dass die Daten ihren Weg zielgerichtet über erforderliche Zwischenknoten zum Zielsystem finden. Eine iterative, mittels Zwischenknoten abgestützte Weiterleitung der Daten bzw. Nachrichten erfordert allerdings eine fehlerfreie Datenübertragung, die aufgrund des Einsatzes qualitativ hochwertige Kabel zunehmend gewährleistet ist. Zudem muss a) ein geeignetes Übertragungsmedium zwischen den Netzelementen (Zwischenknoten) vorhanden sein und es müssen b) die Daten bei der Übertragung an die Eigenschaften des Mediums angepasst werden.

Als Gedanken- bzw. Architekturmodell hat hierzu Anfang der 80er Jahre das internationale Standardisierungsgremium *International Organization for Standardization* (ISO) ein Referenzmodell für die Kommunikation offener Systeme (*Open Systems Interconnection*, OSI) vorgeschlagen, das die Kommunikationsfunktionen für Rechnersysteme über offene Datennetze in sieben Schichten einteilt ([X.200 1994]). Inzwischen ist dieses Modell in allen Bereichen der technischen Kommunikation und weit über die reine Datenkommunikation hinaus anerkannt. Alle modernen Kommunikationnetze orientieren sich an den Prinzipien und Festlegungen des OSI-Referenzmodells. Auch wenn spezielle Systeme in manchen Punkten Anpassungen des Modells erforderlich machten – wie beispielsweise für ATM-Systeme – behalten viele Prinzipien ihre Gültigkeit.

2.2.1 Die Architektur des OSI-Referenzmodells

Abb. 2.2 skizziert die sieben Schichten des OSI-Referenzmodells am Beispiel der Kommunikation zweier Rechner, die über zwei Netzknoten Daten miteinander austauschen. Die sieben Schichten bzw. Layer lassen sich grob in zwei Abschnitte, den der Transportprotokolle und den der Anwendungsprotokolle, untergliedern. Die Anwendungen, angesiedelt in der obersten Schicht, stellen in diesem Modell die eigentlichen Quellen und Senken der Kommunikation dar. Dabei folgt das OSI-Referenzmodell drei Grundprinzipien:

1. Funktionen, die für die Kommunikation notwendig sind, sind geschichtet.

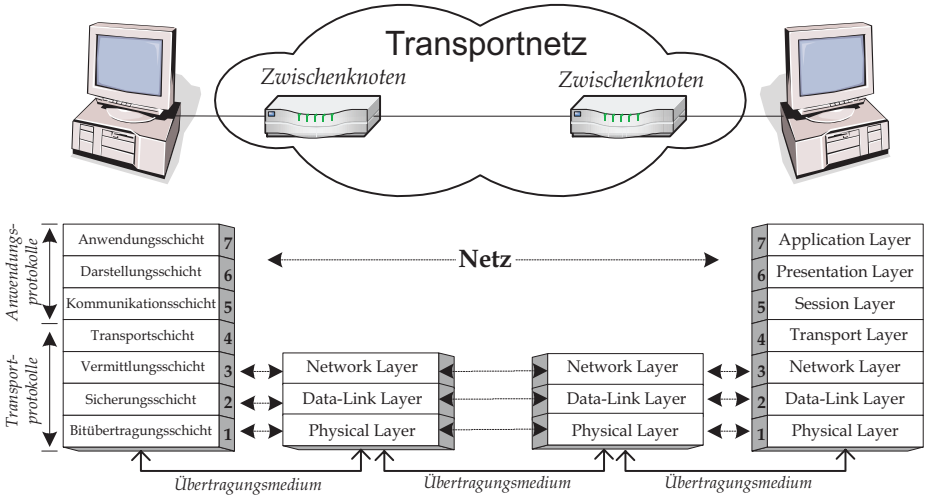


Abb. 2.2: Das Sieben-Schichten-OSI-Referenzmodell

2. Dienstleistungen werden für über- und untergeordnete Schichten erbracht.
3. Protokolle führen die Kommunikation zwischen Schichten gleicher Ebene aus.

Diese Grundprinzipien werden in den nächsten Abschnitten detailliert erläutert.

2.2.2 Die sieben OSI-Funktionen

Das OSI-Referenzmodell ist ein Gedankenmodell, bei dem die Kommunikation stringent in aufgabenbezogene, funktionale Schichten untergliedert ist. Dabei bilden die Schichten 1 bis 4 die Transportfunktionen. Die Schichten 5 bis 7 beschreiben die Anwendungsprotokolle (vgl. Abb. 2.2). Ihre Aufgaben und Funktionen sind:

Schicht 1, Physical Layer: Die Bitübertragungsschicht stellt die Parallel-Seriell-Wandlung in binäre Signale zur Übertragung für eine Übertragungsstrecke bereit. Zu dieser werden auch die physikalischen Anschlussbedingungen gerechnet, wie z.B. die Übertragungsbitrate, elektrische bzw. optische Charakteristika der Schnittstellen im Netz. Die Bitübertragungsschicht stellt im Grunde die Funktionen zur Übertragung der Bitsequenzen bereit, die von der übergeordneten Schicht erzeugt bzw. an diese übergeben werden. Die zentrale Funktion besteht darin, die Bitsequenzen in physikalische Sendesignale umzusetzen und diese an die Eigenschaften des Übertragungsmediums anzupassen. Eine entsprechende Modulationstechnik sorgt für eine optimale Anpassung

des Leistungsdichtespektrums der Sendefolge an die zur Verfügung stehende Bandbreite, die sich stark an den Eigenschaften des eingesetzten Mediums orientiert.

Schicht 2, Data-Link-Layer: Die Sicherungsschicht enthält fehlersichernde Übertragungsmechanismen. Damit wird die ungesicherte Übertragung der Schicht 1 mit Hilfe der Funktion von Schicht 2 in eine gesicherte Übertragung überführt. Verfahren zur Fehlererkennung und -korrektur sorgen dafür, dass auf jedem Wegeabschnitt Bitübertragungsfehler erkannt und behoben werden. Weiterhin findet eine Datenaufteilung in Blöcke, Blocknummerierung, Generierung und Auswertung von Prüfbytes der Schicht 3 statt.

Schicht 3, Network Layer: Die Vermittlungsschicht ist verantwortlich für den Aufbau der Durchschaltevermittlung sowie für die Überwachung der physikalischen Verbindung. Es wird festgelegt, wie eine Netzverbindung zwischen den Endsystemen zu Stande kommen soll. Bei paketvermittelter Kommunikation werden zusätzliche Funktionen zur Steuerung und Kontrolle des Transfers der Pakete sowohl für die Signalisierungs- als auch für die Nutzdaten ausgeführt. Hierzu gehört z.B. die wichtige Flusskontrolle der Pakete.

Schicht 4, Transport Layer: Die Transportschicht überwacht, steuert und beendet den Transport der Protokolldateneinheiten und führt die logische Verknüpfung der beteiligten Endgeräte durch. Weiterhin wird eine Anpassung an unterschiedliche Netzeigenschaften, Ende-zu-Ende-Fehlerkontrolle, Adressübersetzung und bei Bedarf eine Datensegmentierung vorgenommen.

Schicht 5, Session Layer: Die Kommunikationsschicht führt die Kommunikationssteuerung durch. Zu dieser gehören Auf- und Abbau sowie Kontrolle und Verbindungsidentifikation der logischen Verbindungen zwischen den Prozessen, also z.B. die Dialogsteuerung zwischen einem Endgerät und einer entfernten Datenbank. Als weitere Aufgabe obliegt ihr die Synchronisation von verteilten Prozessen ebenso wie die Umschaltung zwischen unterschiedlichen Betriebsarten einer Applikation. Die Session Layer hält Transportaufgaben von der Anwendung fern und stellt für diese Koordinationsdienste bereit, wie in [ISO 8326:1987] und [ISO 8327:1987] detailliert beschrieben wird.

Schicht 6, Presentation Layer: Die Darstellungsschicht legt fest, wie die Informationen in einer gemeinsamen Sprache auszutauschen und darzustellen sind. Explizit wandelt sie Datenstrukturen – z.B. Alphabet-Konvertierung und gegebenenfalls eine Datenkompression – um und passt diese an das von den Endgeräten erwartete Format an.

Schicht 7, Application Layer: Die Anwendungsschicht führt die System- und Anwendungssteuerung durch, bereitet die Nachrichteninhalte für die Kommunikation auf und bildet die Quelle und Senke einer Kommunikation. Ebenso wird der Kommunikationspartner identifiziert und eine Berechtigungsprüfung vorgenommen. Weiterhin wird eine Wahl der Übermittlungsgüte und Übermittlungsparameter getroffen.

2.2.3 Die OSI-Dienste

Grundsätzlich ist jeder Schicht (N) ein entsprechendes Dienstkonzept zugeordnet. Diesem Konzept liegt eine Diensterbringung (Sicherung) zugrunde, die nicht nur der nächsthöheren, sondern allen darüberliegenden Schichten von Nutzen ist. Eine höhere Schicht $(N+1)$ nutzt somit die Summe aller ihr untergeordneten Schichten. Dabei entspricht eine Schicht (N) einer Instanz, häufig als *Entity* bezeichnet, die z.B. als Arbeitseinheit übersetzt werden kann. Instanzen der Schichten kommunizieren lediglich mit der jeweils vertikal benachbarten Schicht, also nach oben $(N+1)$ und nach unten $(N-1)$. Die nicht unmittelbar an N (z.B. für $N=7$) angrenzenden Schichten $(N-2), (N-3), ..., (N-5)$ werden von Schicht N nicht wahrgenommen. Sie sind für die Schicht N völlig transparent (Abb. 2.3). In horizontaler Richtung nimmt eine Schicht (N) nur die auf gleicher Ebene eines benachbarten Netzelementes befindlichen Schicht[4] (N) wahr (dies deuten die horizontalen Pfeile in Abb. 2.2 an). Die vertikale Kommunikation zwischen den Schichten erfolgt über Dienstelemente (*Primitives*), die die kleinsten unteilbaren Nachrichteneinheiten darstellen. Die Primitives kommunizieren dabei mit dem jeweiligen Dienstzugangspunkt[5] (*Service Access Point*, SAP) einer Schicht (Abb. 2.3). Es existieren vier Primitives:

Request: Die Schicht N fordert einen Dienst der Schicht $N-1$ an.

Indication: Die Schicht $N-1$ teilt der Schicht N einen Request mit.

Response: Die Schicht N antwortet auf eine Indication der Schicht $N-1$.

Confirmation: Die Schicht $N-1$ beantwortet einen früheren Request der Schicht N.

Dabei fügt jede Schicht (N) den Daten (*Service Data Unit*, SDU) für die nächsthöhere Schicht $(N+1)$ Protokollinformationen (*Protocol Control Information*, PCI) hinzu. Zusammen bilden diese die Protokolldateneinheiten (*Protocol Data Unit*, PDU) einer Schicht. Abb. 2.3 zeigt die vertikale Kommunikation zwischen den Schichten $(N-1, N, N+1)$ mittels Dienstelementen. Beim Durchlauf der einzelnen Schichten im OSI-Referenzmodell wiederholt sich dieser Vorgang. Auf der anderen Seite, z.B. im Endgerät des Empfängers, werden beim Durchlauf von unten nach oben jeweils Protokollinformationen abgezogen, bis schließlich die eigentlich zu übertragenden Informationen übrig bleiben. Die Protokollinformationen werden von der Empfängerschicht ausgewertet und weiterverarbeitet. Dabei ist das Schichtenprotokoll, das das äußere Verhalten eines Systems bestimmt, im Allgemeinen standardisiert.

---

[4] Die horizontal kommunizierenden Schichten werden oft auch als *Peer-N-Instanzen* oder *N-Entitys* bezeichnet.

[5] Allerdings können auf einen Dienstzugangspunkt mehrere Verbindungen von einer höheren Schicht zugreifen (*Multiplexen*), so dass auf der Empfängerseite die Daten zu den unterschiedlichen Verbindungen aufgeteilt werden müssen (*Demultiplexen*). Der umgekehrte Vorgang (*Splitten*) ist ebenso möglich, indem eine Schicht die Daten der höheren Schichten auf mehrere Verbindungen der tieferliegenden Schichten verteilt, die dann auf der Empfängerseite wieder zusammengefügt werden müssen (*Recombining*).

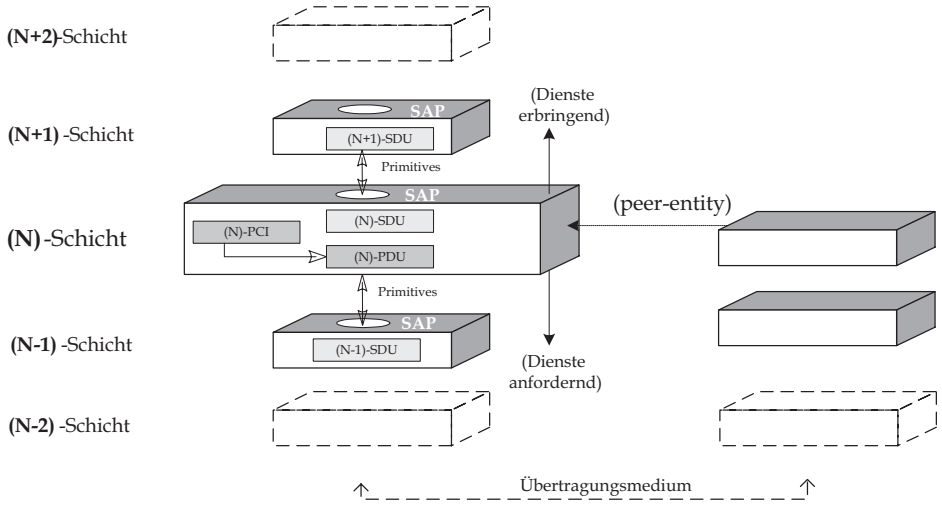


Abb. 2.3: Vertikale Kommunikation zwischen Schichten im OSI-Referenzmodell

Nachfolgend wird näher auf die Protokolle der Schichten eingegangen; hier sind die Schichten 1 bis 4 des OSI-Referenzmodells transportorientiert (Abb. 2.2) und von spezieller Bedeutung. Sie regeln nicht nur den Zugang zum Netz – dies ist Aufgabe der Schicht 1 bis 3 –, sondern sind auch für den Transport der Daten über das Netz von Endgerät (Datenendeinheit, DEE) zu Endgerät verantwortlich.

2.2.4 Die OSI-Protokolle

Um den Dienst einer bestimmten Schicht erbringen zu können, kommuniziert die entsprechende Instanz mit der Instanz der gleichen Schicht im Partnersystem, ihrer Partnerinstanz (*Peer Entity*). Die Kommunikation mit der Partnerinstanz geschieht durch Austausch von Nachrichten. Der vorgeschriebene Austausch dieser Nachrichten wird Protokoll genannt. Jede Schicht im OSI-Referenzmodell hat ein solches Schichtenprotokoll, um den ihr zugewiesenen Dienst an die höheren Schichten erbringen zu können.

Die OSI-Protokolle sind herstellerneutrale Protokolle, die die einzelnen Schichten des OSI-Referenzmodells funktional unterstützen. In der Anfangsphase, nach der Standardisierung des Referenzmodells im Jahre 1983, wurden einige Protokolle für die Transportschicht die Kommunikationssteuerungsschicht und die Anwendungsschicht entwickelt. Tab. 2.1 gibt einen Überblick der gängigen Protokolle in den einzelnen Schichten.

Die Bitübertragungsschicht (Layer-1) wird von den OSI-Protokollen in allen erdenklichen Mechanismen, vom einfachen Modem bis zum 2 Gbit/s Crossconnect-

Tabelle 2.1: Liste der gängigen OSI-Protokolle

OSI-Referenzmodell	**ISO/OSI-Protokolle**
Anwendungsschicht	X.400 (ISO 10021) FTAM (ISO 8571) CMIP (ISO 9596) CMIS (ISO 9595) X.500 (ISO 9594) VTS (ISO 9040,9041)
Darstellungsschicht	OSI-Präsentation ISO 8822/8823 ASN.1 ISO 8824/8825
Kommunikationsschicht	OSI-Session ISO 8326 CLNP ISO 8327 CONS
Transportschicht	OSI-Transport ISO 8473 CLNP ISO 8602 CONS
Vermittlungsschicht	OSI-CLNM, OSI-Cons ISO 8473 CLNP ISO 8348 CONS ISO 8878 und ISO 8208-X.25 ISO 9542 ES-IS-Protokoll ISO 10584 IS-IS-Protokoll
Sicherungsschicht	LAPB, LLC Ethernet (CSMA/CD) IEEE 802.3 Token-Bus IEEE 802.4 FHSS, DSSS IEEE 802.11 Token-Ring IEEE 802.5 Logical Link-Controller für:
Bitübertragungsschicht	Telefon/ISDN Punkt-zu-Punkt Punkt-zu-Multipunkt FHSSS, DSSS Token-Ring IEEE 802.5 ATM

Switch, unterstützt. Die Protokolle der Sicherungsschicht (Layer-2) unterstützen alle Zugangsverfahren, angefangen vom *High Level Data Link Control* (HDLC), *Logical Link Control* (LLC), CSMA/CD, Token-Bus und Token-Ring bis zu FDDI. Die Vermittlungsschicht (Layer-3) ist bei den OSI-Protokollen zweigeteilt. Die Unterteilung erfolgt in der Unterstützung verbindungsloser und verbindungsorientierter Dienste. Als Inter-Domain-Routing-Protokolle sind ES-IS und IS-IS zu nennen. Die Transportschicht (Layer-4) sorgt für eine transparente Verbindung zwischen den Endsystemen. Der entsprechende Dienst steht in verbindungsloser oder verbindungsorientierter Form zur Verfügung. Die Transportprotokolle bieten unterschiedliche Transportklassen und Dienstgüten. Insgesamt stehen fünf Transportklassen zur Auswahl. Die Kommunikationssteuerungsschicht (Layer-

5) ist aufgeteilt in verbindungslose und verbindungsorientierte Dienste. Die Darstellungsschicht (Layer-6) benutzt als Codier- bzw. Decodiersprache die *Abstract Syntax Notation*, Vers. 1 (ASN.1). Für die Anwendungsschicht (Layer-7) werden anwendungsspezifische Protokolle bereitgestellt. Die bekanntesten sind FTAM, X.400, X.500, VTS, CMIP und CMIS.

Das Prinzip über den Austausch von Protokollen lässt sich theoretisch gut mit Hilfe endlicher Automaten beschreiben, indem ein Protokollaustausch als Prozesskopplung verstanden werden kann. Der Prozessbegriff bei endlichen Automaten[6] beschreibt innere Zustände (z.B. *idle*, *transition*, *initial state*, *final state*), Zustandsänderungen und Eingangs- und Ausgangssignale zum Austausch von Botschaften und Protokolleinheiten als Träger der Botschaften. Durch Zustandsübergänge (transition) werden andere wohldefinierte Zustände (z.B. final state) erreicht. Ausgelöst z.B. durch ein bestimmtes Eingangssignal erzeugen diese vorgegebene Ausgangssignale. Erst durch die Kopplung der Prozesse in den Partnerinstanzen über den Austausch von Protokolldateneinheiten (PDU) wird der eigentliche Dienst einer Schicht erbracht. Der Ablauf des Protokolls wird als Prozedur bezeichnet.

Das OSI-Referenzmodell dient heutzutage im Allgemeinen zur Orientierung bei Neuentwicklungen oder Ergänzungen von bestehenden Kommunikationstechnologien. Dabei werden die getroffenen Zuordnungen – in Form von sieben Schichten – nicht immer von allen Technologien eingehalten. Zum Teil finden sich Abweichungen in den in einzelnen Schichten bereitgestellten Funktionen, zum Teil werden Funktionen mehrerer Schichten in einer zusammengefasst. Ein Beispiel für eine spezielle Modifikation ist die von der IEEE vorgeschlagene IEEE-Protokollarchitektur für Zugriffsverfahren auf ein geteiltes Medium in lokalen Netzen. Dabei sind die Funktionen der Layer-2 auf drei Teilschichten unterteilt, die von oben nach unten als Logical Link Control-, Framing- und Medium Access Control-Teilschicht benannt wurden ([IEEE 802.2] und [IEEE 802.3]). Auf den Begriff der Data-Link-Layer wurde dagegen verzichtet.

Eine Protokollarchitektur mit weniger als sieben Ebenen liefert das Internet-Schichtenmodell. Bei diesem Modell kommen lediglich fünf Schichten zur Anwendung. Tab. 2.2 zeigt die Unterschiede zwischen OSI-Layer und Internet-Protokoll-Architektur. Die Schichten 1 bis 4 sind analog zu denen des OSI-Referenzmodells gehalten, dagegen werden die Funktionen der OSI-Schichten 5 bis 7 im Internet in der Application Layer zusammengefasst.

Für die VPN-Technologie sind einige der Absicherungsmöglichkeiten für die einzelnen Schichten, die nach und nach entwickelt wurden, von erheblicher Bedeu-

[6] Die Theorie der endlichen Automaten findet in der Informatik eine breite Anwendung [Raasch 1992]; dabei ist der Begriff der endlichen Automaten eine Umschreibung der diskreten dynamischen Systeme. Es gibt im Prinzip die Klasse der kombinatorischen und die Klasse der sequentiellen Maschinen, die zu den endlichen Automaten gezählt werden. Endliche Automaten kommen überall dort zum Einsatz, wo (große) Systeme ihr internes und externes Verhalten durch aktuelle und vergangene Ereignisse ändern. Die Theorie wird auch bei der Risikoanalyse von komplexen Systemen mit Zustandsänderungen eingesetzt, wie z.B. in [Böhmer 1998b] detailliert ausgeführt wird.

tung. Diese werden in Kapitel 6 eingehender diskutiert. Zunächst soll das für die VPN-Technologie wichtige Internet-Protokoll in den Versionen IPv4 und IPv6 betrachtet werden.

2.3 Das Internet-Protokoll in der Version IPv4 und IPv6

Das Internet-Protokoll definiert einen unzuverlässigen verbindungslosen Übertragungsmechanismus, der oftmals nur mit seiner Kurzform (IP) bezeichnet wird. Geprägt wurde das IP, das auf der Vermittlungsschicht (Layer-3) (Abb. 2.2) angesiedelt ist, durch das *Transmission Control Protocol* (TCP, TCP/IP) sowie das *User Datagram Protocol* (UDP) auf Transportebene (Layer-4). [RFC 791, 793 und 768] definieren die Protokolle; ausführlicher ist allerdings z.B. [Comer 1995].

Obwohl das IP in seiner Version IPv4 längst nicht mehr dem Stand der Technik entspricht, definiert es doch drei wesentliche Eigenschaften, die weiterhin in der offenen Kommunikationswelt ihre Gültigkeit behalten:

1. IP definiert die Basiseinheit des Datenverkehrs, die überall in TCP/IP-Netzwerken genutzt wird. Es spezifiziert das exakte Datenformat.
2. IP-Software ermöglicht eine Wegefindung. Die so genannte Routing-Funktion ermittelt iterativ einen Weg von der Quell- bis zur Zieladresse.
3. Das IP-Protokoll hält eine Reihe von Regeln parat, die eine ungesicherte (unzuverlässige) Paket-Versendung beinhalten. Diese Regeln folgen Handlungsanweisungen, wie Router und Host bei Fehlermeldungen verfahren sollen und unter welchen Bedingungen Pakete verworfen werden sollen.

Das Internet-Schichtenmodell hat eine etwas andere Entwicklung genommen als die vom OSI/ISO-Referenzmodell abgeleitete Protokollarchitektur. Diese folgt dem OSI/ISO-Referenzmodell nicht vollständig. Eventuell liegt dies an der früheren Entwicklung des Internet-Schichtenmodells. Tab. 2.2 zeigt die beiden Schichtenmodelle im Vergleich und ergänzt Abb. 2.2 durch die Internet-Protokollbeispiele. Die vor dem ISO-Referenzenmodell entwickelte Internet-Protokollarchitektur ist mit Anpassungen zur darunterliegenden Leitungsebene und zur darüberliegenden Applikationen verbunden. Zwischen einem physikalischen Netzwerk und der IP-Architektur besteht eine recht große Ähnlichkeit. In einem physikalischen Netzwerk wird die Übertragungseinheit als Frame bezeichnet, die aus einem Protokollkopf und den Transportdaten besteht. Der Protokollkopf liefert dabei Informationen wie z.B. über die physikalische Quell- und Zieladresse. Bei der IP-Architektur heißt die Basis-Übertragungseinheit *Internet Datagram* oder kurz IP-Datagramm, das – vergleichbar mit einem physikalischen Netzwerk – in Protokollkopf und Transportdaten aufgeteilt ist. Im Protokollkopf sind ebenfalls Quell- und Zieladressen gespeichert. Im Fall von IP handelt es sich um IP-Adressen, beim Frame-Protokollkopf um physikalische Adressen.

Tabelle 2.2: Vergleich zwischen OSI-Layer und Internet-Schichtenmodell

OSI-Layer	**Internet**	**Internet-Protokollbeispiele**
Applikation	Anwendungen	Telnet (Virtual Terminal) FTP (File Transfer Protocol) SMTP, RPC , HTTP
Presentation		
Session		
Transport	Transport	TCP UDP
Network	Network	IP
Link	LLC und MAC	IEEE 802.3
Physical	Medium	Koax, Twisted Pair, Fiber

Im Hinblick auf eine Reihe von Anforderungen, für die das IP-Protokoll ursprünglich nicht ausgelegt war, wurde seit 1995 eine grundlegende Überarbeitung der Version IPv4 vorgenommen, die nach einer Zwischenversion schließlich in der Version 6 (IPv6) ihren vorläufigen Abschluss fand. Für weitere Vertiefungen sind [RFC 1881-1888] und [RFC 2460-2467] aufschlussreich. Wichtige Erweiterungsfelder betreffen den zu knapp gewordenen Adressraum mit nun 128 Bit für Quell- und Zieladresse statt der bisher 32 Bit. Weiterhin wurde eine bessere Unterstützung für Quality-of-Service-Anforderungen (Abschn. 2.3.3) und für Sicherheitsmaßnahmen (vgl. Abschn. 7.4) erreicht, wie Verschlüsselungs- und Authentifizierungsverfahren, und zwar unter Verwendung von zusätzlichen Protokollköpfen.

Das Internet-Protokoll beherrscht die gesamte Kommunikationswelt im Datenbereich (Paketvermittlung) und künftig auch die im Sprachbereich. Mit dem sich mehr und mehr durchsetzenden SIP[7] -Protokoll gegenüber dem H.323-Protokoll in der IP-basierten Sprachübertragung Voice-over-IP, VoIP, scheint sich die Prognose zu bewahrheiten. Dies trifft ebenso für die herkömmliche VPN-Technologie zu, die im Wesentlichen durch dynamisch zugewiesene Bandbreiten gekennzeichnet ist. Das Internet-Protokoll beherrscht auch VPN der zweiten Generation, die durch Privatsphäre, Dienstgütenparameter, wie Quality of Service (QoS) und Class of Service (CoS) , oder auch durch MPLS geprägt sind.

Aufgrund dieser elementaren Bedeutung für die VPN-Technologie ist es wichtig, sich mit dem IP-Protokoll eingehend auseinander zu setzen, speziell mit den Unterschieden zwischen IPv4 und IPv6. Abb. 2.4 zeigt das IPv4- und das IPv6-Protokoll im Vergleich, um Gemeinsamkeiten und Unterschiede hervorzuheben. Die Bildlegende zeigt, in welchen Feldern bei IPv4 Veränderungen vorgenommen

[7] Das *Session Initiation Protocol* (SIP) wurde im März 1999 von der IETF [RFC 2543] als Standard für die Übermittlung interaktiver Kommunikationsdienste einschließlich Sprache über IP-basierte Netze vorgeschlagen. SIP ist aus den Protokollen SMTP und HTTP hervorgegangen, d.h. SIP verwendet für die Kommunikation zwischen SIP-Client und SIP-Server textbasierte Nachrichten.

und welche Felder gänzlich entfernt wurden.

Ein gern eingesetzter Schutz für ein VPN, das über eine IPv4-Overlaystruktur geführt wird, erfolgt durch IPSec (Abschn. 7.4). Stellt IPSec beim IPv4-Protokoll noch eine Ergänzung dar, ist es beim IPv6-Protokoll weitsichtig in die Spezifikation, neben dem größeren Adressraum, mit aufgenommen worden. In absehbarer Zeit wird sich IPv6 flächendeckend durchsetzen – Schätzungen zufolge in der zweiten Hälfte des Jahres 2005 beziehungsweise im Jahre 2006. Somit ist eine hinreichende Absicherung des IP-Protokolls systemimmanent gegeben. Deshalb wird in diesem Abschnitt nur kurz auf das IPv4-Protokoll eingegangen, um dann auf die Vorzüge des IPv6-Protokolls und dessen Unterschiede zu IPv4 hinzuweisen.

IPv4 wurde 1981 als Standard spezifiziert [RFC 791]. Die ersten Diskussionen darüber, dass der 32-Bit IPv4-Adressraum, d.h. eine theoretische Adressierung von 2^{32} Endgeräten zu knapp für eine globale Expansion des Internets ist, kamen schon Ende der achtziger Jahre auf. Diese Abschätzungen gaben der IETF Anlass, sich mit einer neuen Protokollversion zu beschäftigen. Denn IP-Adressen wurden klassenbasiert vergeben. Die meisten Hochschulen, Forschungseinrichtungen und Unternehmen nutzten zu dieser Zeit Class-B-Adressen. Aufgrund dieser Prognosen initiierte die Internet Engineering Task Force (IETF) die ROAD-Arbeitsgruppe, um das Routing weiterzuentwickeln. Zu den Ergebnissen der Arbeitsgruppe zählen mehrere Hilfskonstruktionen wie das *Classless Internet Domain Routing* (CIDR) und Techniken wie das *Network Address Translation* (NAT).

Zunächst wirft der Sprung von der Versionen 4 auf 6 die Frage auf, was mit Version 5 geschah. Die IP-Version 5 (IPv5) gab es nur im Labor. Im Protokollkopf des Internet-Protokolls existiert zwar ein Versionsfeld, das bei IPv4 den Wert 4 und bei IPv6 entsprechend den Wert 6 enthält. Eine *5* an dieser Stelle kennzeichnet ein experimentelles Protokoll für Echtzeitströme, das ST-2 (*Internet Stream Protocol*, Version 2) hieß und das vom RSVP (*Resource Reservation Protocol*) zur Bandbreitenanforderung bei Routern) abgelöst wurde. Damals war ST-2 vorgesehen um Audio- und Videosignale per Multicast zu übertragen und somit die Bandbreiten-Reservierungsvorteile, die ATM bietet, in IP-Netze zu bringen. Doch dieser Ansatz gelangte nie zur Serienreife.

Aus heutiger Sicht erscheint das IPv4-Protokoll überholt und nicht mehr zeitgemäß in seinen Möglichkeiten. Allerlei Hilfskonstruktionen und Ergänzungen sind eingeführt worden, die sich auch bei der VPN-Technologie niederschlagen bzw. diese beeinflussen. So wurde z.B. der aufkommenden Adressknappheit mit einer Umsetzungsmethode, auch bekannt als NAT (*Network Address Translation*), begegnet. In Abschn. 6.2.2 wird NAT in Zusammenhang mit einer Firewall näher behandelt. Ein ähnlicher Ansatz, um der Adressknappheit zu begegnen, wurde bei flüchtigen, also nicht permanenten, IP-Adressen mit DHCP (*Dynamic Host Configuration Protocol*) erreicht (vgl. Abschn. 2.3.1 und Abschn. 7.4.8). Weiterhin wurden Ergänzungen, um einen möglichen kalkulierbaren kontinuierlichen Datagrammstrom zu ermöglichen. Um den Anforderungen nach QoS gerecht zu werden, RSVP entwickelt, um unter IPv4 die Reservierung von Ressourcen und damit

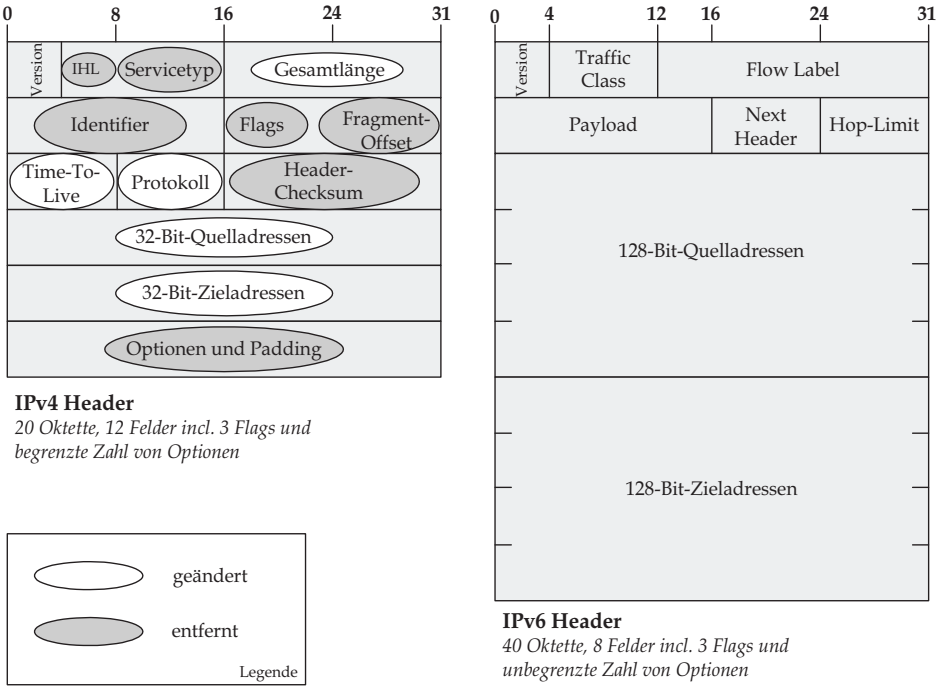


Abb. 2.4: Strukturvergleich zwischen dem Kopffeld des herkömmlichen komplexen IPv4- und des neuen, vereinfachten IPv6-Protokolls

QoS-Garantien zu realisieren. Abschn. 2.3.4 widmet sich dieser Problematik.

Da sich der eingeschlagene Weg einer Ressourcenreservierung und damit Garantien für einen Quality of Service im IPv4-Netz zu realisieren als schwer gangbar erwies, wurde die Idee der Class of Service (CoS) verfolgt. Das Prinzip der Serviceklassen soll ermöglichen, dass sich ein Unternehmen für seinen wichtigen Datenverkehr einen besseren und damit teureren Service erkaufen kann als z.B. private Anwender, die eher günstige Tarife vorziehen.

Das bestehende IPv4-Protokoll besitzt ein Feld mit der Bezeichnung Servicetyp (Abb. 2.4), das der Idee des Quality of Service sehr nahe kommt. In diesem Feld bezeichneten ursprünglich die ersten 3 Bits die Art und Priorität des Datenverkehrs, mit den folgenden 3 Bits konnten erhöhte Anforderungen an Verzögerung, Bandbreite und Zuverlässigkeit gestellt werden und die letzten 2 Bits waren reserviert für zukünftige Entwicklungen. Heutzutage wird dieses Feld nur von wenigen Routern in seiner ursprünglichen Form interpretiert. Ein Ansatz, der dieses nahezu obsolete Feld Servicetyp reaktiviert und mit geänderter Struktur für priorisierbaren Datenverkehr verwendet, also eine Einteilung des Datenverkehrs in verschiedene Quality of Service bietet, sind die *Differentiated Services* (DiffServ) die im Abschn. 2.3.4 diskutiert werden. Neben den Problemen der

Adressknappheit und der Dienstgüten in IP-Netzen galt es, die ineffiziente Fragmentierung zu verbessern, ein Mobile-IP-Konzept zu entwerfen und eine Antwort auf die Multicast-Anforderungen der heutigen geschäftlichen Kommunikation zu geben.

Eine für die VPN-Technologie wichtige Ergänzung erfuhr das IPv4-Protokoll mit der IPSec-Spezifikation bzw. dem IPSec-Framework (vgl. Abschn. 7.4). Damit wird der ungesicherten Datagrammübertragung auf Netzebene, die Pakete mit Hilfe von Routing-Verfahren unter Umständen auf verschiedenen Wegen von einer Quelle zum Ziel befördert, Rechnung getragen.

2.3.1 BOOTP/DHCP und Mobile-IP

In der Regel benötigt ein System drei Informationen, um mit einem TCP/IP Netzwerk zu kommunizieren: die IP-Adresse, um das System im Netzwerk eindeutig zu identifizieren, die Subnetzmaske, um das Netzwerk bzw. untergeordnete Teile des Netzes zu bestimmen, und die Adresse eines Router, falls das System auch mit anderen Geräten bzw. Netzwerken kommunizieren soll. Diese drei Informationen bilden die minimale Angabe, die für eine Kommunikation mit einem TCP/IP-Netzwerk ausgetauscht werden muss. Gerade für die VPN-Technologie, speziell für die Remote-Access-VPN (End-to-Site), ist es wichtig, von entfernt gelegenen Standorten, wie z.B. einem Hotel oder einem Bahnhof, bei Bedarf eine gesicherte Verbindung zum Firmennetzwerk zu erhalten (vgl. Abschn. 7.4.8).

Die Grundidee, um temporär mit einem Netzwerk zu kommunizieren, ist dem in die Jahre gekommenen *Bootstrap Protocol* (BOOTP) [RFC 951] entlehnt, das eine Weiterführung und Verbesserung mit dem *Dynamic Host Configuration Protocol* (DHCP) [RFC 2131, RFC 2132] erfahren hat. Doch diese Flexibilität ist noch nicht ausreichend für heutige und zukünftige Kommunikationsanforderungen. Erst in dem jüngst spezifiziertem Mobile-IP [RFC 2002] scheint eine geeignete Lösung gefunden zu sein.

Bootstrap Protocol (BOOTP)

BOOTP wurde mit dem Ziel entwickelt, Computer (Terminals), die ohne Festplatte (*diskless hosts*) ausgestattet sind, über ein Netzwerk zu booten. Es erlaubt die notwendige automatische Initialisierung, um die erforderlichen Bootparameter über das Netz ins Terminal zu laden. Dabei spezifiziert BOOTP nicht, wie der notwendige Ladevorgang (Download) des Betriebssystem ins RAM des Terminals geschieht. Dies wird mittels TFTP (*Trivial File Transfer Protocol*) [RFC 906] vollzogen. Manuelle Tastaturbefehle sind dabei nicht erforderlich. Mittels diese Art der simplen Terminals – die aus heutiger Sicht als *Thin Clients* bezeichnet werden – wurden später Workstations und Router (mittels BOOTP) konfiguriert.

Der BOOTP-Prozess beinhaltet folgende Schritte:

1. Das Terminal ist durch eine eigene Hardware-Adresse bestimmt, die sich normalerweise im ROM des Terminals befindet.

2. Nach Anschalten des Terminals sendet dieses mittels UDP-Datagramm die Hardware-Adresse zum Server. Im Regelfall kennt das Terminal seine eigene IP-Adresse und die des Servers nicht und schickt die IP-Adresse (0.0.0.0) unter Ausnutzung der UDP-Portnummer (67) mit der Broadcast-Adresse (255.255.255.255) zum Server.
3. Der Server erkennt das Terminal an der mitgeschickten Hardware-Adresse und sucht die dazugehörigen Konfigurationsdaten nebst IP-Adresse des Terminals aus seinen Tabellen heraus. Der Server füllt dann die verbleibenden Felder des angekommenen Datagramms auf und schickt dies an den UDP-Port (68) des Terminals zurück. Dabei existieren drei unterschiedliche Methoden, auf die hier nicht weiter eingegangen werden soll. Dem Leser sei hierzu [Comer 1995] empfohlen.
4. Erreicht das zurückgeschickte UDP-Datagramm das Terminal, erhält das Terminal seine eigene IP-Adresse und kann den Bootstrap-Prozess beginnen.

Mittels BOOTP kann von zentraler Stelle aus eine beliebige Anzahl von Terminals, die mit dem BOOTP-Server Kontakt aufnehmmen wollen, konfiguriert werden. Allerdings ist zuvor eine statische Tabelle mit Einträgen für jedes Terminal anzulegen und zu pflegen.

Dynamic Host Configuration Protocol (DHCP)

Ein wesentlicher Nachteil bei BOOTP besteht darin, dass jeder Host statisch im Netz eingebunden sein muss. Wenn eine BOOTP-Konfigurationsnachricht einmal erstellt ist, wird sie ständig verwendet und ändert sich so gut wie nicht. Somit ist BOOTP ungeeignet für mobile Notebooks, die unregelmäßig im Netz angemeldet sind und keine eigene permanente IP-Adresse benötigen. Die nicht benötigten IP-Adressen können aber bei IP-Adressmangel temporär an andere Geräte vergeben werden. D.h. das mobile Endgerät erhält keine feste IP-Adresse, sondern eine zum jeweiligen Netzwerk, in dem es sich gerade befindet, passende Adresse. Genau für diese Anforderungen – der dynamischen Zuweisung von IP-Adressen und Konfigurationsparametern – ist das DHCP spezifiziert worden. Somit pendelt die Anzahl der vergebenen IP-Adressen in einer Domain um einen Mittelwert.

DHCP geht in seiner Grundspezifikation auf das [RFC 2131] und auf das [RFC 2132] zurück, das eine enge Verbindung bzw. eine Weiterentwicklung des BOOTP-Protokolls darstellt. Das Dynamic Host Configuration Protocol (DHCP) ist im Prinzip ein Framework zur Konfigurationsweitergabe eines Hosts in einem TCP/IP-Netzwerk. Außerdem bietet es eine Weiterentwicklung hinsichtlich einer automatischen und wiederverwendbaren Netzwerkadresse mit Konfigurationsdaten.

Für eine Implementierung von DHCP sollten die zwei folgenden sicherheitsrelevanten Punkte beachtet werden:

- DHCP basiert auf UDP und ist damit im Prinzip unsicher. Im normalen Gebrauch könnte sich ein nicht autorisiertes Endgerät in einem DHCP-fähigen

Netzwerk problemlos einbuchen und ggf. Informationen wie Passwörter u.ä. ausspähen. Es erhielte eine gültige IP-Adresse und Konfiguration, da keine Sicherungsmöglichkeiten bestehen. Dies könnte allerdings unterbunden werden, wenn auf den Endgeräten voreingestellte IP-Adressen, verknüpft mit einer MAC-Adresse, angewandt werden. Bei dieser Lösung geht allerdings ein großer Vorteil von DHCP verloren, da der Arbeitsaufwand der Administratoren erheblich steigt und die dynamische Wiederverwendung von nicht benötigten Adressen entfällt.

- In einem DHCP-fähigen Netzwerk, in dem eine dynamische Adresszuweisung vorgenommen wird, ist zu keinem Zeitpunkt vorherzubestimmen, welche IP-Adresse welchem Endgerät zugewiesen wird. Dies führt im Falle eines statischen DNS-Server unmittelbar zu Problemen, da eine Namensauflösung und IP-Adresszuordnung unmöglich wird. Insofern zieht ein DHCP-fähiges Netzwerk auch sofort eine dynamische Namensauflösung, ein *Dynamic Domain Name System* (DDNS), nach sich. Dabei beruht DDNS auf der allgemein verwendeten, am Berkeley Institut entwickelten *Berkeley Internet Name Domain* (BIND).

Allerdings muss berücksichtigt werden, dass DDNS in seiner Spezifikation keine speziellen Sicherheitsfunktionalitäten aufweist. Somit sind für die Verwendung von DHCP/DDNS, in Verbindung mit einem Remote-Access-VPN, Nachbesserungen erforderlich (Abschn. 7.4.8).

Abb. 2.5 zeigt den Vorgang der Einbuchung eines mobilen Endgerätes (Notebooks) in ein Netzwerk in vier Schritten. Neben einem DHCP-Server wird auch ein DDNS-Server angesprochen. Zum einfacheren Verständnis des Ablaufes sind hier der DHCP-Server und der DDNS-Server getrennt dargestellt. Im regulären Betrieb befinden sich diese beiden Dienste auf einem Computer.

Eine Einbuchung in vier Schritten verläuft wie folgt:

1. Der DHCP-Client führt den üblichen Datenaustausch mit einem DHCP-Server durch, um Konfigurationsdaten und IP-Adresse anzufordern.
2. Der DDNS-Client, ebenfalls auf dem Endgerät installiert, schickt eine Aktualisierungsnachricht *(update request)* inklusive der vom DHCP-Server erhaltenen IP-Adresse zum DDNS-Server, um den in der DDNS-Datenbank befindlichen *Resource Record*, der für das Endgerät eingerichtet wurde, zu finden. Begleitend wird ein öffentlicher Schlüssel *(Public Key)* mitgeschickt; gleichzeitig werden alle Resource Records mit einer digitalen Signatur versehen. Die Kombination von Schlüssel und Signatur identifiziert das Endgerät eindeutig und damit ist der Rechnername *(hostname)* gültig. Falls die Aktualisierung gelingt, wird diese in der Datenbank aufgenommen und ab sofort ist das Endgerät mit seinem Rechnernamen ansprechbar.
3. Im Anschluss fordert der DHCP-Client eine *lease renewal message* vom DHCP-Server. Diese Nachricht enthält neben zwei Zeitstempeln den für gültig erachteten Rechnernamen.

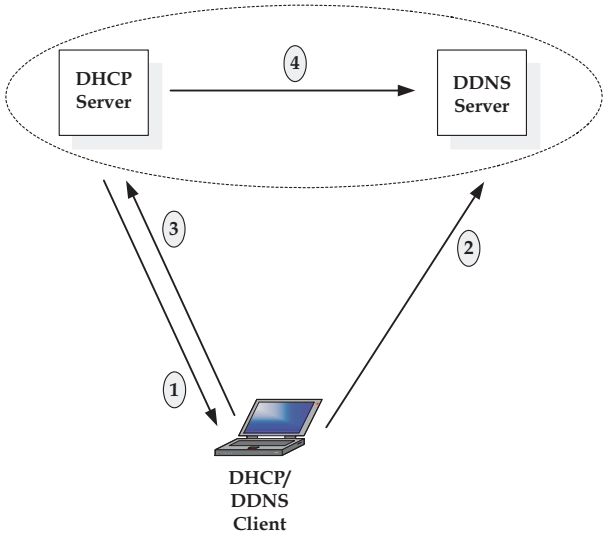


Abb. 2.5: Nachrichtenaustausch bei einer DHCP-Netzanmeldung

4. Abschließend schickt der DHCP-Server eine Aktualisierungsnachricht *(PTR Resource Record*[8]*)*, in der sich eine Zuordnung von IP-Adresse und Rechnernamen befindet, zum DDNS-Server.

Die Grundidee des BOOTP- und des DHCP-Protokolls, bei denen das Endgerät keine eigene permanente Netzwerkadresse besitzt und diese entweder statisch oder dynamisch zugewiesen bekommt, ist nicht die einzige moderne Idee einer Zuweisung von Netzwerkadressen in einem TCP/IP-Netzwerk. Die Umkehrung der Idee, dass ein mobiles Endgerät immer nur eine einzige IP-Adresse besitzt, egal in welchem Netzwerk sich das Endgerät eingebucht hat, wird mit Mobile-IP verfolgt.

Mobile-IP

Mit Mobile-IP, einem Standardprotokoll gemäß [RFC 2002], gelingt der Datentransport über mehrere Netze hinweg, ohne eine IP-Adressänderung einzurichten und ohne Konflikte in einem der bestehenden Netze zu erzeugen. Mobile-IP hält die kontinuierliche Verbindung eines Routers mit dem Internet auch in verschiedenen Netzen aufrecht. So können beispielsweise Passagiere in Flugzeugen oder Zügen über mobile Endgeräte wie Laptops oder PDAs jederzeit und ohne Unterbrechung auf das Internet zugreifen.

[8] DNS wird üblicherweise verwendet, um zu einem Namen die dazugehörige IP-Adresse zu ermitteln. Im umgekehrten Fall, wenn die IP-Adresse bekannt ist, jedoch nicht der Name, ist zur reversen Auflösung ein *Pointer Record* (PTR) erforderlich.

Normalerweise ist ein Gerät mit einer IP-Adresse, das in einem anderen Subnetz eingebracht wurde, nicht erreichbar. Mobile-IP jedoch erlaubt einem Gerät, immer die gleiche IP-Adresse *(home address)* zu nutzen. Dies wird durch eine temporäre IP-Adresse *(care-of-address)*, die jeweils in das umgebene IP-Netz (Domain) passt, erreicht. Jedes Paket, das zum mobilen Endgerät geschickt wird, wird vom dazugehörigen Agenten des Endgerätes im Heimatnetz abgefangen und durch einen Tunnel zur temporären IP-Adresse (Gastadresse bzw. c/o-Adresse) geschickt. Nach Durchqueren des Tunnels wird das IP-Paket dem eigentlichen Endgerät übergeben. Das mobile Endgerät dagegen nutzt ausschließlich seine eigene IP-Adresse, die im Heimatnetz definiert ist. So können IP-Pakete ohne Adressprobleme wieder zurückgeschickt werden. Beim Zurücksenden wird dann der reguläre Standard-Routingweg eingeschlagen.

Abb. 2.6 zeigt, wie ein IP-Paket, von einem Netzsegment (10.160.10.0./24) abgeschickt, vom Host (A) zum mobilen Endgerät (B) gelangt. Dabei werden vier Schritte durchlaufen, falls das mobile Endgerät eine Antwort zurückschickt:

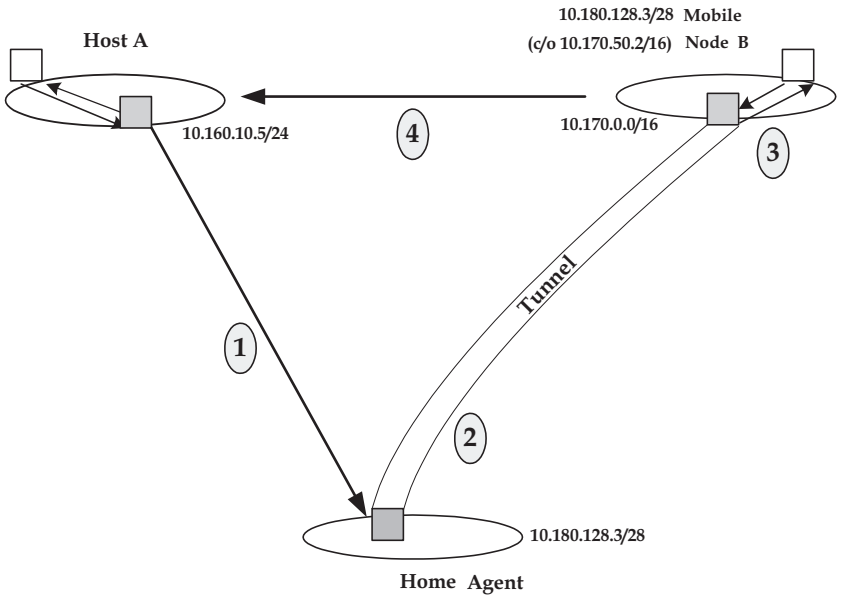


Abb. 2.6: IP-Paketaustausch

1. Host (A) (10.160.10.5/24) schickt in seinem Netzsegment eine Nachricht (Datagramm) an Host (B), ein mobiles Endgerät mit der Zieladresse (10.180.128.3/28). Die Router im Netzsegment (10.160.10.0/24) erkennen, dass sich die Zieladresse außerhalb des eigenen Segments befindet und routen das Paket in das aus maximale 14 Hosts bestehende Netzsegment (10.180.128.0/28).

2. Im Netzsegment (10.180.128.0/28) wird der lokale Agent des mobilen Endgerätes aktiv, fängt das Datagramm ab und baut einen Tunnel zur augenblicklichen Gastadresse *(care-of-address)* des mobilen Endgerätes auf.
3. Der im Gastnetz (10.170.0.0/16) verweilende Agent erwidert die Tunnelanfrage; mit einer IP-in-IP-Kapselung wird ein Tunnel[9] errichtet. Anschließend gelangen die IP-Pakete in das Gastnetz, in dem sich das mobile Endgerät augenblicklich befindet. Durch die Gastadresse (10.170.50.2/16), die dem Endgerät beim Einbuchen ins Gastnetz zugewiesen wurde, ist eine aktuelle Zieladresse für die IP-Pakete vorhanden. Sie können Host (B) nunmehr erreichen.
4. Für eine Antwort, die an Host (A) gerichtet ist, wird vom mobilen Endgerät nicht der Tunnel genutzt, sondern die regulären Routing-Mechanismen eines TCP/IP-Netzwerkes.

Die Heimatadresse *(home address)* definiert eine statische Adresse, die stets zum mobilen Endgerät gehört und nicht getauscht wird – dies ist also völlig anders als bei BOOTP und DHCP. Ebenso gehört zur Heimatadresse des mobilen Endgerätes ein Subnetz mit einem IP-Präfix, in dem sich die Heimatadresse befindet.

Interessant ist nun die Frage, wie das Gastnetz das mobiles Endgerät identifiziert, das eine temporäre IP-Adresse benötigt. Dies geschieht durch wiederholt ausgesendete spezielle *Internet Control Message Procotol*-Nachrichten (ICMP), den so genannten *agent advertisement messages*, die das Netzwerk von der Existenz des mobilen Endgerätes unterrichten. Falls ein neu ins Netz eingebuchtes Endgerät aufgrund dieser speziellen Nachrichten erkennt, dass es sich in seinem Heimatnetz befindet – in der Abb. 2.6 ist dies die Domain (10.180.128.3/28) –, wird der Mobile-IP-Service nicht benutzt und arbeitet mit seiner Heimatadresse. Wenn sich das neu eingebuchte Endgerät aber in einem fremden Netz befindet, erhält es von diesem eine Gastadresse. Diese Gastadresse kann z.B. mittels DHCP zwischen dem Gastagenten und dem mobilen Endgerät ausgehandelt werden. In [RFC 2002] sind zwei unterschiedliche Verfahren beschrieben, die jedoch beide auf einen Austausch von bestimmten UDP-Datagrammen zurückgehen. Dabei wird die Registrierungsanforderung zum Port 434 geschickt.

Bemerkenswert ist, dass die Kommunikation zwischen dem Gastagenten und dem mobilen Endgerät auf dem Link Layer geschieht, da die normalen IP-Routing-Mechanismen erst eingesetzt werden können, wenn eine Gast-IP-Adresse erfolgreich vergeben wurde. Andernfalls wäre das mobile Endgerät nicht erreichbar.

Die skizzierte Lösung ist flexibel und einfach zu realisieren, da die neue Funktionalität keine spezielle Software benötigt, sondern auf jedem IP-fähigen Router eingesetzt werden kann. Darüber hinaus kann Mobile-IP die Gefahr eines möglichen Adressenengpass minimieren; der Administrationsaufwand für Geräte, die oftmals in unterschiedlichen Netzen eingebunden sind, reduziert sich.

[9] Grundlegende Ausführungen zur Tunneltechnik sind im Abschn. 7.1 zu finden.

2.3.2 Ende-zu-Ende-Flusskontrolle mittels TCP

Die zwei wichtigsten Protokolle der Transportschicht sind heute das *User Datagram Protocol* (UDP) [RFC 768] und das *Transmission Control Protocol* (TCP) [RFC 793]. Vielleicht wird sich dies durch das *Real Time Transport Protocol* (RTP) [RFC 1889, 1890] zur Übertragung für multimediale Daten in Echtzeit ändern. UDP und RTP[10] werden in diesem Kontext nicht weiter verfolgt, siehe dazu beispielsweise [Stevens 1994] oder [Comer 1995].

Ausschlaggebend für die weitere Betrachtung von TCP ist seine herausragende Bedeutung für das IP. Außerdem bietet TCP eine Eigenschaft, die sowohl für die VPN-Technologie als auch für Frame Relay und ATM bedeutsam ist: es ist die Fähigkeit, ein *Virtual Circuit* (VC) zu bilden. Das Attribut *virtuell* vermittelt der Anwendung den Eindruck, dass ein eigens für sie geschalteter Kanal zur Verfügung steht. Real erfolgt der Datentransport durch ein paketvermitteltes IP-Netz, das keine Kanäle kennt, sondern Datagramme verschickt.

Die grundsätzliche Aufgabe der Transportschicht besteht darin, separate Kommunikationsbeziehungen zwischen Anwendungsprogrammen zu ermöglichen, die potenziell auf verschiedenen Computern (Host-Systemen) ablaufen. Häufig wird als Umschreibung der TCP-Transportaufgabe der Begriff einer *Ende-zu-Ende-Kommunikation* verwendet. Zur Paketunterscheidung einzelner Anwendungsprogramme, die den Computer auf der Transportschicht verlassen, dienen reservierte Portnummern, die einen dezimalen Wert zwischen 0 – 1023 einnehmen können, als *well-known ports*. Die dezimalen Werte *(ephemeral ports*[11]*)* von 1024 – 65535 sind frei verfügbar und können beliebig eingesetzt werden. Ein Tripel aus Protokoll, Portnummer und IP-Adresse wird als *Socket* bezeichnet. Sockets stellen Kommunikationsendpunkte dar. Jeder TCP-Verbindung ist eindeutig einem Socketpaar zugeordnet. Eine weitere Aufgabe der Transportschicht ist die Steuerung des Informationsflusses sowie die Gewährleistung einer zuverlässigen *(reliable)* Kommunikation. Zwar basiert diese auf der ungesicherten Zustellung von IP-Datagrammen *(Best Effort)*, dennoch werden bei einer Fehlererkennung automatisch geeignete Maßnahmen wie Bestätigungsprozeduren *(acknowledgement)* und Sendewiederholungen *(re-transmission)* getroffen.

TCP arbeitet verbindungsorientiert und bietet Anwendungen jeweils einen zuverlässigen, innerlich jedoch nicht strukturierten Bytestrom an, über den sie kommunizieren können. Eine TCP-Verbindung hat immer genau zwei Endpunkte, durch die sie eindeutig identifiziert wird. Broadcast und Multicast sind allerdings nicht direkt anwendbar, da diese UDP benötigen.

Abb. 2.7 zeigt ein TCP-Segment, bestehend aus einem TCP-Kopf und TCP-Daten, die in einem IP-Datagramm transportiert werden. Der TCP-Kopf besteht aus 20

---

[10] Das RTP-Protokoll wird auch als Unterstützungsprotokoll für Sprachübertragungen in IP-Netzen (VoIP) hinzugezogen.

[11] „Ephemerisch“ stammt vom griechischen *ephemeros* ab, was so viel bedeutet wie kurzlebig, vergänglich.

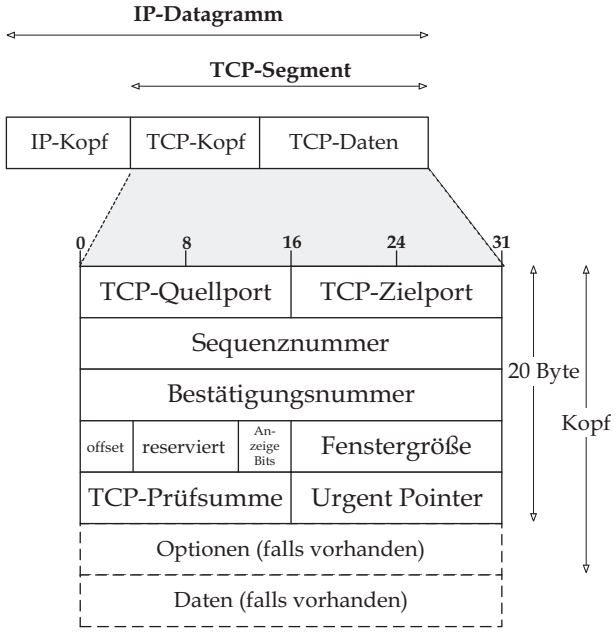


Abb. 2.7: TCP-Segment eingebettet in ein IP-Datagramm

Bytes, gegenüber 8 Byte eines UDP-Kopfs. Doch die genaue TCP-Kopfgröße hängt jeweils von den Optionen ab. Die Bedeutung der einzelnen Felder in der Abb. 2.7 ist hier zusammengestellt:

- Zusammen mit den beiden IP-Adressen im IP-Kopf dient der jeweils 16 Bit umfassende Quell- und Zielport zur eindeutigen Identifikation einer TCP-Verbindung.
- Die 32 Bit breite Sequenznummer beschreibt die Position der Daten eines Segmentes im Bytestrom des Senders. Beim Verbindungsaufbau legt der Sender die erste ISN-Sequenznummer[12] *(Initial Sequence Number)* fest. Ebenso wird das SYN-Flag gesetzt. Da TCP in einem Duplexbetrieb arbeitet, muss jede Seite ihre eigene Sequenznummer verwalten.
- Die ebenfalls 32 Bit umfassende Bestätigungsnummer *(ACK)*, die nur bei gesetztem ACK-Flag gültig ist, gibt die Sequenznummer desjenigen Bytes an, das

[12] Die konkrete Auswahl einer ISN ist prinzipiell sicherheitsrelevant, wie [Bellovin 1989] in seinem Aufsatz ausführt. In seinem Beispiel, bei dem ein Angriff simuliert wird, wird deutlich, dass es einem Außenstehenden gelingen kann, dem Server einen beliebigen anderen Rechner als Kommunikationspartner vorzutäuschen. Da bei bestimmten Diensten, z.B. *rsh* und *rlogin*, die Zugangskontrolle häufig allein auf der IP-Adresse des Klienten beruht, ergibt sich daraus die Möglichkeit des widerrechtlichen Eindringens in ein fremdes System.

der Empfänger als nächstes erwartet. Damit wird automatisch der korrekte Empfang aller Bytes quittiert.

- Die Kopflänge (*data offset*) gibt an, wieviel 32-Bit-Worte zum Kopf gehören bzw. bei welchem Offset die Nutzdaten beginnen. Diese Angabe ist erforderlich, da die Länge der Optionen unterschiedlich sein kann. Mit den zur Verfügung stehenden 4 Bits für das Offset ergibt sich eine maximale Kopflänge von 60 Bytes.
- Die Anzeige-Bits, die ebenfalls 4 Bit umfassen, enthalten laut [RFC 793] insgesamt 6 Flags je Bit (URG, ACK, PSH, RST, SYN, FIN), von denen pro Segment mehrere gleichzeitig gesetzt werden können.
- Mit Hilfe der Fenstergröße *(window)* informiert der Empfänger den Sender, wieviel Bytes er noch akzeptieren kann. Diese Angabe ist im Zusammenhang mit der Bestätigungsnummer zu interpretieren und dient der Flusskontrolle. Bedingt durch die zur Verfügung stehenden 16 Bit kann ein Fenster maximal 65535 Bytes umfassen. Dabei spielt das Fenster eine besondere Rolle (*Sliding Window*), wie nachfolgend ausgeführt wird.
- Der Zeiger auf Vorrangdaten ist nur bei gesetztem URG-Flag gültig und stellt einen positiven Offset dar. Allerdings schreibt TCP nicht explizit vor, wie mit Vorrangdaten umzugehen ist. Es ist jedoch davon auszugehen, dass diese schnellstmöglich zu verarbeiten sind.
- Es gibt verschiedene Optionen unterschiedlicher Länge, von denen vor allem die Angabe der maximalen Segmentlänge MSS (*Maximum Segment Size*) Verwendung findet.

Der Aufbau einer TCP-Verbindung erfolgt in drei Schritten *(three-way handshake)*. Um einen möglichst hohen Datendurchsatz zu erreichen, verwendet TCP eine intelligente, allerdings komplexe Technik, die unter dem Begriff *Sliding Window* zusammengefasst ist. Mit dem Sliding-Window-Prinzip wird dem Sender ermöglicht, mehr als ein Paket aussenden zu dürfen, bevor eine Quittung (ACK) erforderlich wird. Die Quittung beschränkt sich nicht auf genau ein Paket, sondern kann geschlossen den Empfang von mehreren oder auch allen Paketen belegen. Abb. 2.8 zeigt im unteren Teil (a) und (b) einen TCP-Verbindungsaufbau in Form eines gleitenden Fensters. Sliding Window besagt, dass jeweils ein bestimmter zusammenhängender Teil des Datenstroms, d.h. eine Bytefolge, von einem Fenster überdeckt wird, das mit fortschreitender Kommunikation von vorn nach hinten durch den Strom gleitet. Sender und Empfänger verwalten jeweils ein eigenes Fenster. Da bei TCP durch den Duplexbetrieb beide Partner Pakete sowohl senden als auch empfangen, existieren folglich insgesamt vier Fenster. Der Empfänger teilt dem Sender im Feld Fenstergröße des TCP-Kopfes die aktuelle Größe des Empfangsfenster mit. Diese Größe ist in Bezug zur Bestätigungsnummer zu interpretieren und gibt die maximale Bytezahl an, die der Empfänger noch akzeptieren kann.

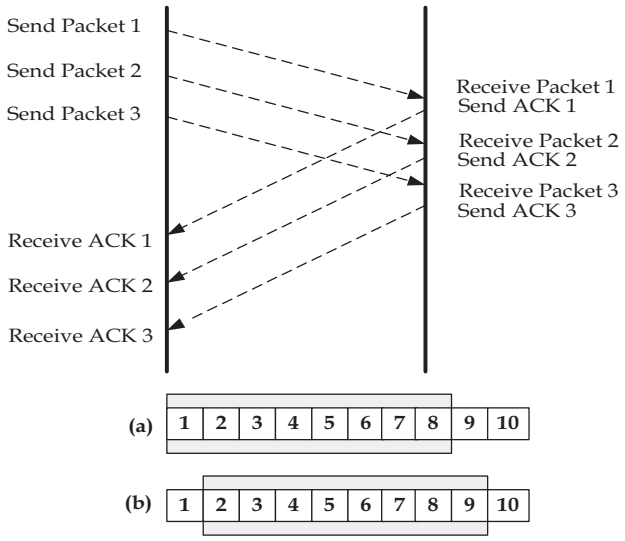


Abb. 2.8: Paketaustausch mittels Sliding-Window-Verfahren

TCP ist für eine effiziente Fluss- und Fehlerkontrolle und effektive Fehlerbehandlung ausgelegt. Nachteilig ist allerdings, dass TCP nicht für eine Breitbandübertragung optimiert ist. Dies kann dazu führen – falls ein TCP-Paket nicht innerhalb eines Time-out-Intervalls quittiert wird –, dass die Senderate der Verbindung über die TCP-Fenstersteuerung reduziert und erst sukzessive an den ursprünglichen Wert wieder herangeführt wird (*slow start, congestion avoidance, fast retransmit, fast recovery*) [RFC 2581].

Auf breitbandigen Verbindungen, wie z.B. Glasfaserstrecken, gehen Pakete oftmals durch Pufferüberläufe an den Knoten verloren. Die TCP-Kontrolle reagiert auf derartige Ereignisse mit einer drastischen Reduktion der Senderate aller betroffenen Verbindungen, was zu einer erheblichen Durchsatzverringerung führt. Im Extremfall kann sogar ein oszillierender Wechsel von Über- und Unterlastphasen hervorgerufen werden. Abhilfe schafft der *Early Packet Discard-Mechanismus* [Romanow 1995], der im Fall einer Überlastung nicht Fragmente, sondern TCP-Dateneinheiten als Ganzes vernichtet. Eingeleitet wird dieser Mechanismus durch eine Schwellwertüberschreitung in der Pufferbelegung.

Als Ende-zu-Ende-Protokoll kann die TCP-Flusskontrolle in Netzen erst in einer konkreten Fehlersituationen nach erfolgtem Time-out-Intervall reagieren. Mit zunehmender Datenrate wächst allerdings die in der Zwischenzeit ins Netz abgegebene Datenmenge, die bei voller Ausschöpfung der Kapazität bis zum *Bandwidth Delay Product* ansteigt. Folglich reicht eine Ende-zu-Ende-Flusskontrolle aus der isolierten Sicht einer Verbindung nicht aus, um Datenverlusten und -wiederholungen durch Überlast vorzubeugen. Dazu sind Zulassungs- und Kontrollverfahren des Verkehrs an den Quellen oder an den Netzknoten erforderlich.

Das klassische TCP/IP-Protokoll kann Daten mit einer Absicherung gegen Übertragungsfehler transportieren. Es bietet jedoch lediglich einen Best-Effort-Mechanismus, ohne eine angemessene Behandlung verschiedener Verkehrsarten im Fall einer Überlastsituation im Netz vorzunehmen.

Anzumerken ist abschließend, dass TCP als Protokoll und nicht als eine spezielle Software zu verstehen ist. Der Unterschied zwischen einem Protokoll und einer Software entspricht dem Unterschied zwischen einer Programmiersprache und einem Programm-Compiler, wie etwa der Fortran-99-Compiler und die Computersprache Fortran-99.

TCP und UDP werden in der VPN-Technologie berücksichtigt, in der beide Protokolle bei dem so wichtigen *Traffic Engineering* des MPLS-VPN eine Rolle spielen. Doch bevor auf die MPLS-Technologie (vgl. Kapitel 8.1) eingegangen wird, ist es sinnvoll, die Dienstgüte, die zunehmend mit VPN in Verbindung gebracht wird, zu diskutieren.

2.3.3 Dienstgüte CoS und QoS in IP-Netzen

Ausgehend von der allgemeinen VPN-Definition auf Seite 6 wird deutlich, dass die dynamisch zugewiesene Bandbreite nichts über die Qualität der Bandbreitenzuweisung, also die Dienstgüte, aussagt. Für reine IP-Netze stellt jedoch eine Dienstgütenforderung bezüglich der Bandbreite eine ernsthafte Herausforderung dar. Denn ursprünglich kennt das IP, historisch bedingt, nur *eine* Dienstgüte während der Datenübertragung, die mit dem Begriff *Best Effort* umschrieben wird. Diese Dienstgüte, die noch heute das Internet beherrscht, beinhaltet, dass nach dem Prinzip *First in, First out* verfahren wird. Demzufolge werden alle Übertragungsanforderungen mit der gleichen Priorität, nämlich streng sequenziell, abgearbeitet. Das bedeutet, dass Daten, die aufgrund der Zieladresse das Gerät auf einem bestimmten Port verlassen, z.B. HTTP auf dem Port 80, solange warten müssen, bis alle zuvor eingetroffenen Pakete verarbeitet sind. Ist der Speicher überfüllt, beginnt der Router damit, Pakete zu verwerfen. Es existierte bisher keine Möglichkeit zur Bandbreitenreservierung für spezielle Verbindungen oder eine Bevorzugung von besonderen Übertragungen. Insofern zeichnet sich ein hoher Handlungsbedarf ab. Eine kurzfristige Verbesserung wurde durch die *Random Early Discard*-Technik (RED) erreicht, die die Auslastung der Eingangs-Queues effizient steuert. Dies verbessert den Durchsatz bei Überlastung. Wirft der Router dennoch Daten aus dem Speicher, lassen sich mit *Weighted Random Early Discard* (WRED) Prioritäten beim Löschen festlegen.

Kommen wir dann zum Unterschied zwischen von Class of Service und Quality of Service. Auch wenn es unterschiedliche Definitionen für Quality of Services gibt, lassen sich prinzipielle Unterscheidungsmerkmale gegenüber den Class of Services festhalten:

Quality of Services (QoS): Hierunter werden Dienstgüten verstanden, die für eine einzelne Sitzung (Session) eingerichtet sind.

Class of Service (CoS): Hierbei werden gleichartige Datenströme in einer Klasse zusammengefasst, der vom Netz eine oder mehrere Dienstgüten zugeordnet werden. Einzelne Sessions erhalten damit keine individuellen Dienstgüte (QoS).

Eine Dienstklasse setzt sich aus Untergruppen möglicher Dienstgüte-Parameter zusammen. Dabei stehen die Eigenschaften dieser Klassen im direkten Verhältnis zu den Anwendungen. Die Gesamtheit aller Dienstklassen spiegelt folglich die Leistungsfähigkeit des Übertragungssystems wider.

Als Beispiel für Classes of Service kann eine Flugreise betrachtet werden. Es gibt einen regulären Fluggast, der in der Economy Class reist. Die Business Class bekommt einen besseren Service als der normale Fluggast in der Economy Class. Mit einem Premium Service wird die First Class bedient. Sie genießt am meisten Aufmerksamkeit vom Bordpersonal, steigt zuletzt ein und als erste wieder aus und bekommt einen bevorzugten Gepäckservice.

Zu den eingesetzten QoS-Verfahren gehören solche zur Bandbreitenreservierung (RSVP), zur Priorisierung des Datenverkehrs (Diffserv) und zur Bandbreitenlimitierung durch Sprachcodierung und Paketoptimierung. Der Dienstgüte (QoS) werden diejenigen Verfahren bzw. Techniken zugerechnet, die den Datenfluss im LAN bzw. im WAN dahingehend bestimmen, dass der Dienst mit einer festgelegten definierten Qualität beim Empfänger ankommt. Somit handelt es sich um die Charakterisierung eines Dienstes, der für den Nutzer unmittelbar sichtbar ist und dessen Qualität an bestimmten Parametern gemessen werden kann. Im Fall eines Netz- bzw. VPN-Outsourcing können diese mit speziellen Servicevereinbarungen (*Service Level Agreement*, SLA) zwischen Nutzer und Betreiber des VPN (Netzdienstleister) gekoppelt werden. Abschn. 9.2.3 beleuchtet den Aspekt der Servicevereinbarungen genauer. Auf die Definition und Verfahren zur Einhaltung der Dienstgüten wird nachfolgend eingegangen.

Für die Dienstgüte hat sich bis dato keine allgemein gültige Definition durchsetzen können, so dass die Netzwerkwelt von vier z.T. divergierenden Interpretationen beherrscht wird. So haben die ITU ebenso wie das IETF und das ATM-Forum eigene Definitionen erarbeitet. Aber auch die OSI veröffentlichte eigene Definitionen zur Dienstgüte:

1. Die ITU hat ein hierarchisches QoS-Modell entwickelt, das neben den technischen Aspekten eines Dienstes die Verfügbarkeit und die Bedienbarkeit der Endgeräte berücksichtigt. Auf dieser Grundlage definierte die ITU drei Dienstklassen, die ATM als Basistechnik voraussetzen. Dies sind der *ATM Block Transfer* (ABT), die *Deterministic Bit Rate* (DBR) und die *Statistical Bit Rate* (SBR).
2. Die IETF hat für die Echtzeitübertragung im Internet mehrere Ansätze entwickelt. Dazu gehören das Protokoll IPv6, in dessen Header das Flow-Label-Feld definiert wurde. Daneben gibt es die Priorisierung des Datenverkehrs mittels DiffServ und die Reservierung der Bandbreite mittels IntServ. Mit diesen Verfahren können Echtzeitdaten auch über IPv4 transportiert werden, wo-

bei die Verbindungen in Klassen aufgeteilt und die Ressourcen für eine bestimmte Klasse reserviert sind. Darüber hinaus kommt bei MPLS zur Priorisierung des Datenverkehrs SBM[13] für globales QoS und ein Warteschlangenverfahren für die priorisierte Verarbeitung von Echtzeitdaten zum Einsatz.

3. Bei der ATM-Technik sind mit der Dienstgüte die Serviceparameter einer virtuellen ATM-Verbindung verknüpft. Dazu gehören u.a. die Zellenverlustrate und die Zellenverzögerung.
4. Im OSI-Referenzmodell werden bestimmte Dienste definiert, die von der Vermittlungsschicht der übergeordneten Transportschicht angeboten werden. Weiterhin werden bei den OSI-Protokollen bei Aktivierung der Transportschicht mit dem Verbindungsaufbau gleichzeitig Dienstgüteparameter vereinbart.

In der Praxis ist die Realisierung von Quality of Service durch proprietäre Lösungen und somit durch das Manko geprägt, dass es derzeit keinen herstellerübergreifenden professionellen QoS gibt. Allerdings gewinnt QoS für die Abwicklung von verzögerungsempfindlichen Geschäftsprozessen innerhalb des Intra- und z.T. auch Extranets zunehmend an Bedeutung. Um den Anforderungen an die Übertragung von zeitkritischen Daten gerecht zu werden, müssen die Übertragungsfaktoren wie Latenzzeit, *Jitter*, Paketverlustrate, Bandbreite und die Verfügbarkeit, in definierten Grenzen gehalten werden.

Bereits 1994 wurde ein Übersichtsdokument zur Dienstintegration mit dem [RFC 1633] von der IETF im Internet veröffentlicht. [RFC 1633] schlägt eine bis dato grundlegend neue Idee vor: eine individuelle Behandlung und Kontrolle von Verkehrsflüssen nicht nur Ende-zu-Ende vorzunehmen, sondern unter Beteiligung der Vermittlungsknoten. Denn die herkömmlichen Vorgehensweisen eignen sich eher weniger für eine Unterstützung von Echtzeit- und multimediafähigen Diensten. Problematisch ist nämlich insbesondere:

- nach wie vor wird das klassische IP beibehalten,
- die Schaffung von getrennten, nicht integrierten Netzen herrscht vor,
- eine teure überdimensionierte Ressourcenbereithaltung zur Vermeidung von Engpässen ist die Regel,
- nur eine Best-Effort-Priorisierung des Verkehrs wird vorgenommen.

Im Laufe der Zeit haben sich die nachfolgenden typischen vier Dienstgütemerkmale (Parameter) entwickelt:

Bandbreite: minimale, mittlere, maximale

Verzögerung: inklusive der als Jitter bezeichneten zeitlichen Schwankungen

[13] SBM ist als Mapping der unterschiedlichen Ansätze für ein globales QoS zu verstehen.

Zuverlässigkeit: gegenüber Ausfällen, Störungen und Übertragungsfehlern

Verfügbarkeit: Bit- und Paketfehlerraten

Allerdings dürfen durch den Einsatz von QoS-Parametern andere Dienste, die nicht vornehmlich auf Qualitätsgarantien angewiesen sind, in ihrer Gesamtheit bei einer Ressourcenaufteilung nicht gravierend benachteiligt werden. Somit erfordert dieser Anspruch eine Kontrolle, falls zufällig auftretende Verkehrslast-Situationen dauerhafte Beeinträchtigung herbeiführen. Diese können ausgelöst werden durch Unterschiede zwischen Anwendungen mit hohen oder niedrigen Datenraten und speziell bei TCP, mit kurzen bzw. langen *Round-Trip*-Verzögerungen[14] (RTT) [Biaz und Vaidya 1999].

Folgende QoS-Kontrollmaßnahmen können unterschieden werden:

Ende-zu-Ende-Kontrolle unter Mitwirkung von Netzknoten

- Eine Ende-zu-Ende-Kontrolle regelt den Verkehr allein beim Sender. Neben der von TCP durchgeführten isolierten Behandlung von Verbindungen gibt es Vorschläge für eine zwischen allen Sendern abgestimmte Gesamtkontrolle in Netzen von begrenzter Ausdehnung [Frank 1999].
- Die Kontrolle kann entweder die Menge der Daten beschränken, die ohne Empfangsbestätigung verschickt werden (*Sliding-Window-Verfahren*), oder auf die Senderate selbst einwirken (*Rate-based Control*). Der Token-Leaky-Bucket-Filter mit seinen beiden Spezifikationen (T-Spec, R-Spec) kombiniert beide Varianten. Abgesehen davon, dass in den Routern und Switches genügend Pufferplatz vorausgesetzt wird, greifen diese Filter nicht aktiv in die Ende-zu-Ende-Kontrolle ein.
- Unter Mitwirkung der Vermittlungsknoten kann schneller auf deren Belastungssituation eingewirkt werden. Hoch- und Überlastsituationen können explizit am Pufferfüllstand *Upstream* gemessen und auf dem Weg zu den Sendern weitergemeldet werden. Unter den in einem Puffer zwischengespeicherten Dateneinheiten können somit Verbindungen oder Verkehrsflüsse eine Bevorzugung bei der Weiterleitung und bei Pufferüberläufen erfahren.

Priorisierung mittels Reservierung durch Zugangskontrolle und Signalisierung

- Ein IP-Verkehr kann in verbindungslosen Protokollen über spezielle Kennzeichnungen im Protokollkopf priorisiert werden. Dabei ermöglichen höhere Prioritäten höhere Durchsatzraten und geringere zeitliche Verzögerungen. Dennoch bleiben die QoS-Eigenschaften abhängig vom Gesamtverkehr, der mit gleicher und noch höherer Priorität für eine Netz(über)last sorgt.

[14] TCP nutzt die *Round Trip Time* (RTT) um den herrschenden Paketdurchsatz (*throughput*) im Netz zu bestimmen. Danach wird dann das Sliding Window ausgerichtet.

- Eine Priorisierung kann durch Benutzer, Anwendungen oder Netzprotokolle an den End- oder Vermittlungssystemen eingerichtet werden. Dabei ist eine Benutzerkontrolle an dieser Stelle sinnvoll, wenn gleichzeitig die möglichen Prioritäten, z.B. mit einem Accounting und einer Rechnungsstellung, gekoppelt sind, da ansonsten Stufen mit geringerer Priorität vermieden werden.
- Generell tritt bei einer Priorisierung wie bei einer Reservierung das Problem auf, die Berechtigung einer Anforderung durch Autorisierung und Authentifizierung festzustellen. Denn nur so lässt sich beabsichtigter wie unbeabsichtigter Missbrauch sowie eine Blockierung (*Denial of Service*) von Ressourcen verhindern. Eine Authentifizierung ist verbindungsorientiert und durch kryptographische Verfahren abzusichern, was zunächst auf den Einsatz eines IP-VPN abzielt. Allerdings kommt IPv6 mittels IPSec dieser Forderung ebenfalls nach.
- Eine Ressourcenreservierung im Netz erfordert eine Anwendung zum Erkennen freier Kapazitäten, die dann – außer bei Störeinflüssen – garantiert zur Verfügung gestellt werden. So können beispielsweise in ATM-Netzen nicht genutzte Reservierungen durchaus an Best-Effort-Dienste weitergegeben werden. Auch eine Kombination von Mindestgarantien mit einer fairen Aufteilung der darüber hinaus verfügbaren Ressourcen ist sinnvoll.
- Reservierungen mit Zulassungskontrolle sind wichtig für Dienste, die ohne gewisse Mindestanforderungen nicht auskommen, wie z.B. eine Video-Übertragung. So können Video-Übertragungen ihre Senderate nur in einem gewissen Rahmen mit verminderter Bildqualität anpassen, die aber unterhalb einer Mindestrate zusammenbricht. Wird allerdings eine Überlast bereits durch die Summe der Mindestraten gleichzeitig gewünschter Video-Übertragungen erreicht, z.B. bei einer Netzüberbuchung, so ist es überlegenswert, eine größtmögliche Anzahl der Video-Übertragungen mit garantierter Mindestqualität zuzulassen, als allen eine faire (gleiche) Aufteilung mit (untragbar) schlechter Qualität zu bieten.

Granulierung der Dienstklassen kontra Verkehrsflüsse und Verbindungen

- Eine Priorisierung oder Reservierung kann durch Einteilung in Verkehrsklassen (*Type of Service*, TOS) oder Verkehrsflüsse erreicht werden. Innerhalb einer Klasse reicht allerdings auch eine Gleichbehandlung der Übertragungskapazität nicht aus.
- Reservierungen für eine Dienstklasse mit fairer Aufteilung bedeuten aber noch keine Reservierung für jede einzelne Anwendung, sondern eine Abhängigkeit der gebuchten QoS-Eigenschaft von der Anzahl der aktiven Teilnehmer in der Klasse. Sie ist daher nur effizient, wenn die zeitlichen Auslastungsschwankungen in den Klassen keine unvorhersehbaren Grenzwerte überschreiten.
- Reservierungen für einzelne Verkehrsflüsse bzw. Verbindungen ermöglichen QoS-Garantien nach speziellem Bedarf jeder Anwendung – soweit im voraus

bekannt. Sie bringen vor allem im Backbone-Bereich von Netzen, in denen viele Verkehrsflüsse überlagert werden, einen erheblichen Aufwand mit sich, da Informationen und Zustände pro aktivem Verkehrsfluss bereitzuhalten sind. Die Skalierbarkeit solcher Reservierungsschemata in großen Netzen ist auf eine gezielte Aggregation von individuellen Verkehrsflüssen zu größeren Einheiten im Backbone angewiesen.

2.3.4 Integrierte und differenzierte Dienste

Eine der technischen Herausforderungen für das Internet, die Intranetze oder ganz allgemein IP-Netzwerke – und somit auch IP-VPN – besteht darin, ein hohes Maß an Flexibilität und Dienstgüten zuverlässig bereitzustellen. Nach den Ausführungen zur Dienstgüte und QoS-Kontrollmaßnahmen im vorigen Abschnitt wird jetzt auf die Technik der integrierten und differenzierten Dienste in IP-Netzen eingegangen.

Derzeit wird die Einführung von QoS-Eigenschaften in IP-Netzen unter den Schlagworten integrierte Dienste – in enger Verbindung mit dem Ressource Reservation Protocol (RSVP) – und differenzierte Dienste diskutiert [Mankin 1998] und [Xiao 1999]. Außerdem lassen sich beim Multiprotocol Label Switching (MPLS), das eine kombinierte Routing- und Switching-Architektur vorschlägt, ebenfalls QoS-Eigenschaften neben einer hohen Flexibilität erreichen [Lakshman 1998] (vgl. Abschn. 8.1).

Resource Reservation Protocol (RSVP)

Das Resource Reservation Protocol (RSVP) wurde 1997 von der IETF durch eine Reihe von RFCs [RFC 2205 bis 2210] zum Standard ernannt. Es ist ein Signalisierungsprotokoll und kein Routing-Protokoll, das nach einer ersten Nachricht vom Absender zum Empfänger (dies können auch mehrere sein) auf dem Rückweg die durchlaufenden Router veranlasst, Bandbreite, Pufferspeicher bzw. Verzögerungseigenschaften für nachfolgende Pakete des Absenders zur Verfügung zu stellen. D.h. alle folgenden Pakete nehmen den gleichen Weg. Sind die Ressourcen tatsächlich verfügbar, stellen die Vermittlungssysteme (Zwischenrouter) die Verbindung in der gewünschten Qualität her und halten diese solange aufrecht, bis die Übertragung beendet ist.

Die Idee der integrierten Dienste basiert auf einer Reihe von Kontrollmechanismen, insbesondere auf die der Zulassungskontrolle und Reservierung, die die Paketbearbeitung in den Puffern der Vermittlungsknoten steuern (vgl. Abb. 2.10). Einen Überblick hierzu bietet [RFC 1633]. In erster Linie galt es bei der Integration von Diensten Verzögerungs- und Bandbreitenanforderungen für spezielle Übertragungen zu ermöglichen. Im Hintergrund der Überlegungen stand eine gerechte Ressourcenaufteilung, die es bis dato für die anspruchslosen TCP/IP-Netze nicht gab.

Gleichzeitig wurden mit dem *Integrated Service Model* zusätzlich zur regulären Best-Effort-Serviceklasse[15] zwei unterschiedliche Serviceklassen eingeführt, die in Abhängigkeit von den zu übertragenden Applikationen engere oder weitere QoS-Eigenschaften erfordern. So benötigen Echtzeitapplikationen eine garantierte Verzögerung, während andere Applikationen geringere Ansprüche an eine Verzögerung stellen. Die IntServ-Arbeitsgruppe schlug demzufolge ein Dreiteilung für das Verhältnis von Auslastung und Bandbreite vor, und zwar mit folgenden Eigenschaften:

Hard Real Time: Vorgesehen für Anwendungen, die äußerst empfindlich auf Störungen reagieren, wie z.B. eine Streaming-Applikation.

Delay Adaptive: Vorgesehen für Anwendungen, die leichte Verzögerungen ohne Qualitätseinbuße hinnehmen können.

Elastic Applications: Vorgesehen für Anwendungen, bei denen eine größere Zeitverzögerung toleriert werden kann und sich ein Zwischenspeichern von Daten unbedeutend auf den Dienst auswirkt.

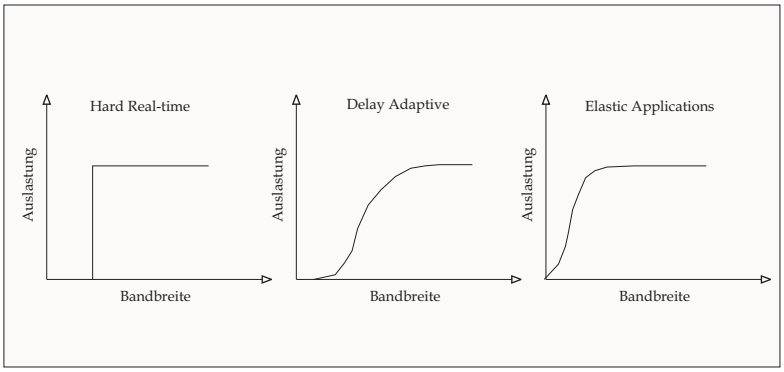


Abb. 2.9: Anforderungsbedarf für verschiedene Anwendungen im Internet gemäß IntServ-Arbeitsgruppe

Von den ursprünglich fünf Dienstklassen gewannen nur zwei an Bedeutung: zum einen der *Guaranteed Service* [RFC 2212], und der *Controlled Load Service* [RFC 2211]. Dabei bedeutet:

Guaranteed Service: Es wird eine garantierte Bandbreite mit einer Laufzeitobergrenze zugesichert, die keine Paketverluste aufweist. Somit wird eine garantierte Gesamtübertragung vom Sender zum Empfänger erzwungen, die eine bestimmte Zeitspanne nach Abschicken der Datenpakete nicht überschreitet.

[15] Von der IETF wurde die Arbeitsgruppe IntServ initiiert, die 1997 das erste RFC veröffentlichte. Die Arbeitsgruppe bearbeitet seitdem Probleme, die bei der Übertragung von Echtzeitdaten in IP-Netzen auftreten, und sucht nach Lösungen, diese effizienter zu unterstützen.

Damit wird nicht nur der Durchsatz als Maß der Dienstgüte gemessen, sondern auch die Verzögerungszeiten. Mit einem Token-Bucket-Filter (Abb. 8.14) kann dieser Service technisch umgesetzt werden.

Controlled Load Service: Mittels Lastenmanagement wird eine kontrollierte Bandbreite erreicht, die dem Best-Effort-Verfahren in schwach belasteten Netzen entspricht. So wird spezifiziert, dass für einen Datenfluss die Weiterleitungsgeschwindigkeit nicht abnimmt, auch wenn der Netzwerkverkehr zunimmt. Eine Implementierung kann auch oberhalb der Layer-2 erfolgen, denn die maximale Transferrate eines Übertragungsmediums ist eine konstante Größe. Ein Realisierungsansatz kann durch das RSVP-Protokoll erfolgen. Ein Vorteil von RSVP ist, dass sowohl die unteren Schichten, als auch die Hardware, eines Transportmediums weiter verwendet werden können, da lediglich der Durchsatz verändert wird.

Folgen alle Pakte eines Dienstes einem speziellen Weg, kommt dies einer Reservierung von Übertragungseigenschaften gleich, die Dienstgüten für den errichteten Pfad im Internet einrichten. Eine Reservierung wird durch die speziellen Nachrichten *(path-message)* und *(rsv-message)* vorgenommen.

Trifft eine RSVP-Nachricht (*path-message*) auf den ersten RSVP-Router, wird in diesem die Adresse des *Last-Hop-Field* hinterlegt. Diese stellt im Allgemeinen die Adresse des Senders dar (vgl. Abb. 2.10). Gleichzeitig trägt der Router seine eigene IP-Adresse ins *Last-Hop-Field* der RSVP-Nachricht ein und sendet diese zum Wegeaufbau an den nächsten Router. Dort geschieht der gleiche Vorgang des IP-Adressaustausches. Dieser Vorgang setzt sich fort, bis der Empfänger erreicht wird.

Der Empfänger schickt anschließend seinerseits eine RSVP(rsv)-Nachricht *(rsv-message)* auf den vorgezeichneten Weg zurück und hinterlässt in jedem auf diesem Weg befindlichen Router die gewünschte QoS-Eigenschaft, die im *Flow Descriptor* des Routers gespeichert wird.

Im Router findet die eigentliche Verkehrskontrolle (*Traffic Control*) statt, indem im die abhängigen Fluss- und Filtereinstellungen *Flow Spec.* und *Filter Spec.* den Bedürfnissen des Empfängers angepasst werden. Dabei werden die Filtereinstellungen (Filter Spec.) im Zusammenspiel mit dem *Packet Classifier* verändert. Die Flusseinstellungen, die auf einen Satz von Parametern (*Invocation Information*) zurückgreifen, die in die Gruppe der Verkehrsspezifikation T-Spec[16] und der der Service Anforderungsspezifikation *R-Spec*[17] untergliedert sind, wirken auf den *Packet Scheduler*. Abb. 2.11 zeigt das Zusammenspiel der angesprochenen Komponenten.

---

[16] Im Hintergrund der *Traffic Specification* arbeitet der Token-Bucket-Filter, der eine Kontrolle des Datenflusses ausübt, indem Charakter (*Token*) in periodischen Zeitintervallen nur dann in den Puffer (*Bucket*) gelassen werden, wenn die Anzahl der Token geringer als die der Paketlänge ist.

[17] Die *Service Request Specification* ordnet die QoS-Anforderungen entsprechend dem der Applikation zugrunde liegenden Datenfluss in die *Controlled Load Services* ein, z.B. für Echtzeitanwendungen, wie Videokonferenzen oder der Guaranteed Service für Datenübertragungen, die in einer bestimmten Zeit übermittelt sein müssen.

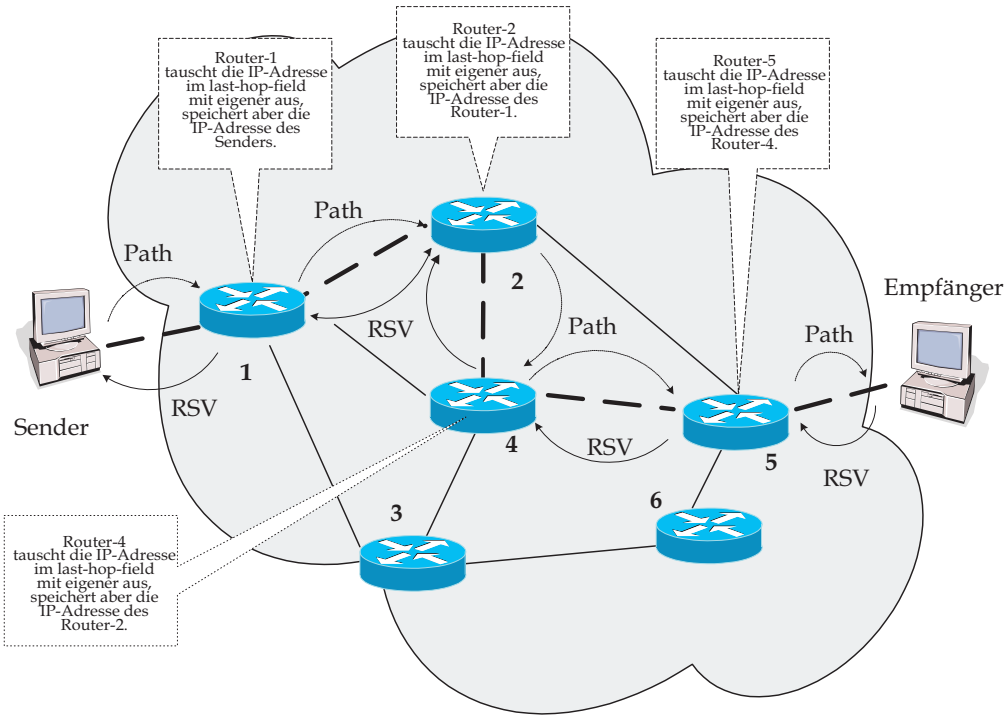


Abb. 2.10: Wegefindung in einer Domain mittels path- *und* rsv-messages

Wichtig in der Verkehrsbehandlung gemäß Abb. 2.11 sind die Routerkomponenten *Packet Scheduler*, *Packet Classifier* und *Admission Control*, die maßgeblich an der Steuerung der Datenflüsse beteiligt sind:

Packet Scheduler: Der P-Scheduler organisiert die Weiterleitung der unterschiedlichen Datenflüsse in Router- und Host-Systemen in Abhängigkeit von ihrer Service-Klassenzugehörigkeit. Es kommen spezielle Warteschlangenverfahren und Verarbeitungsalgorithmen wie *queue management* und *schedule algorithm* zur Anwendung.

Packet Classifier: Der P-Classifier identifiziert die beim Router eintreffenden IP-Pakete und ordnet sie spezifischen Klassen zu. Dabei werden alle Pakete mit der gleichen Klassenzugehörigkeit später vom P-Scheduler in gleicher Weise behandelt. Die Klassenzugehörigkeit wird durch die beiden Adressen (Source-IP/Destination-IP) des IP-Paketes, der (Ziel)Port-Nummer oder einer Klassifikationsnummer aus dem Type of Service (TOS)-Feld bestimmt.

Packet Admission Control: Mit dieser Kontrollsequenz kommt ein Algorithmus zur Anwendung, der entscheidet, ob genügend Routing-Kapazitäten für die angeforderte QoS-Eigenschaft eines neuen Datenflusses zur Verfügung stehen

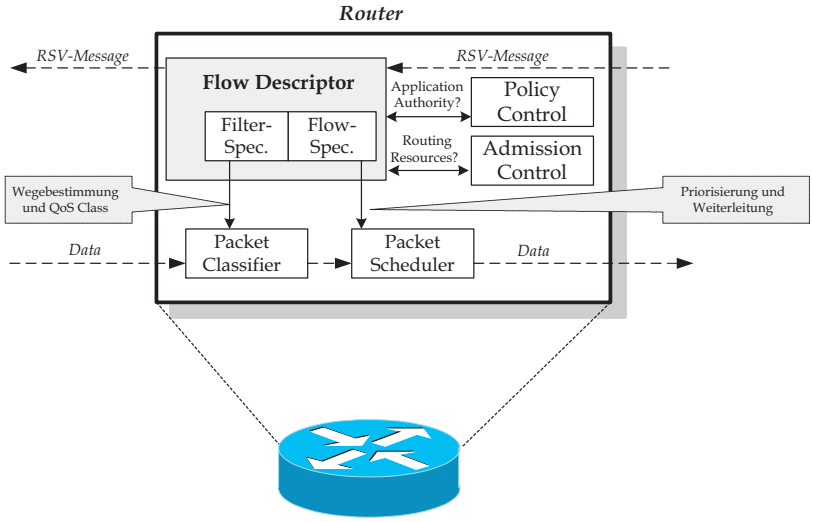


Abb. 2.11: Verkehrsbehandlung von Datenflüssen in einem RSV-fähigen Router

oder nicht. Ist die Kapazität momentan erschöpft, wird der Datenfluss abgewiesen. Andernfalls wird er angenommen und entsprechende Reservierungen im P-Classifier und im P-Scheduler vorgenommen.

Als anschauliches Beispiel sei in diesem Zusammenhang eine Videokonferenz genannt, die zwischen zwei Host-Systemen durchgeführt wird. Hierfür sind kontinuierliche Verbindungen erforderlich. Für das simplex Protokoll RVSP bedeutet dies, dass in beide Richtungen eine komplette Reservierung vorgenommen werden muss. Um ein verzögerungsfreies Bild zu übertragen, initiiert jede der beidseitig benutzten Videoanwendungen einen eigenen Datenfluss mit einer minimalen Bandbreite von 128 kbps und einer minimalen Verzögerungsrate von 100 ms. Allerdings ist eine Reservierung flüchtig, denn bei Ressourcenknappheit oder wenn die Berechtigung nicht verifizierbar ist, wird eine Reservierung mit Fehlermeldung abgewiesen. Hinzu kommt, dass die Reservierungen periodisch bestätigt werden müssen. All dies kann zu erheblichen Störungen bei der Übertragung führen. Außerdem werden Ressourcen für den Verkehrsfluss bereitgehalten, wenn alle Router auf dem Weg die Signalisierung akzeptieren. Eine Flusskennzeichnung wird durch Routing-Tabellen-Einträge erreicht (vgl. das Servicetyp/Traffic-Class-Feld in Abb. 2.4).

Ein Verkehrsfluss bzw. Fluss ist nach der IETF gemäß [RFC 2460] eine Folge von gekennzeichneten Paketen (Datagrammen), die von einer bestimmten Quelle zu einem bestimmten Ziel (n:n, oder n:m) gesendet werden, verbunden mit einer von der Quelle gewünschten Routing-Behandlung in den Netzknoten. Im Gegensatz dazu werden die entsprechenden Verbindungen in ATM-Netzen durch eine Reservierung in RSVP über einen *soft state* aufrechterhalten; d.h. Reservierungen

sind in regelmäßigen Zeitintervallen zu wiederholen (*refreshing*) sonst werden sie automatisch abgebrochen.

Der Begriff der Granularität bei Einsatz des RSVP-Protokolls bezieht sich auf einzelne Verkehrsflüsse. Allerdings mangelt es noch an der dafür notwendigen Aggregation von Verkehrsflussinformationen im Backbone-Bereich, die für RSVP nicht standardisiert ist. Demzufolge bleibt eine Skalierung der integrierten Dienste über RSVP vorerst beschränkt [RFC 2208]. Jedoch hat die IETF das Signalisierungsprotokoll inzwischen zum RSVP-TE erweitert, das bei MPLS eine Rolle spielt. Einige Hersteller (Lucent/Ascend) haben bei der Implementierung von MPLS, beim sogenannten *Traffic Engineering*, auf RSVP-TE gesetzt (vgl. Abschn. 8.1). Dagegen lösen ATM-Netze das gleiche Problem mit einer einstufigen Hierarchie von virtuellen Pfaden und Kanälen (vgl. Abschn. 8.4). Eine ähnliche Lösung für IP-Netze wird mittels MPLS verfolgt.

Wegen der beschränkten Skalierbarkeit bei RSVP wird derzeit unter der Bezeichnung *differenzierte Dienste* diskutiert, inwieweit in einer recht groben Granularität von Verkehrsklassen eine QoS-Unterstützung erreicht werden kann. Zur Differenzierung bieten sich im IPv4-Header das bisher nutzlose Servicetyp-Feld an, dem das Traffic-Class-Feld im IPv6-Protokollkopf entspricht. Derzeit ist allerdings nur die Aufteilung beider Felder im [RFC 2474] für differenzierte Dienste standardisiert.

Differentiated Services (DiffServ)

Im Gegensatz zur Signalisierung, die bei RSVP angewandt wird, findet beim *DiffServ* eine Klasseneinteilung in unterschiedliche Gruppen statt. Dies bedeutet, dass jeglicher Verkehr bezüglich seiner Gruppenzugehörigkeit eingeordnet wird. Dieser ist wiederum mit unterschiedlichen QoS-Parametern behaftet und wird entsprechend übertragen. Das [RFC 2475] beschreibt die bei DiffServ zugrunde liegende Architektur. Die Grundidee von DiffServ soll auf Andrew Odlyzkos, der in den 80ern bei den AT&T Bell-Laboraties gearbeitet hat, zurückgehen. Er hat das Pariser Metro-Tarifmodell als Vorbild genommen. Nach diesem wird die Transportleistung in mehrere Klassen bzw. Verkehrskategorien abgestuft. Auch für DiffServ hatte die IETF seinerzeit eine Arbeitsgruppe eingerichtet, die sich im Dezember 1998 mit dem [RFC 2474] der öffentlichen Diskussion stellte.

Im DiffServ-Ansatz wird das Servicetyp-Feld (Type of Service, TOS) im IPv4-Header (Abb. 2.4) neu definiert. Dieses Feld benutzte ursprünglich 3 Bit, um die Art und Priorität des Netzwerkverkehrs zu steuern, wie etwa in Netzknoten, in denen Kontrollpakete mit höchster und Standardverkehr mit niedrigster Priorität verarbeitet werden. Ergänzend existiert noch ein Bit, mit dem Forderungen nach kurzen Verzögerungszeiten, großem Datendurchsatz oder hoher Verlässlichkeit signalisiert werden können. Die übrigen 2 Bit werden reserviert für künftige Entwicklungen. Wenige der heute eingesetzten Router interpretieren allerdings dieses Servicetyp-Feld und so wurde es in der IPv6-Spezifikation in der ursprünglichen Form nicht übernommen. Die IETF definierte es daher komplett neu.

In der Neudefinition des Differentiated-Services-Prinzip werden die ersten 6 Bit des Servicetyp-Feldes des IPv4-Protokoll in modifizierter Form verwendet, um insgesamt 64 Serviceklassen als Class of Service (CoS) zu definieren. Jede dieser Klassen ist mit einem anderen (unterschiedlichen) Verhalten der Router, die DiffServ unterstützen, gekoppelt. Es werden unterschiedliche Prioritäten bei der Ver-

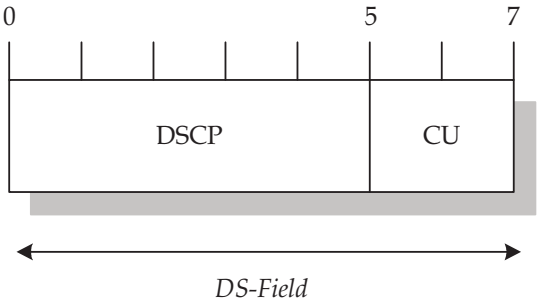


Abb. 2.12: Das 6 Bit lange DS-Feld

arbeitungsgeschwindigkeit (Warteschlangenverhalten) oder die unterschiedlich hohe Wegwerfwahrscheinlichkeit eines Paketes bei zu hohem Datenaufkommen (Traffic) definiert, wobei jeder Serviceklasse ein Regelsatz zur Verfügung steht, der als *Per-Hop-Behavior* (PHB)-Regel bezeichnet wird.

DiffServ definiert unterschiedliche Servicelevels: *Expedited Forwarding* (EF), *Default Forwarding* (DF) und *Assured Forwarding* (AF). So dient z.B. die EF-Einstellung als ein sehr hoch priorisiertes PHB-Verhalten, das zum Austausch von Kontrollinformationen für die Router selbst bestimmt ist; beispielsweise ein Routing-Update. Hierfür wird der 6 Bit DSCP-Wert 101100 vergeben. Als Default DSCP-Wert wurde 000000 vorgeschlagen, der im Grunde den Best-Effort-Dienst darstellt. Das 2 Bit-Feld (CU) *currently unused* in Abb. 2.12 ist derzeit unbenutzt und für zukünftige Entwicklungen reserviert. Weil nicht jeder Datenfluss verwaltet werden muss, ist DiffServ erheblich einfacher in seiner praktischen Umsetzung als IntServ. Die Daten werden nur am Eingang des DiffServ-Netzes (Domain) bearbeitet, indem eine Einordnung in die QoS-Klassen erfolgt. Dazu wird das DSCP-Feld (*Differentiated Service Code Point*) im DiffServ-Header gemäß den o.g. Zuordnungen markiert. Dieses Feld entspricht dem Servicefeld (TOS) im IPv4-Header beziehungsweise dem Traffic-Class-Feld im IPv6-Header und dient dazu, die einzelnen Datenströme eines Verkehrsbündels auseinander zu halten.

Die DiffServ-Steuerungsmöglichkeiten erfordern von einem Router, dass er eine Warteschlangenverarbeitung und ein Management zur Priorisierung für ankommende Pakete vornehmen kann. Die Paketbehandlung im Router selbst hängt neben den DSCP-Einstellungen stark von seiner Kapazität und Konfiguration ab. Falls beispielsweise ein IP-Paket einen Router passiert, der acht unterschiedliche Warteschlangen verwaltet (Abb. 2.14), die alle verschiedene Prioritäten besitzen, wird das DS-Feld benutzt, um eine Zuordnung des IP-Pakets zu einer Warte-

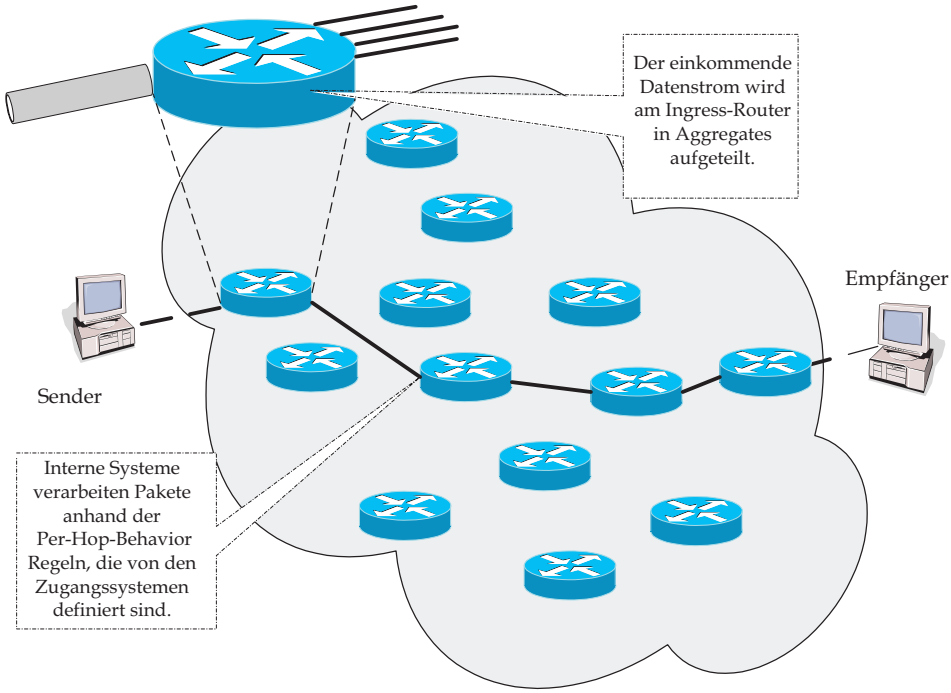


Abb. 2.13: Übermittlung einzelne Datenströme in „Aggregates“ beim DiffServ-Ansatz

schlange vorzunehmen. Dabei reicht die Verarbeitungspriorität von Null bis zur höchsten Priorität Sieben. Ein weiteres Beispiel ist ein Routertyp, der nur eine Warteschlange kennt und das DS-Feld dahingehend interpretiert, dass passierende IP-Pakete in einer Überlastsituation, gemäß der Priorisierung durch das DS-Feld, vernichtet werden. Pakete mit der Default-Kennung Null werden zuerst und die mit einer hohen Prioritäten-Kennung zuletzt verworfen (*strict priority queuing*). Alternativ hierzu gibt es das *weighted fair queuing*, bei dem die Datenströme gewichtet versendet werden. Jeder Ausgang bekommt einen bestimmten Prozentsatz der verfügbaren Bandbreite. Dadurch lassen sich auch Daten mit niedrigsten Prioritäten fortlaufend versenden. Je nach Auslastung der Ausgänge ist es möglich, die gerade verfügbare Bandbreite dynamisch zuzuweisen (vgl. Abb. 2.14).

Die mit der DiffServ-Technologie verbundenen QoS-Garantien sind allerdings nicht für eine Ende-zu-Ende-Verbindung ausgelegt, sondern beziehen sich auf sogenannte DiffServ-Domains. Die dafür zuständige IETF-Arbeitsgruppe sieht eine DiffServ-Domain als einen durch gleiche DiffServ-Richtlinien (*Policys*) abgegrenzten Teil eines IP-Netzwerkes an, die in koordinierender Weise administriert werden. Die DiffServ-Domains sind dabei nicht notwendigerweise identisch mit ty-

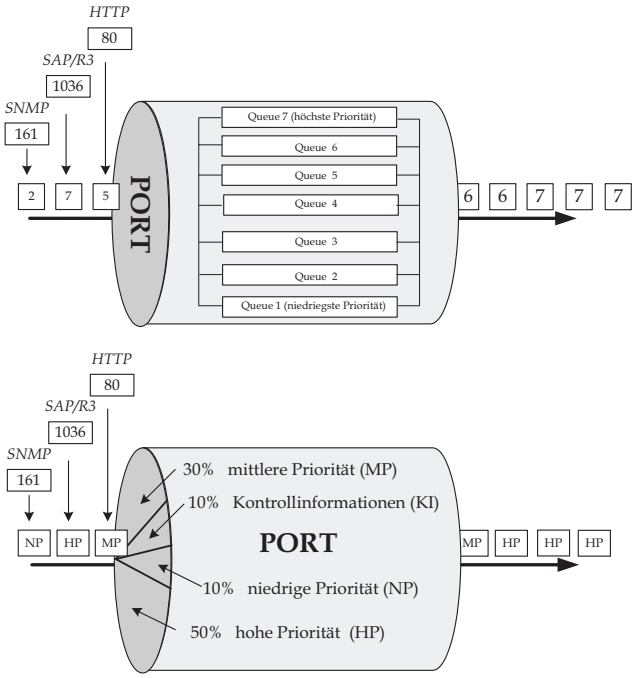


Abb. 2.14: Warteschlangenverhalten eines Routers nach Interpretation des DS-Feldes

pischen Domains eines Intranets. Es können völlig autonome Systeme[18] bzw. Gebiete mit unterschiedlichen Vertrauensbereichen und Netzwerktechnologien gebildet werden, wie z.B. durch Zell- oder Frame-basierte Technologien.

Eine DiffServ-Domain wird einerseits durch gebietsbildende Eckkomponenten eingerichtet *(boundary components)*, die unterschiedliche DiffServ-Domains verbinden können, und andererseits durch interne Komponenten *(interior components)*, die innerhalb einer Domain angesiedelt sind. Als Beispiel einer DiffServ-Domain kann ein entsprechend ausgestattetes *Corporate Network* (CN) oder auch ein umfangreiches IP-Netz eines Internet Service Providers (ISP) angeführt werden. Die Administration einer DiffServ-Domain verfolgt dabei die Aufgabe, dass die vergebenen SLA eingehalten und ausreichend Kapazitäten bereitgestellt werden. Dies wird in der Regel mit geeigneten Netzüberprüfungs- und Steuerungstechniken erreicht.

Die erste standardisierte Neudefinition des Servicetyp-Feldes (TOS) wurde En-

[18] Die Idee und Definition eines autonomen Systems bezieht sich auf eine Gruppe von Routern, die unter einer einzigen Kontrollinstanz verwaltet werden. Router, die zu einem autonomen System gehören, das meistens den Kernbereich (Backbone, Core-Netz) eines umfangreichen Netzes beinhaltet, haben eigene Mechanismen, um Wegefindung, Prüfungsverfahren, Kontrollmethoden und Konsistenzprüfungen der Routen vorzunehmen.

de 1998 vorgenommen [RFC 2474]. Wie weit sich allerdings diese Möglichkeit der Verkehrssteuerung vor einer flächendeckenden Einführung von IPv6 effektiv auswirkt, ist wohl stark davon abhängig, wie schnell sich die UMTS-Technologie im Mobilfunkbereich, die IPv6 einsetzt, durchsetzen wird. Auch ist die endgültige Definition der verschiedenen Classes of Service und das damit verbundene Verhalten der Router noch nicht abgeschlossen. Daher ist dieses Verfahren bislang kaum implementiert.

Der Vorteil von DiffServ ist jedoch, dass diese Technik der Verkehrssteuerung sukzessive eingeführt werden kann. Um einen Class of Service möglichst effizient zu erreichen, sollten möglichst alle Router auf dem Datenweg DiffServ unterstützen. Ein Router, der DiffServ nicht kennt, verhält sich im schlimmsten Falle allen Serviceklassen gegenüber neutral.

Eine Steuerung der DiffServ-Werte, die von einem Netzwerkadministrator für verschiedene Kunden unterschiedlich eingestellt werden muss, kann, je größer das Netz ist, kaum noch manuell erfolgen. Ebenso ist eine manuelle Einstellung zu statisch, um den heutigen dynamischen Anforderungen, die an ein Netz gestellt werden, gerecht zu werden. Somit ist es erforderlich, flexible klassenbasierte Einstellungen zu definieren, die alle gemeinsam mit einem Regelwerk während des laufenden Betriebes kontrolliert und gegebenfalls geändert werden können.

Durch die heute vorherrschenden heterogenen Administrationswerkzeuge ist es notwendig, dass ein standardisiertes Format eingesetzt wird, das idealerweise die Richtlinien in einem allgemein zugänglichen Repository zur Verfügung stellt. Dies ermöglicht das *Lightweight Directory Access Protocol* (LDAP), das allgemein für industrielle Anwendungen benutzt wird. Denn Richtlinien bzw. Policy-Rules für unterschiedliche Service-Level sind in dem LDAP-Directory-Schema gespeichert und können von allen Geräten – wie z.B. Router, Proxys, Hosts, Policy-Server – importiert werden.

2.4 Übungen

1. Es reichen i.d.R. drei Größen aus, um in einem Netz zu kommunizieren. Wenn dies korrekt ist, wozu werden dann die Layer-2-Adressen (MAC) benötigt?
2. Welche zwei Möglichkeiten gibt es für eine leitungsgebundene Kommunikation, Vertraulichkeit zu erreichen?
3. Welche sicherheitsrelevanten Nachteile hat der Einsatz von DHCP bei Verwendung von Mobile-IP?
4. Worin besteht der Unterschied zwischen CoS und Qos?
5. Wie werden die Verfahren Priorisierung und Reservierung in IP-Netzen umgesetzt?

6. Was ist ein autonomes System, und welche Protokolle liefern eine Verbindung zwischen autonomen Systemen?
7. Welche Ergänzungen muss das IP-Protokoll (Best Effort) erfahren, damit es für Videokonferenzen geeignet ist?
8. Welche prinzipiellen/strukturellen Unterschiede gibt es zwischen der LAN-Technologie und WAN-Technologie?
9. Im Ethernet (IEEE 802.3) wird als Zugriffsmethode CSMA/CD eingesetzt. Hierdurch entsteht im LAN eine Collisions-Domäne. Wie sieht dies im WLAN aus?
10. Wieviel Hosts sind in dem Netzsegment (10.180.128.3/28) des Heimatnetzes in dem Beispiel der Abb. 2.6 vorhanden?
11. Wie wird das TOS Feld (Type of Service) in einem Router behandelt, der ein Packet Classifier einsetzt?
12. Was wird mit dem Leaky-Bucket-Verfahren erreicht?
13. Welche Aufgaben übernimmt die Layer-2 gemäß OSI-Schichtenmodell?

3 IuK-Sicherheit

Kapitel 3 beschäftigt sich mit der *Informations- und Kommunikationssicherheit* von VPN. Zu den Absicherungsmaßnahmen zählen sowohl technische als auch organisatorische Vorkehrungen, um Vertraulichkeit, Verfügbarkeit, Integrität und Beherrschbarkeit zu gewährleisten. Nur langsam setzt sich in den Unternehmen die Auffassung durch, eine eigene Sicherheitsstrategie für die Informations- und Kommunikationsverarbeitung entwerfen zu müssen. Allein auf Sicherheitsprodukte zu setzen – so die Erkenntnis – reicht heutzutage bei weitem nicht mehr aus. Dabei stützt sich der jeweilige Sicherheitsansatz auf das Sicherheitsparadigma, das die Bereiche von Sicherheitspolitik, Sicherheitsarchitektur und Sicherheitskonzeption einschließlich operativer Umsetzung in einer hierarchischen Weise berücksichtigt. Damit ermöglicht das Sicherheitsmodell nicht nur die optimale Einbettung eines VPN, sondern bietet auch die Grundlage für eine umfassende Kommunikationstrategie mit Geschäftspartnern, Zulieferfirmen und Endverbrauchern. Bislang werden zwei grundsätzlich verschiedene Arten von Kommunikationsnetzen unterschieden:

- Verteilnetze ohne Rückkanal, in denen alle Teilnehmerstationen vom Netz die gleiche Information (Fernsehen, Radio) erhalten und jeder Teilnehmer lokal auswählt, ob und was er empfangen will. Dies gilt insbesondere in fast allen realisierten und geplanten öffentlichen Verteilnetzen, in denen Kommunikation nur in der Richtung vom Netz zum Teilnehmer stattfindet.
- Vermittlungsnetze, in denen jede Teilnehmerstation vom Netz individuell nur das erhält, was der Teilnehmer angefordert oder ein anderer Teilnehmer an ihn gesendet hat. In Vermittlungsnetzen wird generell in beiden Richtungen kommuniziert.

Langfristig wird jedoch die Bildung eines einzigen Netzes für alle Dienste angestrebt – ein dienstintegrierendes Netz, das zumindest im Teilnehmeranschlussbereich preiswerter ist als mehrere verschiedene Netze. Über ein breitbandiges dienstintegrierendes Vermittlungsnetz ($\geq 1Mbit/s$) könnten dann alle jene Dienste zusammen angeboten werden, die über ein breitbandiges Kabelverteilnetz und ein schmalbandiges Vermittlungsnetz ($\leq 1Mbit/s$) verfügbar sind. Auch zusätzliche Dienste, die eine breitbandige Kommunikation zwischen den Teilnehmern erfordern, wie z.B. das Bildtelefon, könnten eingerichtet werden. In der Folge werden:

- Computer vermehrt in die Kommunikation miteinbezogen werden,
- mehr und mehr lokale Netze (auch adhoc Netze) entstehen und
- Netzübergänge zu Fern- bzw. zu Weitverkehrsnetzen an Bedeutung gewinnen.

Der Aufbau der neuen Informationssysteme bringt nicht nur Vorteile mit sich, da Aufwand und Zeit eingespart werden können, sondern es entstehen auch neue Risiken und Gefahrenquellen. Durch technisches oder menschliches Versagen, durch höhere Gewalt, durch vorsätzliche oder fahrlässige Handlungen oder auch organisatorische Mängel können Schäden unterschiedlicher Art und Höhe verursacht werden. Bei allen Kommunikationsnetzen, egal ob im Sprach- oder Datenbereich, stellt sich also die Frage, wie gut die Teilnehmer vor Schaden geschützt sind und insbesondere ist zu klären, wie mit welchen Mitteln mehr Sicherheit erreicht werden kann. Im Folgenden werden, ausgehend vom Begriff der *Informations- und Kommunikationssicherheit* (IuK-Sicherheit), Schutzziele und Mechanismen zur Schadensabwehr betrachtet. In diesem Zusammenhang werden gängige, wenngleich unterschiedlich ausgerichtete Verfahren wie *GsHb*, *ITSec*, *Common Criteria* und *BS7799* aufgegriffen.

3.1 Definition IuK-Sicherheit

Der Begriff der Computer- bzw. Datensicherheit umfasst all jene Maßnahmen, die die Daten und Programme einzelner Benutzer und Systeme vor zufälligen oder beabsichtigten Zugriffen schützt. Konnte IBM im Jahre 1975 als größter und einflussreichster Hersteller von Datenverarbeitungssystemen noch folgende Definition „Security := Prevention of access to or use of data or programs without authorization[1]“ liefern, zeigt sich heute ein etwas anderes Bild. Damals wurde noch strikt zwischen Datenverarbeitung, die in einem Rechenzentrum stattfand, und Sprachkommunikation (sprich: Analogtelefone) getrennt. Ähnliche Sichtweisen zeigen auch die frühen Kriterienwerke zur IT-Sicherheit wie, z.B. das *Orange Book* aus dem Jahre 1985. Die Abb. 3.6 gibt einen Überblick über die Entwicklung und ihre zeitliche Einordnung der wichtigsten Kriterienwerke.

In Deutschland wiederum zeigt das jährlich überarbeitete *IT-Grundschutzhandbuch* des *Bundesamtes für Sicherheit in der Informationstechnik* (BSI) zahlreiche – mittlerweile als allgemein gültig anerkannte – Standard-Sicherheitsmaßnahmen, Umsetzungshinweise und Hilfsmittel für unterschiedliche IT-Infrastrukturen [BSI 2004a].

Darüberhinaus ist hervorzuheben, dass eine partikuläre Sicht auf die IuK-Sicherheit und eine vorschnelle Einschränkung auf technische Aspekte nicht ausreicht. Statt dessen ist z.B. mit [Rannenberg et al. 1996] von *mehrseitiger Sicherheit* zu sprechen, insofern hier die Systemanforderungen aller Beteiligten – Systembetreiber, Hersteller und Benutzer – berücksichtigt werden. D.h., dass IT-Sicherheit stets von mehreren Seiten, aus Sicht verschiedener Gruppen beleuchtet werden muss. Die Ziele und Anforderungen der unterschiedlichen Interessensgruppen können dabei durchaus divergieren. Der Anstaz einer mehrseitigen Betrachtungsweise lässt sich unter dem Begriff *duale Sicherheit*, subsumieren [Dierstein 2002]. Ihnen liegen die Forderungen zugrunde, dass

[1] IBM Data Processing Glossary GC20-1699-4, File No. S360/S370-20, 5th Edition, December 1972.

- sichere IuK-Systeme verlässlich sein müssen und weder Daten (Informationen) noch die Datenverarbeitung (Funktionen und Prozesse) in ihrem Bestand, ihrer Nutzung oder ihrer Verfügbarkeit unzulässig beeinträchtigt werden dürfen,
- sichere Systeme beherrschbar sein müssen, d.h., dass die Rechte oder schutzwürdigen Belange ihrer Benutzer weder direkt noch indirekt durch das Vorhandensein bzw. durch die Nutzung von IuK-Systemen unzulässig beeinträchtigt werden dürfen.

Ein IuK-System ist aus technischer und organisatorischer Sicht sicher, d.h. verlässlich, wenn seine Funktionsweise den angegebenen Forderungen genügt. Ein sicheres IuK-System verfügt über:

Vertraulichkeit *(confidentiality)***:** weder unbefugte Einsichtnahme von Daten, unbefugtes Erschließen von Informationen noch unbefugtes Interpretieren von Daten

Integrität *(integrity)* **:** keine unbefugte, unbemerkte Veränderung der Daten oder Funktionen des Systems

Verfügbarkeit *(availability)***:** Ausführung der Prozesse (Funktionen) des Systems zum vorgegeben Zeitpunkt und Ablauf im vorgegebenen Zeitrahmen

Aus Sicht der Betroffenen bzw. der Benutzer der IuK-Systeme können für die Beherrschbarkeit zwei weitere Eigenschaften hinzugefügt werden:

Zurechenbarkeit *(accountability)***:** Von jedem Prozess bzw. jeder Funktion und dessen Ergebnissen muss während seines Ablaufs oder danach feststellbar sein, welcher Instanz dieser zuzurechnen ist. Mit anderen Worten: Es muss eindeutig sichergestellt werden, welche Komponenten von welcher Person bedient oder ausgelöst wurden.

Verbindlichkeit *(liability)***/Rechtsverbindlichkeit** *(legal liability)***:** Von jedem Prozess bzw. jeder Funktion und dessen Ergebnissen muss auch Dritten gegenüber beweiskräftig nachweisbar sein, welche Instanz ihn zu verantworten hat.

Diese fünf Eigenschaften beschreiben umfassend die Bedeutung der IuK-Sicherheit. Sie sind damit die übergreifenden Ziele eines jeden Sicherheitskonzepts. Sobald ein Kommunikationssystem mittels eines Sicherheitskonzepts geplant und umgesetzt wurde, wird es – sofern entsprechende Maßnahmen getroffen wurden – nur sehr schwer zu kompromittieren sein. Um diese These zu untermauern, werden im Folgenden drei unterschiedliche Sicherheitsaspekte näher betrachtet:

- **Attacken/Angriffe:** Darunter werden Aktionen verstanden, die das Ziel verfolgen, widerrechtlich in fremde Systeme einzudringen, um in den Besitz vertraulicher Informationen zu gelangen.

- **Mechanismen:** Hierbei geht es um Verfahren, Methoden und Maßnahmen zur Erkennung und Verhinderung von Attacken sowie um die Behebung eventueller Schäden, die durch bereits erfolgte Angriffe entstanden sind.
- **Dienste:** Hierunter werden die von einer Sicherheitsarchitektur zur Verfügung gestellten Funktionen bzw. Leistungen verstanden. Die einzelnen Dienste verfolgen das Ziel, unter Nutzung unterschiedlicher Mechanismen eine bestimmte Menge von Attacken abzuwehren.

Bei genauer Betrachtung der Attacken kommen diejenigen Bedrohungen zu Tage, die mit Hilfe von Mechanismen unterbunden werden sollen. Anhand von unterschiedlichen Beispielen werden im Folgenden unterschiedliche Formen von Angriffen bzw. Attacken kategorisiert und vorgestellt. Ausgangspunkt ist dabei der normale Informationsfluss (Abb.3.1) von einer Datenquelle zu einem Ziel:

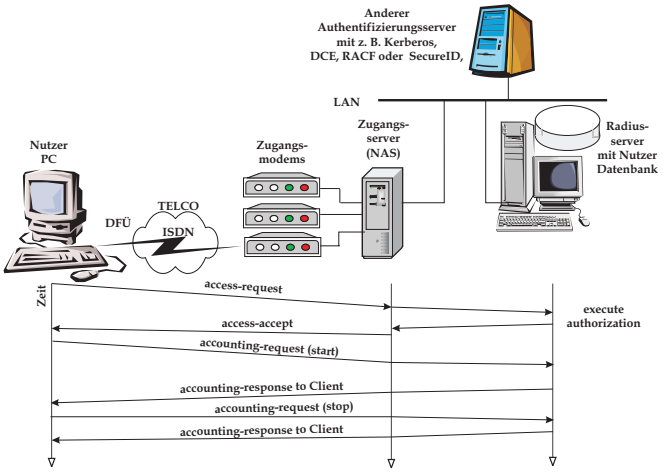


Abb. 3.1: Ungestörter Informationsfluss zwischen Quelle (Kreis mit Linien) und Ziel (Kreis mit Karos)

Die konkrete Ausprägung der Endpunkte spielt theoretisch keine Rolle und kann auf einem abstrakten Niveau verbleiben. Es kann sich also genauso gut um Dateien als auch um Hauptspeicherbereiche handeln, die sich entweder auf demselben Rechner oder auf einem vernetzten Client/Server-System befinden. In erster Linie geht es um den Datentransport über ein Netz. Nach Absenden der Daten besteht in der Regel keine Kontrolle mehr über die Informationen auf dem Wege zum Empfänger. Weiterhin ist nicht sichergestellt, ob die Informationen überhaupt ohne Manipulationen ihr Ziel erreichen. Beispielsweise kann jeder auf dem Weg liegende Router die weiterzuleitenden Datenpakete mitlesen, verändern, kopieren oder vernichten. Auch haben Router und Endsysteme die Möglichkeit, Pakete mit beliebigem Inhalt und die zugehörigen Adressen neu zu bilden und diese anschließend zu versenden.

Eine Kategorisierung möglicher Attacken sowie eine Zuordnung, gegen wen oder was sich die Attacken richten, ist nachfolgend zusammengestellt. Dabei ist ein Informationsfluss immer von der Quelle (Kreis mit Linien) zum Ziel (Kreis mit Karos) dargestellt.

Unterbrechung, gerichtet gegen die Verfügbarkeit: Die Verbindung zwischen Quelle und Ziel wird unterbrochen (Abb. 3.2), so dass kein Informationsfluss mehr möglich ist. Dies kann mittels Hard- oder Software passieren, z.B. durch eine physikalische Unterbrechung der Datenleitung oder durch modifizierte Routing-Einträge. Auch *Denial-of-Service-Attacken* (DoS) gehören zu dieser Kategorie, bei der eine Firewall solange mit IP-Paketen überflutet wird, bis sie unter der Last versagt.

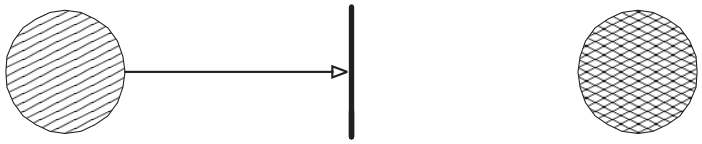


Abb. 3.2: Unterbrochener Informationsfluss zwischen Quelle (Kreis mit Linien) und Ziel (Kreis mit Karos)

Abhören, gerichtet gegen die Vertraulichkeit: Ein nicht autorisierter Beteiligter (Person, Programm oder Computer) gelangt in den Besitz einer vertraulichen Information. Dies kann durch Abhören einer Datenleitung, z.B. mittels Sniffer, Lesen von IP-Paketen oder durch widerrechtliches Kopieren von Dateien geschehen. Abb. 3.3 skizziert den Vorgang des Abhörens. Einem unbefugten Dritten (weißer Kreis mit gestrichelter Außenlinie) gelingt die Beschaffung vertraulicher Informationen.

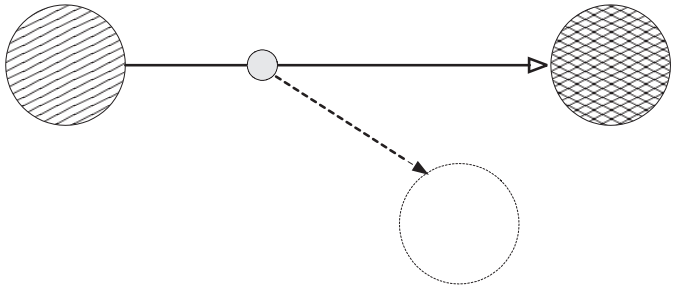


Abb. 3.3: Abgehörter Informationsfluss (gestrichelter Pfeil) durch einen unbefugten dritten Teilnehmer (weißer Kreis mit gestrichelter Außenlinie)

Fälschung, gerichtet gegen die Authentifikation: Die beim Empfänger (Ziel) eingetroffene Nachricht stammt nicht von der vermeintlichen Quelle, sondern wurde in deren Namen von einem Angreifer erzeugt und versandt. Dies ist z.B. realisierbar, indem selbstgenerierte Datenpakete mit gefälschter Absenderadresse in das

Transportnetz eingespeist werden (Abb. 3.4). Eine andere Variante ist, dass die beim Empfänger eingetroffene Nachricht zwar von der richtigen Quelle stammt, jedoch nicht von der Person, der das Endgerät zugeordnet ist. Dieses Szenario kann schnell erfolgen, wenn der Zugriff zu einem Computer nicht oder nur mit unzureichenden Passwörtern gesichert ist (Abb. 3.4). Von der eigentlichen Quelle (Kreis mit Linien) wird überhaupt keine Information an das Ziel (Kreis mit Karos) geschickt. Ein unbefugter Teilnehmer (weißer Kreis mit gestrichelter Außenlinie) versendet Datenpakete mit der vermeintlichen Adresse der Quelle. Dies kann beispielsweise mit einer E-Mail geschehen, die nicht signiert ist.

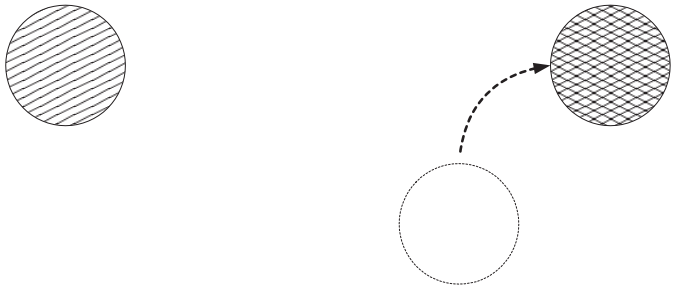


Abb. 3.4: Gefälschter (gestrichelter Pfeil) Informationsfluss durch einen unbefugten Dritten (weißer Kreis mit gestrichelter Außenlinie)

Modifikation, gerichtet gegen die Integrität: Eine vertrauliche Nachricht wird von einem nicht autorisierten Beteiligten abgefangen, modifiziert und in veränderter Form (Abb. 3.5) an das Ziel (Kreis mit Karos) weitergeleitet. Als Beispiele hierzu sind das Modifizieren von IP-Paketen in einem Router oder auch die Wertemanipulation einer Datei im Dateisystem zu nennen. Aus den in

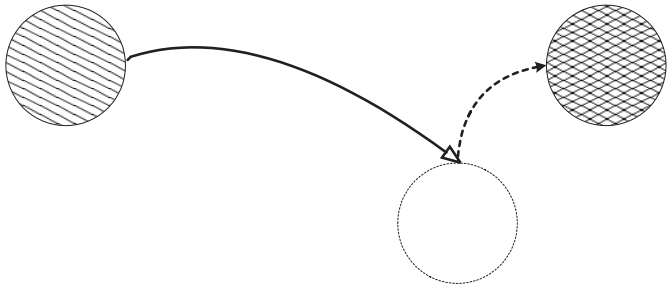


Abb. 3.5: Modifizierter (gestrichelter Pfeil) Informationsfluss durch einen unbefugten dritten Teilnehmer (weißer Kreis mit gestrichelter Außenlinie)

den Abbildungen aufgezeigten Möglichkeiten, einen Kommunikationsteilnehmer zu schädigen, wird mehr als deutlich, dass dringender Handlungsbedarf besteht, die Kommunikation abzusichern. Hierfür werden Maßnahmen definiert

und entwickelt, um die IuK-Sicherheit hinsichtlich Vertraulichkeit, Verfügbarkeit, Integrität und Verbindlichkeit zu gewährleisten. Ziel dieser Maßnahmen ist es, mögliche Schädigungen erheblich zu erschweren. In einer ersten groben Näherung kann zugrunde gelegt werden, dass die Investitionen zur Umsetzung der Maßnahmen nicht die monetären bzw. immateriellen Werte, wie das Firmenimage, die die Kommunikationsbeziehungen beinhalten, übersteigen dürfen. Außerdem gilt der Grundsatz, dass es eine hundertprozentige Absicherung nicht gibt.

3.2 Verfahren zur Erlangung der IuK-Sicherheit

Jede Kommunikationsverbindung zwischen einzelnen Teilnehmern muss abgesichert werden. Es reicht nicht mehr aus, allein die Datenübertragung, wie z.B. bei einem VPN praktiziert, abzusichern. Vielmehr muss das gesamte Kommunikationssystem, in dem ein VPN eingebettet ist, betrachtet werden, wenn eine vollständige, also technische und organisatorische IuK-Sicherheit erreicht werden soll. Welche Methoden zur Sicherung bzw. welche Kriterienwerke derzeit verfügbar und praktikabel sind, ist Gegenstand dieses Abschnittes.

Schon in den frühen 80er Jahren wurde in den USA ein Kriterienwerk zur Sicherheit für Daten, das *Orange Book*, zusammengestellt (Abb. 3.6). In den europäischen Ländern setzte eine ähnliche Entwicklung, Kriterienwerke zur Informations- und Kommunikationssicherheit zu entwickeln, ungefähr fünf bis sechs Jahre später ein. Aufgrund der zögerlichen Kommerzialisierung des Internets auf dem europäischen Kontinent wurde erst 1990 ein harmonisiertes europäisches Gesamtwerk (ITSEC) entwickelt. Zu den europäischen Ländern, die zuvor eigene Werke entworfen hatten, zählten damals die G4-Länder, Großbritannien, Niederlande, Frankreich und Deutschland. Abb. 3.6 zeigt die europäische Entwicklung in wolkenartiger Umrandung. Als eines der wesentlichen deutschen Organe ist das *Bundesamt für Informationssicherheit* (BSI) zu nennen, das dem Innenminister unterstellt ist. Das BSI ist aus der *Zentralstelle für das Chiffrierwesen* (ZfCH), ursprünglich beim *Bundesnachrichtendienst* (BND) angesiedelt, über den Umweg einer *Zentralstelle für Sicherheit in der Informationstechnik* (ZSI), ab dem 01.01.1990 hervorgegangen. Das BSI hat mit dem *IT-Grundschutzhandbuch*[2] [BSI 2004a], das jährlich fortgeschrieben wird und bis zum mittleren Schutzbedarf ausgelegt ist, ein Quasi-Standardwerk geschaffen, das nicht nur richtungsweisend für alle Bundesbehörden ist, sondern auch in der Wirtschaft nachhaltige Beachtung findet. Ein Schattendasein führt indessen das *IT-Sicherheitshandbuch*, in dem ein vierstufiges Verfahren mit insgesamt 12 Schritten vorgeschlagen wird. Das IT-Sicherheitshandbuch hat sich nicht so etabliert wie das IT-Grundschutzhandbuch, nicht zuletzt wegen der umständlichen und wenig transparenten Vorgehensweisen, die vorgeschlagen werden [Lampe 1993]. Eine Alternative stellen hier die am

[2] Anzumerken ist, dass eine Überarbeitung halbjährlich stattfindet, jedoch nur einmal im Jahr eine Gesamtausgabe im *Bundesanzeiger* publiziert wird.

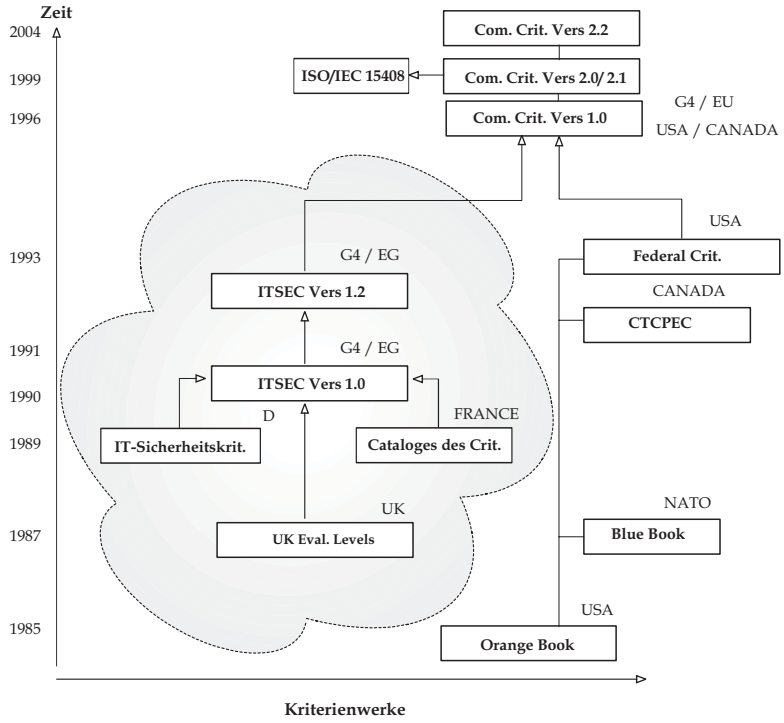


Abb. 3.6: Zeitliche Einordnung und Entwicklung wichtiger Kriterienwerke

Markt verfügbaren Risikoanalysen dar, die jedoch recht unterschiedlich einzustufen sind.

Liegt der Schutzbedarf[3] eines Kommunikationssystems deutlich im Bereich „hoch“ bis „sehr hoch“ müssen jenseits der Grundschutzmaßnahmen weitere dedizierte Absicherungen getroffen werden. Dazu müssen Risiken, denen das jeweilige System ausgesetzt ist, näher untersucht werden. Risikoanalysen gibt es allerdings in unterschiedlichen Varianten. Sie sind je nach Vorgehensweise mehr oder weniger geeignet, wertvolle Informationen über das zu untersuchende Kommunikationssystem zu liefern. Die hier favorisierte Methode wird im nächsten Abschnitt detailliert erläutert.

3.2.1 Risikoanalysen

Versicherungsgesellschaften haben sich schon immer für das Risiko interessiert und versucht, dies zu qualifizieren und zu quantifizieren – und das sowohl dia-

[3] Eine Schutzbedarfsfeststellung kann mit dem IT-Grundschutzhandbuch beschriebenen Verfahren erarbeitet werden.

gnostisch als auch prognostisch. Nach der [DIN VDE 3100-2 1987] setzt sich das Risiko, das mit einem bestimmten technischen Vorgang oder Zustand verbunden ist, aus einer Wahrscheinlichkeitsaussage der zu erwartenden Häufigkeit des Eintritts eines zum Schaden führenden Ereignisses und das beim Ereigniseintritt zu erwartende Schadensausmaß zusammen. Ähnliche Ausführungen sind auch bei [Mock 2003] zu finden. Verfahren, die nach dieser Norm vorgehen, haben sich in der IuK-Technologie noch nicht etabliert. In anderen Branchen z.B. in der Versicherungsbranche, in der Chemie mit der *HaZard and Operability Studies*-Methode (HAZOP) [DIN IEC 1998] oder auch in der Fertigungsindustrie mit der *Failure Mode and Effect Analysis*-Methode (FMEA) [DIN IEC 2001] werden vergleichbare Verfahren seit geraumer Zeit erfolgreich eingesetzt. Bevor nun detailliert auf die Risikoanalyse eingegangen wird, werden zunächst einige Überlegungen zu wichtigen Begriffen, die direkt und indirekt bei einer Risikoanalyse genutzt werden, vorangestellt.

Eine etwas abstrakte, jedoch mit allen für eine Risikoanalyse notwendigen Begriffen versehene Darstellung, liefert die Betrachtung der Wechselbeziehungen zwischen Werten, Schwachstellen, Bedrohungen und Risiken sowie Eigentümern von Werten. Der Schutz von interessanten Werten mittels Sicherheitskonzept fällt in den Verantwortungsbereich der Eigentümer dieser Werte. Abb. 3.7 zeigt die untereinander bestehenden Abhängigkeiten [ISO 15408:1999]. Evident ist allerdings die Tatsache, dass nicht nur Schwachstellen oder nur Bedrohungen alleine vorhanden sein müssen, um ein Risiko entstehen zu lassen, sondern es müssen beide Größen, also Schwachstelle und Bedrohung, existieren und zusammmenwirken. Dem hier verfolgten Ansatz wird der *CCTA Risk Analysis and Management Method* (CRAMM) gefolgt. Doch CRAMM greift auf eine Bibliothek mit mehr als 3000 Einträgen zurück, somit handelt es sich um ein wissensbasiertes Verfahren. In dieser Arbeit wird jedoch nicht auf die Bibiliothek von CRAMM zurück gegriffen, sondern durch eine Risikoszenarientechnik ergänzt. Damit wird ein ereignisorientiertes Verfahren eingesetzt. Oftmals sind nur Kenntnisse über Schwachstellen beim Eigentümer vorhanden, so dass nur Schwachstellen in Sicherheitskonzepten begegnet wird (Abb. 3.7). Eine alleinige Betrachtung der Schwachstellen ist jedoch nicht zielführend. Auch die Eliminierung der Eintrittswahrscheinlichkeit aus der Risikobetrachtung, wie es das BSI in seiner Risikanalyse auf Basis von IT-Grundschutz vorsieht, wird einer DIN-konformen Risikobetrachtung nicht gerecht [BSI 2004b].

Risiko, Sicherheit und Gefahr

Wird der Begriff Risiko näher betrachtet, lassen sich bestimmte Beziehungen herleiten, z.B. der Begriff der Sicherheit und der Gefahr. Diese allgemein gebräuchlichen Begriffe stehen in einer methodischen Relation zum Begriff des Risikos. Veranschaulicht werden kann das Risiko anhand einer Skala. Abb. 3.8 zeigt die eindeutige Beziehung zwischen den Begriffen Sicherheit, Risiko und Gefahr. Ausgehend von dieser Skala wird deutlich, dass der Betrieb eines Systems ohne Schutzmaßnahmen ein hohes (vermeidbares) Risiko in sich birgt. Durch geeignete

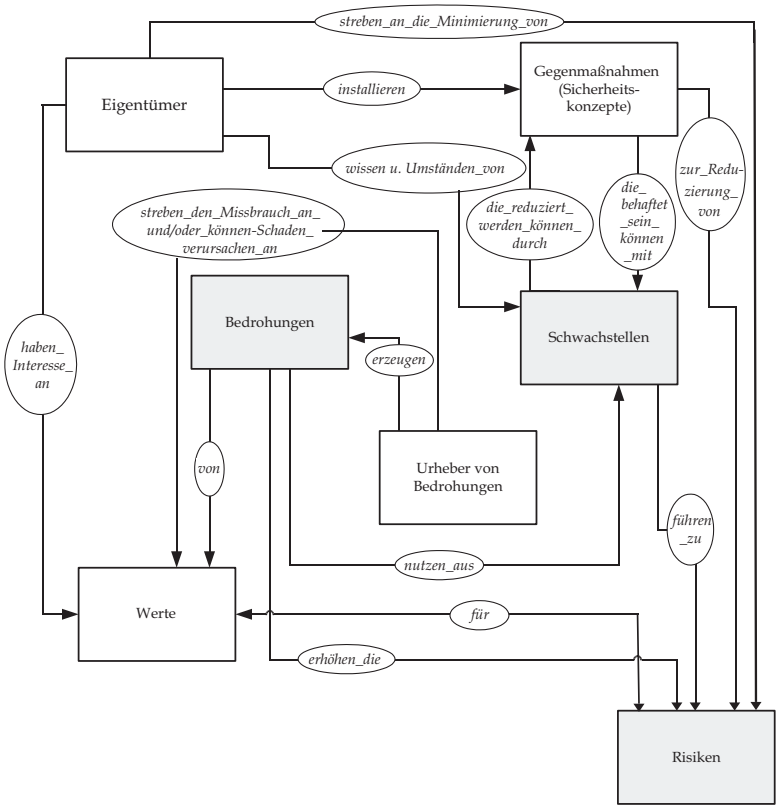


Abb. 3.7: Beziehungen zwischen Eigentümer, Werten, Schwachstellen, Bedrohungen und Risiken

Maßnahmen kann das Risiko reduziert und der Gefahrenbereich eingeengt werden. Weiterhin wird deutlich, dass der Begriff der Sicherheit ein relativer Begriff ist, der sich nur durch ein Nichtvorhandensein von Risiken definieren lässt und dass sich nur im unwahrscheinlichen Fall der Abwesenheit von Restrisiken eine 100%ige Sicherheit einstellt.

Wird das Risiko – und mit ihm die Schadenserwartung – auf ein Minimum reduziert, so spricht man von relativer Sicherheit. Das verbleibende Risiko wird dann als Restrisiko bezeichnet. Erfolgt hingegen eine Reduzierung des Risikos nicht auf ein Minimum, sondern auf höhere Werte, so existiert ein als Grenzrisiko bezeichneter Schwellenwert, bei dessen Überschreiten der Zustand der Gefahr erreicht wird. Die Gefahr liegt somit zwischen der Sicherheit und dem nicht reduzierten Risiko.

Netzinfrastrukturen, in die VPN eingebettet sind, sind vielfach nicht einfach zu überschauen. Wenn eine komplette Analyse durchgeführt werden soll, spielen nicht nur technische Komponenten eine Rolle, sondern auch organisatorische und

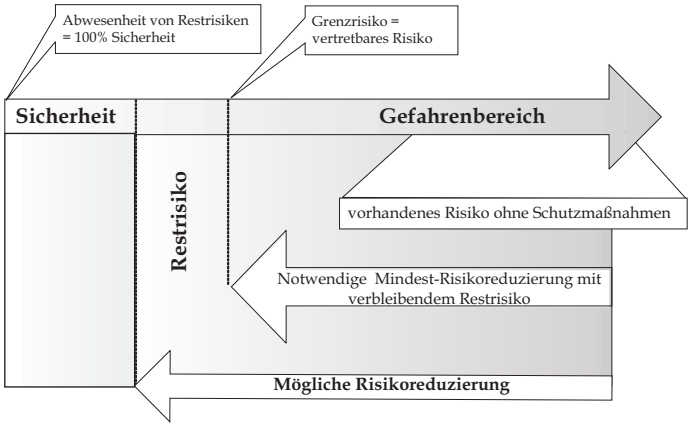


Abb. 3.8: Risikoachse mit den Begrifflichkeiten Sicherheit, Gefahr und Risiko

rechtliche Aspekte. Da der Umfang eines aus standardisierten Maßnahmen abgeleiteten Sicherheitskonzept für ein VPN die Grenzen der Praktikabilität und Akzeptanz sprengen würde, treten bei solch komplexen Systemen individuelle Risikoanalysen an die Stelle pauschalisierter Aussagen zum Grundschutz. Um die vorhandene Komplexität einer Netzinfrastruktur für eine Analyse zu reduzieren bzw. überschaubarer zu machen, kann es sinnvoll sein, mit einem Schichtenmodell die abhängigen Komponenten einzeln und im Zusammenspiel mit anderen Komponenten zu betrachten. Gleichzeitig liefert das Architekturmodell eine gute Basis, um die Frage der Vollständigkeit einer Risikoanalyse zu beantworten.

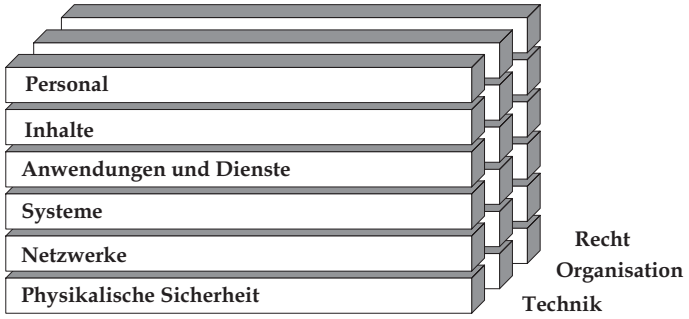


Abb. 3.9: Komplexe Abhängigkeiten als Schichten im Architekturmodell

Wird ein Architekturmodell wie in Abb. 3.9 benutzt, das die jeweiligen Abhängigkeiten – angefangen von Personalaspekten bis hin zur physikalischen

Sicherheit – in horizontalen Schichten beschreibt und diese mit rechtlichen, organisatorischen und technischen Aspekten, die vertikal angeordnet sind, durch Abfragen verknüpft, kann die Frage der Vollständigkeit einer Risikoanalyse beantwortet werden. Die Abfragen richten sich nach den vom BSI definierten Schutzzielen (Vertraulichkeit, Integrität und Verfügbarkeit). Eine konsequente Anwendung des Architekturmodells ermöglicht die Entflechtung der bei großen Systemen komplexen Abhängigkeiten. Sie bildet die Grundlage für die Bedrohungs- und Schwachstellenanalyse, indem jede horizontale Ebene sowohl mit jeder vertikalen Ebene als auch mit den übrigen horizontalen Ebenen in der Analyse durch Abfragen oder durch dynamische Untersuchungen in Beziehung gesetzt werden. Damit wird die Komplexität, die derartige Untersuchungen nach sich ziehen, erheblich reduziert.

Die nachfolgend beschriebene Vorgehensweise zur Durchführung einer Risikoanalyse geht über die Empfehlungen des BSI, das Risikoanalysen nur für hochschutzbedürftige IT-Systeme vorsieht, hinaus. Zur strukturierten Durchführung individueller Risikoanalysen bietet sich die folgende Methode an, die die in Abb. 3.7 vorhandenen Größen nach [DIN VDE 3100-2 1987] berücksichtigt.

Schadensbestimmung in komplexen Systemen

Die quasiobjektive Methode der Schadensbestimmung in komplexen Systemen ist im Detail bei [Böhmer 1998b] nachzulesen. Die Methode fußt auf der [DIN VDE 3100-2 1987] und damit auf dem allgemein anerkannten Grundsatz zur Risikobestimmung.

Das Risiko *(r)* ist das Produkt aus Eintrittswahrscheinlichkeit eines Ereignisses *(Ep)* und Schadenumfang *(d)*:

$$r = Ep \cdot d \;\; (risk = Eventprobability \times damage) \tag{3.1}$$

Gleichung 3.1 kann dahingehend interpretiert werden, dass ein geringes Risiko *(r)* dann besteht, wenn mit einer geringen Wahrscheinlichkeit ein wenig schädigendes Ereignis eintritt. In dem Maße, wie Eintrittswahrscheinlichkeit und/oder Schadensumfang wachsen, wächst auch das Risiko.

Die Einheit des Risikos wird in monetären Maßeinheiten, also einer Währung, gemessen. Dies folgt aus der Eintrittswahrscheinlichkeit eines Ereignisses, die dimensionslos ist, sich zwischen 0 und 1 bewegt und dem ersten Axiom[4] der Wahrscheinlichkeit genügt. Weiterhin wird die Eintrittswahrscheinlichkeit eines Ereignisses auf einen Zeitraum von 365 Tagen bezogen. Damit ist diese Analyse, im Gegensatz zur kardinalen Risikobewertung, wie sie oft in den USA verwendet wird, ereignisgetriggert und orientiert sich an den vorgegebenen Schutzzielen des BSI. Es werden jedoch nicht alle erdenklichen Ereignisse untersucht, sondern nur diejenigen, die auf den gefundenen Schwachstellen $(Schw)$ der IST-Analyse aufsetzen und die mit aktiven und passiven Bedrohungen $(b_0 + b_1 + ...b_n)$ in einem

[4] Das erste Axiom der Wahrscheinlichkeit besagt, dass Ereignisse, deren Eintrittswahrscheinlichkeit Null ist, durchaus eintreten können [Kreiszig 1982].

direkten Verhältnis stehen. Dabei können beispielsweise mehrere unterschiedliche Bedrohungen auf dieselbe Schwachstelle wirken. Für die Grundbedrohung, die immer vorhanden ist, steht die Größe (b_0).

Eine Verknüpfung zwischen Bedrohung und Schwachstelle wird durch ein Risikoszenario (r_{sz}) hergestellt. Die Szenarientechnik hilft dabei, mittels möglicher Risikoereignisse, die sich in der Zukunft abspielen, Rückschlüsse auf die Gegenwart zu ziehen.

In der Praxis wird Gleichung 3.1 in i Risikoszenarien $(r_{sz(i)})$, wie in Gleichung 3.2 dargestellt, überführt.

$$r_{sz(i)} = Ep_{i(\sum_{j=1}^{m} b_j \cdot \sum_{k=1}^{l} Schw_k)} \cdot d_i \tag{3.2}$$

Für jedes i-te-Risikoszenario wird dann jeweils die i-te-Eintrittswahrscheinlichkeit, die abhängig ist von der j-ten-Bedrohung und der k-ten Schwachstelle, mit der Schadenauswirkung d_i gebildet. Die Risikoszenarien werden anschließend gemäß ihrer Eintrittswahrscheinlichkeit bzw. ihrer relativen Häufigkeit und ihren Auswirkungen in eine (3×3)-Matrix (Abb. 3.10) eingetragen.

Dieser umfassende Ansatz hat – im Gegensatz zu reinen Schwachstellenanalysen – den unschätzbaren Vorteil, dass sie verkettete Ereignisse berücksichtigen, wenn die Szenarientechnik konsequent angewandt wird. Insbesondere verkettete Ereignisse lassen sich schwer erfassen. Doch gerade diese haben oft gravierende Auswirkungen, so dass ihre Beachtung für einen umfassenden Ansatz zwingend erforderlich ist.

Mit dieser Technik werden i Risikoszenarien unter Berücksichtigung von k Schwachstellen $(Schw_{k=1,..l})$ bezogen auf das betrachtete System und Bedrohungen, abgeleitet aus der IST-Analyse und bezogen auf die Schutzziele (Verfügbarkeit, Vertraulichkeit und Integrität) entwickelt. Bei der Bestimmung der Eintrittswahrscheinlichkeit der Szenarien werden die Gefährdungen aus dem Zusammenwirken der beiden Faktoren Bedrohung und Schwachstelle abgeleitet. Im Sinne von Aktio und Reaktio wirkt die Bedrohung auf die Schwachstelle und löst somit das Szenario aus. Bedrohungen $(b_0 + b_1 + ...b_n)$ lassen sich unterteilen in:

- die Betriebsbedrohung, die ohne zusätzliche Bedrohungen eine endliche Lebenszeit der Anlage bewirkt,
- zufällige unbeabsichtigte Bedrohungen wie Unwetter, Stromausfall, Komponentenausfall oder auch Fehlbedienungen und
- vorsätzliche Bedrohungen mit der Absicht, das System aus seinem Soll-Zustand zu bewegen und damit einen Störfall auszulösen oder es gar zu zerstören.

Aus dieser Unterteilung der Bedrohungsarten kann, zusammen mit bekannten Bedrohungen aus dem Betrieb von IT-Systemen, eine Liste von möglichen Bedrohungen erstellt werden (siehe auch [ISO 7498-2:1989]). Die Zusammenstellung

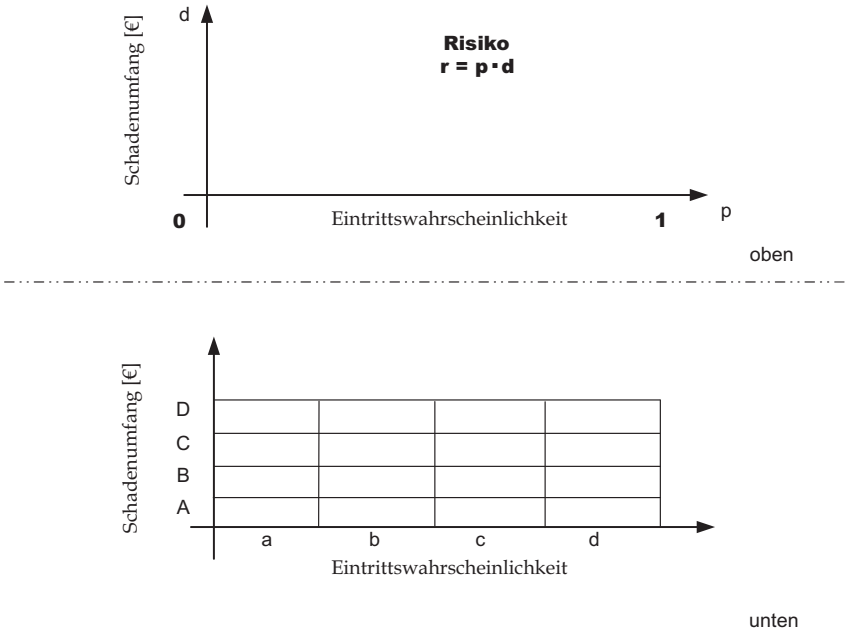


Abb. 3.10: Veranschaulichung des Risikos (oben) und der Risikoszenarienmatrix (unten)

und der Umfang der Liste stehen in direktem Verhältnis zum Untersuchungsaufwand. Weiterhin lassen sich Informationssysteme oder auch Teilsysteme nach Kriterien bewerten, die in ganz Europa (ITSEC) bzw. auch global wie z.B. die *Common Criteria*, anerkannt sind. Diese Verfahren sind jedoch verhältnismäßig zeitaufwändig und kostspielig. Außerdem sind für derartige Untersuchungen autorisierte Unternehmen[5] erforderlich. Ferner werden häufig nur für einzelne Komponenten, wie z.B. Chipkarten oder Firewall-Systeme, Evaluierungen nach den Kriterienwerken durchgeführt. Ein Überblick über die Strukturierung und wie die Kriterienwerke im Verhältnis zueinander stehen, wird im nachfolgenden Abschnitt ausgeführt.

3.2.2 ITSEC und Common Criteria

Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (*Common Criteria for Information Technology Security Evaluation*, CC) sind seit Dezember 1998 in der Version 2 verfügbar. Das Kriterienwerk ist praktisch auf alle informationstechnischen Produkte und Systeme gleich gut anwendbar und ermöglicht eine Bewertung nach Sicherheitseigenschaften. Dies bedeutet,

[5] Auf der Homepage des BSI (http://www.bsi.de) ist eine Liste der zertifizierten Komponenten und der anerkannten Zertifizierungsstellen zu finden.

dass vorhandene Sicherheitsmaßnahmen einer Prüfung und Bewertung unterzogen werden können. Die Bewertung liefert dann eine vergleichbare Aussage über den Grad der Vertrauenswürdigkeit der Sicherheits- bzw. Gegenmaßnahme, die die Risiken für die zu schützenden Werte vermindert. Mit der Version 2 der CC ist eine ISO-Version erreicht worden [ISO 15408:1999].

Die Common Criteria stellen eine Weiterentwicklung und Harmonisierung der europäischen Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC) des Orange Book (TCSEC) der USA und der kanadischen Kriterien (CTCPEC) dar. Dabei sind die Common Criteria wesentlich umfassender in ihren Hintergrundinformationen und Erklärungen zu den Einzelanforderungen. Die Kompatibilität zu den Basiswerken bzw. Basiskriterien bleibt jedoch weitgehend gewahrt (Abb. 3.6).

3.2.3 Vergleich zwischen CC und ITSEC

Aufgrund vieler Gemeinsamkeiten zwischen den Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC) und den Common Criteria wurde vereinbart, dass alle Zertifikate, die auf Basis der ITSEC ausgegeben wurden, auch nach Einführung der CC ihren Wert behalten. Das Ziel der Harmonisierungsbemühungen von IT-Sicherheitskriterien war die formale gegenseitige Anerkennung von Evaluationsergebnissen.

Wie die ITSEC erlauben die Common Criteria eine getrennte Prüfung und Bewertung der Funktionalität und der Vertrauenswürdigkeit.[6] Die CC bieten mit etwa 150 detaillierten Funktionalitätskomponenten viel konkretere Funktionalitätskriterien als die ITSEC. Dennoch kann, wie bei den ITSEC auch, jede sinnvolle sicherheitsspezifische Funktion evaluiert werden, die nicht explizit in den Kriterien aufgelistet ist. Eine Bewertung der Vertrauenswürdigkeit erfolgt bei den CC[7] durch sieben, bei der ITSEC durch sechs Vertrauenswürdigkeitsstufen. Diese entsprechen inhaltlich in etwa den E-Stufen der ITSEC. EAL2 aus den CC entspricht also der Stufe E1 der ITSEC und EAL7 ist E6 nahezu gleichgestellt. Allerdings ist EAL1 in der Hierarchie unterhalb von E1 des ITSEC angesiedelt. Dies ist aus Gründen des einfacheren Zugangs zur Evaluation festgelegt worden.

Wie bei ITSEC bilden bei den CC Sicherheitsvorgaben die Grundlage für die Evaluation. Den CC können Prüfkriterien entnommen werden, an denen die Sicherheitsvorgaben, ob ein Sicherheitskonzept dem Sicherheitsproblem angemessen ist, evaluiert werden. Das Konzept der ITSEC-Funktionsklassen wird in den CC durch Schutzprofile abgelöst. Wird ein Vergleich gezogen zwischen der

---

[6] Unter Funktionalität bzw. Funktionalitätsklassen, die auf den Grundfunktionen, wie z.B. Identifikation und Authentifizierung, Rechteverwaltung, Rechteprüfung, Übertragungssicherung beruhen, werden die Klassen F1 bis F10 gebildet. Z.B. entspricht die Funktionalitätsklasse F1 der TCSEC-Klasse C1: benutzerbestimmbarer Zugriffschutz.

[7] Die Vertauenswürdigkeitsstufen sind bei den CC durch den Begriff *Evaluation Assurance Level* (EAL) definiert.

Anwendungsbreite von Orange Book, ITSEC und den Common Criteria, wird deutlich, dass die Common Criteria das größte Spektrum hinsichtlich der Vertrauenswürdigkeit und Funktionalität abdecken. Abb. 3.11 macht diesen Sachverhalt deutlich. In Tab. 3.1 werden die Vertrauenswürdigkeitskriterien der ITSEC den

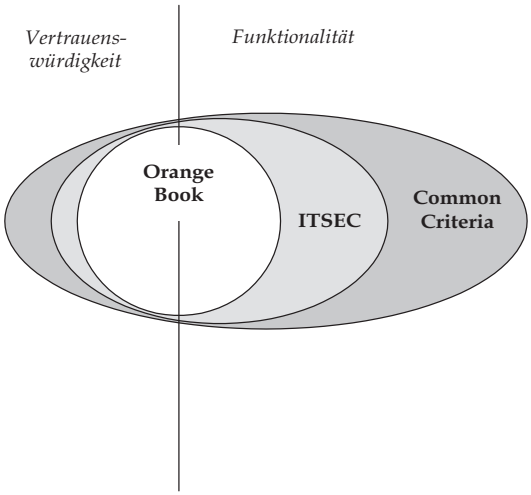


Abb. 3.11: Vergleichende Betrachtung zwischen Vertrauenswürdigkeit und Funktionalität der Kriterienwerke Orange Book, ITSEC und Common Criteria (Quelle: BSI)

Common Criteria gegenübergestellt. Es ist deutlich zu erkennen, dass die ITSEC-Kriterien in leicht veränderter Form in den Common Criteria wiederzufinden sind. Wird beispielsweise der Entwicklungsprozess betrachtet, der nach den vier Vertrauenswürdigkeitsbewertungen (Anforderungen, Architekturentwurf, Feinentwurf und Implementierung) gegliedert ist und einen beachtlichen Anteil einer Evaluationsarbeit darstellt, ist diese Bewertung in den Common Criteria (Funktionale Spezifikation, Entwurf auf hoher Ebene, Entwurf auf niedriger Ebene, Darstellung der Implementierung) deutlich wiederzuerkennen (Tab. 3.1).

Wirksamkeitsaspekte, wie Eignung und Zusammenwirken der Funktionalität, werden in den Common Criteria bei der Evaluation der Sicherheitsvorgaben berücksichtigt. Die Stärke der Mechanismen heißt jetzt Stärke des Evaluationsgegenstands (EVG) der Sicherheitsfunktionen und kann – ähnlich wie in den ITSEC – mit niedrig, mittel oder hoch bewertet werden.

3.2.4 Kurzüberblick Common Criteria

Es ist absehbar, dass sich die Common Criteria als Standardkriterien für die Sicherheit in der Informationstechnik weltweit durchsetzen werden. Als technische Grundlage hierzu dient eine allgemein akzeptierte Evaluationsmethode (*Common Evaluation Methodology*, CEM), auf die die gemeinsamen IT-Sicherheitskriterien

Tabelle 3.1: Gegenüberstellung der Vertrauenswürdigkeiten zwischen ITSEC und Common Criteria (Quelle: BSI)

ITSEC	Common Criteria
Anforderungen	Funktionale Spezifikation Sicherheitsmodell
Architekturentwurf	Entwurf auf hoher Ebene
Feinentwurf	Entwurf auf niedriger Ebene
Implementierung	Darstellung der Implementierung Funktionaler Test
Konfigurationskontrolle	CM Automatisierung CM Leistungsvermögen CM Anwendungsbereich
Programmiersprachen und Computer	Werkzeuge und Techniken
Sicherheit beim Entwickler	Sicherheit bei der Entwicklung
Benutzerdokumentation	Benutzerhandbuch
Systemverwalter Dokumentation	Systemverwalterhandbuch
Anlauf und Betrieb	Installation, Generierung und Anlauf
Auslieferung und Konfiguration	Auslieferung
Eignung der Funktionalität	Evaluation der Sicherheitsvorgaben
Stärke der Mechanismen	Stärke der EVG Sicherheitsfunktionen
Bewertung der Konstruktionsschwachstellen Bewertung der operationellen Schwachstellen	Schwachstellenanalyse
Benutzerfreundlichkeit	Missbrauch

(CC) Bezug nehmen. Dabei beschreiben die Kriterien, was evaluiert wird, und die Methodologie, wie evaluiert werden soll. Bei näherer Beschäftigung mit den Common Criteria wird deutlich, dass sich diese in drei zusammengehörige Teile gliedern lassen:

Teil 1: Einführung und allgemeines Modell

In diesem Abschnitt werden Grundlagen der IT-Sicherheitsevaluation und der allgemeine Geltungsbereich der CC erläutert. In den Anhängen der CC finden sich hierzu Schutzprofile[8] (*protection profiles*) und Sicherheitsvorgaben bzw. -ziele (*security targets*) für den zu prüfenden Evaluationsgegenstand (EVG)[9].

[8] Die Anforderungen an die Funktionalität und die Vertrauenswürdigkeit können in Schutzprofilen für bestimmte Produkttypen zusammengefasst werden. Weiterhin enthalten die Schutzprofile einen ausführlichen Beschreibungsteil, in dem unter anderem das Sicherheitskonzept beschrieben und die Bedrohungen den Anforderungen gegenübergestellt werden.

[9] Unter EVG wird ein IT-Produkt (z.B. Firewall) oder ein IT-System sowie die dazu gehörigen Systemverwalter- und Benutzerhandbücher verstanden.

Teil 2: Funktionale Sicherheitsanforderungen

Dieser Teil enthält einen umfangreichen Katalog von Funktionalitätsanforderungen. Er stellt ein Muster für die Beschreibung der Funktionalität eines EVG dar. Von diesem kann allerdings in begründeten Fällen abgewichen werden. Zusätzlich werden Zusammenhänge zwischen Bedrohungen, Sicherheitszielen und funktionalen Anforderungen aufgezeigt.

Teil 3: Anforderungen an die Vertrauenswürdigkeit

Im dritten Teil sind Anforderungen an die Vertrauenswürdigkeit zu finden. Die Common Criteria besitzen sieben hierarchische Vertrauenswürdigkeitsstufen. Ein Evaluationsergebnis basiert somit immer auf einer der Vertrauenswürdigkeitsstufen (EAL), eventuell ergänzt durch weitere Anforderungen.

3.2.5 Sicherheitsarchitektur offener Systeme

In Abschn. 2.2.1 wurde das OSI-Referenzmodell diskutiert, das für die Kommunikation offener Systeme entworfen wurde und in erster Linie Anwendungen einen Datenaustausch ermöglicht, die in räumlich verteilten, heterogenen Rechnersystemen platziert sind. Ferner wurden Funktionen zum Schutz der zwischen den Anwendungsprozessen transportierten Informationen definiert. Dieser Abschnitt gibt einen Überblick über die Funktionen und die dazugehörigen Mechanismen.

Die Grundidee der Sicherungsmaßnahmen ist, dass der Aufwand für einen Missbrauch, z.B. die Beschaffung bzw. Modifizierung im Sinne der allgemeinen Schutzziele, wie in Abschn. 3.1 erläutert, deutlich höher liegen als der eigentliche Nutzwert der Daten. Für kryptographische Absicherungsmaßnahmen heißt dies, dass die Zeitdauer für die Dechiffrierung der Daten derartig lang wird, dass die Informationen zwischenzeitlich ihren Wert verloren haben.

Im zweiten Teil des Protokoll-Referenzmodells wird eine Sicherheitsarchitektur definiert, die sowohl Sicherheitsdienste zum Schutz des Datenaustausches offener Systeme beschreibt als auch angibt, in welchen Funktionsschichten diese Dienste zu integrieren sind (siehe [ISO 7498-2:1989]). Es werden Realisierungsmechanismen angeführt, auf die sich die Sicherheitsdienste beziehen. Dabei entsprechen die Maßnahmen den allgemeinen Architekturelementen der Kommunikationsprotokolle.

Anzumerken ist an dieser Stelle, dass sich die OSI-Sicherheitsarchitektur ausschließlich auf den Informationsaustausch zwischen Kommunikationspartnern bezieht. Darüber hinaus gehende Aspekte, z.B. die Absicherung der Endgeräte – von der Aufstellung über den Zugriff bis hin zu organisatorischen Regelungen – können dem Grundschutzhandbuch des BSI entnommen werden. Systeme, die einen hohen bis sehr hohen Schutzbedarf erfordern, können mit speziellen Risikoanalysen und den entsprechenden Gegenmaßnahmen abgesichert werden. Somit ist die OSI-Sicherheitsarchitektur bestenfalls *ein* Baustein im umfangreichen Sicherheitskonzept eines Unternehmens. Ausführungen zu einem Sicherheitskonzept sind in Abschn. 3.2.6 zu finden.

Sicherheitsdienste und Mechanismen

Konkret beschreibt die OSI-Sicherheitsarchitektur Sicherheitsdienste und die zugeordneten implementierenden Mechanismen, die vom Referenzmodell optional bereitgestellt werden. Die Sicherheitsdienste wiederum lassen sich in fünf Dienstgruppen zusammenfassen (Abb. 2.3):

Authentifikationsdienste: Sie erfordern lokal gespeicherte Informationen und solche, die zur Durchführung einer Authentifikation notwendig sind (vgl. Kapitel 5). Sie werden auch als *Credentials*, z.B. im Kerberos-Verfahren, eingesetzt. Es werden die zwei Dienste *Peer Entity Authentication* und *Data Origin Authentication* unterschieden. Bezogen auf das OSI-Modell bedeutet dies:

- *Peer Entity Authentication*: Falls ein Dienst in Schicht N benutzt wird, der mit der gleichberechtigten Instanz N des Kommunikationspartners Daten austauscht, muss gewährleistet werden, dass es sich tatsächlich um den gewünschten Kommunikationspartner handelt.
- *Data Origin Authentication*: Dieser stellt sicher, dass die Instanz der Schicht N die empfangenen Daten von der Peer-Entity-Instanz erhalten hat. Allerdings wird nicht sichergestellt, dass Daten auf dem Transportweg nicht kopiert oder verändert wurden.

Zugriffskontrolldienste: Sie schützen vor unberechtigtem Zugriff auf Ressourcen. Es kann sich dabei um OSI- und um Nicht-OSI-Ressourcen handeln, auf die mit OSI-Protokollen zugegriffen wird.

Dienste zur Datenvertraulichkeit: In dieser Rubrik lassen sich vier unterschiedliche Dienste einordnen, bei denen jedoch alle einen Schutz vor unberechtigtem Offenlegen von Daten gewährleisten:

- *Connection Confidentiality* sichert die Vertraulichkeit aller Nutzdaten einer Schicht-N-Verbindung zu.
- *Connectionless Confidentiality* gewährleistet auch die Vertraulichkeit einzelner verbindungsloser Schicht-N-Servicedateneinheiten.
- *Selective Field Confidentiality* kann als eine Variante dieser beiden Dienste angesehen werden, indem die Vertraulichkeit selektiver Felder in den Protokolldateneinheiten einer Verbindung oder einzelner verbindungsloser Servicedateneinheiten garantiert wird.
- *Traffic Flow Confidentiality* stellt die Vertraulichkeit derjenigen Informationen sicher, die durch Ausspähen eines Verkehrsflusses gewonnen werden können.

Dienste zur Datenintegrität: Auch hier gibt es mehrere – insgesamt fünf – unterschiedliche Dienste, die sich, anders als die vorgenannten, gegen aktive Bedrohungen richten:

- *Connection Integrity with Recovery* stellt die Integrität aller Nutzdaten einer Schicht-N-Verbindung sicher und unterbindet jegliches Einfügen, Löschen, das Modifizieren oder Wiedereinspielen (*Replay*) von Protokolldateneinheiten. Außerdem wird einer Verbindungswiederherstellung entgegengewirkt.
- *Connection Integrity without Recovery* entspricht dem zuvor genannten Dienst, allerdings ohne eine Absicherung beim Versuch, eine Verbindung wiederherzustellen.
- *Selective Field Connection Integrity* liefert die Integrität ausgewählter Felder von Protokolldaten einer Verbindung.
- *Connectionless Integrity* stellt die Integrität einzelner verbindungsloser Servicedateneinheiten sicher.
- *Selective Field Connectionless Integrity* stellt die Integrität einzelner ausgewählter Felder sicher.

Dienste zur Verbindlichkeit: Zur Sicherstellung der Nicht-Abstreitbarkeit von Kommunikationsaktivitäten existieren zwei Dienste:

- *Non-Repudiation with Proof of Origin* liefert dem Empfänger die eindeutige Herkunft einer Nachricht.
- *Non-Repudiation with Proof of Delivery* sorgt dafür, dass der Sender einer Nachricht jederzeit nachweisen kann, dem jeweiligen Empfänger eine Nachricht übermittelt zu haben.

Eine Umsetzung der aufgelisteten OSI-Sicherheitsdienste beruht auf Sicherheitsmechanismen, von denen den Verschlüsselungstechniken, die in Kapitel 4 detailliert beschrieben werden, eine entscheidende Bedeutung zukommt. Neben dem Einsatz von unterschiedlichen Verschlüsselungsverfahren (symmetrisch und asymmetrisch) wird nicht nur für die Vertraulichkeit von Daten gesorgt, sondern ebenso dafür, dass elektronische Daten digital signiert werden und deren Integrität geschützt wird.

Zugriffskontroll-Verfahren werden üblicherweise an den Endpunkten und/oder an jedem beteiligten Netzknoten einer Kommunikationsbeziehung eingesetzt. Mittels dieser Mechanismen wird entschieden, ob ein Sender zur Kommunikation mit einem Empfänger berechtigt ist oder nicht. Dabei folgen alle Verfahren einer der beiden folgenden Methoden:

- Zugriffsrechte, hinterlegt in Datenbanken in Form einer Zugriffskontrollmatrix oder -liste.
- Authentifizierungsinformationen wie Passwörter, die den Zugriff zur gewünschten Anwendung im System ermöglichen oder auch kryptographische Verfahren, die in Kombination mit Handshake-Protokollen zum Schutz gegen Replay-Attacken verwendet werden (vgl. Kapitel 5).

Abb. 3.12 listet die Beziehungen zwischen den OSI-Sicherheitsdiensten und -mechanismen auf. Dabei gilt, dass zur Bereitstellung einiger Dienste eine Kombination mehrerer Mechanismen notwendig ist. Die einzelnen Mechanismen sind Gegenstand von Kapitel 4 und 5. Hier sei kurz das *Traffic Padding* erwähnt, das im Prinzip auf die Einbindung von Füllmustern zum Schutz vor unerlaubter Verkehrsanalyse beruht.

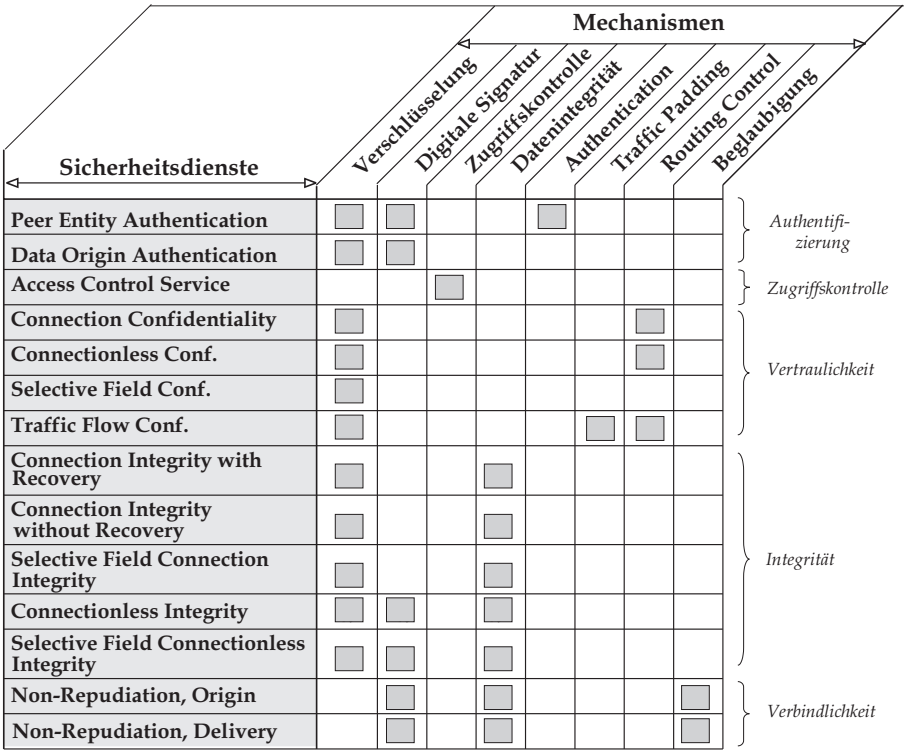


Abb. 3.12: Zusammenhang zwischen Sicherheitsdiensten und -mechanismen gemäß ISO 7498-2

Sicherheitsdienste und Schichtenmodell

Die Zuordnung der Sicherheitsdienste in den OSI-Schichten ist optional und direkt abhängig vom konkreten Anwendungsfall. In Tab. 3.2 wird gezeigt, in welchen Schichten die in Abb. 3.12 aufgeführten OSI-Sicherheitsdienste angeboten werden.

In jeder Schicht, in der ein Sicherheitsdienst zu finden ist, werden auch entsprechende Sicherheitsmechanismen bereitgestellt. Deutlich ist zu erkennen, dass die Majorität der OSI-Sicherheitsdienste auf Schicht 7 angesiedelt ist, gefolgt von denen auf Schicht 3 und Schicht 4. Die beiden einzigen Sicherheitsdienste auf

Tabelle 3.2: Sicherheitsdienste im OSI-Referenzmodell orientiert an Transport- und Anwendungsschichten gemäß ISO-7498-2

	OSI-Schichten						
	Transport				**Anwendungen**		
Dienste	1	2	3	4	5	6	7
Peer Entity Authentication			X	X			X
Data Origin Authentication			X	X			X
Access Control Service			X	X			X
Connection Confidentiality	X	X	X	X			X
Connectionless Confidentiality		X	X	X			X
Selective Field Confidentiality							X
Traffic Flow Confidentiality	X		X				X
Connection Integrity with Recovery				X			X
Connection Integrity without Recovery			X	X			X
Selective Field Connection Integrity							X
Connectionless Integrity			X	X			X
Selective Field Connectionless Integrity							X
Non-Reputation, Origin							X
Non-Reputation, Delivery							X

Schicht 1 sind der *Connection Confidentiality*- und der *Traffic Flow Confidentiality*-Dienst (Tab. 3.2). Diese Dienste wirken einer passiven Bedrohung entgegen und sind auf Punkt-zu-Punkt- und Punkt-zu-Mehrpunkt-Verbindungen ausgelegt. Dabei wird als Hauptmechanismus in dieser Schicht auf die vollständige Verschlüsselung gesetzt. Auf Schicht 2 werden der Connection- und der Connectionless-Confidentiality-Dienst zur Verfügung gestellt, die sich ebenfalls auf Verschlüsselungsmechanismen stützen. Auf der Netzwerk-Schicht 3 werden Sicherheitsdienste, wie z.B. *Peer Entity Authentication*, *Data Origin Authentication*, *Access Control*, *Connection Confidentiality*, *Connectionless Confidentiality*, *Traffic Flow Confidentiality*, *Connection Integrity without Recovery* und *Connectionless-Integrity*, alleine oder in Kombination mit anderen, angeboten. Diese sind im Wesentlichen, wie Abb. 3.12 deutlich macht, auf Verschlüsselungsverfahren einschließlich digitaler Signatur und gesichertem Passwortaustausch zurückzuführen. Auf der Transport-Schicht 4 werden die gleichen Sicherheitsdienste wie auf Schicht 3 angeboten, allerdings mit Ausnahme des Traffic-Flow-Confidentiality-Dienstes. Hinzu kommt der Dienst *Connection Integrity with Recovery*. Auf Schicht 5 und Schicht 6 werden keine Sicherheitsdienste bereitgestellt. In der Anwendungsschicht (Schicht 7) werden alle der zuvor aufgeführten Sicherheitsdienste einzeln oder in Kombination angeboten. Abb. 3.12 und der Tab. 3.2 zeigen das ganze Spektrum an Möglichkeiten zur Absicherung einer Kommunikationsverbindung. Hiervon wird in der VPN-Technologie auf unterschiedliche Weise Gebrauch gemacht. Alle Absicherungsverfahren lassen sich auf diese Grundstrukturen zurückführen. Allerdings reicht eine Absicherung allein auf Kommunikationsebenen nicht aus, um ein VPN wirkungsvoll und betriebssicher zu unterhal-

ten. Nachfolgend wird daher das Thema der Sicherheitsphilosophie, die in jedem Unternehmen vorhanden sein sollte, diskutiert.

3.2.6 Sicherheitsparadigma und Sicherheitspyramide

Neben den Sicherheitsbetrachtungen und -analysen in den zuvor diskutierten Abschnitten für offene Systeme muss es ein einheitliches Gesamtregelwerk in einem Unternehmen geben, nach welchem Grenzen und Pflichten der IT-Sicherheit festgeschrieben werden. Das Gesamtregelwerk folgt dem derzeit allgemein akzeptierten Sicherheitsparadigma, das sich in Form einer Pyramide darstellen lässt. Die Sicherheitspyramide ist vorderseitig in vier Ebenen unterteilt (Abb. 3.13). Diese sind hierarchisch untereinander verbunden. Auf der Querseite ist der Bezug zur Unternehmensplanung dargestellt. So ist die Security Policy-Ebene als strategische, die Security Konzepte-Ebene als taktische und die Security Architektur-Ebene sowie die Security Tools und Systeme-Ebene als operationelle Maßnahmen zu verstehen.

Die IT-Sicherheitspolicy beschreibt das Rahmenwerk, in dem sich die IT-Sicherheit im Unternehmen bzw. in der Behörde organisatorisch und technisch bewegen darf. Dieses Rahmenwerk stellt eine grundsätzliche Richtlinie dar, wie IT-Sicherheit im Unternehmen betrieben wird und welche Grenzen willkürlich gesetzt werden. Die in der IT-Sicherheitspolitik definierten Rahmenbedingungen bilden das Gerüst für alle weiteren darunter liegenden Ebenen. Sie werden von höchster Stelle, also von der Geschäftsführung, festgelegt. Hier werden die Sicherheitsziele eines Unternehmens definiert und der IT-Sicherheitsprozess[10] beschrieben. Weiterhin beschreibt die IT-Sicherheitspolitik die Vorgehensweise zur Erstellung und Weiterentwicklung eines IT-Sicherheitskonzeptes.

Das Rahmenwerk bzw. Richtlinie, die durch die IT-Sicherheitspolitik gebildet wird, weist im Allgemeinen vier Ebenen auf, von denen die jeweils hierarchisch übergeordnete Ebene die Rahmenbedingungen für die darunter liegenden Ebenen festlegt (Abb. 3.13). Dies wird durch die sich umhüllenden Dreiecke angedeutet. Die IT-Sicherheitspolitik bildet damit das auf höchster Ebene angesiedelte unternehmensweite Rahmenwerk zur IT-Sicherheit.

Das IT-Sicherheitskonzept, auf der Ebene unterhalb der IT-Sicherheitspolitik platziert, hat zur Aufgabe, konkrete Richtlinien für spezifische Themen mit unterschiedlichen Geltungsbereichen, und zwar in Abhängigkeit von Bedrohungspotenzialen und Schwachstellen, zu definieren. Ziel ist ein angemessenes durch die IT-Sicherheitspolitik abgestecktes Sicherheitsniveau. Hier kommt das Grundschutzhandbuch (GsHb) des BSI [BSI 2004a] zum Einsatz, wenn die Absicherung von Systemen mit mittlerem und niedrigem Schutzbedarf erreicht werden soll. Eine Schutzbedarfsanalyse liefert hierzu eindeutige Aussagen. Für Absicherungen mit einem System von hohen bis sehr hohen Schutzbedarf kommen nur noch individuelle Maßnahmen in Frage. Weiterhin unterliegt das IT-Sicherheitskonzept in

[10] Oftmals ist der Sicherheitsprozess auch gleichzeitig in das Qualitätsmanagement eingebunden, was durchaus sinnvoll und anstrebenswert ist.

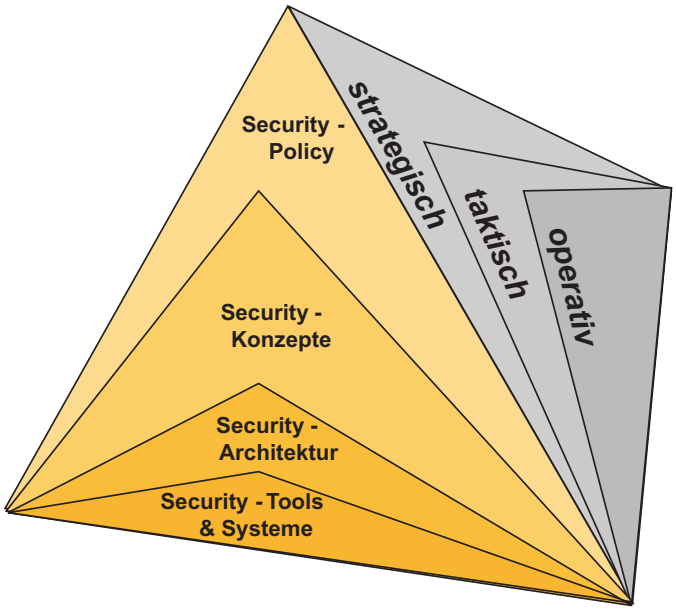


Abb. 3.13: Hierarchische Regelung zur IT-Sicherheit in Form einer Sicherheitspyramide

gut geführten Unternehmen einem ständigen Fortschreibungsprozess, um mit der kurzlebigen Informationstechnologie Schritt zu halten.

Auf der nächsten, der dritten Ebene ist die IT-Sicherheitsarchitektur angesiedelt, die den Vorgaben der Konzeptebene folgt. Hier wird die Abbildung der im IT-Sicherheitskonzept vorgegebenen Rahmenbedingungen konkret auf die tatsächliche IT-Infrastruktur durchgeführt. Bestandteile einer solchen IT-Sicherheitsarchitektur sind neben der Beschreibung der IT-Plattform auch konkrete Schutzmaßnahmen wie Konzepte zum Virenschutz zur Datensicherung oder die Vergabe von Benutzerrechten. Die operative Umsetzung (Implementierung) wiederum ist der untersten Ebene der IT-Sicherheit vorbehalten. Diese setzt die Maßnahmen, die aus dem IT-Sicherheitskonzept und der IT-Sicherheitsarchitektur resultieren, physikalisch um.

Es zeigt sich, dass jede Ebene den Rahmen für die tiefer liegenden Ebenen bestimmt. Dabei nimmt die Detailtiefe und die Technikorientierung von den oberen zu den unteren Ebenen zu, während die organisatorischen Aspekte abnehmen. Eine VPN-Planung sollte die entsprechenden Ebenen der Sicherheitspyramide berücksichtigen (Abb. 3.13). Zunächst sollte überprüft werden, ob die vorhandenen Sicherheitskonzepte[11] für einen Fernzugriff mittels VPN ausreichen. Existieren bereits Konzepte für Fernzugriffe, sollte der Anpassungsaufwand nicht allzu

[11] Häufig existieren Sicherheitskonzepte, denen ein Zwiebelschalenmodell zugrunde gelegt wurde.

groß werden. Gleiches gilt für die Architekturebene[12] der Sicherheitspyramide. Wird jedoch zur Absicherung der Endgeräte eine Chipkartenlösung, etwa mit einer PKI (*Public-Key-Infrastruktur*) eingesetzt, nimmt der Aufwand deutlich zu.

Fraglich ist allerdings, wie sich die Anwendung einer unternehmensweite Sicherheitspyramide, -policy, -architektur und -konzeption auf allen Ebenen, überprüfen lässt. Auch die Art und Weise der Kopplung der vier Ebenen untereinander hat Einfluss auf die tatsächliche IuK-Absicherung eines Unternehmens. Die eingangs vorgestellten Methoden und Kriterienwerke überprüfen ausschließlich Teilaspekte. Ein Verfahren zur Gesamtbeurteilung der tatsächlichen IuK-Absicherung eines Unternehmens ist Gegenstand des nächsten Abschnitts.

3.2.7 Evaluierung der Gesamtunternehmenssicherheit

Werden Unternehmen nach dem Status ihrer IT-Sicherheit befragt, so wird in erster Linie auf die Virenabwehr, Firewall-Systeme, *Intrusion Detection Systeme* (IDS) etc., also auf technische Komponenten, verwiesen. Besser ausgerüstete Firmen haben darüber hinaus umfangreiche Sicherheitsrichtlinien, z.T. gestützt auf das GsHB des BSI und besitzen eine eigene IT-Revision. Dennoch sind die meisten dieser Firmen weit entfernt vom umfassenden *Enterprise Security Management* (ESM). Es berücksichtigt das Gesetz zur Kontrolle und Transparenz für Aktiengesellschaften (KonTraG), Artikel V oder HGB § 289, § 315, führt eigene Risikoanalysen bezüglich der IT-Sicherheitsinfrastruktur durch und hat ein IT-Sicherheitskrisen-Management, das im Bedarfsfall in wenigen Stunden einsatzbereit ist [Böhmer 2000].

Derzeit existieren eine Reihe von Regelungen und Werken, die in diesem Kapitel angesprochen wurden und die sich je nach Ausprägung an unterschiedliche Zielgruppen in einem Unternehmen richten. So konzentriert sich das Grundschutzhandbuch in erster Linie auf technische Aspekte, und nur wenige Anteile sind dem IT-Sicherheitsmanagement gewidmet. Im Gegensatz dazu richtet sich das BS 7799-2:2000 an das Sicherheitsmanagement und zielt weniger auf die Absicherung von technischen Komponenten ab. Es verfolgt nicht nicht nur die technische IT-Sicherheit, sondern fordert ein geschäftsmodellbezogenes *Informationssicherheitsmanagementsystem* (ISMS). Das Gesetz zur Kontrolle und Transparenz für Aktiengesellschaften (KonTraG) betrachtet dagegen bestandsgefährdende Risiken in erster Linie aus wirtschaftlicher Sicht. Allen oben genannten Zielgruppen werden in jüngster Zeit vermehrt Prüfungen in Form von Auditierungen – teils Interview-basiert, teils Tools-gestützt – angeboten. All diese haben eines gemeinsam: sie betrachten jeweils nur einen Teilausschnitt. Darüber hinaus macht keine Prüfung vergleichende Aussagen zur Positionierung des untersuchten Unternehmens zu anderen Firmen (*Security Benchmark*). Somit besteht ein erheblicher Bedarf nach einem griffigen, praxisnahen Verfahren zur Gesamtbeurteilung der Unternehmenssicherheit, wenn die IT-Sicherheit als Wettbewerbsfaktor eingesetzt

[12] In dieser könnte eine VPN-Lösung technisch als Sicherheitsinsel mit wohldefinierten Schnittstellen implementiert werden.

wird. Diesen Anspruch erfüllt das neu entwickelte *IT-Security-Scoring*-Verfahren, in das viele Erfahrungen und Ideen aus langjährigen Beratungsprojekten zur IT-Sicherheit eingeflossen sind [Böhmer 2001-b]. Das *IT-Security-Scorecard*-Verfahren (IT-SSV) beinhaltet eine diagnostische Methode, die basierend auf metrischen Größen und typischen Kennzahlen die Beurteilung des IT-Sicherheitsniveaus eines gesamten Unternehmens zulässt. Dabei werden alle in einem Unternehmen an der IT-Sicherheit beteiligten Größen in ihrem komplexen Zusammenspiel von technischen, organisatorischen und rechtlichen Komponenten in der Methode berücksichtigt. Sie werden in ihrer Gesamtheit in einem Unternehmen sowie im Vergleich zu anderen Unternehmen bewertet. Dieses Verfahren räumt mit den oben aufgeführten Unzulänglichkeiten auf und bietet Unternehmen die Chance, eine umfassende Aussage zu ihrem Gesamtsicherheitsniveau und damit auch zur Positionierung am Markt zu erhalten.

Das generisch gehaltene IT-Security-Scorecard-Verfahren besteht im Wesentlichen aus vier Hauptmodulen und resultiert aus den Überlegungen zur Lieferantenbewertung.[13] Dabei ermöglichen die vier Hauptmodule (Sicherheitsmanagement, Betriebswirtschaft, IT-Security-Strategie, IT-Security-Betrieb) in ihrer Ergebniswichtung eine Steuerung der betrachteten Branche und der Firmen selber. Bei großen Firmen ist beispielsweise eher eine gleiche Ergebniswichtung (25%) der vier Hauptmodule vorzunehmen. Hinter dem Verfahren steht die Modellvorstellung eines Verzweigungsbaumes, der ausgehend vom Stamm vier Hauptverzweigungen hat; und jeder der vier Hauptverzweigungen besitzt wiederum einer Reihe von Verästelungen. Diese können weitere Verästelungen beinhalten.

Die vier Hauptmodule umfassen die Bereiche des Sicherheitsmanagements, der Betriebswirtschaft, die IT-Sicherheitsstrategie und schließlich betriebliche Aspekte der IT-Sicherheit. Jedem Modul sind drei Segmente (Bausteine) zugeordnet, die auf die Module angewandt werden. Dabei enthalten alle Segmente die gleichen Oberthemen: Organisation, Recht und Technik/Methoden. Die Verfeinerung der Fragestellungen in den jeweiligen Segmenten ist dagegen modulabhängig.

Abb. 3.14 zeigt die vier Hauptmodule und die untergeordneten Segmente. Aus einer Evaluation der Gesamtunternehmenssicherheit resultiert eine Punkteeinstufung in Scoringklassen, die rechts in Abb. 3.14 zu sehen sind. Das Verfahren kann sowohl zur Erstbewertung als auch zur laufenden Bewertung eingesetzt werden. Begonnen wird mit einem Workshop, um das Unternehmen entsprechend zu sensibilisieren. Die Ergebnisse von zeitlich in größeren Abständen (Jahr) durchgeführten Evaluationen können ins Verhältnis gesetzt werden. Somit lässt sich eine kontinuierliche Optimierung einführen [Böhmer 2001-b].

Entscheidend für die Anwendung der Methode ist die geeignete Wahl der Messpunkte, die sich auf die Haupt- und Nebenkriterien in den jeweils vier Modulen verteilen. Dabei wird eine bestimmte Gewichtung sowohl der Messpunkte als auch der Haupt- und Nebenkriterien vorgegeben. An den Messpunkten werden empirische und metrische Größen gemessen.

[13] Methoden zur Lieferantenbewertung nehmen in der Betriebswirtschaft einen breiten Raum ein.

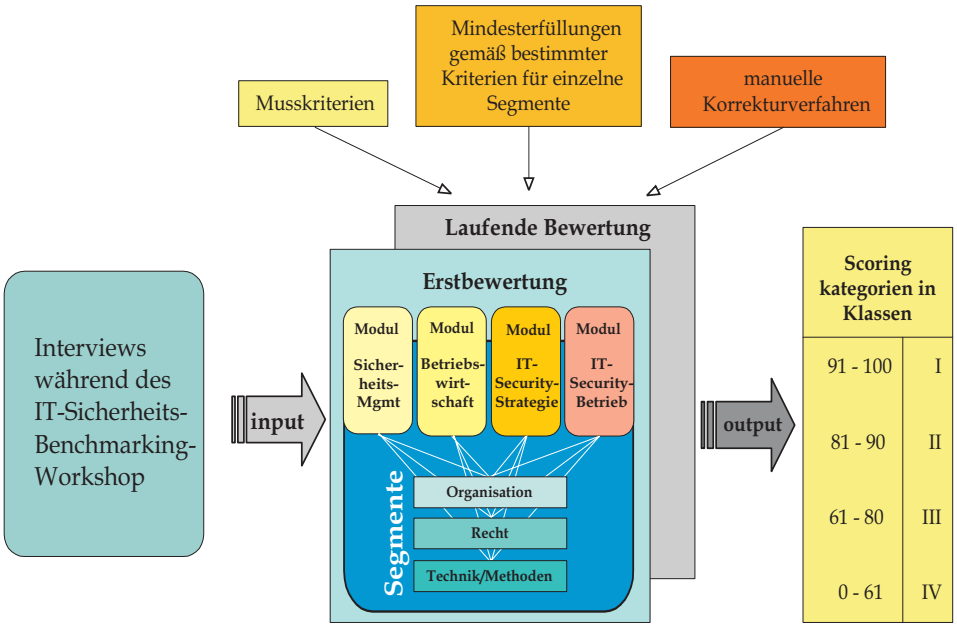


Abb. 3.14: Das IT-Security-Scorecard-Verfahren (IT-SSV)

Rechts in der Abb. 3.14 sind die Scoringkategorien in Stufen als Ergebnis des Ratings dargestellt. Die fünf Stufen (V-I) drücken mögliche Reifegradzustände der IT-Sicherheitsorganisation aus. Mittels dieser Reifegradermittlung kann eine IT-Sicherheitsorganisation eine Verbesserungsstrategie entwickeln. Wird die Reifegradermittlung in Verbindung mit der Planung und Umsetzung von Verbesserungen z.B. jährlich wiederholt, erfüllt die IT-Sicherheitsorganisation die Voraussetzung, ihren Reifegrad[14] kontinuierlich weiterzuentwickeln. Dies kommt einer Qualitätssteigerung gleich und führt in dem anzustreben Zustand der Stufe (I) zu einer erwachsenen IT-Sicherheitsorganisation. Aufgrund der Analyse der Ergebnisse werden Verbesserungsmaßnahmen (Strategie, Politik) ergriffen. Diese Maßnahmen bilden den Ausgangspunkt für die Planung (u.a. die Einrichtung optimierter Sicherheitsprozesse), deren Umsetzung den gewünschten Reifegradzustand liefern soll.

3.2.8 IT-Security Capability Maturity Model (IT-SecCMM)

Der Begriff „erwachsen“ ist der ISO 9000:2000 Norm entlehnt. Diese rückt die Fähigkeit der Organisation, aus Erfahrungen zu lernen und die Qualität ständig

[14] Die Steigerung des Prozessreifegrades ist vor allem durch das *Capability Maturity Model* (CMM) der Carnegie Mellon University für die Entwicklung von Software bekannt geworden.

zu steigern, stärker in den Mittelpunkt. Das EFQM -Modell[15], das neun Schwerpunkte setzt, nimmt u. a. den Qualitätskreis[16] von [Deming 1998] als Vorbild. Übertragen auf das IT-SecCMM bedeutet dies, dass je höher der Reifegradzustand eines Unternehmen diagnostiziert wird, je „erwachsener" ist dieses Unternehmen im Sinne der IT-Sicherheit [Böhmer 2004-a]. Die fünf Stufen des Modells sind in

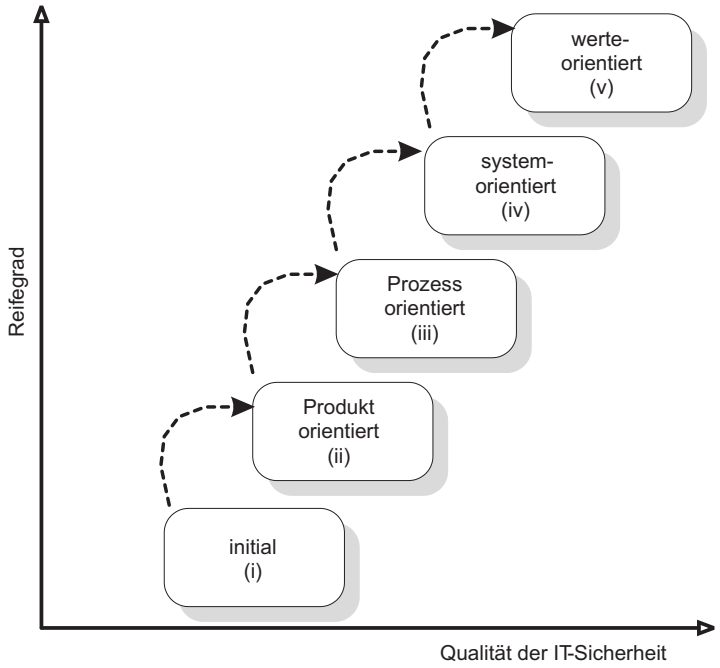


Abb. 3.15: Mögliche Reifgradzustände einer IT-Sicherheitsorganisation

der Abb. 3.15 dargestellt und zeigen den Weg und das Ziel für ein Unternehmen bei der Verbesserung seines Reifegradzustandes. Dabei bilden die fünf Reifegradstufen jeweils Zustände, die keiner Dynamik mehr unterliegen.

Das IT-SecCMM Modell orientiert sich an den Ideen, die die Carnegie Mellon University mit dem Capability Maturity Model (CMM) für die Softwareentwicklung vorgeschlagen hat. Ebenso wie das Ursprungsmodell basiert das IT-SecCMM auf fünf Reifgradstufen. Dabei liefert das Modell keine Hilfestellung wie der nächste Reifegrad zu erreichen ist. Es wird lediglich der Reifzustand selber definiert. Weiterhin ist das IT-SecCMM als Minimal-Modell zu verstehen. Denn es werden Eigenschaften definiert, die einen Reifezustand bzw. eine Reifeklasse beschreiben.

---

[15] EFQM steht für *European Foundation for Quality Management*.

[16] Der Qualitätskreis von Deming beschreibt das bekannte PDCA-Modell, das auch im BS 7799-2:2000 Eingang gefunden hat und den Kreislauf des ISMS darstellt.

Im Gegensatz zu dem CMM, das die Softwareentwicklung im Fokus hat und Software bekanntlich in einem Produkt mündet, hat das IT-SecCMM den Service im Fokus. Der Gebrauch eines Produktes ist typischerweise getrennt von der Entstehung des Produkts zu sehen. Ein Service dagegen wird so genutzt, wie dieser produziert wird.

Stufe I zeigt den untersten Reifegrad. Unternehmen auf diesem Niveau haben keine IT-Sicherheit bzw. beginnen erst, sich damit auseinander zu setzen.

Stufe II bringt einen geringen Reifegrad zum Ausdruck. Das Unternehmen hat hier seine IT-Sicherheit lediglich auf Sicherheitskomponenten, wie z.B. Firewall-Systeme und Virenscanner, beschränkt.

Stufe III kennzeichnet besser ausgelegte Unternehmen, in denen bereits in IT-Sicherheitsprozesse gedacht und gehandelt wird und IT-Sicherheitsprodukte als Mittel zum Zweck eingesetzt werden.

Stufe IV stellt systemorientierte Unternehmen dar, die z.B. abteilungsübergreifend ihre IT-Sicherheit ausgelegt und aufeinander abgestimmt haben. Weiterhin sollte bereits ein gewisses Maß an taktischen Vorgaben und Verfahren der IT-Sicherheit im Unternehmen, neben operativen IT-Sicherheitstätigkeiten, beherrscht und angewendet werden.

Stufe V - als höchster Reifegrad - bezeichnet Unternehmen, die ihre IT-Sicherheit an ihrer Wertschöpfungskette ausrichteten und nicht nur taktische, sondern auch strategische IT-Sicherheitsentwicklung, neben den operativen IT-Sicherheitstätigkeiten, beherrschen und anwenden [Böhmer 2004-b].

3.3 Übungen

1. Welche beiden Betrachtungsgrößen sind bei der CRAMM-Methodik zu berücksichtigen, wenn eine Risikoeinschätzung über eine hochschutzbedürftige VPN-Kommunikation vorgenommen werden soll?
2. Welche Schutzziele verfolgt die IuK-Sicherheit?
3. Welche Unterschiede sind zwischen der mehrseitigen IT-Sicherheit gegenüber der IuK-Sicherheit anzuführen?
4. Welche Sichtweise kommt bei der mehrseitigen IT-Sicherheit zur IuK-Sicherheit hinzu?
5. Welcher Bezug könnte prinzipiell zwischen den Common Criteria und einem VPN-Produkt hergestellt werden?

6. Wie könnte eine typische Richtlinie (Security Policy) aussehen, wenn das VPN zur Absicherung von personenbezogenen Daten eingesetzt werden soll?
7. Wie könnte das dazugehörige Konzept aussehen?
8. Wie könnte die dazugehörige Architektur aussehen?
9. Wie könnte die dazugehörige operative Umsetzung aussehen, wenn es sich um ein VPN im Weitverkehrsnetz handelt?
10. Entwerfen Sie nach dem generischen Security Scorecard-Verfahren ein System mit vier Ebenen.

4 Verschlüsselung

Eine der Aufgaben eines Secure VPN – z.B. in Bezug auf die VPN-Overlay-Techniken – besteht darin, die zu transportierenden Informationen für unbefugte Dritte unleserlich zu machen. Hierdurch wird die Privatsphäre bei der Datenübertragung sichergestellt. Datenpakete bzw. IP-Pakete werden auf ihrem Wege über unsichere und öffentliche Netze bzw. Netzknoten in einer besonderen Art und Weise „reversibel" modifiziert. Wie diese Modifizierung aussehen kann und wie die Möglichkeit der Reversibilität genutzt wird, wird in diesem Kapitel erörtet.

Die Grundidee der Verschlüsselung ist leicht vermittelbar: Ihr liegen die Prinzipien der geschickten Buchstabenvertauschung und der Buchstabenersetzung zugrunde, die in blockorientierten oder in kontinuierlichen Datenübertragungen eingesetzt werden. Zur Vertiefung sei z.B. [Stallings 1998] oder [Buchmann 2001] empfohlen.

Im Weiteren wird zunächst auf die klassische Kryptographie eingegangen. Der Rückblick auf die Anfänge der Kryptographie erleichtert das Verständnis der modernen Kryptographie. Nur zu deutlich wird dabei, dass die Geschichte der Kryptographie eine Geschichte der Kriege ist. Dem kryptographisch versierten Leser ist allerdings auch gleich der Einstieg in Abschn. 4.2 möglich.

Die Begriffe Kryptologie und Kryptographie sind ursprünglich aus den griechischen Wörtern *kryptos* (verborgen) und *logos* (Wort, Rede) bzw. *graphein* (schreiben) abgeleitet. Manche Autoren verwenden beide Termini synonym, andere grenzen die Begriffe untereinander ab. Im vorliegenden Werk unterliegen die Begriffe folgenden Unterscheidungen:

- **Kryptographie** (*cryptography*): Wissenschaft zur Entwicklung von Kryptosystemen und Maßnahmen zur Ver- und Entschlüsselung (Chiffrierung und Dechiffrierung) von Daten.
- **Kryptoanalyse** (*cryptoanalysis*): Kunst des Brechens von Kryptosystemen bzw. die Aktivitäten zur unbefugten Entschlüsselung chiffrierter Daten und Nachrichten zum Zwecke der Rückgewinnung der ursprünglichen Information. Sie dient zur Untersuchung der Stärke eines kryptographischen Verfahrens.
- **Kryptologie** (*cryptology*): Mathematische Disziplin, die sowohl die Kryptographie als auch die Kryptoanalyse umfasst.

Die grundlegende Aufgabe der Kryptographie besteht in der Geheimhaltung von übertragenen oder gespeicherten Informationen vor Unbefugten. Kryptosysteme erzielen diese Geheimhaltung, indem sie die Zeichen einer Nachricht derartig

transformieren (verschlüsseln), dass das entstandene Chiffrat für Unbefugte keine rekonstruierbare semantische, statistische oder strukturelle Korrelation zum Original mehr aufweist.

4.1 Verschlüsselungstechniken

Nachfolgend werden die beiden grundlegenden Verschlüsselungskategorien, die *Substitution* und die *Transposition*, näher erläutert. Dabei werden zunächst Vertreter der Klasse zum Ersetzen einzelner oder mehrerer Zeichen vorgestellt. Anschließend werden Klassenvertreter zum Vertauschen bzw. Umstellen einzelner Buchstaben diskutiert. Als grundlegende Weiterentwicklung können die *Roter*-Verfahren aufgefasst werden, in denen beide Verfahren (Substitution und Transposition) gekoppelt sind und abwechselnd angewandt werden.

4.1.1 Substitutionstechniken

Im Prinzip ist die vertrauliche Nachrichtenübermittelung ein Problem, das die Menschheit seit jeher beschäftigt. Es gibt etliche Aufzeichnungen, die belegen, dass schon Julius Cäsar (100 - 44 v. Chr.) vor diesem Problem gestanden hat. Wie konnte er den Kohorten in Gallien Marschbefehle schicken, ohne dass seine Botschaften den feindlichen Kimbern und Teutonen bekannt wurden? Ein in die Literatur als „Cäsars Verschlüsselung“ eingegangenes Verfahren soll im Folgenden näher erläutert und so ein Grundverständnis für die vertrauliche Nachrichtenübermittelung in VPN erreicht werden. Weiterhin wird die Bedeutung des Schlüssels diskutiert.

Julius Cäsar soll ein einfaches Prinzip der Substitutionstechnik benutzt haben. Unter dem Begriff Substitution werden im Allgemeinen Tausch- oder auch Ersatzverfahren verstanden. Dabei kann das ersetzte Zeichen aus einem Zeichenvorrat stammen, der sich aus Buchstaben, aber auch aus anderen Zeichen zusammensetzt. Er hat jeden Buchstaben im Alphabet durch einen anderen Buchstaben ersetzt, und zwar durch den, der im Alphabet drei Buchstaben hinter dem ursprünglichen liegt. Für den letzten Buchstaben wird wieder am Anfang des Alphabets begonnen. Die vollständige Transformation[1] für das Alphabet lautet dann:

Klartext:	a	b	c	d	e	f	…	t	u	v	w	x	y	z
Chiffrat:	D	E	F	G	H	I	…	W	X	Y	Z	A	B	C

Durch diese einfache Transformation wird ein Klartext durch den Chiffriervor-

[1] Sobald Buchstaben zur Veranschaulichung der Verschlüsselung eingesetzt werden, gilt, dass der Klartext immer mit kleinen Buchstaben und das Chiffrat mit großen Buchstaben geschrieben werden.

gang völlig verändert. Eine vertrauliche Nachrichtenübermittlung könnte damals folgendermaßen gelautet haben:

Klartext:	treffe	mich	nach	der	toga	party
Chiffrat:	WUHIIH	PLFK	QDFK	GHU	WRJD	SDUWB

Wird jetzt jedem Buchstaben im Alphabet eine natürliche ganze Zahl von $a = 1$ bis $z = 26$ zugewiesen, kann ein Algorithmus entwickelt werden. Für jeden Buchstaben im Klartext (p) kann durch Substitution das Chiffrat (C) erzeugt werden.

$$C = E(p) = (p + 3)\ mod(26) \tag{4.1}$$

Hierbei kommt die in der Krypthographie so wichtige *Modulo-Funktion*[2] zum Einsatz. Wird jetzt eine Substitution nicht auf drei Buchstaben beschränkt, wie in dem Beispiel mit der Toga-Party, kann generell der Cäsar-Algorithmus mit

$$C = E(p) = (p + k)\ mod(26) \tag{4.2}$$

ausgedrückt werden. Dabei wird zugrunde gelegt, dass (k)[3] in Gleichung (4.2) nur zwischen 1 bis 25 variieren darf. Die Umkehrung der Chiffrierung (Verschlüsselung), also das Dechiffrat (D), ist recht einfach, es muss die Gleichung (4.2) nur nach p aufgelöst werden.

$$p = D(C) = (C - k)\ mod(26) \tag{4.3}$$

Deutlich wird in diesem Zusammenhang, dass die Chiffrierung umkehrbar ist, also eine reversible Eigenschaft besitzt. Diese reversible Eigenschaft ist die Basis jeglicher Verschlüsselungsalgorithmen. Natürlich gibt es eine Reihe mathematischer Algorithmen, die umkehrbar sind, aber nicht alle sind gleich gut für die Praxis der vertraulichen Nachrichtenübermittlung geeignet.

Ein Verfahren, das unter dem Begriff *Brute-Force-Attack* in die Literatur eingegangen ist, sei hier – wiederum für das einfache Beispiel der Toga-Party – vorgestellt. Falls eine nicht-eingeweihte (autorisierte) Person das Chiffrat (WUHIIH PLFK QDFK GHU WRJD SDUWB) in die Hände bekommt und nicht weiß, wie die Substitution zu Stande gekommen ist, kann sie durch einfaches zyklisches Ausprobieren aller möglichen 25 Substitutionen bzw. Schlüssel versuchen, den Klartext zu reproduzieren. Nachfolgende Liste zeigt nur die ersten vier Substitutionen, die vollständig durchprobiert wurden.

WUHIIH PLFK QDFK GHU WRJD SDUWB

---

[2] Die Modulo-Arithmetik beschreibt eine Restwertberechnung. Im vorliegenden Fall wird immer eine Division mit der Zahl 26 durchgeführt. Für x=24 wird in der Gleichung (4.1) mit der Modulo-Arithmetik $27 \div 26 = 1$ gesetzt, d.h. der Restwert entspricht der Zahl 1. Es wurde jedoch per Definition die Zahl $a = 1$ gesetzt, so dass das Chiffrat C = E(1) = A lautet.

[3] Dabei wird k als Schlüssel bezeichnet.

Key						
1	vtghhg	okej	pcej	fgt	vqic	rcta
2	usfggf	ujdi	obdi	efs	uphb	qbsz
3	treffe	mich	nach	der	toga	party
4	sqdeed	lhbg	mzbg	cdq	snfz	ozqx
5	rpcddc	dgaf	eyaf	...,	...,	...,
6	qobccb	...,	...,			
⋮	...					

Nach der dritten Verschiebung hätte ein Kryptoanalyst das Chiffrat wieder in den Klartext überführt. An diesem Beispiel wird deutlich, dass der Kryptoanalyst ein leichtes Spiel hätte, da ihm drei wichtige Informationen zur Verfügung stünden:

1. Der Ver- und Entschlüsselungsalgorithmus ist bekannt.
2. Es gibt aufgrund des verwendeten Alphabets offensichtlich nur 25 Schlüssel, die eingesetzt werden können.
3. Die Sprache des Klartextes (Deutsch) ist bekannt und leicht wiedererkennbar.

Dennoch beinhaltet das Chiffrat jede mögliche Permutation der 26 Buchstaben im Alphabet. Dies sind immerhin 26! [4], mit anderen Worten mehr als 4×10^{26} mögliche Permutationen. Im Vergleich dazu ist der bekannte *DES-Algorithmus* [5] mit einem 56-Bit-Schlüssel und einem Schlüsselraum von 2^{56} oder größer als 7×10^{16} ungefähr 10er Potenzen kleiner als der Cäsar-Algorithmus.

Weiterhin kommt im o.g. Beispiel dem Kryptoanalysten zugute, dass die Sprache bekannt ist, denn jede Sprache hat ihre speziellen Charakteristika, so z.B. die Anzahl des Buchstaben (*e*) oder (*z*). Der Buchstabe (*e*) kommt im lateinischen (romanischen) Sprachgebrauch wesentlich häufiger vor als der Buchstabe (*z*) oder (*y*). Die relative Häufigkeit der auftretenden Buchstaben in Klartext-Sätzen einer Sprache zu ermitteln und sie mit dem Chiffrat zu vergleichen, gibt einen markanten Hinweis über den Zusammenhang zwischen Chiffrat und Klartext.

Ist das Chiffrat lang genug, können die relativen Frequenzen der Buchstaben des Chiffrats in Prozent angegeben werden. Wird anschließend nach Buchstabenkombinationen gesucht und verglichen, können sehr schnell große Erfolge erzielt werden. Natürlich gehört etwas Fingerspitzengefühl und Übung dazu. Dass diese Art der Analyse in der Geschichte häufig eingesetzt wurde, wird durch die Tatsache bestätigt, dass nach genau diesen Gesichtspunkten, nämlich der relativen Häufigkeit der auftretenden Buchstaben, Samuel F.B. Morse 1844 das nach

[4] Das Ausrufezeichen (!) beschreibt den mathematischen Begriff der Fakultät, der allgemein die Multiplikation von $1 \times 2 \times 3 \times 4 \times \cdot \times n$ bedeutet. Abgekürzt kann $n! = \prod_{k=1}^{n} k$, gelesen werden: n Fakultät. Im vorliegenden Fall ist $n = 26$.

[5] DES ist die Abkürzung für *Data Encryption Standard*. DES wurde 1976 in den USA als Federal Standard angenommen. Ab 1981 wurde DES auch von der ANSI als Standard X3.92-1981 unter der Bezeichnung *Data Encryption Algorithm* (DEA) geführt.

ihm benannte Alphabet entwickelte. So haben in seinem (engl.) Alphabet die häufigsten Zeichen die kürzesten Symbole. So wird das (*e*) durch einen (·) Punkt übermittelt. Der zweithäufigst vorkommende Buchstabe ist das (*t*), das im Morse-Alphabet durch ein (–) dargestellt wird. Damit wird deutlich, dass monoalphabetische Verschlüsselungen leicht zu dechiffrieren sind, denn sie spiegeln die relative Häufigkeit der Buchstaben im Alphabet wider.

Lange[6] galt die Verschlüsselung von Playfair[7], die auf einer 5×5-Matrix und einem Schlüsselwort beruht, als unbrechbarer Algorithmus. Wird z.B. das Schlüsselwort *WILDFANG* gewählt, wird der Rest der 5×5-Matrix von links nach rechts und von oben nach unten mit den verbleibenden Buchstaben des Alphabets aufgefüllt. Tab. 4.1 zeigt diese Matrix mit *WILDFANG* als Schlüsselwort.

Um eine Verschlüsselung durchzuführen, müssen folgende Chiffrierregeln beachtet werden:

1. Ein Klartext wird chiffriert, indem immer zwei aufeinanderfolgende Buchstaben gleichzeitig transformiert werden.
2. Jeder Buchstabe des Alphabets tritt nur einmal in der 5×5-Matrix auf; die Buchstaben (IJ) werden als ein Buchstabe betrachtet.
3. Buchstaben, die im Klartext doppelt auftreten, werden mit einem Füllbuchstaben, z.B. (x), entstellt. So wird das zu verschlüsselnde Wort Brunnen zu Brunxnen verschleiert, bevor es chiffriert wird.
4. Buchstaben, die im Klartext in der gleichen Reihe liegen, werden durch den rechten Nachbarbuchstaben ersetzt. Ist das Ende der Matrix-Reihe erreicht, wird in der gleichen Reihe wieder vom Anfang begonnen, z.B. (df) wird durch (FW) ersetzt.
5. Buchstaben, die im Klartext in der gleichen Spalte liegen, werden durch den direkt folgenden Buchstaben in der Spalte ersetzt. Wird das Ende der Matrix-Spalte erreicht, wird in der gleichen Spalte wieder von oben angefangen, z.B. (wu) wird durch (AW) ersetzt.
6. Ansonsten gilt, dass jeder erste Buchstabe einer Buchstabenkombination im Klartext durch den Buchstaben ersetzt wird, der in der gleichen Reihe steht, jedoch die Position der Spalte des zweiten Buchstaben einnimmt. Somit bleiben die Transformationen reihenkonform. Z.B. wird (ed) zu (MW) und (ns) zu (BQ).

Die den Chiffrierregeln zugrunde gelegten Beispiele entstammen der nachfolgend aufgeführten 5×5-Matrix mit dem Schlüsselwort *WILDFANG*.

---

[6] Der *Playfair-Algorithmus* war der Standard-Algorithmus der Engländer im Ersten Weltkrieg und wurde auch noch im Zweiten Weltkrieg von den alliierten Truppen benutzt.

[7] Benannt nach dem Baron Playfair von St. Andrews; kurioserweise wurde jedoch der Algorithmus 1854 von dem britischen Wissenschaftler Sir Charles Wheatstone entwickelt.

Der Playfair-Algorithmus zählt zu den monoalphabetischen Verschlüsselungen. Er bringt es mit den 26 Buchstaben des Alphabets immerhin auf $26 \times 26 = 676$ Diagramme, so dass die Identifizierung eines einzelnen Diagramms recht schwierig ist. Auch die relativen Häufigkeiten der Buchstaben zeigen eine wesentlich größere Variation als bei einer einfachen Transformation, wie z.B. beim Cäsar-Algorithmus. Eine Frequenzanalyse der Buchstaben wird somit erheblich erschwert. Obwohl der Playfair-Algorithmus scheinbar einen hohen Grad an Vertraulichkeit erreicht, ist er dennoch leicht zu brechen, wie die Alliierten im Zweiten Weltkrieg zu ihrem Leidwesen erfahren mussten. Denn eine Schwäche des Playfair-Algorithmus liegt darin, dass ein Großteil der Struktur des Klartextes erhalten bleibt. Einige hundert Buchstaben eines Chiffrates genügen, um den Algorithmus zu finden.

Tabelle 4.1: Playfair Verschlüsselung mit Schlüsselwort „Wildfang“

W	**IJ**	**L**	**D**	**F**
A	**N**	**G**	B	C
E	H	K	M	O
P	Q	R	S	T
U	V	X	Y	Z

Eine andere Möglichkeit, die monoalphabetische Verschlüsselung zu verbessern, ist die geeignete Ergänzung von unterschiedlichen Buchstaben und die Verlängerung des Schlüssels. Dies kann im Extremfall dahingehend ausarten, dass der Schlüssel genauso lang ist wie der Klartext. Diese Art der Verschlüsselung ist als Vigenère-Verschlüsselung in die Literatur eingegangen. Diese Technik der Substitution hat folgende Merkmale:

1. Eine Menge von zueinander in Beziehung stehenden monoalphabetische Substitutionsregeln werden benutzt.
2. Ein Schlüsselwort bestimmt, welche spezifische Regeln für die Transformation benutzt werden.

Um diese Arbeitsweise zu verstehen, ist es hilfreich, eine 26×26-Matrix zu konstruieren, die das gesamte Alphabet auf einer Zeile der Matrix abbildet (Tab. 4.2), jedoch mit einer Verschiebung der Anfangsbuchstaben von Zeile zu Zeile. Ähnliche Verschiebungen sind auch beim Cäsar-Algorithmus verwendet worden. Die nach seinem Entwickler benannte Vigenère-Tafel ist in Tab. 4.2 in Auszügen dargestellt. Um eine Chiffrierung mit der Vigenère-Tafel durchzuführen, ist ein Schlüssel bzw. Schlüsselwort notwendig. Angenommen der Buchstabe (*e*) sei der Schlüssel und der Buchstabe (d) soll chiffriert werden, so wird in der Reihe ausgehend vom Schlüssel (*e*) die Spalte gesucht, in der der Buchstabe (d) in der ersten Zeile steht. Die Verschlüsselung lautet dann (H) (Tab. 4.2).

Soll jetzt eine ganze Nachricht verschlüsselt werden, wird ein Schlüssel generiert, der genauso lang ist wie die Nachricht. Hierbei wird ein Schlüsselwort solange

Tabelle 4.2: Vigenère-Tafel mit einer zeilenweisen Verschiebung der Anfangsbuchstaben

	a	b	c	**d**	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	v	**w**
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	V	W	X
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	V	W	X	Y
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	V	W	X	Y	**Z**
e	E	F	G	**H**	I	J	K	L	M	N	O	P	Q	R	S	T	V	W	X	Y	Z	A
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	…						
g	G	H	I	J	K	L	M	N	O	P	Q	…										
h	H	I	J	K	L	M	N	O	…													
i	I	J	K	L	M	…																
j	K	L	M	…																		
k	L	M	…																			
⋮																						
⋮	…																					

wiederholt, bis die Nachricht und das Schlüsselwort gleich lang sind. Angenommen, das Schlüsselwort lautet *deceptive* und die Nachricht „*we are discovered save yourself*“ ist zu transformieren , wird dies erreicht:

Schlüsselwort:	deceptivedeceptivedeceptive
Klartext:	wearediscoveredsaveyourself
Chiffrat:	ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Die Dechiffrierung verläuft umgekehrt wie die Chiffrierung. Ein Schlüsselbuchstabe wird aus dem Schlüsselwort genommen, z.B. das erste (d) von *deceptive*, und damit in der Vigenère-Tafel in jene Zeile gegangen, die mit dem (d) beginnt. Jetzt wird nach rechts in der gleichen Reihe das (Z) gesucht. Darüber in der gleichen Spalte, jedoch in der ersten Zeile, ist der Klartextbuchstabe (w) zu finden.

Eine gewollte Schwierigkeit des Chiffrates ist, dass mehrere Chiffrat-Buchstaben für einen Schlüsselwortbuchstaben gebildet wurden. So tritt der Buchstabe (d) im sich wiederholenden Schlüsselwort *deceptive* mehrmals auf, wird jedoch im Chiffrat unterschiedlich transformiert. Das zweite (d) taucht als (R) im Chiffrat wieder auf. Dieser Mechanismus erschwert eine Frequenzanalyse, vereitelt diese jedoch nicht gänzlich, wie weiter unten ausgeführt wird. Aber nicht jegliche Information wird vom ursprünglichen Klartext verwischt, denn die *periodische* Wiederholung des Schlüsselwortes stellt eine erhebliche Schwäche dar. So wird bei dem Schlüsselwort *deceptive* der 1., 10. und 19., etc. Buchstabe mit der gleichen Substitution transformiert. Vigenère schlug daraufhin einen so genannten *Auto Key* vor, der mit dem Klartext konkadiniert wird:

Schlüsselwort:	deceptivewearediscoveredsav
Klartext:	wearediscoveredsaveyourself
Chiffrat:	ZICVTWQNGKCEIIGASXSTSLVVWLA

Dennoch ist die Technik nicht stabil genug gegenüber einer Frequenzanalyse, da

der Schlüssel und der Klartext die gleiche Frequenzverteilung der Buchstaben haben. Als ultimative Entwicklung wurde daher ein Schlüsselwort generiert, das so lang ist wie der Klartext, jedoch keinen statistischen Bezug zum Klartext hat. Ein derartiges System wurde 1918 von Vernam vorgeschlagen. Es arbeitete mit binären Daten.

$$C_i = p_i \bigoplus k_i \tag{4.4}$$

Dabei bedeutet:

$p_i =$ i-tes binäres Bit des Klartextes
$k_i =$ i-tes binäres Bit des Schlüssels
$C_i =$ i-tes binäres Bit vom Chiffrat
$\bigoplus =$ exklusive Oder-Operation

Die exklusive Oder-Operation beschreibt die in der Kryptographie wichtige *XOR-Operation*[8]. Eine Dechiffrierung erfolgt einfach durch eine nach p_i aufgelöste Gleichung

$$p_i = C_i \bigoplus k_i \tag{4.5}$$

Die Bedeutung des Schlüssels ist die eigentliche Essenz dieser Technik. Schon damals folgerte Vernam, dass durch ein Endlosband eine Schlüsselwiederholung eintreten könnte. Obgleich die Verwendung eines sehr sehr langen Schlüssel die Kryptoanalyse erheblich erschwert, kann durch ein geeignetes Chiffrat oder durch einen bekannten Klartext der Algorithmus erkannt und somit wieder rücktransformiert werden.

In Anlehnung an den Vernam-Algorithmus kam der Armee-Offizier Joseph Mauborgne auf die brilliante Idee, einen zufälligen Schlüssel zu generieren, der keine Wiederholungen in sich birgt und so lang ist wie der Klartext selbst, aber zu diesem keinen statistischen Bezug hat. Somit entstand der bekannte *One Time Pad*[9], der bis heute als nicht zu entschlüsseln eingestuft wird. Allerdings müssen Sender und Empfänger den Zufallsschlüssel sorgfältig aufbewahren.

Abschließend sei zu den Substitutionstechniken noch folgende Klassifizierungen unterschiedlicher Substitutionstypen erwähnt. Substitutionen nennt man:

- monoalphabetisch, falls jedem Zeichen oder jeder Zeichenfolge über einem Alphabet *A* eindeutig ein Zeichen bzw. eine Zeichenfolge über einem Alphabet *B* zugeordnet ist,

[8] Die exklusive Oder-Operation spiegelt die zwei unterschiedlichen Zustände in einem Computer wider: 0 und 1. Es gilt, wenn A=1 und B=0, dann ist A $\bigoplus$ B = 1, wenn A=0 und B=1, dann ist A $\bigoplus$ B = 1, wenn A=1 und B=1, dann ist A $\bigoplus$ B = 0 und wenn A=0 und B=0, dann ist A $\bigoplus$ B = 0.

[9] One Time Pad (OTP) ist das einzige Verfahren, das sich unabhängig von der Rechnerleistung nachweislich nicht brechen lässt. Auch beliebig viel Geheimtext liefert nicht genug Informationen, um daraus den Klartext oder den Schlüssel zu rekonstruieren.

- polyalphabetisch, falls jedem Zeichen oder jeder Zeichenfolge über einem Alphabet A ein Zeichen oder eine Zeichenfolge über den Alphabeten $B_1, ...B_n$ zugeordnet ist,
- monograpisch, falls sie Einzelzeichen ersetzen und
- polygraphisch, falls sie Zeichenfolgen ersetzt.

Einen völlig anderen Ansatz verfolgt die Transpositionstechnik, die im Weiteren näher erläutert wird.

4.1.2 Transpositionstechniken

Alle bisher aufgezeigten Verfahren zur Verschlüsselung basieren auf einer Verschiebung bzw. Substitution von Buchstaben: Jeder Buchstabe des Klartextes wird hierbei durch einen Repräsentanten im Chiffrat ersetzt. Ein völlig anderer Ansatz, auf dem viele moderne Kryptoverfahren beruhen, wie z.B. der DES-Algorithmus, benutzt die Buchstaben des Klartexts selbst. Hier werden die Buchstaben nach bestimmten Verfahren durcheinander gewürfelt, also einer Permutation der Buchstabenplätze in einem Text unterworfen.

Ein sehr einfaches Verfahren, von dem viele andere moderne Verfahren abgeleitet wurden, ist die *Rail Fence Chiffrierung*, die den Klartext in ein geometrisches Muster transponiert. Es gibt etliche Muster, die vorstellbar und durchführbar sind, und im Laufe der Zeit wurden diese Muster ausgefeilter und immer komplizierter. Ein einfaches Muster ist z.B. das Zickzack-Muster mit der Tiefe von zwei. Im Beispiel „Treffe mich nach der Toga Party“

```
t e f m c n c d r o a a t
 r f e i h a h e t g p r y
```

lautet die vollständige Transposition:

TEFMCNCDROAATRFEIHAHETGPRY

Dieses Beispiel ist für die Kryptoanalyse trivial zu dechiffrieren. Ein wesentlich komplexeres Schema entsteht, wenn der Klartext Zeile für Zeile in eine Matrix geschrieben und anschließend Spalte für Spalte gelesen wird und die Spalten dabei permutieren. Der Schlüssel entspricht der Permutationsordnung der Spalten sowie der Anzahl der Zeilen.

Im nächsten Beispiel wird wieder der obige Text bearbeitet und in eine 4×7-Matrix geschrieben sowie mit den zwei Füllbuchstaben y und z vervollständigt. Das Chiffrat wird entsprechend dem Schlüssel (Permutationsvorschrift) vertikal gebildet.

Schlüssel:	4 3 1 2 5 6 7
Klartext:	t r e f f e m
	i c h n a c h
	d e r t o g a
	p a r t y y z
Chiffrat:	EHRRFNTTRCEATIDPFAOYECGYMHAZ

Da jedoch eine einfache Transposition mittels einer Frequenzanalyse dechiffriert werden kann, wird der Vorgang wiederholt. Somit wird das soeben gebildete Chiffrat als Eingangstext in dieselbe Matrix mit derselben Permutationsvorschrift genommen.

Schlüssel:	4 3 1 2 5 6 7
Eingangstext:	e h r r f n t
	t r c e a t i
	d p f a o y e
	c g y mh a z
Resultat:	RCFYREAMHRPGETDCFAOHNTYATIEZ

Das Resultat, eine doppelte Transposition, ist eine wesentlich komplexere Permutation, die nicht mehr so einfach zu rekonstruieren ist.

Diese simplen Beispiele legen nahe, dass eine Vielfachverschlüsselung einen Algorithmus hervorbringt, der für einen Kryptoanalysten signifikant schwieriger zu dechiffrieren ist. Dies gilt prinzipiell für die Substitutionstechnik wie für die Transpositionstechnik. In einer geeigneten Kombination beider Verfahren entstanden so genannte *Rotor-Maschinen*, die mit der Drei-Rotor-Maschine Enigma[10] einen Höhepunkt erreichte und den Grundstein der heutigen DES-Verschlüsselung legte.

Aus diesen einfachen historischen Beispielen wird jedoch auch deutlich, dass jeder vermeintlich sicher geltende Code entschlüsselt wurde. Einer der entscheidenden Nachteile ist neben den Algorithmen selbst – die unbedingt geheim gehalten werden mussten – die Notwendigkeit, dass die Buchstabenverschiebung, z.B. beim Cäsar-Algorithmus und beim Kennwort des Playfair-Algorithmus (hier: Wildfang), dem Empfänger vertraulich zugeleitet werden mussten. Erst dann war eine vertrauliche Kommunikation mglich.

Mit der aufkommenden Datenverarbeitung der späten 40er und Anfang der 50er Jahre wurde es immer einfacher und schneller, unterschiedliche Algorithmen

[10] Die deutsche Enigma, aber auch die Variante Purple, die in Japan eingesetzt wurde, spielten im Zweiten Weltkrieg ein entscheidene Rolle. Das Entschlüsseln der mit der Enigma chiffrierten Nachrichten hat maßgeblich zum Ausgang des Zweiten Weltkrieges beigetragen.

durchzuprobieren. Die Kryptoanalyse verzeichnete zu dieser Zeit große Erfolge. In dieser Zeit fand ein Paradigmenwechsel statt. Man erkannte, dass eine Geheimhaltung des Algorithmus *security by obscurity* auf die Dauer nicht aufrecht zu erhalten sein würde. Der niederländische Philologe Auguste Kerckhoff (1835-1903) hatte dies schon wesentlich früher in seinem 1883 erschienen Buch (*La Cryptographie militaire*) gefordert, in dem er treffend das später nach ihm benannte Prinzip formulierte:

> Die Sicherheit eines Kryptosystems darf nicht von der Geheimhaltung des Algorithmus abhängen. Die Sicherheit darf sich ausschließlich auf die Geheimhaltung des Schlüssels begründen.

Weiterhin wurde intensiv am Problem der sicheren Weitergabe des Kennworts (hier: *WILDFANG*) unter vertraulichen Bedingungen gearbeitet. Nachfolgend wird dargestellt, wie dies mit den heutigen Methoden der Kryptographie gelöst wird.

4.2 Symmetrische Kryptosysteme

Kennzeichnend für symmetrische Kryptosysteme ist, dass für die Chiffrierung und Dechiffrierung dieselben geheimzuhaltenen Schlüssel benötigt werden. Oft wird diese Eigenschaft in der Literatur mit dem Begriff *Secret-Key-Verfahren* bezeichnet. In Abschn. 4.1.1 wurde der gravierende Schwachpunkt des Schlüsselaustausches der symmetrischen Kryptosysteme bereits angedeutet. Dennoch werden heutzutage vornehmlich symmetrische Kryptosysteme benutzt, wenn Sender und Empfänger erreichen wollen, dass die zwischen ihnen ausgetauschten Nachrichten geheim bleiben sollen. Üblicherweise werden Transportmedien wie vernetzte Computer oder das Telefonnetz benutzt, die von Dritten abgehört werden können. Der praktische Einsatz von symmetrischen Kryptosystemen wird heute gerne in Kombination (hybride kryptographische Systeme) mit speziellen Verfahren, die einen sicheren Schlüsselaustausch garantieren, ergänzt.

Ein Vorteil der symmetrischen Kryptosysteme gegenüber asymmetrischen Verfahren[11] liegt in der hohen Geschwindigkeit beim Verschlüsselungsvorgang. Heutzutage weit verbreitete symmetrische Verfahren sind z.B. DES, AES, Triple DES, IDEA und Blowfish, die im Internet und auch bei IPSEC, dem wohl derzeit bedeutendsten Verschlüsselungsverfahren für VPN, zur Anwendung kommen. Weiterhin erweisen sich symmetrische Kryptosysteme als sehr wertvoll, z.B. zur Datenspeicherung, wenn sensible Informationen so aufzubewahren sind, dass sie nicht in Besitz unbefugter Dritter gelangen sollen. Solange der Schlüssel geheim bleibt, sind die Daten geschützt, auch wenn das zu ihrer Speicherung verwendete

[11] Im Gegensatz zum symmetrischen Verfahren werden unterschiedliche Schlüssel zu Ver- und Entschlüsselung genutzt.

Medium (Festplatte, Diskette etc.) von Fremden eingesehen werden kann. Allerdings hat der Verlust des Schlüssels durch den Schlüsseleigentümer fatale Folgen, denn die Informationen sind nicht mehr rekonstruierbar.

Ein weiteres Anwendungsgebiet der symmetrischen Verfahren ist die Authentifikation. Sie beruht in der Regel auf dem Besitz eines Geheimnisses, oftmals ein Passwort, mit dem die Identität festgestellt werden soll. Wird allerdings das Passwort weitergegeben – legal oder illegal –, kann dies zum Missbrauch des Systems oder der Anwendung führen.

4.2.1 Blockchiffre und Stromchiffre

Bei den symmetrischen Verfahren können zwei Abgrenzungen erfolgen. Als eine Kategorie haben sich die kontinuierlichen Algorithmen oder auch Stromchiffren *(Stream Ciphers)* entwickelt. Bei diesen Verfahren wird der Klartext bit- oder byteweise (manchmal auch 32-Bit-Worte) geschlossen verarbeitet. Beispiele von Stromchiffren in der klassischen Kryptologie sind die Vigenère-Chiffrierung oder auch die Vernam-Verschlüsselung. Ein Spezialfall ist das bereits diskutierte One Time Pad (OTP). Der Klartext wird über die Funktion XOR mit einer langen binären Folge von Signalen verkünpft. Die Wiederholungsrate der binären Signale ist dabei größer als die zu verschlüsselnde Nachricht lang ist. Die Nachricht wird demnach als eine Folge von Zeichen so kodiert, dass die einzelnen Zeichen des Alphabets verschlüsselt werden. Die Zeichen werden jedoch nicht notwendigerweise unabhängig voneinander verschlüsselt. Zu beachten ist bei den Stromchiffren die Eigenschaft der Synchronisierung:

1. In synchronen Stromchiffren hängt die Verschlüsselung von ihrer Position innerhalb der Nachricht ab, oder allgemeiner, noch von allen Klartext- und/oder Schlüsseltextzeichen. Kryptosysteme mit dieser Eigenschaft unterliegen der Schwierigkeit der Synchronisation bei Verlust oder Hinzufügen eines Schlüsseltextzeichen. Eine Entschlüsselung kann nicht mehr ohne weiteres durchgeführt werden. Hängt gar die Ver- und Entschlüsselung nicht nur von der Position innerhalb der Nachricht ab, sondern auch von allen vorhergehenden Klartext- und/oder Schlüsseltextzeichen, müssen Ver- und Entschlüssler sich auch bei Verfälschung nur eines Schlüsseltextzeichens neu synchronisieren.
2. In selbstsynchronen Stromchiffren hängt die Verschlüsselung nur von einer beschränkten Anzahl direkt vorhergehender Schlüsseltextzeichen ab. Damit kann sich der Entschlüssler auch bei Verlust oder Hinzufügen beliebig vieler Schlüsseltextzeichen, spätestens nach Entschlüsselung der eben erwähnten Anzahl der Schlüsseltextzeichen, wieder mit dem Verschlüssler synchronisieren.

Manche Autoren sehen die Definition von synchronen Stromchiffren jedoch wesentlich enger. Diese Sichtweisen sind allerdings für das weitere Verständnis nicht unbedingt erforderlich und werden daher nicht weiter betrachtet.

Die Stromchiffrierung hat in der Praxis eine ähnlich hohe Bedeutung wie die Blockchiffrierung. Jedoch unterstützen viele Protokolle bzw. deren Implementierungen, deutlich weniger kontinuierliche als blockorientierte Verfahren. Eine relativ verbreitete Stromchiffre[12] ist das RC4-Verfahren. Nachdem seine Spezifikation lange nicht öffentlich zugänglich war[13], hat sich dies kürzlich geändert. RC4 wurde 1987 von keinem Geringeren als Prof. R. Rivest[14] entworfen und zeigt dennoch Schwächen [Fluhrer et al. 2001]. Die zunächst nur theoretischen erkannten Schwächen konnten dann in einem Praxis-Test im AT&T-Lab-Research Institut bestätigt werden [Stubblefield et al. 2001].

Als zweite Kategorie wurden blockorientierte Algorithmen bzw. Blockchiffren (*block ciphers*) entwickelt. Bei den blockorientierten Verfahren erfolgt die Verschlüsselung des Klartextes (in einem gegebenen endlichen Alphabet) generell in Bit-Blöcken fester Länge. Oft hat dieser feste Bit-Block eine Länge von 64 Bit, wie z.B. bei DES, Triple DES und IDEA. Nachfolgend werden verschiedene Blockverfahren vorgestellt. Denn eine Nachricht, die in 64 Bit-Blöcke zerlegt wird, kann auf unterschiedliche Art und Weise reversibel modifiziert werden. Dabei gehen alle symmetrischen Blockverfahren, die derzeit genutzt werden, auf das Feistel-Block-Verfahren [Feistel 1973] zurück. Nur die bedeutendsten Blockverfahren[15] ECB, CBC, CFB und OFB werden hier diskutiert:

- Elektronisches Codebuch (ECB)
- Blockchiffre mit Blockverkettung (CBC)
- Schlüsseltextrückführung (CFB)
- Ergebnisrückführung (OFB)

Die beiden Verallgemeinerungen PCBC und OCFB werden nicht behandelt; dazu siehe z.B. [Denning 1983] oder auch [Pfitzmann 1998].

Jedem dieser vier Verfahren (ECB, CBC, CFB und OFB) ist ein eigener Abschnitt gewidmet, denn diese nicht übermäßig komplexen Modi können auch in eigenen Applikationen verwendet werden. Mit selbstentwickelten Verfahren ist jedoch mit großer Sorgfalt umzugehen. Dies zeigt das Beispiel der in Version vier des Authentifizierungssystem Kerberos zur Integritätssicherung eingesetzte, nicht standardisierte PCBC-Verfahren, das dem CBC ähnelt. PCBC enthielt einen Fehler, so dass das Verfahren in Kerberos 5 durch CBC ersetzt wurde.

---

[12] Beispielsweise wird RC4 nach IEEE 802.11b im *Wireless Encryption Protocol* (WEP) eingesetzt. Ebenso findet RC4 Verwendung bei SSL, Oracle-SQL und im Microsoft Windows-Betriebssystem.

[13] Die RC4 vertreibende Firma RSA, dessen Mitbegründer Prof. R. Rivest ist, sah den Algorithmus als Firmengeheimnis an.

[14] Prof. Rivest ist Mitentwickler des bekannten RSA-Algorithmus. Das „R" in dem RSA-Algorithmus, entstammt seinem Namen.

[15] Die Blockverfahren werden häufig auch als *Modes of Operation* bezeichnet.

ECB

ECB ist das einfachste und naheliegendste Verfahren zur Nutzung eines Blockalgorithmus. Die gesamte Nachricht (Klartext) wird in *n*-Bit-Blöcke zerlegt und jeder Block wird separat mit demselben geheimen Schlüssel chiffriert. Die Zahl *n* entspricht der Blocklänge des anzuwendenden Chiffrierverfahrens, z.B. 64 bei DES und IDEA. Der letzte Block wird bei Bedarf auf volle *n* aufgefüllt. Dies wird als *Padding* bezeichnet. Graphisch ist die Verschlüsselung[16] in Abb. 4.1 dargestellt. Die Nachricht (Klartext) ist durch ein Rechteck skizziert, das in 9 Blöcke (k1,...k9) zu je 64 Bit zerlegt wird. Mittels des geheimen Schlüssels (E) werden chiffrierte Bit-Blöcke (c1,...c9) erzeugt.

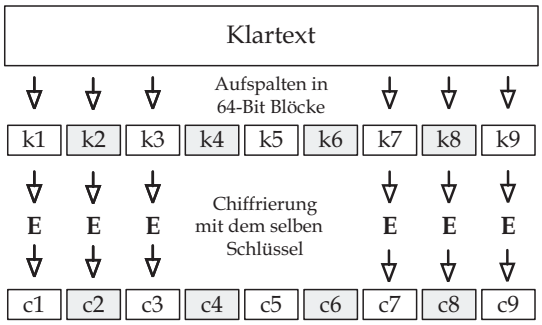


Abb. 4.1: Graphische Veranschaulichung der blockorientierten ECB Verschlüsselung

Das blockorientierte ECB-Verfahren hat einige Charakteristika, die die Verwendung des Verfahrens bestimmen. So wird z. B. jeder Klartextblock immer wieder auf denselben Geheimtext abgebildet, solange derselbe Schlüssel verwendet wird. Damit hängt jedes Bit im chiffrierten Block vom jeweiligen Bit im Klartext und vom Schlüssel ab. Da identische Klartexte identische Chiffren erzeugen, gestattet die Analyse des Geheimtextes in der Regel viele Rückschlüsse auf den Klartext.

Oft weisen Nachrichten eine sehr regelmäßige Struktur und viele Redundanzen auf. Tendenziell spiegeln sich derartige Eigenschaften in den Geheimtexten wieder und ermöglichen, unabhängig von der Stärke der zugrunde liegenden Blockchiffre, verschiedene statistische Attacken. Hauptsächlich aus diesem Grund wird das ECB-Verfahren so gut wie nie zur Verschlüsselung von Nachrichten eingesetzt, die länger als ein Block sind.

Die Dechiffrierung erfolgt analog zur Chiffrierung, nur in umgekehrter Reihenfolge. Auf jeden chiffrierten Block c1 ... c9 wird wiederum der Schlüssel (E) angewandt und somit die Klartextblöcke k1 ... k9 wieder lesbar gemacht (Abb. 4.2).

[16] Da die Eigenschaften dieser und der folgenden Chiffrierverfahren einfacher bei langen Nachrichten zu zeigen sind, wird im Folgenden auf Textbeispiele, wie sie noch im letzten Abschnitt zur Verdeutlichung herangezogen wurden, verzichtet.

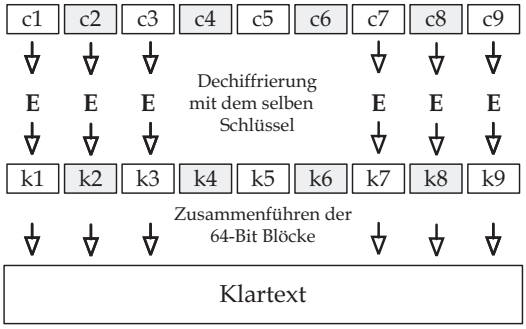


Abb. 4.2: Veranschaulichung des Dechiffriervorgangs beim blockorientierten ECB Verfahren

Ein weiterer gravierender Nachteil der ECB-Verschlüsselung ist die Möglichkeit der Umordnung oder auch Modifizierung der einzelnen *n*-Bit-Blöcke, ohne dass der Empfänger eine Chance hat, dies zu bemerken. Denn es bestehen keinerlei Abhängigkeiten zwischen den einzelnen verschlüsselten Blöcken, wie in Abb. 4.2 durch die separaten Kästchen c1 ... c9 angedeutet ist. Somit lassen sich, wenn die Struktur der Nachricht (z.B. Tabellen mit regelmäßigen Einträgen) bekannt ist, möglicherweise relativ gezielte Manipulationen durchführen, indem einzelne Blöcke des Geheimtextes gegen einen anderen ausgetauscht werden. Damit ist die Integrität der Nachricht verletzt. Diese Tatsache allein birgt allerdings keinen ernsthaften Nachteil, denn a priori wird eine Verschlüsselung nicht zum Schutz der Integrität einer Nachricht verwendet. Wie die Integrität einer Nachricht mittels spezieller Methoden sichergestellt wird, wird in Abschn. 4.5 diskutiert.

CBC

Das CBC-Verfahren arbeitet mit einer Verkettung *(chaining)*, so dass eine Umordnung der Blöcke, wie beim ECB-Verfahren vom Empfänger möglich, nicht unbemerkt bleibt. Genau genommen passiert Folgendes (Abb. 4.3): Der Klartext wird, wie beim ECB-Verfahren, in *n*-Bit-Blöcke zu je 64 Bit zerlegt. Jedoch wird der aktuelle Klartextblock, z.B. k3, *vor* seiner Chiffrierung mit dem Geheimtextblock des vorangegangenen chiffrierten Blocks c2 mittels der XOR-Operation verknüpft. Damit hängt das Ergebnis nicht mehr ausschließlich vom gerade verarbeiteten Klartextblock ab, sondern zusätzlich von seinen Vorgängern. Allerdings wirft diese Art der Verkettung die Frage auf, wie der erste Block k1 behandelt wird (Abb. 4.3), der ja keinen Vorgänger hat. Es wird ein Initialisierungsvektor (IV) benutzt, der in der Praxis häufig aus einer Zeitmarke oder aus anderen zufällig gewählten Bitfolgen besteht.

Mit dieser gängigen Methode der Verkettung wird der am häufigsten kritisierten Eigenschaft des ECB-Verfahrens entgegen gewirkt. In der Literatur sind deutlich unterschiedliche Meinungen darüber zu finden, wie mit dem Initialisierungsvektor (IV) umzugehen ist. Die Frage, ob der IV nebst Geheimtext im Klartext,

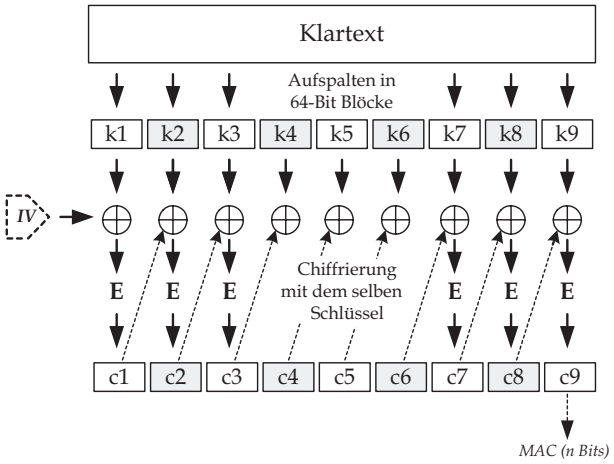


Abb. 4.3: Veranschaulichung des Chiffriervorgangs beim blockorientierten CBC-Verfahren

zum Empfänger hin übertragen, oder ebenso wie der Chiffrierschlüssel geheimgehalten werden sollte, wird kontrovers diskutiert. [Schneier 1996] vertritt im Gegensatz zu anderen Autoren die nachvollziehbare Auffassung, dass der Initialisierungsvektor im Klartext übertragen werden kann. Denn beim CBC-Verfahren handelt es sich, wie beim ECB-Verfahren, um einen Mechanismus, der die Vertraulichkeit gewährleistet, die Integrität – trotz IV beim CBC-Verfahren – jedoch nur sehr rudimentär wahrt. Soll allerdings sowohl Vertraulichkeit als auch Integrität einer Nachricht mittels CBC erreicht werden, sind zwei unterschiedliche Schlüssel zu benutzen: einer für die Datenverschlüsselung und einer für den MAC. Daraus folgt allerdings zwingend, dass der CBC-Algorithmus zweimal anzuwenden ist.

Beim CBC-Verfahren wird ein Padding genutzt, wenn der Klartext kein ganzzahliges Vielfaches der Blocklänge ist, z.B. von 64 Bit. Beim Padding wird der letzte verschlüsselte Block, z.B. c_i, der kürzer ist und nur j Bits besitzt, aufgefüllt. Damit wird der Geheimtext länger als der Klartext. Sollte dies in bestimmten Situationen nicht vertretbar sein, müssen bestimmte Operationen dies unterbinden. Eine Möglichkeit besteht darin, den vorletzten Geheimtextblock, z.B. c_{i-1}, nochmals zu verschlüsseln $(E_k(c_{i-1}))$ und dessen j höchstwertige Bits mit k_i über XOR zu verknüpfen, so dass c_i eine Länge von genau j Bits bekommt.

Im Gegensatz zum ECB-Verfahren lässt sich der CBC-Mechanismus auch für eine Verschlüsselung von Nachrichten oder Datei-Inhalten benutzen, deren Längen die Blocklänge der zugrunde liegenden Chiffre übersteigt. Damit spielt das CBC-Verfahren in der heutigen Kommunikationssicherheit eine nicht unbedeutende Rolle. Abwandlungen des CBC-Mechanismus sind z.B. beim Triple DES zu finden (Abschn. 4.2.3). Da die CBC-Chiffrierung unabhängig von der konkret einge-

setzten Blockchiffre bereits eine schlüsselabhängige Funktion[17] besitzt, wird dieser so genannte CBC-MAC, der 1985 im ANSI-Standard X9.9 beschrieben wird, in der Praxis oft eingesetzt. Neben den gängigen Produkten zur Verschlüsselung von Festplatten in Laptops bzw. Personalcomputern benutzen etliche Banken dieses Verfahren zur Absicherung elektronischer Transaktionen. Das CBC-Verfahren wird auch als das voreingestellte Standardverfahren in Verbindung mit einem durch IPSec abgesicherten VPN benutzt (Abschn. 7.4.4). Als Hash-Wert wird ein bestimmter Teil (n-Bits) des letzten Geheimtextblocks c9 verwendet (Abb. 4.3). In der Regel wird sogar der Initialisierungsvektor (IV) nur aus Null-Bits gebildet.

CFB

Das CFB-Verfahren bietet die Möglichkeit, Dateneinheiten bzw. Nachrichten zu verarbeiten, deren Bit-Anzahl (n) kleiner als die Blocklänge der verwendeten Chiffre ist. Dies gelingt nur, weil das CFB-Verfahren ein Stromchiffre ist. Somit fällt ein Padding weg und damit für einige Anwendungsfälle eine nicht zu vertretende Verlängerung des Klartextes.

Das Verfahren benutzt eine Blockchiffre zur Konstruktion eines Pseudozufallszahlen-Generators und verknüpft dessen Ergebnis über XOR mit der zu verschlüsselnden Nachricht (Klartext)[18]. Zur Realisierung des Pseudozufallszahlen-Generators wird ein Schieberegister eingesetzt, dessen Breite der Blocklänge angepasst ist (meist also 64 Bit) und in dem die Pseudozufallszahlen durch zyklisches Vertauschen erzeugt werden. Um eine definierte Ausgangssituation zu schaffen, wird das Schieberegister zu Beginn mit einem Initialisierungsvektor (IV) besetzt. Dieser muss natürlich dem Sender und Empfänger bekannt sein, um sicherzustellen, dass beide Kommunikationspartner dieselben Zufallsfolgen erzeugen. Damit wird deutlich, weshalb von *Pseudo*zufallszahlen die Rede ist.

Eine weitere Stärke des CFB ist, dass unter Echtzeit-Bedingungen gearbeitet werden kann. Die jeweiligen Daten können ohne zusätzliche Vorkehrungen sofort ver- bzw. entschlüsselt und weitergeleitet werden.

Eine andere Rolle als beim CBC-Verfahren spielt beim CFB-Verfahren der Initialisierungsvektor (IV). Der Vektor muss nicht geheim, aber *unique* sein und zwar für alle mit demselben Schlüssel durchgeführten Verschlüsselungen. Beim CBC-Verfahren handelt es sich wie beim ECB-Verfahren um einen Mechanismus zur Wahrung der Vertraulichkeit. Allerdings wurde beim CBC-Verfahren lediglich empfohlen, unterschiedliche Initialisierungsvektoren (IV) zu wählen, beim CFB Verfahren wird es gefordert.

Ver- und Entschlüsselungsprozess laufen beim CFB-Verfahren prinzipiell identisch ab, allerdings mit dem Unterschied, dass Klar- und Geheimtext ihre Rollen vertauschen (Abb. 4.4):

---

[17] Es ist der Initialisierungsvektor (IV) gemeint, der eine Einweg-Hash-Funktion darstellt, die sich als ein sehr einfaches Verfahren einer kryptographischen Prüfsumme auffassen lässt. Eine kryptographische Prüfsumme wird häufig auch als *Message Authentication Code* (MAC) bezeichnet.

[18] Nach dem gleichen Verfahren funktioniert das schon beschriebene One Time Pad (OTP). Allerdings wird dabei mit einer echten zufälligen Bitfolge gearbeitet.

1. Der aktuelle Registerinhalt (anfangs der Vektor IV) wird mit dem geheimen Schlüssel (E) chiffriert. Als Ergebnis ergibt sich eine *Pseudo*zufallszahl, die jedoch nicht vollständig benutzt wird. Nur die 8 höherwertigen Bit werden weiter verwendet.
2. Diese 8 höherwertigen Bit des Resultats werden mittels einer XOR-Operation mit den ersten 8 Bit des Klartextes verknüpft. Dadurch entsteht das Chiffrat c_1, welches an den Empfänger übertragen wird.
3. Alle anderen Bits im Schieberegister werden um 8 Bit nach links geschoben, wobei die höherwertigen Bits verloren gehen. Somit findet über den erzeugten Geheimtext (c_i) eine Rückkopplung, *Cipher Feedback* genannt, statt.
4. Gleichzeitig wird c_1 als niederwertige Bits in das Schieberegister überführt.

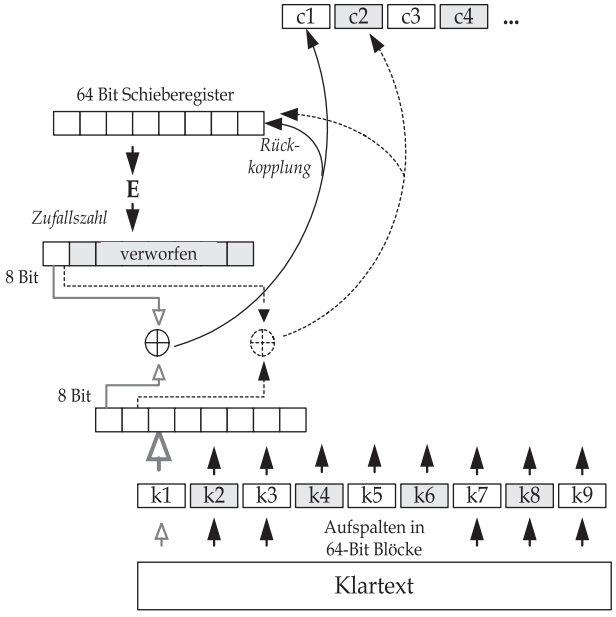


Abb. 4.4: Chiffriervorgang beim CFB-Verfahren für K1 und K2 (gestrichelt)

Der zweite Verschlüsselungsdurchlauf (Abb. 4.4), der zum Chiffrat c_2 führt, ist in gestrichelten Linien dargestellt. Augenfällig ist, dass der in den letzten Beispielen angewandte Klartextblock (unteres beschriftetes Rechteck), der auch hier angedeutet wird, nochmals in je 8 Bit-Blöcke aufgespalten wird. Damit wird deutlich, dass das CFB-Verfahren es gestattet, Dateneinheiten zu verarbeiten bzw. zu verschlüsseln, deren Bitzahl n kleiner als die Blocklänge der verwendeten Chiffre ist. Eine bedeutsame Anwendung ist das Telnet-Protokoll, bei dem es notwendig ist, jedes getippte Zeichen in einem einzelnen Paket zu übertragen.

OFB

Das OFB-Verfahren ist dem CFB-Verfahren sehr ähnlich, jedoch unterscheiden sich beide Verfahren in der Art der Rückkopplung. Bei der OFB-Rückkopplung werden n Bits vom linken Rand des Schieberegisters der erzeugten Pseudozufallszahl wieder zur Bildung des Schieberegisterinhaltes geführt, der zunächst vom Initialisierungsvektor gefüllt worden war (Abb. 4.5). Durch die fehlende Abhängigkeit bzw. Wiederverwendung des Chiffrates $(c_1, c_2, ..., c_i)$ in der Verkettung der Verschlüsselung wird eine Fehlerfortpflanzung vermieden (vgl. Abb. 4.4 mit Abb. 4.5). Es erfolgt eine Linksrotation des Registerinhaltes. Nur bei einem fehlerhaften verschlüsselten Klartext kommt ein fehlerhaft verschlüsseltes Chiffrat zu Stande. Eine Fehlerfortpflanzung ist, anders als beim CFB-Verfahren, beim OFB-Verfahren nicht möglich. Allerdings hat das OFB-Verfahren die gravierende Schwäche, dass ein Fehler im Schieberegister den gesamten nachfolgend verschlüsselten Text unbrauchbar macht.

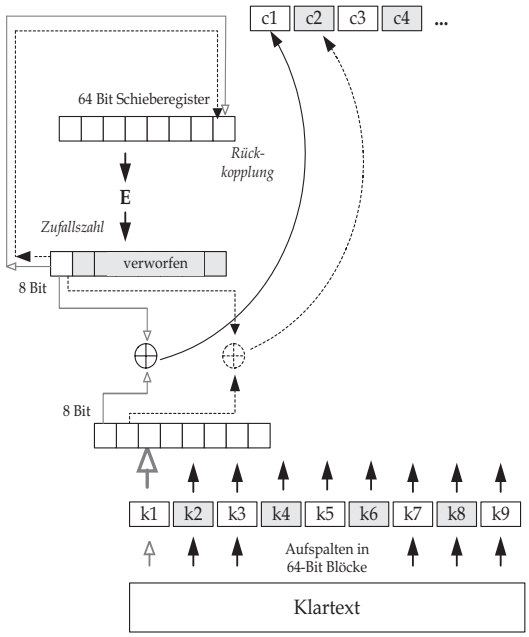


Abb. 4.5: Darstellung des OFB-Verfahrens für K1 und K2 (gestrichelt)

Zusammenfassung

Alle vorgestellten Verfahren (ECB, CBC, CFB, OFB) haben ihre Stärken und Schwächen. Bezogen auf den *Data Encryption Standard* (DES) hat jedoch jedes Verfahren sinnvolle Anwendungsmöglichkeiten. Bevor detailliert auf DES in Abschn. 4.2.2 eingegangen wird, gibt Tab. 4.3 einen Überblick der verschiedenen

Blockmodi. Die Diskussion der Anwendungsmöglichkeiten (Tab. 4.3) schließt mit einigen Überlegungen zur Fehlerfortpflanzung. Es wird gezeigt, wie sich im Chiffrat enthaltene Fehler auf den durch die Dechiffrierung erzeugten Klartext auswirken. Dabei wird zwischen einer Bitmodifikation[19] und Sychronisationsfehlern bzw. Löschen oder Einfügen einer bestimmten Anzahl von Bits differenziert. Die Fehlerfortpflanzung verhält sich in den verschiedenen Blockmodi recht unterschiedlich. Nachfolgend sind die Hauptmerkmale aufgeführt.

ECB:

1. Jede Bitmodifikation in einem Block des Chiffrates beeinflusst den vollen zugehörigen Klartextblock.
2. Synchronisationsfehler sind nicht behebbar.

CBC:

1. Jede Bitmodifikation in einem Block des Chiffrates beeinflusst den vollen Klartextblock und zusätzlich das korrespondierende Bit in seinem Nachfolger.
2. CBC ist selbstsynchronisierend, sofern vollständige Geheimtextblöcke eingefügt oder gelöscht werden, andernfalls sind Synchronisationsfehler nicht behebbar. Ein gelöschter bzw. ein zusätzlich eingefügter kompletter Geheimtextblock verursacht jeweils zwei aufeinanderfolgende fehlerhafte Klartextblöcke. Dabei ist der erste dieser beiden Blöcke leer:

   (a) Das Löschen vom Geheimtextblock c_n hat zur Folge, dass k_n im dechiffrierten Klartext überhaupt nicht und k_{n+1} verfälscht erscheinen.

   (b) Das Einfügen eines zusätzlichen Geheimtextblocks c_x zwischen c_n und c_{n+1} bewirkt beim dechiffrierten Klartext ein Hinzufügen des zusätzlichen Blocks k_x sowie die Verfälschung des unmittelbar nachfolgenden Blocks k_{n+1}.

   Anschließend arbeitet die Entschlüsselung wieder fehlerfrei, da zur korrekten Dechiffrierung jedes Chiffratblocks c_n lediglich dieser selbst (also c_n) sowie sein unmittelbarer logischer Vorgänger c_{n-1} unverfälscht vorliegen und gemeinsam bei der Entschlüsselung Verwendung finden müssen. Dies gilt auch für eventuell weiter vorn aufgetretene Fehler, die keinen Einfluss auf die Entschlüsselung des aktuellen Geheimtextblocks haben.

***n*-Bit CFB:**

1. Jede Bitmodifikation beeinflusst das korrespondierende Bit des Klartextes sowie die nachfolgenden n-Bit-Einheiten, bis das inkorrekte Bit das Schieberegister wieder verlassen hat. Bei einer 64 Bit Chiffre-Blocklänge und wenn n den Wert 8 besitzt (8-Bit CFB), heißt dies, dass jene 8 Byte fehlerhaft dechiffriert werden, die dem Byte folgen, das das inkorrekte Bit enthielt.

[19] Aus 0 wird 1 und umgekehrt, da DES ausschließlich im ASCII-Code arbeitet.

2. Der n-Bit CFB ist selbstsynchronisierend, falls es sich bei der Anzahl der eingefügten bzw. gelöschten Bits um ein ganzzahliges Vielfaches von n handelt. Nach einer bestimmten Anzahl von Schritten befinden sich wieder korrekte Werte im Schieberegister, so dass eine fehlerfreie Dechiffrierung erfolgt.

***n*-Bit OFB:**

1. Eine Bitmodifikation beeinflusst nur das korrespondierende Bit des Klartextes.
2. Synchronisationsfehler sind nicht zu beheben.

Die Tabelle 4.3 gibt einen Überblick über die zentralen Eigenschaften der verschiedenen Blockmodi. Diese spielen wiederum für den symmetrischen Verschlüsselungsalgorithmus DES eine wichtige Rolle.

Tabelle 4.3: Vergleich der verschiedenen Blockmodi

Chiffriertyp	Beschreibung	Anwendung
Elektronisches Codebuch (ECB)	Jeder 64-Bit Block vom Klartext ist untereinander unabhängig mit demselben Schlüssel chiffriert. Synchronisationsfehler sind zu beheben.	■ Sichere Übertragung eines Einzelwertes (z.B. Schlüssel).
Blockchiffre mit Blockverkettung (CBC)	Es wird eine Verkettung erreicht, indem der Chiffrieralgorithmus die XOR-Funktion den nachfolgenden 64-Bit Block des Klartextes mit dem vorhergehenden 64-Bit Block des Chiffrates verknüpft.	■ Allgemein anwendbar für blockorientierte Übertragungsverfahren. ■ Authentifizierung
Schlüsseltextrückführung (CFB)	Arbeitet in Echtzeit.	■ Allgemein anwendbar für blockorientierte Übertragungsverfahren ■ Authentifizierung ■ z.B. Telnet
Ergebnisrückführung (OFB)	Ähnlich wie CFB, jedoch ist der jeweilige Input in den Chiffrieralgorithmus der vorangehende Output des DES Algorithmus.	■ Stromorientierte Übertragung bei verrauschten Kanälen (z.B. Satellitenkommunikation).

4.2.2 DES, Triple DES, IDEA und AES

Nach den unterschiedlichen Aspekten der Blockchiffrierung werden jetzt die in der Praxis häufig eingesetzten Verfahren diskutiert. Derzeit sind DES und Triple DES in VPN-Produkten weit verbreitet. Interessant ist die Entwicklung um den neuen *Advanced Encryption Standard* (AES).

Im Gegensatz zur nichtöffentlichen Evaluation des DES-Algorithmus, der eigentlich von IBM in dem Projekt Lucifer[20] entwickelt wurde, wurden nun für den Nachfolger von DES etliche Algorithmen in einem dreistufigen öffentlichen Zyklus evaluiert. Inzwischen ist das Verfahren beendet und der Algorithmus Rijndael hat das Etikett Advanced Encryption Standard (AES) erhalten [Daemen und Rijmen, 1999]. Nicht nur für künftige VPN-Verschlüsselungssoftware wird dieser neue Standard eine erhebliche Rolle spielen, sondern es werden wahrscheinlich sämtliche Applikationen, die eine symmetrische Verschlüsselungskomponente enthalten, diesen Algorithmus einsetzen. Für den VPN-Einsatz spricht die deutliche bessere Performance gegenüber dem alten DES-Algorithmus.

Die nachfolgend beschriebenen symmetrischen Kryptosysteme müssen bei der Chiffrierung die eindeutige Abbildung der Menge aller möglichen Klartexte auf die Menge der möglichen Geheimtexte zulassen, da sonst keine eindeutige Verschlüsselung mehr durchführbar wäre. Allerdings müssen sämtliche Beziehungen zwischen Klartext, Geheimtext und Schlüssel verborgen bleiben.

Gerade die in einem üblichen Klartext enthaltenen Redundanzen von Wörtern bzw. bestimmten Buchstabenkombinationen müssen auf den Geheimtext nahezu zufällig verteilt sein. Wie schwierig dies ist, hat der Exkurs in die klassische Kryptographie (Abschn. 4.1) gezeigt.

In der Regel wird eine Konfusion und Diffusion nach dem Vorschlag von [Shannon 1949] durchgeführt. Am einfachsten erfolgt eine Konfusion durch eine geeignete Substitution. Eine Diffusion wird erreicht, wenn jedes Bit des Klartextes sowie des Schlüssels eine maximal mögliche Anzahl von Bits des Chiffrats beeinflusst. In Ergänzung zur Konfusion trägt dies zum Verbergen statistischer Zusammenhänge bei und erschwert eine Kryptoanalyse. Die typische hierfür verwendete Technik ist die Transposition (Abschn. 4.1.2), bei der die Reihenfolge der Buchstaben geschickt vertauscht wird.

---

[20] Lucifer war der Name eines Projektes von IBM, das in der 70er Jahren von einem Kryptographenteam durchgeführt wurde. Zu dem Team gehörten unter anderem Don Coppersmith und Horst Feistel. Von Horst Feistel wurde dabei das später nach ihm benannte Feistel-Netzwerk entwickelt. Ziel des Projektes war die Entwicklung einer Verschlüsselungstechnologie, die sich leicht in Hardware implementieren lässt und die außerdem effizient arbeitet. Diese Kriterien setzen voraus, dass nur elementare Prozessoroperationen auszuführen sind und der Speicherbedarf gering ist. Um die Sicherheit zu gewährleisten, muss der Algorithmus Schlüssel aus einem großen Schlüsselraum verwenden können. Die Sicherheit darf dabei nur von der Wahl des Schlüssels und nicht vom Algorithmus selbst abhängig sein, um das Problem der Geheimhaltung des Algorithmus zu vermeiden. Lucifer war das Ergebnis des Entwicklungsprozesses. Er verwendete nur elementare Prozessoroperationen (XOR, ADD,...) und verschlüsselte mit 128 Bit (inklusive Parität), d.h. es gibt 2^{112} verschiedene Schlüssel. Da er auf Feistel-Netzwerken basierte, war auch der Speicherbedarf gering. Damit war die Bedingung für eine effiziente Implementierung erfüllt. IBM reichte Lucifer als Vorschlag auf eine Ausschreibung des NBS (National Bureau of Standards) ein. In dieser Ausschreibung wurde nach einer Verschlüsselungstechnologie für klassifizierte Dokumente der amerikanischen Behörden gesucht, die als offizieller Standard eingeführt werden konnte. Jedoch wurde die vorgeschlagene 128-Bit-Verschlüsselung (inklusive Parität) vom NBS nicht übernommen. Heutzutage gehen noch etliche in Anwendung befindliche Verfahren auf ein Feistel-Netzwerk zurück, so z.B. DES, FEAL, Blowfish, Lucifer, Khufu, Khafree, LOKI, GOST und CAST.

Bereits Shannon hat erkannt, dass durch geeignete Kombinationen von relativ schwachen kryptographischen Verfahren wesentlich stärkere Verfahren entwickelt werden können. Für eine aus Kombinationen hervorgegangene Chiffre prägte Shannon den Begriff Produktchiffre, *Product Cipher*. Die Blockalgorithmen (ECB, CBC, CFB, OFB) gehören zur Klasse der Produktchiffren. Sie verwenden wiederholt und in jeweils verschiedenen Kombinationen unterschiedliche Konfusions- und Diffusionstechniken.

DES

DES steht für Data Encryption Standard und wurde vor mehr als 20 Jahren in den USA zum Federal Standard erhoben und hat erstaunlich lange einer Vielzahl gegen ihn gerichteter kryptoanalytischer Attacken[21] standgehalten. Man hatte seinerzeit das Kerckhoffsche Prinzip berücksichtigt und den DES-Algorithmus veröffentlicht ([NBS 77] oder auch [Landau 2000]).

Inzwischen ist DES allerdings nicht mehr zeitgemäß. Seine primäre Schwäche ist die für heutige Verhältnisse viel zu geringe Schlüssellänge von 56 Bit. Nachdem der Aufwand zum Brechen von DES-Verschlüsselungen mit zunehmender Leistungsfähigkeit der Rechner sowie durch immer günstiger werdende Preise für Computertechnik sinkt, sollte DES so schnell wie möglich gegen ein starkes Verfahren mit deutlich längeren Schlüsseln, z.B. 128 Bit oder mehr, ersetzt werden. Ist allerdings eine Anwendung an DES gebunden und ein Verschlüsselungswechsel derzeit nicht durchführbar, empfiehlt es sich, durch einfach zu implementierende Maßnahmen – wie beispielsweise häufigen Schlüsselwechsel, zufälliges Padding (Einfügen zufälliger Bytes in die Nachricht) und anschließende Komprimierung des Klartextes zur Reduzierung der Redundanz – den Aufwand für den Angreifer erheblich zu erhöhen.

Auch wenn ihre Bedeutung allmählich abnimmt, lohnt es sich, einen genaueren Blick auf die immer noch populäre DES-Verschlüsselung zu werfen. Denn neben dem Einsatz in einigen VPN-Produkten wird das DES-Verfahren breitflächig in Routern und auch im Bankenbereich (Euroscheckkarte) eingesetzt. Die monoalphabetische Chiffrierung DES verschlüsselt nicht Buchstaben, sondern die Ziffern bzw. Symbole 0 und 1, und zwar jeweils 64 in einem Block. Demzufolge werden bei einer Verschlüsselung von Buchstaben diese zuerst mittels ASCII-Code[22] in Bitfolgen, bestehend aus 0 und 1, überführt. Somit ist leicht einzusehen, dass DES ein monoalphabetischer Algorithmus über das Alphabet $(a_1, ..., a_64)$ ist und jedes a_i nur Elemente von $(0, 1)$ enthält. Daraus ergibt sich, dass die Elemente des Klar- und des Geheimtextalphabets die gleiche binäre Länge von 64 haben.

---

[21] In der berühmten Arbeit von [Biham und Shamir 1993] ist der DES-Algorithmus intensiv analysiert worden. 1998 ist es der *Electronic Frontier Foundation* (EFF) gelungen, die dritte DES-Challenge zu lösen, indem es eine im Wesentlichen von Paul C. Kocher entworfene, auf das Suchen von DES-Schlüsseln spezialisierte Maschine einsetzte. Es gelang, den gesuchten DES-Key in ca. 56 Stunden zu ermitteln. Anfang 1999 wurde ein DES-Schlüssel in ca. 22 Stunden mit einer *Known-PlainText-Attack* durch vollständige Suche (*Brute-Force*) gefunden.

[22] Der allgemein bekannte ASCII-Code liegt jedem Tastaturanschlag zugrunde. So wird z.B. der Buchstabe A in (01000001), der Buchstabe B in (01000010) vom Computer binär interpretiert.

Als Schlüssel kommt jede 56 Bit[23] lange Zahl in Frage, die jederzeit geändert werden kann. Bei einem Schlüssel können also *alle* binären Folgen auftreten; es gibt genau 2^{56} oder auch ungefähr $7*10^{16}$ verschiedene Schlüssel. Einige Zahlen gelten als schwache Schlüssel, doch diese lassen sich leicht vermeiden.

Eine effektive Substitution innerhalb der zentralen Verschlüsselungsfunktion (f) (Abb. 4.7) wird durch die Bildung von acht verschiedenen 6×4-Bit-S-Boxen[24] erreicht, die mit L_0 und R_0 bezeichnet werden. Zuvor wird ein 8-Byte-Klartextblock einer kryptographisch unbedeutenden Eingangspermutation unterzogen, die schlüsselunabhängig ist. Abb. 4.6 zeigt den Ablauf der DES-Chiffrierschritte. Die Eingangspermutation (P) dient im Wesentlichen zur Aufspaltung der Klartextblöcke in je zwei 32 Bit (L_0, R_0) Blöcke. Nach 16 identischen Iterationsrunden ($i = 1, 2, 3, \ldots, 16$) wird die inverse Permutation (P^{-1}) durchgeführt. Dabei stellt f die symmetrische Verschlüsselungsfunktion mit den beiden Eingangswerten (L_i, K_i) bzw. (R_i, K_i) dar (Abb. 4.6). Die Funktion f beinhaltet die Hauptkomponente im DES-Algorithmus. Sie kombiniert einerseits die jeweilige (linke oder rechte) Hälfte mit dem rundenabhängigen Schlüssel K_i und verknüpft anschließend über XOR den jeweiligen anderen 32 Bit Block der Runde. Andererseits findet eine nichtlineare Durchmischung statt. Abb. 4.7 zeigt die acht S-Boxen der f-Funktion, die zunächst auf 48 Bit erweitert werden. Diese 48 Bit werden als Eingangsgrößen in insgesamt acht S-Boxen, zu je 6 Bit, verarbeitet. Allerdings verlassen nur insgesamt 32 Bit als Ergebnis die acht S-Boxen. Somit findet eine Bit-Reduzierung bei gleichzeitigem Austausch statt.

Jede der acht S-Boxen hat vier Zeilen mit einer Verteilung von je 2^4 Einträgen (Abb. 4.7). Soll beispielsweise die Eingangsziffer 25 binär **0**1100**1** substituiert werden, geschieht Folgendes: Das erste und letzte Bit der binären Ziffer 25, also **0** und **1**, werden abgespalten (vgl. **0**1100**1** eine Zeile zuvor). Dadurch wird die Zeile (hier die 1. in Abb. 4.7) bestimmt, die weiter verwendet wird. In der ersten Zeile (01)[25] wird die Position bzw. die Spalte binär 1100 der S-Box aufgesucht – die 12. Spalte – und der Wert, der dann in der 1. Zeile (01) steht, substituiert. Es ist die 09 – binär 1001 – und wird als 4 Bit Ausgangsgröße der S_3-Box definiert.

Interessant ist die Frage, wie die Ziffern bzw. Zahlenfolgen in den vier Zeilen der S-Box, also die 2^4 Einträge, zu Stande kommen. Sie sind willkürlich gewählt und für jede der acht S-Boxen bei DES festgelegt. Durch die Festlegung lässt sich der Vorgang umkehren, was bei einer Dechiffrierung notwendig wird. Weiterhin tritt bei den S-Boxen der Lawineneffekt zu Tage, indem bei einer kleinen Änderung der Eingangsbits die Hälfte der Ausgangsbits geändert werden.

Die Wahl der S-Boxen ist keineswegs trivial, wie viele Vorschläge etlicher Kryptologen zeigen. Jedoch gilt allgemein, dass, je größer die Anzahl der Einträge der

---

[23] Aus Paritätsgründen muss der eigentliche 64 Bit-Schlüssel auf 56 reduziert werden.

[24] S-Boxen stellen in der Regel den einzigen nichtlinearen Schritt eines Algorithmus dar und beeinflussen die Sicherheit des Verfahrens maßgeblich. Es gibt unterschiedliche Ansätze, S-Boxen zu wählen. So z.B. die S-Box zufällig zu wählen, wobei jedoch mindestens 8 Input-Bits gewählt werden müssen.

[25] Es resultieren bei 2-Bit genau vier mögliche (00,01,10,11) Zeilen.

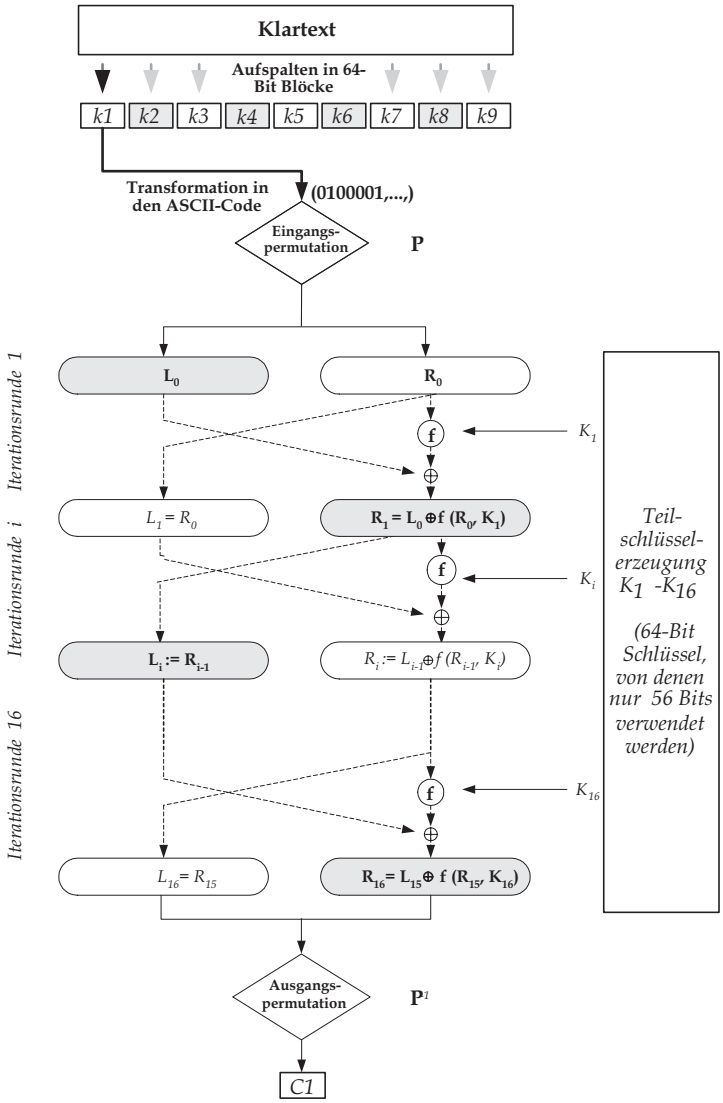


Abb. 4.6: Darstellung des DES-Chiffriervorgangs

S-Boxen ist, um so besser eine nichtlineare Durchmischung erfolgt. Als untere Grenze hat sich im Lauf der Zeit eine Eingangsgröße von 8 Bit ergeben. Weiterhin hat sich als sinnvoll erwiesen, die Boxen wie bei der f-Funktion bei DES schlüsselabhängig zu gestalten.

Obwohl das NBS den Data Encryption Standard nach einer kontrovers geführten Debatte 1992 nicht wieder als Standard bestätigen wollte, wurde DES in Erman-

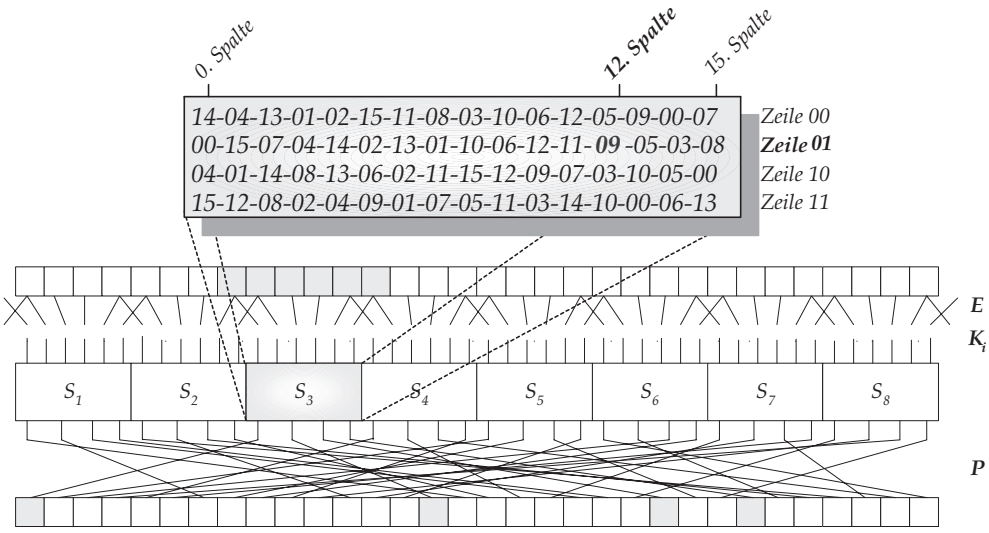


Abb. 4.7: Zentrale f-Funktion des DES-Algorithmus

gelung einer echten Alternative im Jahr 1993 für weitere fünf Jahre als Standard verabschiedet.

4.2.3 Triple DES

Unter *Triple DES* wird ein Ansatz verstanden, der den DES-Algorithmus durch Mehrfachverschlüsselung sicherer macht. Ziel ist, die bisher getätigten Investitionen in DES-basierte Soft- und Hardware zu schützen. Gerade für VPN-Gateways, die ausschließlich mit DES arbeiten, ist dies eine probate Methode. Das Problem der relativ kurzen Schlüssel wird durch Anwendung mehrerer DES-Operationen (Ver- und Entschlüsselungen) mit verschiedenen Schlüsseln gelöst. Diese inzwischen generell anerkannte Methode wird oft als EDE (*encrypt-decrypt-encrypt*) bezeichnet.

Es gibt verschiedene Formen des Triple DES. Einige nutzen zwei Schlüssel, andere setzen drei verschiedene 56 Bit-Schlüssel ein. Dadurch wird eine effektive Schlüssellänge von 112 bzw. 168 Bit erreicht. Werden beispielsweise zwei Schlüssel benutzt, so heißt dies, dass für die beiden Verschlüsselungsoperationen dieselben Schlüssel eingesetzt werden. Gleichung 4.6 zeigt den Ablauf des Chiffrierens für einen Klartextblock K_1.

$$C_1 = E_{Sch_1} \times (D_{Sch_2} \cdot [E_{Sch_1} \cdot K_1]) \tag{4.6}$$

Damit ist C_1 das 64-Bit-Chiffrat des Klartextblocks K_1. Sch_1 und Sch_2 bezeichnen die unterschiedlichen Schlüssel. E_{Sch_1} beschreibt den Verschlüsselungsvorgang

mit dem ersten Schlüssel. D_{Sch_2} beschreibt den Entschlüsselungsvorgang mit dem zweiten Schlüssel. Wenn die in Gleichung 4.6 beiden unterschiedlichen Schlüssel gleich gewählt werden, wird eine einfache DES-Operation ausgeführt. Damit ist eine Interoperabilität mit konventionellen DES-Systemen gegeben. Eine Transformation des Chiffratblockes C_1 sieht dann wie in Gleichung 4.7 beschrieben aus:

$$K_1 = D_{Sch_2} \times (E_{Sch_2} \cdot [D_{Sch_1} \cdot C_1]) \tag{4.7}$$

Allerdings führt nicht bei allen Blockalgorithmen diese Mehrfachverschlüsselung zu einer Sicherheitserhöhung. Dies hängt von der algebraischen Struktur ab. Handelt es sich bei einem Verfahren im algebraischen Sinne um eine *Gruppe*[26], so lässt sich für jedes Schlüsselpaar (Sch_1, Sch_2) ein Sch_3 erzeugen, so dass

$$ESch_2\,(E_{Sch_1} \cdot K_1) = E_{Sch_3} \cdot K_1 \tag{4.8}$$

gilt. Wenn vermeintlich mit 112 Bit verschlüsselt wird, kann es also bei falscher Schlüsselwahl ungünstigerweise passieren, dass DES aufgrund der Gruppeneigenschaften vorliegt. Somit kann unter Umständen eine trügerische Sicherheit entstehen. Es hat lange gedauert, bis der Nachweis, dass DES zu einer algebraischen Gruppe gehört, gelungen war. Dies wurde zwar immer angenommen, jedoch erst 1992 explizit nachgewiesen.

Deutlich wird hier auch eine Schwierigkeit für VPN-Gateways: Werden sie von unterschiedlichen Herstellern geliefert, können beide Geräte mit Triple DES arbeiten. Nutzt jedoch einer der Hersteller zwei und der andere drei Schlüssel, können sie die ausgetauschten Daten nicht entschlüsseln. Somit sind Geräte, die Triple DES nutzen, zunächst einem Schlüsseltest auf Kompatibilität zu unterziehen.

4.2.4 IDEA

Beim IDEA (*International Data Encryption Algorithm*) handelt es sich um einen relativ neuen blockorientierten symmetrischen Verschlüsselungsalgorithmus. Der Algorithmus wurde von Xuejia Lai und James L. Massey an der ETH Zürich in den Jahren 1990-1991 entwickelt. Eine anfängliche Version hielt einer differentiellen Kryptoanalyse nicht stand, so dass durch eine Optimierung und über den Umweg der Namensvariante IPES (*Improved Proposed Encryption Standard*) schließlich im Jahre 1992 die heutige Version IDEA entstand.

Nach der Meinung vieler Kryptologen ist IDEA einer der besten und sichersten Blockalgorithmen, die derzeit zur Verfügung stehen. Das Verfahren ist in Europa und in den USA patentiert. Für kommerzielle Anwendungen wird daher eine Lizenz vom Patentinhaber, der Schweizer Ascom-Tech AG, fällig. Zur Anwendung kommt IDEA im Sicherheitswerkzeug PGP (*Pretty-Good-Privacy*), bei der

[26] Für eine algebraische Gruppe gilt, wenn a, b, c Elemente dieser Gruppe sind, dass $(ab) \cdot c = a \cdot (bc)$ ist. Weiterhin existiert ein neutrales Element, so z.B. $ea = a$, und zu jedem a gibt es ein Inverses $a^{'}$ mit $a^{'}a = e$.

SecureShell (SSH)[27] und SSL bzw. TLS[28]. IDEA ist genau wie DES ein Blockalgorithmus, der 64-Bit-Blöcke mit demselben Schlüssel ver- bzw. entschlüsselt und dabei acht Runden durchläuft. Anschließend wird eine Output-Transformation durchgeführt. Die Schlüssel sind 128 Bit lang und damit länger als bei DES.

Durch eine neue Design-Philosophie lässt sich IDEA auf 16-Bit-Prozessoren recht effizient implementieren, obgleich die Multiplikationen nicht gerade ressourcenfreundliche Operationen sind. Aktuelle Software-Implementierungen des IDEA sind nach Aussagen von [Schneier 1996] ungefähr doppelt so schnell wie vergleichbare DES-Realisierungen. Damit verfügt der IDEA-Algorithmus eigentlich über alle Voraussetzungen, um für eine VPN-Gateway-Implementierung geeignet zu sein. Die Vorteile des IDEA-Algorithmus liegen auf der Hand: IDEA ist bei längeren Schlüsseln schneller und damit auch sicherer als DES. Jedoch wird IDEA eher selten in eine VPN-Lösung[29] integriert. Möglicherweise liegt dies an der Lizenzpolitik von ASCOM.

4.2.5 AES

AES ist kein Verschlüsselungsalgorithmus, wie vielleicht vermutet werden könnte. AES heißt *Advanced Encryption Standard* und steht für die Nachfolge von DES. In einem öffentlichen Auswahlverfahren von August 1998 bis Oktober 2000 wurde ein geeigneter Algorithmus gesucht, der den DES-Algorithmus ersetzen sollte. Als Prämisse galt, dass ein frei verfügbarer symmetrischer 128-Bit-Blockchiffre benutzt werden sollte.

Jeder Algorithmus, der die erste Runde schaffen wollte, musste Schlüssellängen von 128, 192 und 256 Bits unterstützen. Unter den Teilnehmern aus Australien, Belgien, Kanada, Costa Rica, Frankreich, Japan, Südkorea, den USA, Großbritannien, Israel und Norwegen war auch Deutschland vertreten. Die Telekom hatte einen Algorithmus mit dem Namen Magenta ins Rennen geschickt. Nicht nur der Ausrichter, das NIST (*National Institute of Standards and Technology*), sondern auch die weltweite Kryptogemeinde analysierten die eingereichten Algorithmen wie LOKI97, RIJNDAEL, CAST-256, DEAL, FROG, DFC, E2, Crypton, Magenta, HPC, Mars, RC6, SAEFER+, TWOFISH und SERPENT. In der zweiten Runde blieben nur fünf Algorithmen übrig, und zwar drei Entwicklungsgruppen aus den

---

[27] SSH ist ein Remote-Login-Protokoll, das von dem finnischen Informatiker Tatu Ylönen entwickelt wurde. Es ist ein kryptographisches Protokoll, das sich durch ein sehr hohes Sicherheitsniveau auszeichnet.

[28] SSL steht für *Secure Socket Layer* und ist im Grunde nur durch ein Internet-Draft beschrieben. Ein RFC zu SSL existiert nicht; anders als SSH ist SSL kein eigenständig nutzbares Protokoll. Jedoch hat SSL (z.B. Version 3.0) eine erhebliche Bedeutung erlangt. Jeder heutzutage gängige Browser sowie verschiedene WWW-Server unterstützen SSL. Eine Weiterentwicklung erfährt SSL in dem *Transport Layer Security*-Protokoll in der Version 1.0. Es wird erwartet, dass TLS seinen Vorgänger SSL in nicht allzu ferner Zukunft ablösen wird.

[29] So wird IDEA bisher nur in der LineCrypt-Produktfamilie der Deutschen Telekom und in dem Siemens-Produkt, TranSON, verwendet.

USA, eine belgische und eine international besetzte Gruppe. Es handelte sich um namhafte und bekannte Kryptologen, die ihre Algorithmen in die letzte Runde schicken konnten:

- *MARS* wurde von IBM in Armonk, New York entwickelt.
- *RC6* wurde von RSA Laboratories in Bedford, Massaschusetts entworfen.
- *RIJNDAEL* stammt von Joan Daemen und Vincent Rijmen aus Belgien.
- *SERPENT* ist aus dem internationalen Team, bestehend aus Ross Anderson, Eli Biham und Lars Knudsen aus Großbritannien, Israel und Norwegen, hervorgegangen.
- *TWOFISH* ist aus einem Kreis entstanden, der sich fast ausschließlich um Bruce Schneiers Firma Counterpane Internet Security Inc. in Minneapolis gebildet hat.

Im Oktober 2000 wurde der Sieger bekannt gegeben. Gewonnen hatte der Algorithmus RIJNDAEL, der nach Mitteilungen des NIST im Sommer 2001 als neuer Standard endgültig verabschiedet wurde. Dieser neue Algorithmus wird aller Voraussicht nach eine weitreichende Verbreitung erfahren – ähnlich wie seinerzeit DES.

4.2.6 RIJNDAEL

Hinsichtlich der kryptoanalytischen Attacken boten alle fünf Finalisten vergleichbar gute Ergebnisse. Bei der Performanceanalyse bot der Rijndael-Algorithmus auf breiter Ebene jedoch hervorragende Resultate und trug so den Sieg davon. Sowohl bei Software- als auch Hardware-Implementierungen auf unterschiedlichen Plattformen (Unix, Intel) belegte der Rijndael-Algorithmus die ersten Ränge. Gleichzeitig sind die Anforderungen an Ressourcen aufgrund der sehr niedrigen Speicheranforderungen erfreulich niedrig.

Der Rijndael-Algorithmus [Daemen und Rijmen, 1999] basiert nicht auf einem Feistel-Netzwerk (wie DES), sondern schreibt Datenblocks und Schlüssel je nach Länge in 4x4, 4x6 bzw. 4x8 Matrizen einzelner Bytes. Er arbeitet mit 128, 192 und 256 Bit-Schlüsseln und Blocklängen, die, von der Schlüssellänge unabhängig, ebenfalls 128, 192 oder 256 Bit lang gewählt werden können (Abb. 4.8). Die Anzahl der durchlaufenen Iterationen beträgt je nach Schlüssel- und Blocklänge 10, 12 bzw. 14 Runden. Im Folgenden soll eine Iteration für eine Schlüssel- und Blocklänge von 128 Bit, also für 4x4 Byte-Matrizen beschrieben werden. Jede Iteration besteht aus vier einfachen Operationen (Abb. 4.8). Zunächst wird jedes Byte mittels einer vorgegebenen S-Box, die entsprechend 256 Einträge enthält, substituiert. Der zweite Schritt beinhaltet eine zyklische Verschiebung innerhalb der Zeilen der 4x4 Byte Matrix.

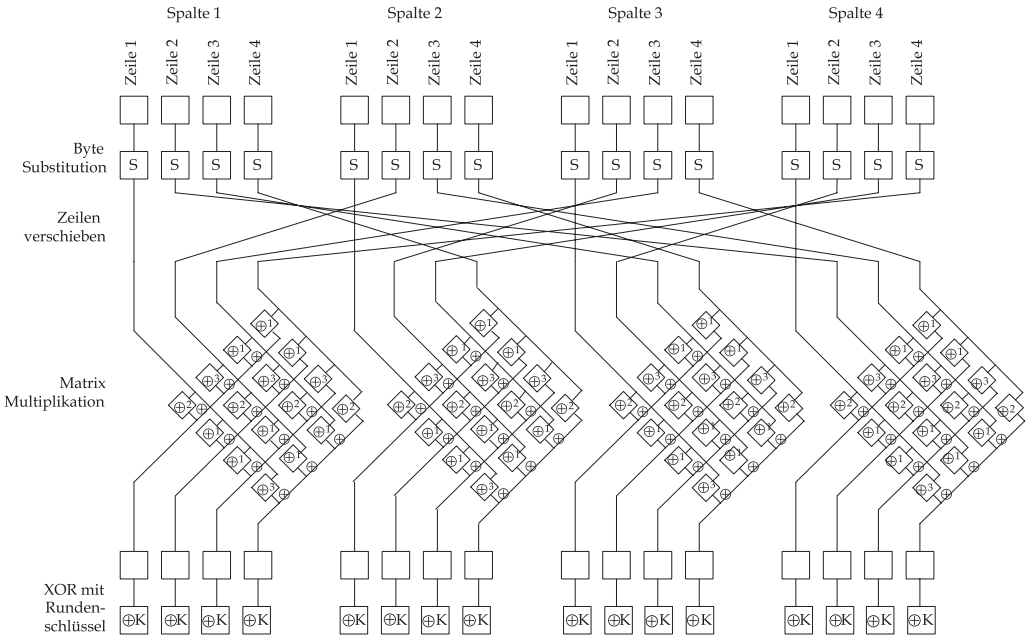


Abb. 4.8: Schema einer Runde des Rijndael-Algorithmus

Die Elemente der ersten Zeile werden nicht, die der zweiten Zeile um eine, die der dritten Zeile um zwei und die der vierten Zeile um drei Elemente nach links verschoben. Der dritte Schritt besteht aus einer Multiplikation der Spalten mit einer vorgegebenen Matrix und der vierte Schritt beinhaltet eine XOR-Verknüpfung der 128 Bit in der 4x4 Byte-Matrix mit dem rundenabhängigen Schlüssel. Die Multiplikationsoperationen $\otimes 2$ und $\otimes 3$ bedürfen dabei einer Erklärung. Die Operation $\otimes 2$ bedeutet einen Bitshift um ein Bit nach links wie bei einer normalen binären Multiplikation mit 2. Weist das Ergebnis allerdings dadurch 9 Bit auf, wird es mit der Binärzahl 100011011 per XOR ($\oplus$) verknüpft. Die Operation $\otimes 3$ erhält man, wenn das Ergebnis der Operation $\otimes 2$ zum Ausgangswert per XOR addiert wird. Die oben gezeigten vier Schritte sind die Hauptbestandteile des Rijndael-Algorithmus, da sie in dieser Anordnung eine Runde des Verschlüsselns zeigen. Diese Runden werden noch umgeben von einer Eingangsaddition ($\oplus$) mit einem Rundenschlüssel und einer nicht ganz vollständigen letzten Runde, bei der die Matrixmultiplikation der Spalten entfällt. Außerdem ist die Ver- und Entschlüsselung beim Rijndael-Algorithmus nicht symmetrisch, so dass zum einen die Implementierung in Hardware etwas aufwändiger wird und zum anderen die Performance beim Entschlüsseln etwas schwächer als beim Verschlüsseln ist.

Allen fünf Finalisten wurde eine ausreichende Sicherheit gegen kryptoanalytische Attacken attestiert, so dass die Entscheidung schwerpunktmäßig auf dem zweiten Kriterium, dem der Performance basieren musste. Tab. 4.4 zeigt die in

drei Kategorieren eingeteilten Geschwindigkeitsergebnisse. Zwischen den Finalisten wurde das Geschwindigkeitsverhalten in (Kbits/s) bei der Ver- und Entschlüsselung sowie die Schlüsselinitialisierung auf unterschiedlichen Hardware- (Intel-Computer, Apple G4, Hewlett Packard, Compaq, SGI, Z80 CPU, Texas Instruments DSP, Smart Cards (ARM)) und Softwareplattformen (C, Assembler, Java) gemessen. Hierbei bietet der Rijndael-Algorithmus auf breiter Ebene hervorragende Ergebnisse. In der Hardware ist der Rijndael-Algorithmus seinen Kon-

Tabelle 4.4: Performance-Vergleich zwischen den fünf Finalisten gemessen über alle Disziplinen

	Encryption und Decryption	**Schlüsselverhalten**
MARS	II	II
RC6	I	II
Rijndael	I	I
Serpent	III	II
Twofish	II	III

trahenten in vielen Implementierungen deutlich überlegen. Teilweise ist der Algorithmus dreimal so schnell wie der Nächstbeste und bis zu 10-mal schneller als der langsamste Kandidat [Lipmaa 2000]. Diese äußerst gute Performance auf einer breiten Basis hat den Ausschlag für die Wahl von Rijndael als AES gegeben. Theoretische Attacken gegen den Rijndael-Algorithmus mit nur sieben Iterationen gegenüber den vorgesehenen 10, 12 und 14 Iterationen werden von [Gilbert 2000] und [Lucks 2000] berichtet. Der Aufwand für eine tatsächliche Attacke wird aber als extrem hoch eingestuft, so dass als Fazit gegen den Algorithmus keine Sicherheitsbedenken geäußert werden.

4.3 Asymmetrische Kryptosysteme

Die asymmetrische Verschlüsselung, auch als *Public-Key-Kryptographie* bekannt, bedeutet, dass zum Ver- und Entschlüsseln zwei unterschiedliche Schlüssel benutzt werden müssen. Dabei kann der Schlüssel, der zur Verschlüsselung genutzt wird, öffentlich bekannt sein. Diese revolutionäre Erkenntnis rückte die Zahlentheorie und damit einen bislang verborgenen Zweig der Mathematik ins Zentrum des öffentlichen Interesses, was niemand vorher für möglich gehalten hätte. Ein neues Zeitalter der Kryptographie begann. Die moderne Kryptographie liefert die Schlüssel und Schlösser des Informationszeitalters und bildet somit einen Eckpfeiler des Interneterfolges. Die postindustrielle Ära stützt sich auf Informationen – die heute wertvollste Ware. Der Austausch digitaler Informationen ist zu einem wichtigen Bestandteil unserer Gesellschaft geworden. Anwendungsgebiete der modernen Kryptographie sind unter anderem die digitale Signatur, die Public-Key-Infrastruktur und die VPN-Technologie.

4.4 Schlüsselaustausch-Verfahren

Der Schlüsselaustausch, der schon bei Cäsar (Abschn. 4.1.1), aber auch noch im *Zweiten Weltkrieg* und lange danach ein immenses, schier unlösbares Problem darstellte, ist durch [Diffie und Hellman 1976] gelöst worden. Allerdings ist im Prinzip das Verfahren des Schlüsselaustausches schon einige Jahre vorher in England entdeckt worden. Das *Government Communication Headquarter* (GCHQ) wurde mit dem Problem des Schlüsselaustausches schon 1969 vom britischen Militär beauftragt, als sich abzeichnete, welche Möglichkeiten eine Miniaturisierung der Funkgeräte nach sich ziehen würden. 1975 hatten James Ellis, Clifford Cocks und Malcom Williamson, die beim GCHQ angestellt waren, hatte alle wesentlichen Elemente der Public-Key-Kryptographie entwickelt, waren jedoch gezwungen, Stillschweigen zu bewahren [Singh 1999]. Interessanterweise wurde das Verfahren zum Schlüsselaustausch von beiden Gruppen völlig unabhängig voneinander entwickelt.

Wollten zuvor zwei Teilnehmer geheime Nachrichten austauschen, mussten sie vorher einen gemeinsamen geheimen Schlüssel vereinbaren. Dies schlug in der Vergangenheit häufig fehl, wie unzählige Zeugnisse belegen. Erst die modernen Methoden der Kryptographie ermöglichen einen verschlüsselten Nachrichtenaustausch von zwei Teilnehmern, die vorher noch nie in Kontakt gestanden haben. Zwei einander eventuell völlig unbekannte Personen oder auch Rechner (VPN-Gateway) können nun ohne vorherigen sicheren Austausch eines gemeinsam genutzten geheimen Schlüssel sofort vertraulich miteinander kommunizieren. Jeder Teilnehmer bzw. jeder Rechner benötigt lediglich den öffentlichen Schlüssel des anderen Partners, dessen Beschaffung keinen sicheren Kanal erfordert, da dieser nicht geheim ist. Nach Aussagen von [Schneier 1996] gibt es lediglich drei Systeme, die sich idealerweise sowohl zur Verschlüsselung als auch für digitale Signaturen eignen: *RSA*, *ELGamal* und *Rabin*. Die beiden erstgenannten werden anschließend diskutiert. Das Rabin-Verfahren hat kaum praktische Bedeutung erlangt.

4.4.1 Diffie-Hellman, RSA, ELGamal, DSA

Diffie-Hellman

Die Public-Key-Kryptographie ist eine noch recht junge Disziplin. Als ihre Erfinder werden Whitfield Diffie und Martin Hellman sowie Ralph Merkle angesehen. Die Public-Key-Kryptographie ist als *Diffie-Hellman-Schlüsselaustausch-Verfahren* in die Literatur eingegangen und ist ebenfalls unter dem Begriff *exponentieller Schlüsselaustausch* zu finden.

Anders als RSA oder ELGamal ist Diffie-Hellman weder zum Ver- und Entschlüsseln von Nachrichten noch für digitale Signaturen geeignet. Es lässt sich jedoch, wie der Name schon andeutet, effizient für den sicheren Austausch eines geheimen Schlüssels über einen unsicheren Kanal (Telefon, Rechnernetz oder

auch Zeitung) einsetzen. Dabei ist nicht erforderlich, dass beide Kommunikationspartner ein gemeinsames Geheimnis (sprich: den Schlüssel) haben müssen. Das Diffie-Hellman-Verfahren kommt im VPN beim Standardsicherheitsprotokoll IPSec (Abschn. 7.4) und dort beim Schlüsselaustausch gemäß IKE (Abschn. 7.4.9) zur Anwendung.

> *Dem Diffie-Hellman-Schlüsselaustausch liegt die fundamentale Idee zugrunde, dass es nicht nötig ist, dem Kommunikationspartner den geheimen Schlüssel auf einem sicheren Kanal bzw. Übertragungsweg zu übermitteln.*

Dies ist von weitreichender Bedeutung, denn – sei es bei Cäsar, im Zweiten Weltkrieg oder später – genau bis 1976 war es notwendig, den geheimen Schlüssel vorab auszutauschen. Er musste, bevor überhaupt verschlüsselt kommuniziert werden konnte, im Vorfeld übermittelt werden. In der Antike wurde der „Schlüssel" auf der kahlgeschorenen Kopfhaut des Kuriers „hinterlegt". Erst nachdem das Kopfhaar nachgewachsen und der Schlüssel vor den Augen Dritter verborgen war, wurde der Kurier losgeschickt. Im Zweiten Weltkrieg übernahmen die sehr gut bewachten Codebücher, die einen täglich wechselnden Codeschlüssel enthielten, diese Aufgabe. Zur Entschlüsselung von Nachrichten, die mit der deutschen Chiffriermaschine (Enigma) verschlüsselt waren, waren die Alliierten auf die Codebücher angewiesen.

[Diffie und Hellman 1976] lösten dieses Problem. Ihr Ansatz basiert auf der Idee, dass es relativ einfach ist, das Modulo einer Primzahl, multipliziert mit einem Exponentialausdruck einer Zahl, zu berechnen. Es ist jedoch nahezu unmöglich, die Umkehrfunktion, also den diskreten Logarithmus der Exponentialfunktion, zu bestimmen, wenn hinreichend große Primzahlen verwendet werden.

Wenn p eine Primzahl ist und g eine natürliche Zahl, so dass gilt $g \leq p-1$, kann die diskrete Exponentialfunktion

$$f(k) = g^k mod\, p \tag{4.9}$$

unter Beachtung von $(1 \leq k \leq p-1)$ gebildet werden. Dabei wird g in der Literatur oft als Generator bzw. Erzeuger oder Primitivwurzel Modulo p bezeichnet. Die Größen (g, p) werden als globale öffentliche Schlüssel oder Elemente definiert.

Hierzu lässt sich die Umkehrfunktion bilden, indem mit

$$dl_g(g^k) = k \tag{4.10}$$

der diskrete Logarithmus (dl_g) von den Größen (g^k) berechnet wird. Als Ergebnis wird die ursprüngliche Eingangsgröße (k) erzielt.

Vor diesem Hintergrund kann nach Diffie-Hellman ein gesicherter Schlüsselaustausch über ein unsicheres Netz erfolgen. Nachfolgend werden die zentralen Schritte des Austausches beschrieben.

Globale Parameter (GP): Von zwei Kommunikationspartnern (A, B) werden eine Primzahl p und eine natürliche Zahl g festgelegt. Diese $GP(g, p)$ können ohne Sicherheitsvorkehrungen[30] über ein unsicheres Netz geschickt werden. Es muss allerdings darauf geachtet werden, dass $g \leq p$ gilt.

Schlüsselerzeugung von A: Nutzer (A) erzeugt eine natürliche Zahl X, die für ihn die Bedeutung eines geheimen Schlüssel X_A hat. Dabei achtet (A) darauf, dass $X_A \leq p$ eingehalten wird. Jetzt wird der öffentliche Schlüssel Y von (A) gebildet, indem $Y_A = g^{X_A} mod\, p$ berechnet wird. Nutzer (A) schickt nun Y_A zu Nutzer (B).

Schlüsselerzeugung von B: Nutzer (B) erzeugt ebenso eine natürliche Zahl X, die für ihn die Bedeutung des geheimen Schlüssels X_B hat. Dabei achtet (B) darauf, dass $X_B \leq p$ eingehalten wird. Der öffentliche Schlüssel Y wird von (B) gebildet, indem $Y_B = g^{X_B} mod\, p$ ermittelt wird. Nutzer (B) übermittelt Y_B zum Kommunikationspartner (A).

Gemeinsamer Schlüssel von A ermittelt: Nutzer (A) nimmt den von (B) erhaltenen öffentlichen Schlüssel Y_B und kann das gemeinsame Geheimnis bzw. den Sitzungsschlüssel (K) berechnen, in dem $K = (Y_B)^{X_A} mod\, p$ bestimmt wird.

Gemeinsamer Schlüssel von B ermittelt: Nutzer (B) nimmt den von (A) erhaltenen öffentlichen Schlüssel Y_A und kann das gleiche gemeinsame Geheimnis bzw. den Sitzungsschlüssel (K) berechnen, indem $K = (Y_A)^{X_B} mod\, p$ gesetzt wird.

Was haben die Nutzer (A, B) erreicht? Beide kennen jetzt einen Schlüssel (K), den sie für eine symmetrische Verschlüsselung benötigen, haben ihn jedoch nicht über ein Netz oder per Kurier etc. verschickt, sondern er wurde über dritte Größen gebildet. Hier stellt sich die Frage, wie die zwei identischen Resultate der Schlüsselbildung (K) von (A, B) möglich sein können. Die nachfolgenden einfachen Umformungen, die die Gesetze der modularen Arithmetik berücksichtigen, liefern die Antwort:

$$\begin{aligned} K &= (Y_B)^{X_A} mod\, p \\ &= (g^{X_B} mod\, p)^{X_A} mod\, p \\ &= (g^{X_B})^{X_A} mod\, p \\ &= g^{X_B X_A} mod\, p \\ &= (g^{X_A})^{X_B} mod\, p \\ &= (g^{X_A} mod\, p)^{X_B} mod\, p \\ &= (Y_A)^{X_B} mod\, p \end{aligned}$$

Ein unbefugter Dritter, der die Kommunikation zwischen (A) und (B) mitliest, muss aus den Größen (p, g, Y_A, Y_B) den diskreten Logarithmus (dl_g) bilden, um

[30] In der Praxis werden natürlich die GP geschätzt übertragen, wie es mit dem Oakley-Protokoll (Abb. 7.4.13) vorgesehen ist.

an den geheimen Sitzungsschlüssel (K) zu kommen. Er kann z.B. versuchen, den geheimen Schlüssel (B) zu berechnen, indem er die Gleichung $K = dl_g(Y_B)$ löst. Dies wird ihm nicht so einfach gelingen, wenn die Primzahl (p) entsprechend groß gewählt wurde. Allerdings gibt es einige Schwachpunkte auf die später eingegangen wird.

Zunächst soll der Diffie-Hellman-Schlüsselaustausch an ein Beispiel, das z.B. beim IPSec-Protokoll im Kern zur Anwendung kommt, durchexerziert werden. Zwei Kommunikationspartner bzw. Hostsysteme (H1, H2) beabsichtigen, eine vertrauliche Kommunikation aufzubauen. Daten, verschlüsselt mit dem symmetrischen AES-Algorithmus, sollen ausgetauscht werden. Hierzu ist es erforderlich, dass beide Kommunikationspartner denselben Schlüssel sowohl zur Verschlüsselung als auch zur Entschlüsselung einsetzen.

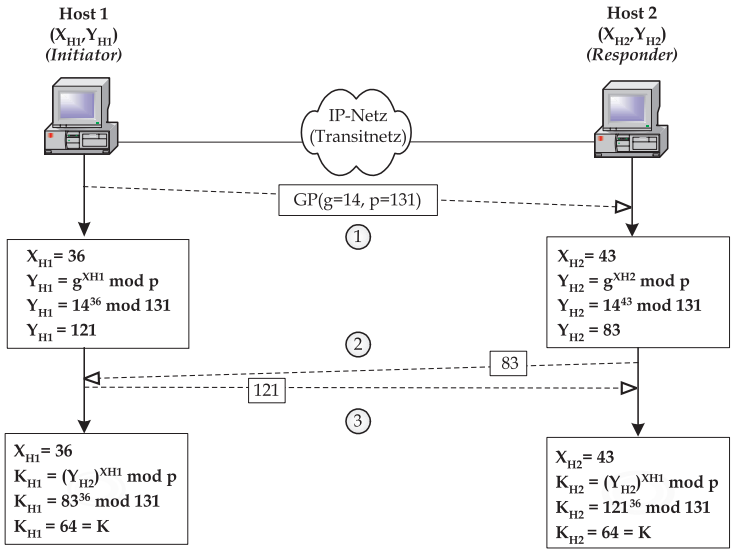


Abb. 4.9: Diffie-Hellman-Schlüsselaustausch (Y_{H1}, Y_{H2}) zwischen zwei Host-Systemen (H1, H2)

Host H1 ergreift die Initiative und schickt Host H2 zunächst die globalen Parameter $(g = 14, p = 131)$. Abb. 4.9 zeigt den zeitlichen Ablauf des Nachrichtenaustausches über das unsichere Internet. Die beiden Hostsysteme sind jeweils durch Gateways, auf die im Einzelnen nicht näher eingegangen wird, gegenüber dem Internet abgesichert. Nach Erhalt der Parameter erzeugen beide Hosts (H1, H2) ihre geheimen Schlüssel $(X_{H1} = 36, X_{H2} = 43)$ sowie ihre öffentlichen Schlüssel (Y_{H1}, Y_{H2}) durch Einsetzen der Werte in die Formeln. Dabei errechnet H1 für sich $(Y_{H1} = 14^{36} mod\ 131 = 121)$ und H2 kommt zu dem Ergebnis $(Y_{H2} = 14^{43} mod\ 131 = 83)$. Anschließend tauschen beide Hosts (H1, H2) die öffentlichen Schlüssel (Y_{H1}, Y_{H2}) aus. Nun kann jeder Host für sich den gemeinsamen Sitzungsschlüssel $(K = K_{H1} = K_{H2})$ errechnen, mit dem dann die symmetrische

AES-Verschlüsselung der eigentlichen Daten vorgenommen werden kann. Durch Einsetzen der Werte folgt für H1 ($K_{H1} = 83^{36} mod\, 121 = 64$) und für H2 analog ($K_{H2} = 121^{43} mod 121 = 64$). Somit lautet der gemeinsame Sitzungsschlüssel (64).

Die Ideen von Diffie-Hellman waren genial, doch ohne weitere Sicherheitsvorkehrungen kann ein Schlüsselaustausch nicht implementiert werden. Denn es gibt, wie oben angedeutet, einige bedenkenswerte Schwachpunkte [Huitema 1998]:

- Im Schlüsselaustausch sind keine Identifizierungsmaßnahmen der beiden Kommunikationspartner vorgesehen.
- Für einen unbefugten Dritten besteht die Möglichkeit, einen *Man-in-the-middle*-Angriff durchzuführen (Abb. 4.10). Es werden dabei die geheimen Schlüssel von (H1, H2) – wie in Abb. 4.9 aufgeführt – wiederverwendet:

  1. Host H1 sendet, wie bereits in Abb. 4.9 dargestellt, seinen öffentlichen Schlüssel $(Y_{H1} = 121)$ zu Host H2.
  2. Ein unbefugter Dritter (D) fängt wie in Abb. 4.10 die Nachricht $(Y_{H1} = 121)$ ab, speichert sie und sendet jetzt unter Ausnutzung der öffentlichen Werte $(g = 14, p = 131)$ an Host H2 eine eigene Nachricht, z.B. $(Y_D = 14^{56} mod\, 131 = 55)$, allerdings mit der User-ID von H1. Der Empfänger H2 glaubt nun, eine Nachricht von H1 vorliegen zu haben. Er speichert daher den öffentlichen Schlüssel von (Y_D) in der Annahme ab, es sei der öffentliche Schlüssel von H1. Ebenso wird die Nachricht von H2 an H1 abgefangen und analog eine Nachricht z.B. $(Y_D = 55)$ an H1 geschickt. In Erwartung, dass diese Nachricht von H2 kommt, wird (Y_D) als vermeintlich öffentlicher Schlüssel von H2 interpretiert.
  3. Jetzt erzeugt H1 einen Sitzungsschlüssel, allerdings mit den Werten des unbefugten Dritten (D), indem er $K_{H1} = Y_D^{X_{H1}} mod\, 131 = 117$ bestimmt. H2 erstellt ebenfalls einen Sitzungsschlüssel mit den Werten von D. Hieraus folgt für $K_{H2} = Y_D^{X_{H2}} mod 131 = 7$. Der unbefugte Dritte (D) erzeugt einen Sitzungsschlüssel für H2, indem er $K_{H2} = Y_{H1}^{X_D} mod : 131 = 7$ errechnet und für H1 bildet D den Sitzungsschlüssel $K_{H1} = Y_{H1}^{X_D} = 117$.
  4. Von nun an teilen die Hosts (H1, H2) ihren Sitzungsschlüssel mit einem unbefugten Dritten (D), von dem sie nichts ahnen, der jedoch in der Lage ist, die eigentlichen Daten, die symmetrisch verschlüsselt werden sollen, ungehindert zu entschlüsseln, mitzulesen und anschließend verschlüsselt an den jeweiligen Host weiterzuleiten.

- Das Verfahren des Schlüsselaustausches ist sehr rechenintensiv, so dass ein *Denial-of-Service*-Angriff denkbar wäre, wenn ein unbefugter Dritter einen Schlüsselaustausch initialisiert und versucht, durch ständige Schlüsselanfragen den Prozessor des Zielrechners mit Berechnung zur geeigneten Schlüsselerzeugung zu beschäftigen. Somit blockiert dieser nach und nach den ganzen Rechner.

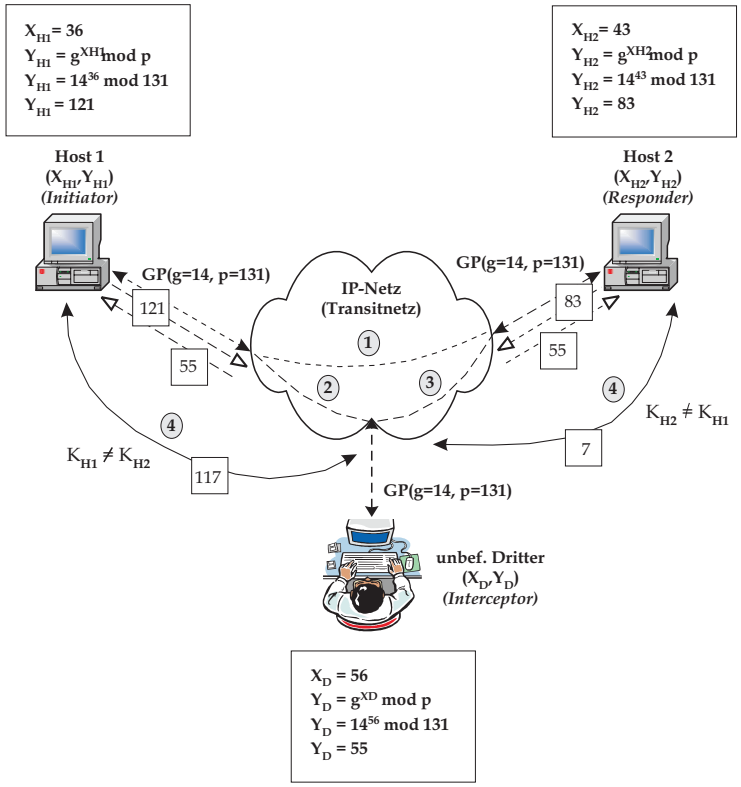


Abb. 4.10: Diffie-Hellman-Schlüsselaustausch (Y_{H1}, Y_{H2}) zwischen zwei Host-Systemen (H1, H2) unter Einfluss eines unbefugten Dritten (D)

Ein geeigneter Vorschlag zur Implementierung des Diffie-Hellman-Austauschprotokolls unter Umgehung der Schwächen ist das *Oakley-Protokoll* (Abschn. 7.4.13), das einen wesentlichen Anteil am IKE-Protokoll als Bestandteil von IPSec besitzt.

RSA

Das asymmetrische Verschlüsselungsverfahren RSA, benannt nach seinen Entwicklern Rivest, Shamir und Adleman, wurde 1978 veröffentlicht [RSA 1978]. Es ist heute das meist verbreitete asymmetrische Verfahren. RSA basiert auf der Nutzung eines Schlüsselpaars, bestehend aus öffentlichem und privatem Schlüssel. Die Schlüssellänge ist dabei variabel. Mit wachsendem Schlüssel steigt zwar der Rechenaufwand für Chiffrierung und Dechiffrierung, jedoch erhöht sich gleichzeitig die Datensicherheit.

Um ein RSA-Schlüsselpaar zu erzeugen, werden zwei große zufällig gewählte und ungefähr gleich lange Primzahlen p und q ausgewählt und miteinander mul-

tipliziert: $n = pq$. Um nun den öffentlichen Schlüssel zu bilden, wird eine zufällig gewählte ganze Zahl e verwendet, die der Bedingung genügt, dass $1 \ll e \ll \phi(n)$ gilt. Weiterhin soll gelten, dass die beiden Zahlen e und $\phi(n)$[31] teilerfremd sind. Mit anderen Worten: Der größte gemeinsame Teiler (ggT) von e und $\phi(n)$ ist gleich 1. Damit existiert nur die 1 als gemeinsamer Faktor mit $ggT(e, \phi(n)) = 1$. Der Funktionswert von $\phi(n)$ lässt sich durch den vorliegenden Sonderfall der Primzahlen p und q relativ einfach bestimmen, indem $\phi(n) = (p-1)(q-1)$ gebildet wird. Wird jetzt e nach obiger Bedingung gewählt, steht der öffentliche Schlüssel durch das Zahlenpaar (e, n) fest. Der private Schlüssel wird durch die Zahl d erzeugt, die mit Modulo $\phi(n)$ das inverse Element zu e bildet, also $d = e^{-1} mod \phi(n)$. Damit stellt das Zahlenpaar (d, n) den privaten Schlüssel dar.

Um diesen Ablauf etwas anschaulicher zu gestalten, werden im anschließenden Beispiel konkrete Zahlen benutzt:

1. Es werden die beiden Primzahlen, $p = 7$ und $q = 17$ eingesetzt.
2. Damit kann $n = pq = 7 \times 17 = 119$ gebildet werden.
3. Weiterhin lässt sich $\phi(n) = (p-1)(q-1) = 96$ ermitteln.
4. Es wird ein e gesucht, das relativ Prim[32] zu $\phi(n) = 96$ und kleiner als $\phi(n)$ ist; in diesem Fall $e = 5$. Damit bildet das Zahlenpaar $(5, 119)$ den öffentlichen Schlüssel.
5. Es wird das Zahlenpaar (d, n) gebildet, indem $de = 1 \ mod\ 96$ und $d \ll 96$ errechnet wird. Der korrekte Wert ist $d = 77$, da sich $77 \times 5 = 385 = 4 \times 96 + 1$ ergibt.

Mit dem gebildeten öffentlichen $(5, 119)$ und privaten $(77, 119)$ Schlüssel kann jetzt weitergearbeitet werden. Der Klartextbuchstabe (K) soll mit dem RSA-Algorithmus verschlüsselt und entschlüsselt werden. Damit wird das Chiffrat (C) von (K) gebildet, indem $C = K^e (mod\ n)$ errechnet wird. Allerdings muss $K \ll n$ gelten. Die Entschlüsselung erfolgt durch $K = C^d (mod\ n)$. Wird der numerische Wert des ASCII-Zeichens von K genommen (75) und entsprechend eingesetzt, so entsteht das Chiffrat $(C = 45)$ (Abb. 4.11). Umgekehrt lässt sich zeigen, dass sich mittels privatem Schlüssel wieder der Klartextbuchstabe (K) erstellen lässt (Abb. 4.11).

Dieses kleine Beispiel soll lediglich ein Gefühl für die Arbeitsweise des RSA-Algorithmus vermitteln. Denn es sind noch einige Randbedingungen für den praktischen Einsatz zu beachten. So sollte z.B. (n) nach den aktuellen Empfehlungen mindestens 768 Bit lang sein. Außerdem sollten die Primzahlen nicht dicht beieinander liegen.

---

[31] Mit $\phi(n)$ ist die Eulersche phi-Funktion gemeint, die für sehr große n im Allgemeinen nicht einfach zu bestimmen ist.

[32] So sind z.B. die Zahlen 8 und 15 relativ Prim zueinander, denn die Teiler von 8 sind 1, 2, 4 und 8 selbst. Für 15 sind die Teiler 1, 3, 5 und 15. Damit haben sie keinen anderen gemeinsamen Primfaktor als die 1 die den größten gemeinsame Teiler bildet.

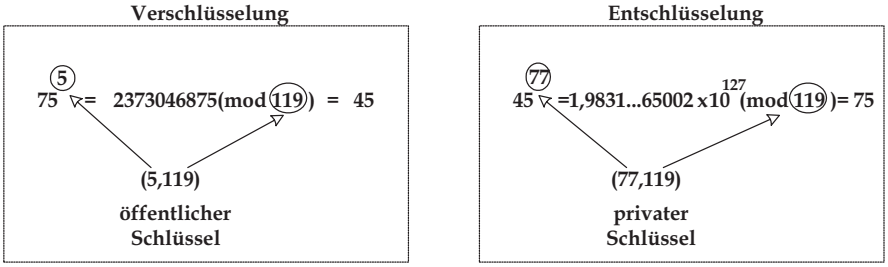


Abb. 4.11: Verschlüsselung und Entschlüsselung nach dem RSA-Algorithmus für den Klartextbuchstaben (K)

Eine weitere Frage, die sich stellt, ist, wie (e) und (p) und (q) gewählt werden müssen. Wenn (e) festgelegt wird, werden anschließend (p) und (q) so gewählt, dass sowohl $p-1$ als auch $q-1$ teilerfremd zu (e) sind. Nach heutigem Erkenntnisstand[33] wird die Sicherheit von RSA nicht negativ beeinflusst, wenn immer derselbe Wert für (e), der auch sehr klein sein kann, genommen wird. Dies bringt den Vorteil, dass kleine Exponenten die mit dem öffentlichen Schlüssel ausgeführten Operationen deutlich beschleunigen, ohne diejenigen negativ zu beeinflussen, die den privaten Schlüssel verwenden. Die am häufigsten genutzten Exponenten sind 3, 17, 65537. Beim Letzten handelt es sich um die vierte Fermatsche-Zahl[34] F_4. Die einzelnen Standards, mit denen vielleicht die VPN-Technologie am ehesten in Berührung kommt, enthalten unterschiedliche Empfehlungen für (e):

- X.509 sieht die Zahl 65537 vor
- PEM zur Mailabsicherung nutzt die Zahl 3
- PKCS #1 lässt die Zahl 3 oder die Zahl 65537 zu

Sicherheit des RSA-Algorithmus

Die Sicherheit des RSA-Verfahrens beruht auf der mathematische Herausforderung, große Zahlen zu faktorisieren. Es gibt zwar streng genommen keinen mathematischen Beweis, jedoch kann zugunsten des RSA-Algorithmus festgehalten werden, dass trotz intensiver Kryptoanalyse bisher kein (öffentlich beschriebener) Weg bekannt wurde, den Algorithmus zu brechen. Dennoch sind auf dem Gebiet der Faktorisierung in den letzten 25 Jahren erstaunliche Fortschritte gemacht worden. Neben diesen Erfolgen könnte es, beispielsweise durch Quantencomputer, zu einem sprunghaften Zuwachs an Rechengeschwindigkeit kommen, und damit wäre es möglich, alle privaten Schlüssel durchzuprobieren *(Brute-Force-Attack)*.

---

[33] Allerdings gibt es neuerdings hierzu auch gegenteilige Aussagen, wie bei [Selke 2000], Seite 70, nachzulesen ist, indem von $e = 3$ abgeraten wird.

[34] Diese ist ebenfalls nach dem großen französischen Mathematiker Pierre Fermat benannt und lässt sich einfach in der Form $2^{2^4} + 1 = 2^{16} + 1$ schreiben. Ihre Binärdarstellung enthält neben 15 Nullen genau zwei Einsen, so dass mit ihr leicht potenziert werden kann.

ELGamal

Ein ähnlich geeignetes Verfahren, um Daten zu verschlüsseln oder digitale Signaturen zu erzeugen, ist das von Taher ELGamal. In seiner 1984 erschienen Dissertation und in [ELGamal 1985] führt er aus, wie – im Gegensatz zum RSA-Algorithmus – zwei unterschiedliche Algorithmen für das Chiffrieren und Signieren eingesetzt werden können. Dieses Verfahren ist stark an das Diffie-Hellman-Verfahren (Abschn. 4.4.1) angelehnt. Bei beiden Verfahren werden die öffentlichen Schlüssel auf dieselbe Weise aus den privaten Schlüsseln berechnet. Nach Ablauf des Patentes von Diffie-Hellman am 29. April 1997 ist auch das Interesse an ELGamal stark gestiegen, da vorher ELGamal diesem Patent unterlag, obwohl für ELGamal kein eigenes Patent existierte. In neueren kryptographischen Protokollen und Werkzeugen wird es zunehmend genutzt. Allerdings ist bis zum Erscheinen des vorliegenden Buches noch keine VPN-Verschlüsselung auf Basis von ELGamal bekannt geworden.

DSA

Obwohl RSA einen de-facto-Standard darstellt, wurde in den USA durch das NIST am 19. Mai 1994 für die Erstellung digitaler Unterschriften ein anderer offizieller Standard verabschiedet. Der *Digital Signature Algorithm* (DSA) nutzt als Hash-Funktion SHA-1 und ist in der FIBS PUB 186 *Digital Signature Standard* (DSS) beschrieben. DSA bzw. DSS kann als eine Modifikation des ELGamal-Signaturverfahrens sowie des Schnorr-Signaturverfahrens betrachtet werden, wobei das ELGamal-Signaturschema eine Basis für weitere Signaturverfahren liefert. Das Schnorr-Signaturschema als eine Weiterentwicklung von ELGamal wurde speziell mit dem Ziel zur einfachen Implementierung auf Chipkarten entworfen. Bei allen drei basiert die Sicherheit auf den diskreten Logarithmus und der Schwierigkeit für einen unbefugten Dritten diesen zu bestimmen.

4.5 Kryptographische Hash-Funktionen

„Eine Hash-Funktion stellt eine Abbildung dar, die für alle Elemente einer Menge von Argumenten einen Funktionswert bildet, dessen Informationsgehalt geringer ist als der seines Argumentes.“

So ist es in jedem Lehrbuch der Informatik nachzulesen. Um diese etwas schwer zugängliche Beschreibung anschaulicher zu machen, soll sie nachfolgend mit einem Adressbuch verglichen werden.

Hash-Funktionen sind Bestandteil des täglichen Lebens, häufig ohne als solche beschrieben und benannt zu werden. Betrachtet man ein gewöhnliches, von nahezu jedem geführtes Adressbuch, so stehen die Namen der Adressaten (Wörter) im Allgemeinen in alphabetischer Reihenfolge. Dabei ist die Zuordnung der Wörter zu den Anfangsbuchstaben eine Hash-Funktion (solange die Wörter nicht noch

sortiert werden). Wörter mit unterschiedlicher Bedeutung und Länge werden in derselben Menge erfasst. Der endlichen Menge der Buchstaben des Alphabets können unendlich viele Namen und Adressen zugeordnet werden. Die Suche nach einer Person wird dadurch beschleunigt, dass mit dem Anfangsbuchstaben des Namens feststeht, wo die Person zu suchen ist. Die Suche in der unstrukturierten Gesamtmenge aller notierter Namen würde einen wesentlich höheren Aufwand erfordern.

Hash-Funktionen wurden in der Informatik ursprünglich für schnelle Sortier- und Suchverfahren eingeführt und es existieren frei verfügbare Sortieralgorithmen [Press et al. 1990]. Eine Geschwindigkeitssteigerung der Sortier- und Suchverfahren wird durch die Komprimierung der Eingabedaten erreicht. Somit erzeugen Eingaben unterschiedlicher Länge Ausgabewerte (Hash-Werte) gleicher Länge. Reine Prüfsummenverfahren sind dagegen für die Kryptographie uninteressant. Denn es ist leicht möglich, mit verschiedenen Nachrichten die gleichen Prüfsumme zu generieren. Als Prüfsummenverfahren könnte z.B. die XOR-Funktion genannt werden. Exemplarisch seien an einem Beispiel die Grenzen der XOR-Funktion für die Kryptographie gezeigt. Der einfache Text „Hallo Bob“ soll dafür herangezogen werden. Dieser entspricht im ASCII-Zeichensatz in hexadezimaler Byte-Folge: 48 61 6C 6C 6F 62 Die dazugehörige XOR-Prüfsumme lautet: $48 \bigoplus 61 \bigoplus 6C \bigoplus 6C \bigoplus 6F \bigoplus 62 \bigoplus = 29$. Durch Modifikation der Textnachricht in „Hallo Tot“ oder in „Hurraton“ wird die XOR-Prüfsumme nicht verändert. Kryptographische Hash-Funktionen stellen, wie das kleine Bespiel verdeutlichen sollte, wesentlich höhere Anforderungen an eine Hash-Funktion als z.B. ein einfacher *Cyclic Redundancy Check* (CRC), der häufig in der Datenübertragung eingesetzt wird.

Die Kryptographie hat spezielle Hash-Funktionen (h) eingeführt, so genannte universelle Hash-Funktionen, aus denen die Einweg-Hash-Funktionen abgeleitet wurden. Deren besondere Eigenschaft, die auch namensgebend war, besteht darin, dass aus den Hash-Werten – oder kurz Hash – nicht auf die Eingaben geschlossen werden kann. Sie haben den Charakter einer Falltür[35], die leicht von der einen Seite zu öffnen ist, aber so gut wie nicht von der anderen Seite. Diese vorteilhafte Eigenschaft wird in der kryptographischen Anwendung genutzt, um die Integrität einer Nachricht sicherzustellen. In der Praxis werden Einweg-Hash-Funktionen (h) auf Grundlage einer Kompressionsfunktion entworfen. Dabei liefert die Funktion (h) einen Hash-Wert z.B. der Länge (n) zu einem größeren Eingabeblock der Länge (M). Die Kompressionsfunktion kann wie folgt ausgedrückt werden:

$$h_n = f(M, h_{n-1}) \tag{4.11}$$

[35] Für ein alltägliches Beispiel sei das Telefonbuch des Großraums Paris aufgeschlagen; die auszuführende Funktion ist die, einem Namen, z.B. Hugo, die entsprechende Telefonnummer zuzuordnen. Da die Namen im Telefonbuch von Paris alphabetisch geordnet sind, ist die Zuordnung einfach. Umgekehrt jedoch aus einer vorhandenen Telefonnummer den zugehörigen Namen zu finden (Invertierung), ist offensichtlich viel schwieriger, falls nur das Telefonbuch von Paris zur Verfügung steht.

Während es bei den Such- bzw. Sortierverfahren unumgänglich ist, von den Hash-Werten auf die Eingaben rückzuschließen, sollen Einweg-Hash-Funktionen genau dies unmöglich machen. Es sind gerade jene Funktionen, die sich zwar leicht berechnen, aber nur schwer invertieren, also umkehren lassen; sie sind damit schwer angreifbar. Zusätzlich sollen Einweg-Hash-Funktionen kollisionsfrei sein, d.h. zwei unterschiedliche sinnvolle Eingaben sollen auf keinen Fall demselben Hash-Wert zugeordnet werden können. Für einen Hash-Wert H(Da) einer Datei (Da) bedeutet die Kollisionsfreiheit[36], dass es – ausgehend vom Hash-Wert H(Da) – nicht möglich ist, eine sinnvolle Datei (Da) zu rekonstruieren.

Zu den in der Praxis am häufigsten eingesetzten Einweg-Hash-Funktionen gehören der von Prof. Rivest entwickelte MD5 (*Message Digest Algorithm No.5*) sowie der vom *National Institut of Standard* (NIST) in Zusammenarbeit mit der *National Security Agency* (NSA) entworfene *Secure Hash Algorithm* (SHA-1). Neben MD5 hat Rivest weitere bekannte Algorithmen entworfen, die alle auf einem Design-Prinzip basieren. Auch SHA-1 lässt sich auf dieses Prinzip – häufig auch als MD-Familie von Hash-Funktionen bezeichnet – zurückführen.

4.6 Elektronische Signatur

Die elektronische Signatur liefert die in den heutigen elektronischen Geschäftsvorfällen so wichtigen Eigenschaften wie Verbindlichkeit und Nachweisbarkeit (Abschn. 3.1). Das auf asymmetrischen Kryptosystemen basierende Signaturverfahren ermöglicht einen gesicherten Schlüsselaustausch und bietet erweiterte Authentifizierung und Signierung. Allerdings steht dem Vorteil der Authentifizierung der Nachteil der Schlüsselverwaltung und -verteilung gegenüber, wenn nicht ein extra Authentifizierungsserver eingesetzt wird. Hier setzt die Public-Key-Infrastruktur an, die genau diese Verwaltung als zentrale Aufgabe verrichtet (Abschn. 4.7).

Die elektronische Signatur dient als Ersatz für die manuelle Unterschrift auf Papier. Nach dem alten Signaturgesetz aus dem Jahre 1997 heißt das jedoch nicht, dass eine eingescannte Unterschrift, die unter ein Dokument gesetzt wird, mit einer elektronischen Signatur gleichzusetzen ist; erst die neuen europäischen Regelungen schaffen hier Veränderungen (Abschn. 4.6.2). Dennoch werden auch bei der elektronischen Signatur die wesentlichen Funktionen einer manuellen Unterschrift nachvollzogen.

Basis der so genannten Public-Key-Verfahren ist die Verwendung unabhängiger Schlüssel für die Chiffrierung wie für die Dechiffrierung. Der Chiffrierschlüssel (öffentlicher Schlüssel) kann jedem bekannt sein, allein der Dechiffrierschlüssel

[36] Der exakte mathematische Beweis der Kollisionsfreiheit steht allerdings noch aus. Jedoch sieht es in der Praxis so aus, dass es zu aufwändig ist, eine Kollision zu finden; der Rechenaufwand ist einfach zu hoch. Und wenn tatsächlich eine Kollision gefunden würde, ist es in der Regel zu spät, damit noch etwas anzufangen.

(privater Schlüssel) muss unter allen Umständen vor unbefugten Dritten fern gehalten werden. Oftmals geschieht dies durch die Auslagerung des privaten Schlüssels auf eine Chipkarte (Abschn. 5.3.2). Auch IPSec, der Quasisicherungsstandard für IP-VPN, kann das asymmetrische Public-Key-Verfahren, mittels *Internet-Key-Exchange-Verfahren* (IKE) (Abschn. 7.4.9) nutzen, um Schlüssel zu generieren und während einer Sitzung zu erneuern bzw. auszutauschen.

4.6.1 Mechanismen einer elektronischen Signatur

Bei der Anwendung der elektronischen Signatur wird ein Hash-Wert mit dem asymmetrischen Verschlüsselungsverfahren kombiniert. Allerdings wird das asymmetrische Verschlüsselungsverfahren in reziproker Reihenfolge (Abschn. 4.4.1) angewandt. Der Urheber des Dokuments unterzeichnet mit seinem privaten Signierschlüssel (Abb. 4.12). Ziel dieser Kombination ist es, die Unversehrtheit (Integrität) und die Urheberschaft (Authentifikation) des unterzeichneten Dokumentes sicherzustellen. Die Überprüfung der Echtheit dagegen kann jederzeit mit dem öffentlichen Signierschlüssel des Urhebers vorgenommen werden. Allerdings dient die elektronische Signatur nicht zur Wahrung der Vertraulichkeit. Dies kann jedoch mit wenig Aufwand nachgeholt werden, wenn das vom Urheber signierte Dokument mit dem öffentlichen Schlüssel des Kommunikationspartners verschlüsselt wird. Abb. 4.12 zeigt den Signiervorgang sowie die Überprüfung beim Empfänger:

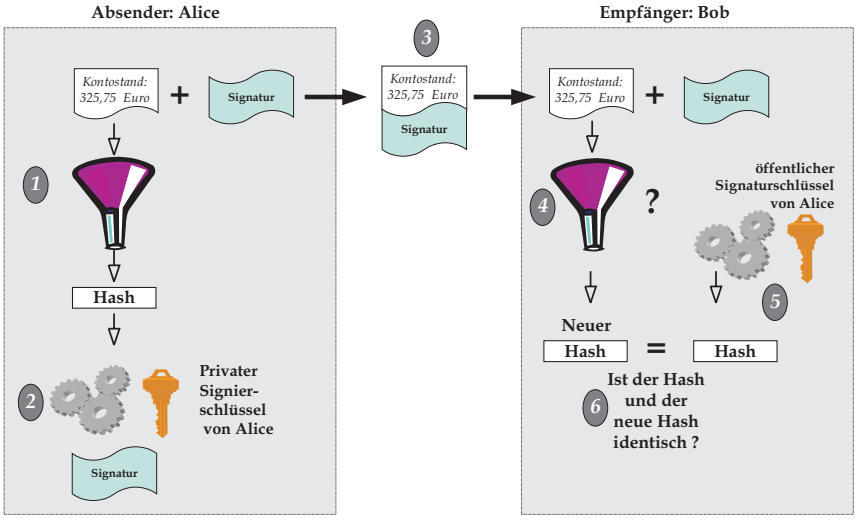


Abb. 4.12: Signiervorgang von Alice (Sender) und Überprüfung bei Bob (Empfänger)

1. Die zu sendende Nachricht wird mit einer geeigneten Hash-Funktion in einen Hash-Wert, auch als *Message Digest* bezeichnet, überführt.
2. Alice[37] als Senderin signiert nun den Hash-Wert, indem sie den privaten Signierschlüssel *(Private Key)* auf den Hash-Wert anwendet und damit eine elektronische Signatur erzeugt. Diese wird an die Originalnachricht angehängt.
3. Originalnachricht und Signatur werden zum Empfänger Bob[38] geschickt.
4. Der Empfänger Bob bildet nach Erhalt der Nachricht einen neuen Hash-Wert von der vermeintlichen Originalnachricht mit der gleichen Hash-Funktion, die auch Alice verwendet hat.
5. Aus der mitgeschickten Signatur wird mittels öffentlichem Schlüssel von Alice *(Public Key)* der von Alice erzeugte Hash-Wert zurückgewonnen.
6. Ein Vergleich der beiden Hash-Werte liefert das Resultat, ob die Nachricht verändert wurde *(Hash-Werte stimmen nicht überein)* oder ob es sich um die Originalnachricht handelt *(Hash-Werte stimmen exakt überein)*.

Hier stellen sich folgende Fragen: Was verbirgt sich hinter einer elektronischen Signatur und wie kann von einer Signatur auf eine bestimmte Person geschlossen werden? Die Antwort liegt im Zertifikat.

Ein Zertifikat bindet die Identität einer Person – in Abb. 4.12 sind dies Alice und Bob – an den öffentlichen Schlüssel. Außer dem Namen können verschiedene weitere Attribute hinzugefügt werden (Abschn. 4.7.1). Damit muss es eine dritte Instanz geben, die die öffentlichen und privaten Schlüssel erstellt, die Identität bei der Auslieferung überprüft und außerdem die öffentlichen Schlüssel verwaltet. Die dazu notwendige Infrastruktur wird unter dem Begriff Public-Key-Infrastruktur zusammengefasst. Neben den rein technischen Randbedingungen werden hohe Anforderungen an den Betrieb gestellt (Abschn. 4.7). Doch bevor auf diese Infrastruktur näher eingegangen wird, soll der Unterschied zwischen digitaler Signatur und elektronischer Unterschrift, die durch die Europäische Kommission eingeführt wurde, verdeutlicht werden.

[37] An dieser Stelle muss für die nachfolgende Ausführung unterstellt werden, dass die beiden Kommunikationspartner ihre öffentlichen Signierschlüssel auf einem vertrauenswürdigen Wege im Vorfeld ausgetauscht haben.

[38] Die Namen Alice und Bob haben sich in die Beschreibung des asymmetrischen Schlüsselaustausches fest eingebürgert und werden üblicherweise zur Illustration von Beispielen verwendet. John Gordon hat diesen interessanten Gedanken in einem recht amüsanten Kurzvortrag *(The Alice and Bob After Dinner Speech, Zürich Seminar, April 1984 by John Gordon by invitation of Professor James Massey, http://www.conceptlabs.co.uk/extras/ZurichSeminarSpeech3.htm)* verfolgt, in dem er aufgrund der gefundenen Beispiele Alice und Bob beruflich und privat gekonnt charakterisierte.

4.6.2 Bedeutung der digitalen und der elektronischen Signatur

Als 1997 in der Bundesrepublik Deutschland das Signaturgesetz (SigG[39]) und die begleitende Signaturverordnung (SigV) erlassen wurde, war der weltweit erste nationale rechtliche Rahmen für eine digitale Signatur geschaffen. Dem Vorbild des deutschen Signaturgesetzes folgend, haben einige europäische Länder eigene Gesetze erlassen, die aber teilweise vom deutschen Gesetz (SigG) und von der Verordnung (SigV) in der Fassung von 1997 stark abwichen.

Aus Sicht der Europäischen Union waren die unterschiedlichen nationalen Alleingänge für einen gemeinsamen Europäischen Markt mehr als ungünstig. In einigen Ländern waren die Zertifizierungsstellen nicht lizenzpflichtig, sondern wurden von Zeit zu Zeit im Betrieb überprüft. Außerdem haben sich die Haftungszusagen für fehlerhafte Zertifikate uneinheitlich entwickelt. In einigen Ländern konnten Haftungsansprüche geltend gemacht werden, in anderen wiederum nicht, wie z.B. in Deutschland. Die Europäische Kommission schuf dann im Dezember 1999 eine einheitliche verbindliche Signaturrichtlinie (Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, [1999/93/EG]), die bis zum 19. Juli 2001 von allen EU-Mitgliedstaaten in nationale Rechtsvorschriften umgesetzt werden musste. Seit dem 19. Juli 2001 existiert in ganz Europa diesbezüglich eine vereinheitlichte Rechtslage.

Im Gegensatz zum außer Kraft gesetzten deutschen Signaturgesetz von 1997, das eine *digitale Signatur* bezeichnet, sieht die Signaturrichtlinie Regelungen für *elektronische Signaturen* vor. Der Begriff *elektronisch* wurde bewusst eingeführt, um gegenüber verschiedenen Techniken offen zu bleiben. Dabei wird zwischen der elektronischen und fortgeschrittenen elektronischen Signatur sowie der qualifizierten Form der fortgeschrittenen elektronischen Signatur unterschieden. Letztere erfordert darüber hinaus ein qualifiziertes Zertifikat und kommt damit der elektronischen Signatur nach dem bisherigen deutschen Signaturgesetz sehr nahe.

Für die einfache elektronische Signatur genügt es, dass Daten zur Authentifizierung in elektronischer Form, die anderen elektronischen Daten beigefügt sind, logisch mit ihnen verknüpft wurden (eingescannte Unterschrift unter einem Dokument). Für eine fortgeschrittene elektronische Signatur hingegen müssen vier Anforderungen erfüllt sein. Sie ist ausschließlich dem Unterzeichner zugeordnet und ermöglicht es, den Unterzeichner zu identifizieren. Sie wird mit Mitteln erstellt, die allein der Unterzeichner unter Kontrolle hat, und ist mit den Daten, auf die sie sich bezieht, so verknüpft, dass nachträgliche Änderungen sichtbar sind (Abb. 4.13).

Alle Dienstleistungen, die im Zusammenhang mit dem Signaturverfahren anfallen, werden von Zertifizierungsdienstanbietern erbracht. Das sind laut Richtlinie

[39] Das so genannte Signaturgesetz (SigG) ist Bestandteil (Artikel 3) des Gesetzes des Bundes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (IuKDG). Eine Verabschiedung erfolgte am 4. Juli 1997 im Bundesrat und ein theoretisches Inkrafttreten am 1. August 1997. Jedoch erst mit dem praktischen Inkrafttreten durch die Schaffung einer PKI (RegTP) am 28. September 1998 war es möglich, Trust Center zu zertifizieren.

alle Stellen oder natürliche und juristische Personen, die Zertifikate ausstellen oder andere Dienste im Zusammenhang mit elektronischen Signaturen anbieten (Abschn. 4.7).

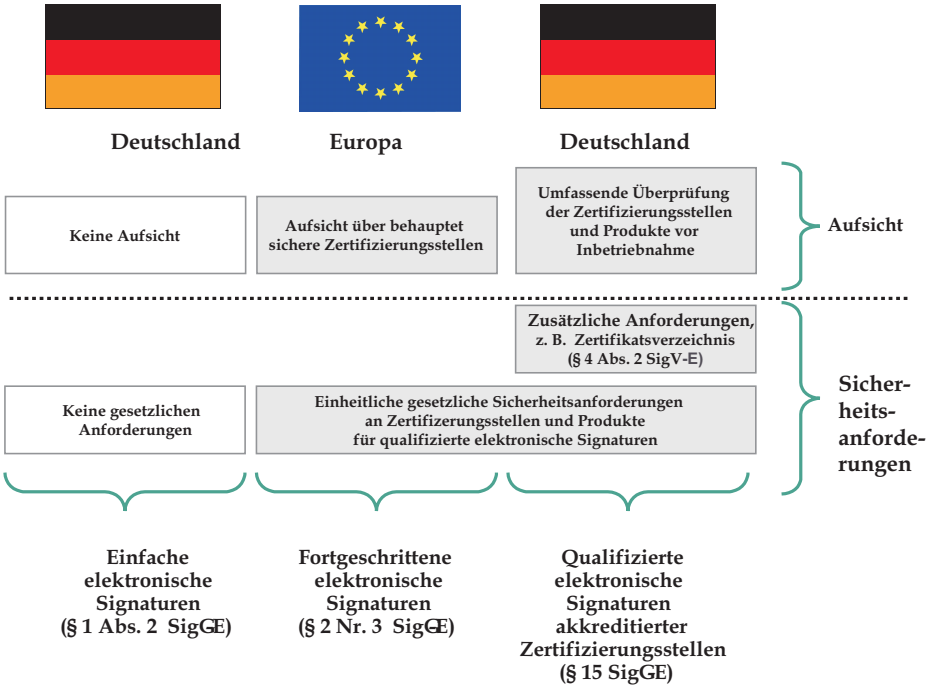


Abb. 4.13: Übersicht SigG und Novellierung/EU-Richtlinie

Die Richtlinie unterscheidet einfache Anbieter von Zertifizierungsdiensten und Anbieter, die qualifizierte Zertifikate ausstellen. Die letzte Gruppe wiederum teilt sich auf in diejenigen, die als akkreditierte Zertifizierungsstellen (ZDAs) auftreten, und diejenigen, die als angezeigte ZDAs – z.B. die D-TRUST GmbH in Berlin – am Markt agieren. Einfache Anbieter stellen Zertifikate und elektronische Bescheinigungen aus, die bestätigen, dass Personen und ihre Signaturprüfdaten zusammengehören. Anbieter, die qualifizierte Zertifikate ausstellen, müssen dagegen hohen Sicherheitsanforderungen genügen, deren Einhaltung und Überwachung den Mitgliedsstaaten obliegt.

4.7 PKI und Trust Center

Die neue Kultur des weltweiten elektronischen Datenaustausches und der Vernetzung birgt sowohl für Unternehmen als auch für Privatpersonen ein immenses

Risiko an E-Mail-Lauschangriffen und Datendiebstahl. Sobald ein Unternehmen online sichtbar ist, kann es die gesamte Spanne der weltweiten Kriminalität zu spüren bekommen. Im Gegensatz dazu erfährt ein Unternehmen, das sich offline verhält, „nur“ die Kriminalität der lokalen Umgebung. Dieser Aspekt wirft etliche Betrachtungen auf, die [Schneier 2000] sehr anschaulich dargestellt hat.

Um dennoch an der weltweiten Kultur des elektronischen Datenaustausches teilzuhaben, die sich vermehrt im Geschäftsleben verbreitet, sind viele Unternehmen dazu übergegangen, eine eigene Public-Key-Infrastruktur (PKI) aufzubauen. Auch wenn meist in einem ersten Schritt nur daran gedacht wird, E-Mails, den Remote-Access-Service sowie die VPN-Verbindungen abzusichern. Andere Unternehmen wiederum, die auf eine eigene PKI verzichten, und so allen damit verbundenen Schwierigkeiten und Anforderungen aus dem Wege gehen, nutzen eine Infrastruktur von speziellen Trust Centern. Trust Center sind, wie der Name schon andeutet, vertrauenswürdige Institutionen, die eine Public-Key-Infrastruktur beherbergen. Zumindest für kleinere Firmen bietet sich diese Auslagerung (Outsourcing) als die kostengünstigere Variante an. Zu den zentralen Aufgaben eines Trust Centers, die in drei Kategorien untergliedert werden können (Abb. 4.14), gehören:

Beglaubigungsleistungen: Hierunter werden alle Tätigkeiten zusammengefasst, die die Authentifizierung von Daten oder Vertrauenswürdigkeiten von Instanzen – z.B. untergeordnete Trust Center – beinhalten (*Registration Authority*, RA). Hierzu zählen auch die Zertifikatsausstellung, Personalisierung und Registrierung von Nutzern einer Sicherheitsinfrastruktur.

Serverfunktionen: Hier werden unter anderem Authentifizierungsserver, um einen Kommunikationspartner sicher zu identifizieren, hinzugerechnet. Auch die Bereitstellung öffentlicher Verzeichnisse (X.500), die den Zugriff auf zertifizierte öffentliche Benutzerschlüssel ermöglichen, zählen zu den Serverfunktionen. Viele symmetrische und hybride Authentifizierungs- und Schlüsselaustauschprotokolle, wie z.B. Kerberos, arbeiten mit einem online verfügbaren Authentifizierungsserver.

Schlüsselmanagement: Dies hat zentrale Bedeutung für ein Trust Center. Es umfasst die Schlüsselgenerierung, die Speicherung und die Ausgabe von Schlüsseln (*Certificate Authority*, CA) sowie die Zurücknahme von Schlüsseln und deren Bekanntgabe (*Certificate Revocation List*, CRL) und ggf. deren Vernichtung.

Die Frage, ob es sinnvoller ist, eine eigene PKI aufzubauen oder sich einem Trust Center anzuvertrauen, ist jedoch nicht so einfach zu beantworten. Denn es gilt zu bedenken, dass die Zertifizierung einer PKI nach dem deutschen Signaturgesetz (SigG) formal nur für den deutschen Rechtsraum gilt. Hat eine Firma internationale Verflechtungen und ein SigG-konformes PKI aufgebaut, nützt das dem Unternehmen wenig, wenn bei Rechtsstreitigkeiten nicht auch nach Deutschem Recht verhandelt wird. Beispielsweise ist bei Geschäftsverbindungen nach Asien umstritten, welches Recht angewandt wird. Besser ist die Situation für ausschließlich

in Europa tätige Firmen, da in Brüssel eine verbindliche europäische Verordnung erlassen wurde. Gegenwärtig existieren die drei folgenden PKI-Varianten:

1. PKI, streng nach dem deutschen Signatur Gesetz (SigG) zertifiziert
2. PKI, konform zur europäischen Gesetzgebung (drei Varianten)
3. PKI, ausgerichtet nach einem unternehmensspezifischem Modell (proprietär)

Mittlerweile existieren einige[40] nach dem Signatur Gesetz (SigG) zertifizierten Trust Center. Zu den wesentlichen Dokumenten des SigG in Deutschland gehört das SigG in der Fassung vom 22. Mai 2001 sowie die Signaturverordnung (SigV) in der Fassung vom 22. November 2001. Außerdem ist der Maßnahmenkatalog des Bundesamtes für Sicherheit in der Informationstechnik (BSI) von besonderem Interesse.

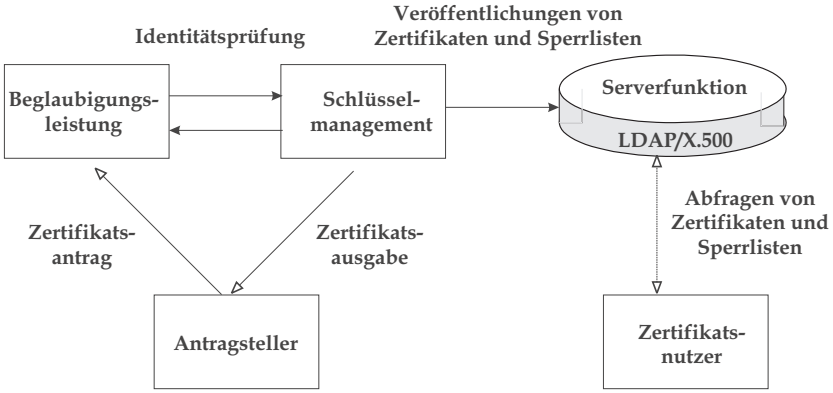


Abb. 4.14: Übersicht über die zentralen Aufgaben einer PKI

[Ellison und Schneier, 2000] haben sich in ihrem lesenswerten Aufsatz kritisch über das Vertrauen, das ein Anwender in ein Trust Center setzen muss, geäußert. Sie beschreiben zehn Risiken im Zusammenhang mit der Nutzung eines Trust Centers.

4.7.1 X.500 und X.509 v3

Wie Abb. 4.14 deutlich macht, spielt die Serverfunktion innerhalb einer PKI eine zentrale Rolle. Damit ist der Begriff X.500, der im Grunde eine Verzeichnisstruktur

[40] Bei der Drucklegung des Buches existierten unter anderem das Trust Center der Telekom (TeleSec), das der Deutschen Post AG (SignTrust) und das TC-Trust Center, die als akkreditierte Zertifizierungsdienstanbieter (ZDA) von der Regulierungsbehörde für Telekommunikation und Post (RegTP) zugelassen wurden. Weitere Informationen sind unter http://www.regtp.de zu finden.

mit baumartigen Charakter beschreibt, und der Begriff X.509 v3, der gemäß der *International Telecommunication Union* (ITU-*T*)[41] einen internationalen Zertifikatsstandard definiert, verknüpft. Dieser ISO-Standard 9594-8, der identisch mit dem X.509 ITU-*T*-Standard X.509 ist, sichert Interoperabilität und beschreibt das Format für die von einem Trust Center signierten elektronischen Zertifikate und die notwendigerweise anfallenden Schlüsselrückrufe (*Certificate Revocation List*, CRL).

Ebenso eng ist X.500 mit X.509 v3 verknüpft. X.509 stellt den Authentifizierungsdienst für den X.500-Verzeichnisdienst bereit. Abb. 4.15 zeigt die X.509-Zertifikate in den drei unterschiedlichen Versionen (v1-v3). Die Graustufen zeigen jeweils die Ergänzungen (v2, v3) ausgehend von X.509 v1 (weiß markiert) an. Heutzutage spielt nur noch die X.509 v3 eine Rolle.

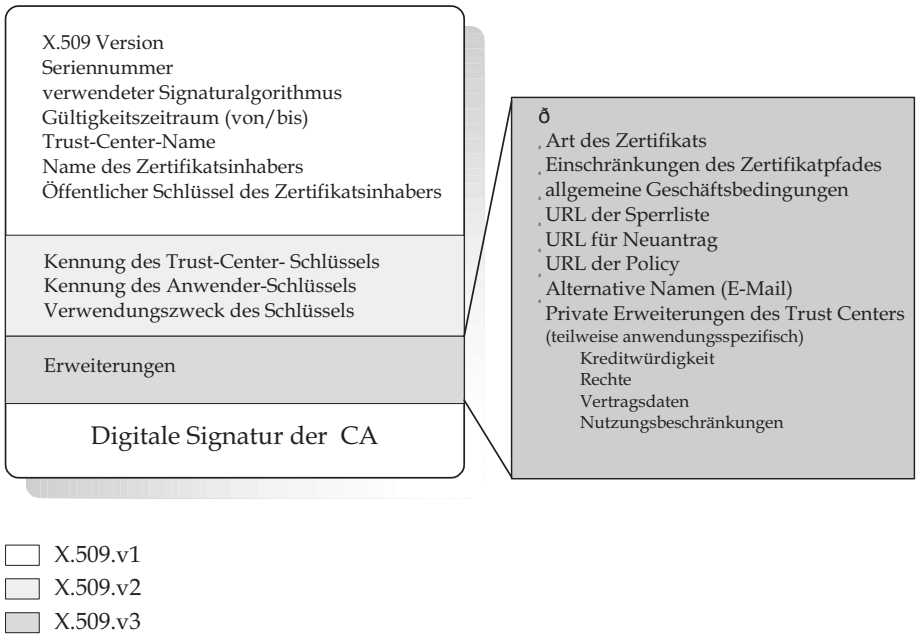


Abb. 4.15: X.509 Formatdarstellung von Zertifikaten in drei unterschiedlichen Versionen

Jede Zertifikatsergänzung schließt die Eigenschaften der Vorgängerversion mit ein. Für X.509 v3 gibt es einen ganzen Ergänzungsblock, bei dem nicht alle Einträge zwingend sind (Abb. 4.15). Am unteren Ende des X.509 v3-Zertifikats befindet sich die digitale Signatur des Herausgebers (*Certification Authority*).

[41] Die ITU-*T* ist als Unterorganisation der Vereinten Nationen die Nachfolgerin des früheren $CCITT$ ($Comité\,Consultatif\,International\,Télégraphique\,et\,Téléphonique$), die ebenfalls den Standard übernommen hat.

X.500 ist der internationale ITU-*T*-Standard (ISO Standard 9594) für einen im Netz verteilten Verzeichnisdienst (*Directory Service*, DS). Dabei wurde die ursprüngliche Version aus dem Jahr 1988 mittlerweile vollständig durch die heute gängige Version von 1993 ersetzt. In X.500-Verzeichnissen lassen sich im Prinzip beliebige Objekte speichern; dabei ist der Dienst abstrakt nach Objektklassen wie z.B. nach Personen bzw. nach Organisationen konzipiert. Weiterhin ist X.500 nachhaltig definiert worden [RFC 1777, 1778, 1959, 1960, 2255, 1823 und 2254].

Einträge von Personen oder Organisationen enthalten z.B. Name, Postanschrift, Telefonnummer und E-Mail-Adresse. Diese Einträge können von Benutzern mit Hilfe geeigneter Software durchsucht werden, um z.B. eine E-Mail-Adresse zu ermitteln oder Zertifikatsüberprüfungen anzustreben bzw. öffentliche Schlüssel von Kommunikationspartnern zu ermitteln (Abb. 4.14). Darüber hinaus können auch Netzdaten, wie z.B. Namen und Adressen von Rechnern, im X.500 verwaltet werden.

Der *Directory Service* (DS) erlaubt den system- und ortsunabhängigen Zugriff auf alle Objekte innerhalb eines Verzeichnisses. Dabei organisiert das Directory alle Objekte in einer hierarchischen Struktur, die beispielsweise nach Ländern, Organisationen und Unterorganisationen geordnet ist. Seine Strukturierung ist vergleichbar mit der hierarchischen Gliederung der X.400-Adressstruktur. X.500 ist eine sehr umfassende Richtlinie für einen Directory Service, die eine ressourcenintensive Implementation nach sich zieht. Um diese Probleme zu umgehen, wurde das Lightweight Directory Access Protocol (LDAP) zur Nutzung eines Directory Service mit schlanken/schmalen Clients entwickelt. Es ist eine vereinfachte Form des *Directory Access Protocol* (DAP) von X.500 und soll die Nutzung von Directory Services für schmale Internet-Clients erleichtern.

Der Directory Service (DS) nach ISO-Standard realisiert ein weltweit verteiltes Informationssystem. Über einen Rootknoten sind alle Länderknoten miteinander verbunden (der deutsche Knoten ist gegenwärtig an der TU-Chemnitz realisiert). An den Landes-Knoten sind die einzelnen Domains im Land (z.B. TU-Darmstadt) angeknüpft. Da die im Directory Service einer Domain gespeicherten Informationen im Allgemeinen weltweit verfügbar sind, müssen insbesondere Aspekte des Datenschutzes berücksichtigt werden. Der Directory Service nach X.500 wird verwendet für:

- Speichern persönlicher Daten von Mitarbeitern wie Name, Dienststelle, Dienst- und Privattelefon, Privatadresse, E-Mail-Adresse
- Speichern von Rechnernamen, Rechneradressen
- Speichern von Betriebsnamen und Filialen
- Speichern sonstiger Informationen

Jeder Directory-Eintrag für ein bestimmtes Objekt besteht aus einer Menge von Attributen, die für diesen Objekttyp spezifisch sind. Ein Attribut besteht aus einem Attributtyp und aus einem oder mehreren Attributwerten (Abb. 4.16). Die

Einträge sind in einer Baumstruktur abgelegt, die als *Directory Information Tree* (DIT) bezeichnet wird. Jeder Knoten im Baum entspricht dabei einem Eintrag. Einträge im Directory müssen zwingend mit einem Namen angesprochen werden. Dazu gibt es zwei Möglichkeiten:

RDN: *Relativ Distinguished Name* ist der einfache Name eines Eintrags, der im Namensattribut des Eintrags gespeichert ist. Beispiel: cn=Walter Mustermann (cn: Abkürzung für common name).

DN: *Distinguished Name* ist der global eindeutige Name, der sich aus den RDNs der übergeordneten Einträge plus RDN des Eintrags zusammensetzt. Vor den einzelnen RDNs steht jeweils ein @ oder ein Komma. Beispiel: @c=de@o=Technische Universität Darmstadt @ou=rz@cn=Walter Mustermann.

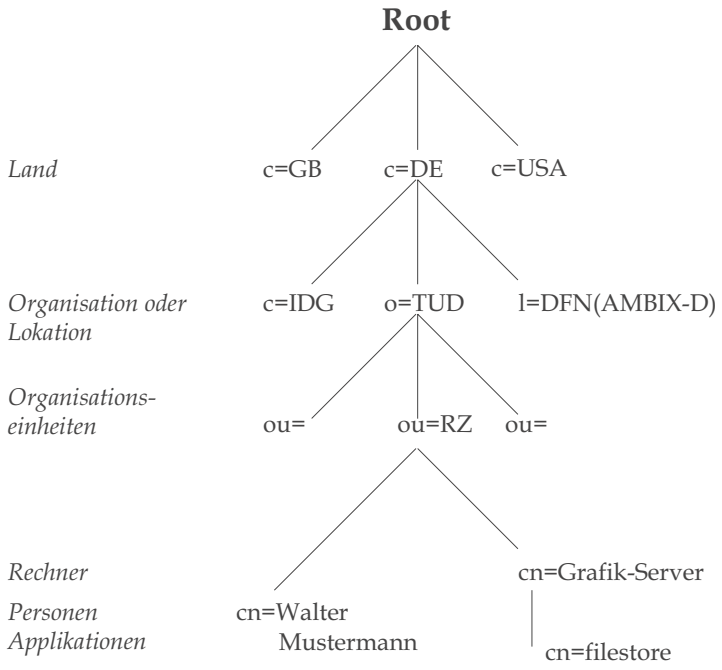


Abb. 4.16: Baumstruktur des weltweit verteilten X.500-Verzeichnis-Dienstes für Objekte der realen Welt

Die Verwaltung der Einträge erfolgt verteilt. Innerhalb des DFN-Vereins ist jede Mitgliedseinrichtung verantwortlich für alle Einträge unterhalb des Organisationseintrages. Eine weiterführende, detaillierte Beschreibung über den X.500-Verzeichnis-Dienst ist bei [Chadwick 1999] zu finden.

4.7.2 Zertifizierung und Validierung

Abb. 4.14 gibt einen Überblick der zentralen Aufgaben einer PKI. Wird zur Absicherung einer VPN-Lösung, etwa eines Remote-Access-VPN, eine PKI eingesetzt – was sinnvoll ist –, so sind im Prinzip die gleichen Prozesse wie in Abb. 4.14 einzurichten. Eine besondere Stellung nimmt dabei der Zertifizierungsprozess ein, der in Abb. 4.17 dargestellt ist. Auf eine zeitliche Betrachtung der Abläufe wird dort aber verzichtet, weil die zeitliche Komponente eine eher untergeordnete Rolle spielt. Denn es ist nicht von besonderer Bedeutung, ob ein Zertifikat z.B. für eine firmeneigene PKI einen Tag früher oder später ausgeliefert wird.

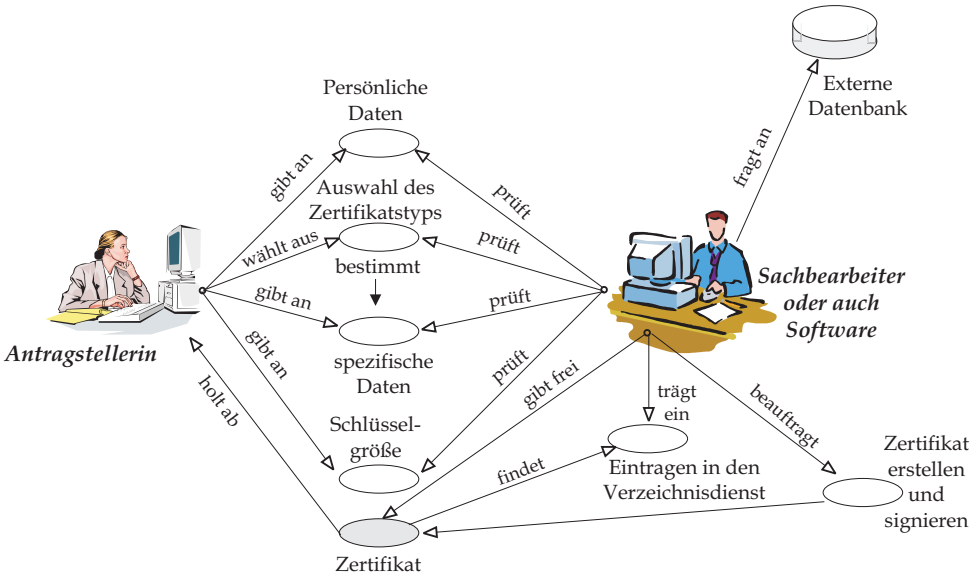


Abb. 4.17: Schematischer Ablauf eines Zertifizierungsprozesses

Der Prozess wird in diesem Fall von einer Antragstellerin initiiert, die ein Zertifikat wünscht und zu diesem Zwecke dem Personalbüro bzw. einem Sachbearbeiter persönliche Daten übermittelt. Nach Eingangsprüfung der Daten wählt die Antragstellerin einen speziellen Zertifikatstyp aus, falls mehrere Typen zur Auswahl stehen. Der Zertifikatstyp legt fest, ob und welche weiteren Daten (z.B. Merkmale aus dem Personalausweis u. ä.) notwendig sind, falls z.B. der Antragstellerin auch Handlungsvollmachten für das eigene Unternehmen ausgestellt wurden. Sind alle Prüfungen erfolgreich durchgeführt, wird mittels Zertifikat ein Schlüsselpaar (öffentlich und privat) an die Identität der Antragstellerin gebunden. Das Zertifikat wird anschließend von der unternehmenseigenen CA signiert. Das Zertifikat und bestimmte Angaben über die Antragstellerin werden freigegeben und in einem Verzeichnisdienst veröffentlicht, so dass von interessierten Personen bzw. Anwendungen der öffentliche Schlüssel beliebig oft eingesehen und

zur Überprüfung herangezogen werden kann. Abschließend kann das Zertifikat von der Antragstellerin abgeholt werden.

Wird eine unternehmenseigene PKI aufgebaut, so können die Prozesse im Prinzip wie in Abb. 4.17 dargestellt ablaufen. Bei einer Zertifikatsausstellung nach dem SigG kann dies, je nach Zertifikatstyp, sogar eine persönliche Identitätsüberprüfung bei Zertifikatsaushändigung erfordern.

Neben den PKI-Pionieren, zu denen z.B. die Firmen Entrust und Baltimore gehören, gibt es am Markt mittlerweile eine Vielzahl von PKI-Produkten und PKI-Firmen. Mehr und mehr machen jedoch auch Open Source PKI-Projekte (http://idx-pki.idealix.org) von sich reden.

4.7.3 PKI-Unterscheidungsmerkmale

In einer PKI können heutzutage nicht nur Produkte bekannter Hersteller eingesetzt werden, sondern – nachdem eine Vielzahl von Produkten auf dem Markt erhältlich sind – es kommt im Wesentlichen darauf an, welche Anforderungen an eine PKI gestellt werden. Voraussetzung ist allerdings immer, dass die relevanten *Public Key Cryptography Standards* (PKCS) eingehalten werden. Aspekte der Open-Source-Philosophie sind ebenfalls nicht von der Hand zu weisen. Welche Lösung auch immer angestrebt wird, es sollte immer darauf geachtet werden, dass eine möglichst hohe Interoperabilität mit den gängigen Lösungen eingehalten wird.

Auch eine Cross-Zertifizierung und die Einrichtung einer Brücken-CA (Bridge-CA) hat sich am Markt behauptet. Die Bridge-CA erlaubt organisationsübergreifende PKI-Lösungen, insbesondere den sicheren E-Mail-Austausch. Das Verlustproblem der Beweiskraft eines Zertifikates ist durch den vielversprechenden FLEXI-PKI-Ansatz[42], der im Rahmen der Arbeitsgruppe um Prof. Buchmann an der TU-Darmstadt entstanden ist und inzwischen kommerziell vertrieben wird, gelöst worden.

Als Evaluationskriterien sollen hier neun Punkte hervorgehoben werden, die bei einer PKI im Eigenbetrieb statt durch Fremdleistung erbracht, unter anderem zu berücksichtigen sind:

1. Wie sehen die Zertifikatsinformationen aus?
2. Gibt es Zertifikatshierarchien, wenn ja, welche?
3. Wie sieht die CA-Subjekt-Nutzer-Beziehung aus?
4. Welche Validierungsmethoden werden zur Verfügung gestellt?
5. Welche Rückrufverfahren werden unterstützt?

[42] Der Flexi-PKI-Ansatz begegnet den beiden großen Problemen, mit denen eine PKI prinzipiell behaftet ist: Zum einen ist dies der Ausfall der Funktionstüchtigkeit der PKI, zum anderen ist es der Verlust der Beweiskraft der elektronischen Signatur. Das Konzept der multiplen Signaturen löst dieses Problem.

6. Gibt es Zertifikatsnutzung für Zugriffsrechte (SSO)?
7. Gibt es eine starke Authentifikation?
8. Ist es eine In-Band- oder Out-Band-Authentifikation?
9. Existieren Möglichkeiten zur Anonymität?

Zum Schluss sollen noch andere Anwendungsszenarien, die neben dem Einsatz einer PKI für eine VPN-Lösung von mindestens gleicher Bedeutung sind, angesprochen werden.

4.7.4 Einsatz von elektronischen Zertifikaten

Für digitale Zertifikate bzw. für eine PKI gibt es ein breites Spektrum an Einsatzmöglichkeiten, die alle das Ziel des vertraulichen elektronischen Datenaustausches haben. Dabei soll die Person, die Informationen versendet, als Urheber dieser Informationen identifizierbar sein. Der Empfänger soll die Informationen im Klartext erhalten und die Integrität der Informationen soll nicht beeinträchtigt werden können.

Bei den folgenden Anwendungsbeispielen stehen diese Aspekte im Vordergrund:

Sichere E-Mail-Anwendungen: Der Inhalt von E-Mail-Nachrichten kann verschlüsselt/entschlüsselt und bei Bedarf digital unterschrieben werden (z.B. mit S/MIME oder PEM).

Sichere Desktopsysteme: PCs bzw. Desktopsysteme können durch authentifizierte Systemzugänge abgesichert werden. Hierzu gehört auch die Möglichkeit, ganze Dateisysteme oder nur dedizierte Dateien zu verschlüsseln. Der endgültige Löschvorgang ist eine weitere wichtige Funktionalität.

Absicherung webbasierter Anwendungen: Ein Zugang zu Internetseiten lässt sich mit authentifizierten Zugangskontrollen vor unerwünschten Zugriffen absichern. Zur Übertragung sensibler Daten (Passwörter, Kreditkartennummern, etc.) kann eine VPN-Technologie auf Anwendungsebene, z.B. mit SSLv3/TLS, eingesetzt werden.

Virtuelle Private Netze: Eine sichere Kommunikation über unsichere Kanäle (z.B. Internet) lässt sich neben der Anwendungsebene auch auf tieferen Schichten einrichten, indem verschlüsselte und authentifizierte Kommunikationskanäle geschaffen werden. VPN bieten bei der Einrichtung von filialübergreifenden Intranets, firmenübergreifende Extranets sowie dem sicheren Fernzugriff auf Unternehmensdaten eine hilfreiche Technologie (vgl. Abschn. 7.4.16).

Sichere Zugangskontrollen: Hierunter wird die Absicherung und der Zugriff von autorisierten Personen auf sensible Informationen verstanden. Dies setzt

allerdings voraus, dass die Anwendungen eine entsprechende Personen-Authentifizierung zulassen, wobei digitale Zertifikate fast zwingend vorausgesetzt werden müssen. Auch kann die Zeiterfassung und die Kantinenabrechnung als Mehrwertdienst erbracht werden.

Eine der wesentlichen Aufgaben bei einem Remote-Access-Zugangs ist es, zuverlässig sicherzustellen, dass nur die autorisierten Personen bzw. Applikationen Zugriff zum Firmennetz erhalten. Dieser Aspekt wird im nächsten Kapitel behandelt.

4.8 Übungen

1. Warum gehört DES zu den monoalphabehtischen Verschlüsselungsverfahren?
2. Welche Open-Source-Produkte können für eine fortgeschrittene elektronische Signatur im Falle einer E-Mail eingesetzt werden?
3. Wie könnten elektronische Zertifikate in der VPN-Technologie (VPN-Gateway zu VPN-Gateway) eingesetzt werden?
4. Beschreiben Sie die Verfahrensunterschiede zwischen der asymmetrischen Verschlüsselung und der elektronischen Signatur.
5. Übertragen Sie mögliche Handhabungen des Telefonbuchs der Metropole Paris mit der Anwendung einer Hash-Funktion (Invertierung).
6. Entwerfen Sie einen eigenen funktionierenden Diffie-Hellmann Schlüsselaustausch gemäß Abb. 4.9.
7. Die einfache Cäsar-Verschlüsselung beinhaltet aufgrund jedweder Permutation der 26 Buchstaben im Alphabet einen Schlüsselraum von 4×10^{26}; der Schlüsselraum von DES ist nur 2^{56} oder etwa 7×10^{16}, ungefähr 10er Potenzen kleiner. Woran liegt das und warum ist DES sicherer als die Cäsar-Verschlüsselung?
8. Verifizieren Sie mit einem eigens entwickelten Computerprogramm die *Auto-Key*-Variante der Vigenère-Verschlüsselung bzgl. des Chiffrats (siehe Seite 95) „ZICVTWQNGKCEIIGASXSTSLVVWLA“.
9. Wie kann bei dem Diffie-Hellman-Schlüsselaustausch-Verfahren eine *Man-in-the-middle-Attack* wirksam unterbunden werden?

10. Wie sehen die Formeln zur Berechnung von K_{H1} und K_{H2} bei Host H1, H2 sowie (D) aus?

11. Begründen Sie den Unterschied zwischen einer Prüfsumme und einer Hash-Funktion, die für kryptographische Zwecke tauglich ist.

12. Warum kann für ein kryptographisches Verfahren keine reine Prüfsummenbildung (CRC) eingesetzt werden?

5 Verfahren zur Authentifizierung

Der Grund einer Authentifizierung im Falle eines VPN resultiert aus dem Bedürfnis, dass zwei Kommunikationspartner bzw. VPN-Gateways abgesichert sein sollen. Authentifizierungsverfahren spielen für die VPN-Technologie eine zentrale Rolle. Sie sichern die virtuellen Netzverbindungen ab und gewährleisten, dass nur autorisierte Nutzer eine Verbindung aufbauen können.

Prinzipiell lassen sich bei der Authentifizierung alle Identifikations- und Authentifizierungsverfahren auf die Überprüfung einer dieser drei Größen (Faktoren) zurückführen:

- Etwas, das man weiß (Passwörter)
- Etwas, das man darstellt (Aussehen, Biometrie)
- Etwas, das man besitzt (Zugriffstoken)

Oftmals können auch mehrere Varianten gekoppelt sein, z.B. bei EC-Karten, die Besitz und Wissen verknüpfen. Bessere Sicherungssysteme zeichnen allerdings den Überprüfungsvorgang komplett auf.

Der Begriff Authentifizierung[1] wird ganz allgemein im Zusammenhang mit Konzepten und Systemen zur Absicherung benutzt. Von besonderer Wichtigkeit ist in diesem Kontext die Authentifizierung eines Computers, der mittels VPN Zugang zum firmeneigenen LAN erlangen will. Dies kann von einem einfachen ungesicherten Passwort über Zwei-Wege-Verfahren, die noch zeitsynchron gekoppelt sind, bis zu den Drei-Wege-Verfahren reichen. In diesem Kapitel werden zunächst die beiden sich vom Sicherheitsaspekt her steigernden Authentifizierungsverfahren diskutiert – die einfachen in Abschn. 5.1, die starken in Abschn. 5.2. Die zeitsynchronen Verfahren mittels *Token* werden in Abschn. 5.3.1 vorgestellt. Abschn. 5.4 schließlich behandelt die in der Praxis häufig vorkommenden und eingesetzten technischen Verfahren.

Grundsätzlich gibt es bei der Absicherung von Informationen und Informationssystemen im Sinne einer Authentifizierung zwei große Gebiete:

- Zugangssicherung bzw. Zugriffssicherung für technische Systeme mit dem Ziel, dass nur autorisierte Subjekte und Objekte, Zugang bzw. Zutritt erlangen können

[1] Häufig wird statt *Authentifizierung* auch *Authentizierung*, *Authentisierung* oder *Authentikation* benutzt. Auch wenn das englische Wort *authentication* heißt, wird authenticate mit authentifzieren übersetzt. Somit müßte das zugehörige Substantiv *Authentifizierung*, bestenfalls noch *Authentifikation* lauten. Die Lektüre des Oxford Großwörterbuches Englisch lässt keinen anderen Schluss zu.

- Integrität und Urheberschaft bei elektronischen Dokumenten mit dem Ziel, die Authentizität eines Dokumentes sicherzustellen

Nachfolgend werden beide Gebiete der Authentifizierung näher erläutert und zur VPN-Technologie Bezug genommen.

Zugangssicherung bei technischen Systemen

Hier soll die Identität einer Person festgestellt werden, die entweder Zugang zu einem technischen System hat, mit dem z.B. auf ein VPN zugegriffen werden soll, oder die Zugriff auf Informationen über ein technisches System erhalten will. Konkrete technische Systeme enthalten üblicherweise Komponenten zur Personenidentifizierung, die jetzt vermehrt aufkommenden biometrischen Verfahren (Fingerabdrücke, Stimme, Iris) oder wie die Komponenten zur Überprüfung von speziellem Wissen (Password, PIN, TAN).

Eine erhebliche Steigerung der Absicherung technischer Systeme kann erreicht werden, wenn die sicherheitsrelevanten Informationen nicht mehr auf dem Rechner gespeichert werden, bei Unix-Systemen in der etc/passwd-Datei, sondern auf eine Chipkarte ausgelagert werden. Derartige Betriebssysteme werden als *Trusted-Operating-Systems* (TOS) bezeichnet. Darüber hinaus gibt es bei solchen Systemen zwei getrennte im Betriebssystemkern definierte Administratoren. Der reguläre Administrator kümmert sich um alle nicht sicherheitsrelevanten Aufgaben, der zweite, der Sicherheitsadministrator, verantwortet die sicherheitsrelevanten Aufgaben, die nur nach dem Vier-Aufgaben-Prinzip bearbeitet werden dürfen. Diese Betriebssysteme sind z.B. in Trust Centern zu finden. Die T-Nova (Telekom) hat ein Forschungsprojekt höchst erfolgreich abgeschlossen, bei dem ein derartiges Betriebssystem (TOS) auf Basis von SUN-Solaris in Zusammenarbeit mit der Firma Argus und der TeleSec-Chipkarte der Telekom entwickelt wurde.

Weiterhin werden Schlüsselaustauschverfahren[2] zwischen den Endstellen (Kopfstellen, Gateways) eines VPN eingesetzt, die unterscheiden, wer (z.B. welche IP-Adresse) rechtmäßigen Zutritt zu einem abgesicherten Tunnel eines VPN erhält und wer nicht. Auch der Zugriff auf ein VPN selbst kann durch unterschiedlich wirkungsvolle Authentifizierungsmethoden abgesichert werden, die in diesem Kapitel noch vertieft diskutiert werden.

Integrität und Urheberschaft bei elektronischen Dokumenten

Bei der Integrität und Urheberschaft handelt es sich mehr um die Authentizität, als um die Echtheit von elektronischen Dokumenten. Um die Echtheit eines Dokumentes prüfen zu können, müssen zwei Fragen beantwortet werden:

1. *Ist das Dokument X unverändert?*
   Bei der Speicherung und Übertragung elektronischer Dokumente soll die Integrität, d.h. die Unverändertheit des Inhalts sichergestellt werden. Dies ist

[2] So verwendet IPSec, das zur Zeit wohl populärste Verfahren bei VPN – das Diffie-Hellman-Schlüsselaustausch-Verfahren zur Identifikationsprüfung.

besonders wichtig, wenn elektronische Dokumente über lange Zeiträume hinweg unverändert erhalten bleiben müssen. Ein aktuelles Beispiel sind die elektronischen Grundbücher oder auch die elektronischen Geburtsurkunden, die in absehbarer Zeit eingeführt werden.

2. *Stammt das Dokument X tatsächlich von der Person Y?*
   Elektronische Dokumente sollen ihrem Urheber eindeutig zuzuordnen sein. Nur wenn die Urheberschaft zweifelsfrei nachweisbar ist, lassen sich z.B. Urheberrechte durchsetzen.

Bei elektronischen Dokumenten kommt sowohl die Zugriffssicherung als auch die Integritätsaspekte zum Tragen. Oftmals wird die Authentizität mittels digitaler Signaturen sichergestellt. Abschn. 4.6 beschäftigt sich eingehend mit digitalen Signaturen.

Im Prinzip lassen sich die Authentifizierungsverfahren gemäß ITU-*T* unterteilen in:

1. *einfache* Authentifizierungsverfahren nach ITU-*T*-Standard X.509[3] (Abschn. 5.1), zu denen z.B. das traditionelle Passwortverfahren zählt, aber auch die Einmal-Passwörter (*One-Time-Password-System*, OTP), die nicht auf die Public-Key-Kryptographie zurückzuführen sind, sondern die Einweg-Hash-Funktionen verwenden.
2. *starke* Authentifizierungsverfahren nach X.509, die so genannte Credentials benutzen, die auf kryptographische Techniken zurück greifen (Abschn. 5.2). Zu ihnen zählen PAP, CHAP, TACACS und RADIUS sowie die Hardwarebasierten Verfahren wie Tokens, Smart Cards und PC-Cards und die oben erwähnten biometrischen Verfahren. Dieser Standard empfiehlt nur die Verwendung starker Authentifizierungsverfahren.

In der Praxis wird häufig keine strikte Trennung der beiden Verfahren vorgenommen, sondern es werden Mischformen (Hybride) eingesetzt. So ist es üblich, eine Chipkarte, auf der sich ein sicher abgelegter Schlüssel befindet, zusätzlich mit einem PIN-Verfahren zur Aktivierung der Chipkarte zu verknüpfen.

Nach der Darstellung dieser zwei Authentifizierungsverfahren wird näher auf die Chipkarten- bzw. Smart Card-Technologie eingegangen, da diese für die VPN-Technologie eine weitreichende Bedeutung als Authentifizierungsmedium erlangt hat bzw. noch erlangen wird.

5.1 Einfache Authentifizierungsverfahren

Die einfachen Authentifizierungsverfahren lassen sich in die einfachen *ungeschützten* und in die einfachen *geschützten* Verfahren aufteilen. Prinzipiell be-

[3] Der X.509-Standard ist eher als Framework zu verstehen, der mittlerweile von der IETF-Arbeitsgruppe (pkix) durch mehrere RFCs erweitert wurde.

ruhen die einfachen Authentifikationsverfahren *(one-way, two-party)* auf Passwörtern zur Benutzerkennung und zur Identifikation. Sie sollten nur für lokale Systemzugänge eingesetzt werden. Denn die *ungeschützten* Verfahren verwenden lediglich statische Passwörter. Diese Verfahren können allerdings in *geschützte* umgewandelt werden, indem eine Einweg-Hash-Funktion auf die Nutzerkennung und auf das Passwort angewandt wird. Dabei beinhaltet diese Funktion neben Kennung und Passwort auch eine Zeitmarke und eine Zufallszahl. Alternativ können Einmalpasswörter verwendet werden, die nach Gebrauch hinfällig sind. [Lamport 1981] hat ein interessantes Schema für ein Einmal-Passwort-System beschrieben. Das Verfahren ist nicht aus der Public-Key-Kryptographie abgeleitet, sondern geht auf die Anwendung von Einweg-Hash-Funktionen zurück. Diese Idee wurde inzwischen in etlichen Implementierungen verwendet.

Bekannt geworden ist die S/Key-Implementierung von der Fa. Bellcore (jetzt Tcordia Technologies Inc.) unter [RFC 1760], die die MD4-Hash-Funktion nutzt. Eine Weiterentwicklung wurde durch die IETF mit dem [RFC 2289] unter dem Namen OTP verfolgt. Das One-Time-Password-System kann dagegen mit MD5, SHA-1 oder mit MD4 als Hash-Funktion betrieben werden. Sie laufen wie folgt ab.
Ein Server verwaltet eine Datenbasis, die pro Nutzer folgende Information enthält:

- Name des Nutzers
- Die ganze Zahl n, die sich bei jeder erfolgreichen Authentifizierung um den Wert 1 reduziert
- Der Wert, der sich bei n-facher Anwendung der Einweg-Hash-Funktion auf das Passwort ergibt, also $hash^n\ (Passwort)$ bzw. $hash\ (hash(...(hash(Passwort))...))$

Allerdings muss angemerkt werden, dass dieses Verfahren mit einigen Beschränkungen behaftet ist:

- Es findet keine echte gegenseitige Authentifizierung der Kommunikationspartner statt. Nach erfolgtem Austausch kann nicht zuverlässig bestätigt werden, ob der Kommunikationspartner, mit dem die Daten ausgetauscht wurden, auch tatsächlich der gewünschte Partner war.
- Ein Schutz vor aktiven Attacken wird nicht geboten.
- Die nach der Authentifizierung ablaufende Kommunikation erfolgt unverschlüsselt, wenn nicht weitere Maßnahmen ergriffen werden. Ein sicherer Schlüsselaustausch ist nicht möglich.

Ungeschützte Authentifizierung

Abb. 5.1 zeigt das Prinzip der einfachen *ungeschützten* Authentifizierung am Beispiel eines lokalen Systemzugangs. Derartige Sicherungssysteme befinden sich allerdings auf einem geringen Niveau, da Passwörter im Grunde keinen wirksamen

Schutz darstellen. Mit dem Wörterbuchangriff *(Dictionary Attack)* – beispielsweise mit dem Werkzeug L0phtCrack[4] – sind gerade unter Windows NT, erhebliche „Erfolge“ erzielt worden. Dies liegt nicht zuletzt an den einfachen Passwörten, die von den Nutzern gewählt wurden, wie [Schneier 2000] anschaulich ausführt. Abb. 5.1 zeigt das einfache Verfahren, das in einer offenen Systemumgebung zur Authentifizierung miteinander kommunizierender Systeme bzw. Instanzen eingesetzt werden kann. In der Abb. 5.1 wählt sich ein Subjekt (A) in das Objekt (B) ein. Die untere Bildhälfte zeigt den schematischen Ablauf. Die Ziffern werden im nachfolgenden Text erläutert.

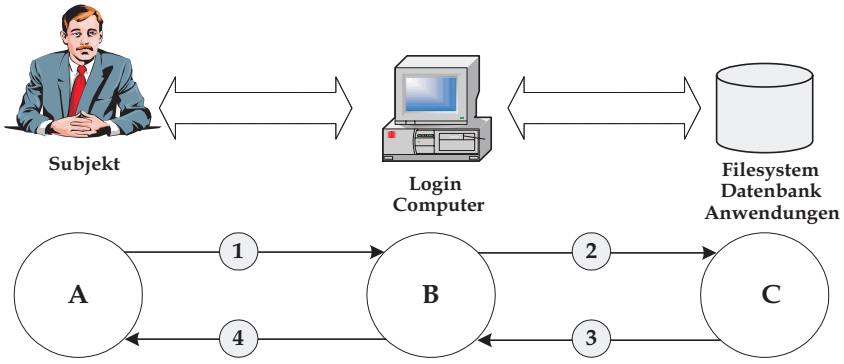


Abb. 5.1: Einfache ungeschützte Authentifizierung

Angenommen, Kommunikationspartner A will sich bei der Instanz B authentifizieren; dabei kennt A seine Kennung sowie das Passwort, die im Vorfeld mitgeteilt wurden. Im ersten Schritt (1) überträgt A seine Kennung und sein Passwort an B. Daraufhin überprüft B in einem zweiten Schritt (2), ob die Kennung von A gültig ist und vergleicht bei positivem Ergebnis das von A mitgeschickte Passwort mit dem zur Kennung von B gehörigen Passwort, das in einer Datenbank abgelegt ist (Schritt 3). Bei einer Übereinstimmung ist die Authentifizierung erfolgreich abgelaufen, andernfalls schlägt sie fehl. Abschließend übermittelt B in Schritt (4) die Bestätigung bzw. Ablehnung an A. Nun kann A bei positiver Authentifizierung mit dem System kommunizieren.

Die Wirksamkeit des Verfahrens ist unmittelbar von der Geheimhaltung des Passwortes sowie von der Wahl des Passwortes abhängig. Daher sollten bei der Wahl des Passwortes einige Regeln beachtet werden, die z.B. im Grundschutzhandbuch des BSI zu finden sind [BSI 2004a]. Passworte gehören zur Gruppe der einfachen Authentifizierungsverfahren und werden wohl in absehbarer Zeit, aufgrund ihres geringen Schutzes, weiter zurück gedrängt werden. Es gibt Gesamtkostenrechnungen die Belegen, das für ein Unternehmen, mit z.B. 1000 Desktop-Arbeitsplätze, es kostengünstiger ist, gegenüber einfachen Passwörtern, Token

[4] Das Programm ist im Internet unter der Adresse http://www.l0pht.com zu finden.

einzusetzen und dabei eine höhere Sicherheit erzielen.

Langfrisitig werden sich mehr und mehr regelrechte Identity-Management-Systeme auf Basis von Meta-Verzeichnissen, die X.509 nutzen, durchsetzen. Damit lassen sich dann Rollen und eine automatisierte Vergabe von Accounts und Berechtigungen - das so genannte Provisioning erreichen.

Geschützte Authentifizierung

Eine höheres Sicherheitsniveau kann durch die Verwendung von Einmal-Passwörtern erzielt werden. Eine Variante zur Erstellung dieser Einmal-Passwörter wurde bereits zu Beginn des Abschn. 5.1 beschrieben. Jetzt soll das ITU-*T*-Standard X.509-Verfahren diskutiert werden, das mit Zufallszahlen und Hash-Werten arbeitet.

Es gibt zwei Möglichkeiten, wie ungeschützte Passwörter in geschützte Einmal-Passwörter überführt werden können. Am Beispiel der Authentifizierung des Kommunikationspartners A gegenüber einem System B sind beide Verfahren in Abb. 5.2 dargestellt. Dabei entspricht der untere Teil des Bildes dem unteren Teil von Abb. 5.1.

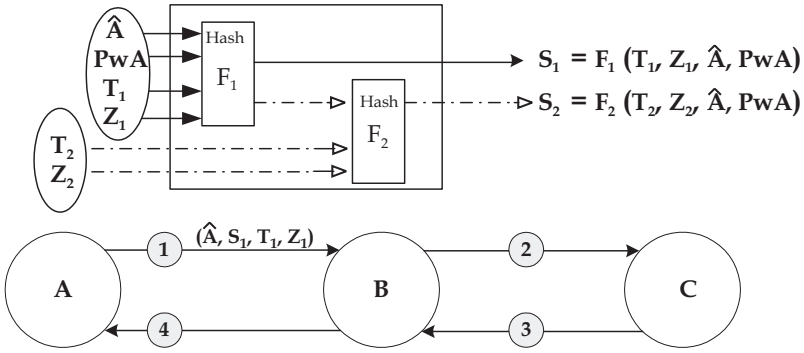


Abb. 5.2: Einfache geschützte Authentifizierung mittels Zeitmarken und Zufallszahlen, Quelle X.509

Die in Abb. 5.2 verwendeten Buchstaben und Ziffern bedeuten:

$\hat{A}$ **:** Kennung des Kommunikationspartners A,

PwA **:** statisches (ungeschütztes) Passwort von A,

T_1, T_2 **:** Zeitmarke 1 und 2,

Z_1, Z_2 **:** Zufallszahl 1 und 2,

F_1, F_2 **:** mathematische Hash-Funktionen, z.B. MD5, SHA-1,

S_1, S_2 **:** geschützte Einmal-Passwörter.

Zu beachten ist, dass beide Verfahren Zeitmarken und Zufallszahlen optional verwenden. Erst die Verwendung von Zeitmarken und Zufallszahlen lassen die geschützten Passwörter durch die nachfolgend beschriebene Methode zu Einmal-Passwörtern werden. Kern des Verfahrens bilden mathematische Hash-Funktionen, die bereits in Abschn. 4.5 beschrieben wurden.

Die Verfahren zur Erzeugung der geschützten Passwörter S_1 und S_2 sind in der oberen Hälfte der Abb. 5.2 dargestellt:

- Das erste Verfahren berechnet aus der Kennung $\hat{A}$ und dem Passwort PwA von A in Verbindung mit der Zeitmarke T_1 und einer Zufallszahl Z_1 mittels der Einweg-Funktion F_1 das geschützte Passwort S_1, wie der schwarze Pfeil andeutet.
- Das zweite Verfahren ist zweistufig ausgelegt. Das wie zuvor erzeugte Passwort S_1 (die oberste unterbrochene Linie) wird zusammen mit einer Zeitmarke T_2 und einer Zufallszahl T_2 einer weiteren Hash-Bildung mittels F_2 modifiziert. Als Ergebnis liegt das geschützte Passwort S_2 vor, wie die unterbrochene Linie und der offene Pfeil zeigen. Die eingesetzten Einweg-Funktionen F_1 und F_2 können verschieden oder identisch sein.

Die Authentifizierung mittels geschützter Passwörter ist in der unteren Hälfte von Abb. 5.2 dargestellt:

Schritt 1: Bei Verwendung von S_1 übermittelt A neben seiner Kennung $\hat{A}$ und seinem geschützten Passwort S_1 die Zeitmarke T_1 und die Zufallszahl Z_1 an B.

Schritt 2: B überprüft als erstes die Gültigkeit der Kennung $\hat{A}$.

Schritt 3: Bei Erfolg liest B das Passwort PwA aus seiner Datenbasis C aus. C liegt sowohl die Kennung $\hat{A}$ als auch das ungeschützte Passwort pwA vor. Zudem ist die Hash-Bildung mittels der Einweg-Funktion F_1 zwischen A und B abgestimmt. Zusammen mit der Kennung $\hat{A}$, der Zeitmarke T_1 und der Zufallszahl Z_1 berechnet B mittels F_1 das geschützte Passwort und vergleicht das Ergebnis mit dem von A übermittelten Wert von S_1.

Schritt 4: Bei Übereinstimmung gilt A als autorisiert und eine Kommunikation wird akzeptiert, andernfalls abgewiesen.

Auch dieser Ablauf stellt die bekannte 1:1-Bezeichnung dar.

Der Ablauf bei der Authentifizierung mit geschütztem Passwortes S_2 ähnelt dem für S_1 beschriebenen Ablauf. Allerdings schickt A an B neben seiner Kennung $\hat{A}$ und seinem geschützten Passwort S_2 die Zeitmarken T_1 bzw. T_2 sowie die Zufallszahlen Z_1 bzw. Z_2.

5.2 Starke Authentifizierungsverfahren

Die starken Authentifikationsverfahren gehen auf die in Abschn. 4.3 beschriebenen asymmetrischen Verschlüsselungsverfahren, auch als Public Key Cryptography Standards (PKCS[5]) bezeichnet , zurück. Sie beruhen in der Regel auf einem Zwei-Wege-Verfahren *(two-way, two-party)*. Im Gegensatz zu den Ein-Wege-Verfahren *(one-way, two-party)*, bei denen sich nur ein Kommunikationspartner einseitig seinem Gegenüber ausweist, identifizieren sich in einem Zwei-Wege-Verfahren beide Kommunikationspartner gegenseitig. Hierfür muss ein Nachrichtenaustausch zur Identifizierung in beide Richtungen erfolgen.

Wird zur Unterstützung eine dritte Instanz zur gegenseitigen Authentifizierung hinzugezogen – häufig als Vertrauensinstanz (*Trusted Third Party*, TTP) bezeichnet –, ist ein Drei-Instanzen-Protokoll wie die Public-Key-Kryptographie notwendig. Sie basiert auf einem Schlüsselpaar – von dem der eine öffentlich und der andere geheim und nur seinem Besitzer bekannt ist – und einer eindeutigen Beziehung der Schlüssel untereinander, indem sich beide Schlüssel ergänzen, jedoch nicht voneinander ableiten lassen.

Wie die einfachen Authentifizierungsverfahren setzen auch starke Authentifizierungsverfahren eine eindeutige Kennung jedes Teilnehmers voraus. Die Zuweisung einer solchen Kennung obliegt bei der Public-Key-Kryptographie einer dritten Instanz. Dabei wird vorausgesetzt, dass jede Kennung einmalig vergeben wird. Die starken Authentifizierungsverfahren identifizieren einen Benutzer anhand des Besitzes eines privaten Schlüssels. Ein zweiter Benutzer kann ermitteln, ob ein Kommunikationspartner im Besitz eines solchen Schlüssels ist und nutzt die so gewonnene Information zur Feststellung der Identität des Kommunikationspartners.

Der ITU-*T*-Standard X.509 beschreibt die Möglichkeit einer Verifikation von öffentlicher Schlüsseln anhand der Zertifikate, die von einer vertrauenswürdigen dritten Instanz (Trusted Third Party oder Trust Center) ausgestellt wurden. Diese bestätigen die rechtmäßige Zugehörigkeit des öffentlichen Schlüssels zum Benutzer. Das Trust Center übernimmt damit eine Beglaubigungsfunktion, ohne die die starken Authentifizierungsverfahren obsolet wären. In Abschn. 4.7 sind hierzu unterschiedliche Fragestellungen diskutiert worden. Der X.509-Standard beschreibt auch, welcher Token in einem Verzeichnis signiert werden kann, jedoch wird kein spezifischer Standard für die digitale Signatur gefordert. Der Standard beschreibt weiterhin eine Ein-Zwei-Drei-Wege-Authentifizierung, die nachfolgend diskutiert wird.

[5] Die PKCS-Spezifikationen wurden ursprünglich von den RSA Laboratories alleine herausgegeben. In der Zwischenzeit hat sich die Zusammenarbeit mit anderen Herstellern weltweit ausgedehnt. Teile der Spezifikationen wurden in andere Standards wie z.B. PKIX, SSL oder SMIME übernommen. Dabei sind inzwischen 15 Standards - PKCS#1 bis PKCS#15 - entwickelt worden.

5.2.1 Ein-Wege-Authentifizierung

Bei der Ein-Wege-Authentifizierung eines Nutzers A gegenüber B findet nur eine einseitige Identifikation statt. Eine Kennungsinformation wird von Nutzer A an Nutzer B geschickt (Abb. 5.3). Die Ein-Wege-Authentifizierung bietet dabei:

- Nachweis der Identität von A, das Einmal-Passwort wurde tatsächlich von A erzeugt
- Nachweis der Identität von B, das Einmal-Passwort wurde tatsächlich an B übermittelt
- Nachweis der Integrität und Originalität[6] des Passwortes.

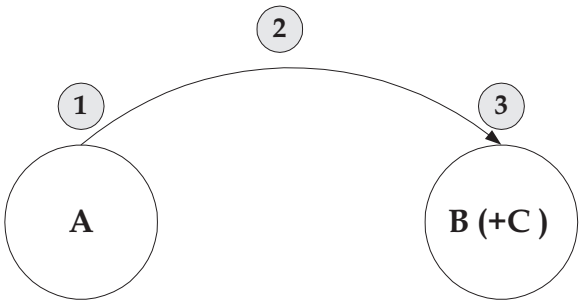


Abb. 5.3: Ein-Weg-Authentifizierung, laut X.509

Das Verfahren der Ein-Wege-Authentifizierung von A gegenüber B ist in Abb. 5.3 dargestellt. Im Einzelnen werden folgende Schritte ausgeführt:

Schritt 1: A generiert eine sich nicht wiederholende Zahl r_A, die zum Aufdecken von Mißbrauch *(Replay Attack)* und Fälschungen dient.

Schritt 2: A übermittelt die folgenden Nachrichten an B:

- Das Zertifikat für den öffentlichen Schlüssel von A.
- Die von A digital signierte Information $t_A, r_A, B, DS\{t_A, r_A, B\}$, t_A ist eine Zeitmarke, die den Generierungs- und den Verfallszeitpunkt der übermittelten Information enthält.

Schritt 3: B führt nun folgende Aktionen aus:

- B erhält aus dem Zertifikat von A dessen öffentlichen Schlüssel.
- B verifiziert die Signatur und damit die Integrität der signierten Daten.

[6] Originalität bedeutet in diesem Zusammenhang, dass es sich um ein Passwort handelt, das nicht schon zwei- oder mehrfach übermittelt wurde.

- B überprüft, ob die Informationen für ihn bestimmt sind.
- B überprüft anhand der Zeitmarke, ob nicht die Zahl r_A wiederholt übermittelt wurde. Dazu erhält r_A eine fortlaufende Sequenz, die durch eine lokale Implementierung auf seine Eindeutigkeit hin geprüft wird. Die Gültigkeit von r_A wird durch die Zeitmarke festgelegt.

5.2.2 Zwei-Wege-Authentifizierung

Bei der Zwei-Wege-Authentifizierung wird im Gegensatz zur Ein-Wege-Authentifizierung eine Antwort von B an A geschickt. Damit bietet die Zwei-Wege-Authentifizierung zusätzlich den Nachweis darüber, dass das Passwort in der Antwort von B tatsächlich an A gesendet wurde und den Nachweis der Integrität und Originalität des als Antwort übermittelten Passwortes. Der Ablauf der

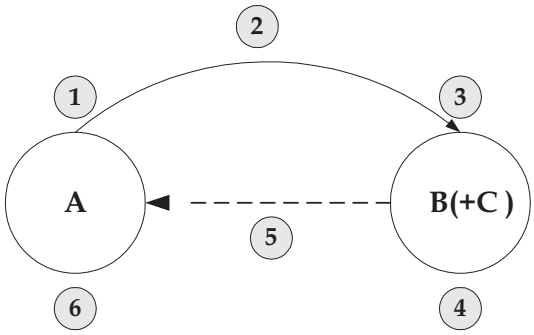


Abb. 5.4: Zwei-Wege-Authentifizierung, gemäß X.509

Zwei-Wege-Authentifizierung ist in Abb. 5.4 dargestellt. Dabei sind die Schritte 1 bis 3 identisch mit den der Ein-Wege-Authentifizierung in Abb. 5.3. Die Abfolge der Schritte 4 bis 6 ähneln inhaltlich denen der Schritte 1 bis 3. Allerdings sind die Positionen der Kommunikationspartner vertauscht. Im einzelnen bedeutet dies:

Schritt 4: B generiert eine nicht wiederkehrende Zahl r_B. Sie dient dem gleichen Zweck wie zuvor r_A.

Schritt 5: B übermittelt folgende Nachrichten an A:

- Das Zertifikat für den öffentlichen Schlüssel von B.
- Die von B digital signierte (DS) Information t_B, r_B, A, r_A mit $DS\{t_B, r_B, A, r_A\}$, t_B ist eine Zeitmarke, die den Generierungs- und den Ungültigkeitszeitpunkt der übermittelten Information enthält.

Schritt 6: A führt nun die folgenden Aktivitäten aus:

- A erhält aus dem Zertifikat von B dessen öffentlichen Schlüssel.

- A verifiziert die Signatur und damit die Integrität der signierten Information.
- A überprüft, ob die Information für ihn bestimmt ist.
- A überprüft die Aktualität der Zeitmarke t_B, und ob die Zahl r_B nicht schon einmal übermittelt wurde.

5.2.3 Drei-Wege-Authentifizierung

Merkmal der Drei-Wege-Authentifizierung ist ein dreifacher Informationsaustausch zur gegenseitigen Authentifizierung zwischen A und B. Ergänzend zur Zwei-Wege-Authentifizierung erfolgt ein weiterer Nachrichtenaustausch zwischen A und B; damit erübrigt sich eine Überprüfung der Zeitmarken. Die Drei-Wege-Authentifizierung bietet das gleiche Sicherheitsniveau wie die Zwei-Wege-Authentifizierung. Der Ablauf der Drei-Wege-Authentifizierung ist in Abb. 5.5 dargestellt. Die Schritte 1 bis 6 sind nahezu identisch mit denen der Zwei-Wege-Authentifizierung. Jedoch können in den Schritten 2 und 5 die Zeitmarken entfallen und somit in den Schritten 3 und 6 auch nicht überprüft werden.

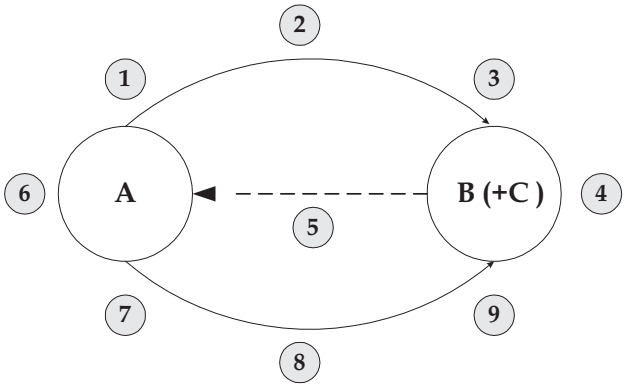


Abb. 5.5: Drei-Wege-Authentifizierung, gemäß X.509

Schritt 7: A überprüft, ob die empfangene Zahl r_A mit der ursprünglich gesendeten Zahl übereinstimmt.

Schritt 8: A übermittelt folgende signierte (DS) Information an B: r_B, B, $DS\{r_B, B\}$.

Schritt 9: B prüft daraufhin:

- ob die Signatur und damit die Integrität der signierten Informationen stimmen
- ob empfangene und gesendete Zahl r_B identisch sind.

Als weitere Variante kann ein elektronischer Zeitstempel eingesetzt werden, der auf beiden Seiten in Abhängigkeit von einem gegebenen Zeitintervall Berechnungen durchführt, die bei beiden Kommunikationspartnern eine jeweils identische Zahl zur Identifizierung erzeugen.

5.3 Zwei-Faktoren-Authentifizierung in der Praxis

Die heute in der Sicherheitstechnologie bevorzugt eingesetzten Verfahren gehen auf eine Zwei-Faktoren-Authentifizierung zurück. Dabei besteht einer der Faktoren aus einem Token oder einer Chipkarte bzw. Smart Card. In diesem Abschnitt wird zunächst auf die Token-Card eingegangen, bei der eine synchrone Zeit sowie kryptographische Schlüssel eine zentrale Rolle spielen. Anschließend wird die Chipkarten- und die Smart Card-Technologie behandelt. Der Smart Card-Technologie wird übrigens eine große Zukunft vorausgesagt, kann sie doch neben der reinen Authentifizierung auch andere Dienste verrichten. Biometrische Verfahren hingegen sind derzeit kaum im operativem Einsatz, gewinnen jedoch zunehmend an Bedeutung.

5.3.1 Zeitsynchrone Authentifizierung mittels Token-Cards

Unter dem abstrakten Begriff Token wird die Information verstanden, mit der sich ein Sender beim Empfänger authentifizieren kann und die im Verlaufe einer starken Authentifikation zwischen Sender und Empfänger ausgetauscht wird. Eine Token-Card, z.B. die SecureID-Card der Firma RSA, ist ein Passwort-Generator, in Umfang und Größe vergleichbar mit einer Chipkarte. Häufig wird diese Technologie zur Authentifizierung bei Fernzugriffen auf das firmeneigene LAN eingesetzt.

Die Token-Card erzeugt in Abhängigkeit von einem Zeitintervall Tokens zur Authentifizierung und zeigt sie auf einem Display an. Beim Token handelt es sich in der Regel um eine sechsstellige ganze Zahl, die sich innerhalb ihrer Gültigkeitsdauer nur ein einziges Mal zur Authentifizierung verwenden lässt. Somit handelt es sich um ein Authentifizierungsverfahren, das Einmal-Passwörter verwendet.

Eine Token-Card ist ein in sich geschlossenes System, das die Tokens – vom Authentifizierungsserver entkoppelt, der ins firmeneigene LAN eingebunden ist – erzeugt. Dabei wird Token nach einem festgelegten Hash-Algorithmus erzeugt. Die Eindeutigkeit der generierten Folge wird durch einen eindeutigen, auf der Token-Card hinterlegten Schlüssel (*Seed*) gewährleistet. Eine interne Quarzuhr sorgt für den zeitlichen Wechsel der Tokens und geht in digitalisierter Form in die Sequenz ein, zu der der Hash-Wert berechnet wird.

Ein Nutzer erhält, begleitend zur Token-Card, eine vierstellige PIN. Die Benutzung der Token-Card kann nur in Verbindung mit dieser PIN erfolgen. Damit wird eine Authentifizierung auf der Basis von Besitz und Wissen erreicht. Die

Token-Card stellt den Besitz dar und die PIN das Wissen. Beides ist zur Authentifizierung zwingend erforderlich, so dass von einer *Zwei-Faktor*-Authentifizierung gesprochen wird. Zur Authentifizierung ist also die Eingabe der PIN und der im aktuellen Zeitfenster gültige Token notwendig.

Der Authentifizierungsserver ermittelt anhand der PIN die Identität des Benutzers und hat somit Zugriff auf den Schlüssel der dem jeweiligen Benutzer zugeordneten Token-Card. Mit der systemeigenen Uhr ist der Server in der Lage, die richtige Sequenz zur Berechnung des Hash-Wertes und damit des Tokens durchzuführen. Der anschließende Vergleich von eingegebenem und auf dem Authentifizierungsserver selbst berechneten Token erlaubt eine Verifizierung, ob die Authentifizierung des Benutzers erfolgreich war oder nicht.

Voraussetzung bei diesem Verfahren ist die zeitliche Synchronität zwischen den Uhren in der Token-Card und im Authentifizierungsserver. Um diese Voraussetzung zu erfüllen, berechnet der Server bei Abweichungen zwischen eingegebenem und berechnetem Token sein Token neu, wobei ein zeitliches Toleranzfenster eine gewisse Ungenauigkeit zulässt. Wird eine Toleranz festgestellt, wird für die spezielle Karte intern der Korrekturwert des Toleranzfensters gespeichert und bei der nächsten Anmeldung wieder verwendet. Somit kann im Toleranzrahmen einer der Server Zeitdifferenzen zwischen seiner lokalen Uhr und der Quarzuhr in der Token-Card kompensieren.

Abb. 5.6 illustriert die zeitsynchrone Authentifizierung eines Notebooks mittels einer Token-Card in fünf Schritten über das öffentliche Fernsprechnetz zu einem Unternehmensnetz. Dabei öffnet sich der Zugang zur ISDN-Plattform firmenseitig durch einen speziellen Zugangsserver (NAS). Doch bevor ein Zugriff auf das LAN des Unternehmens erfolgen kann, wird an einem dafür vorgesehenen Server eine Authentifizierung durchgeführt. Die dazu notwendigen Informationen befinden sich in dem Authentifizierungsserver. Eine Anmeldung läuft wie folgt ab:

1. Zu einem früheren Zeitpunkt muss eine Personalisierung erfolgt sein, bei der der Nutzer eine Token-Card, einen persönlichen kryptographischen Schlüssel und eine zur Token-Card eingerichtete PIN zugewiesen bekommen hat.
2. Der Nutzer liest aus der Token-Card das gerade erscheinende Einmal-Passwort ab (hier: 78901) und fügt seine PIN in die DFÜ-Software seines Notebooks ein.
3. Die DFÜ-Software wählt sich über das öffentliche Fernsprechnetz in den Zugangsserver seines Unternehmens ein. PIN und Token sind transparent über das Netz geschickt worden.
4. Es wird umgehend eine Verbindung zum Authentifizierungsserver aufgebaut und die transparent übertragene PIN sowie das Einmal-Passwort (hier: 78901) übergeben.
5. Im Authentifizierungsserver erfolgt eine Trennung von PIN und Passwort. Zur Identifizierung wird eine Datenbankabfrage mit der PIN als Suchkriterium

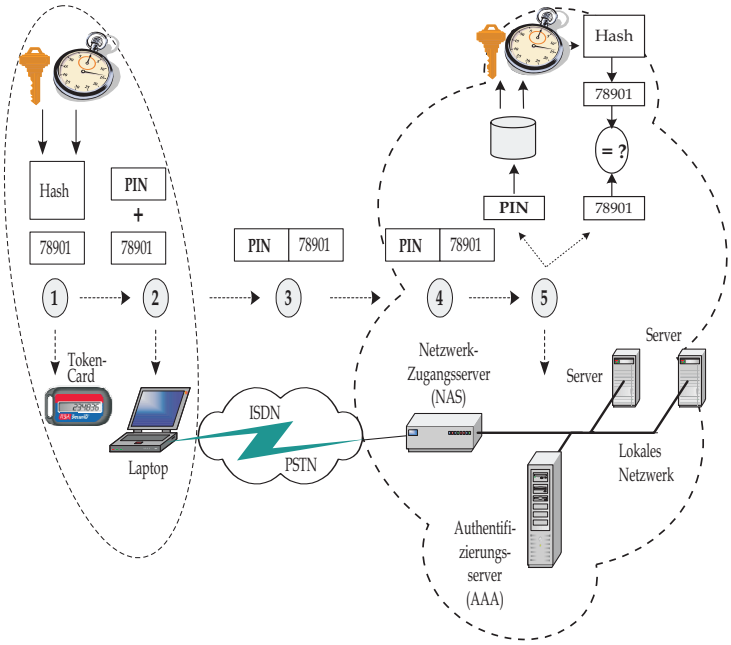


Abb. 5.6: Zeitsynchrone Zwei-Faktoren-Authentifizierung mittels einer Token-Card

(*primary key*) gestartet und der abgelegte kryptographische Schlüssel aufgesucht. Es handelt sich um einen identischen Schlüssel, der auf der zugeordneten Token-Card gespeichert ist. Der Schlüssel wird zur Verschlüsselung der aktuellen Zeitinformation des Servers nach dem gleichen Algorithmus, der in der Token-Card verwendet wird, eingesetzt. Der Authentifizierungsserver berechnet seinerseits ein Einmal-Passwort, das mit dem empfangenen Passwort identisch sein muss. Der abschließende Vergleich entscheidet über die weiteren Aktivitäten des Servers.

Bei positivem Ergebnis erhält der Nutzer einen Zugang ins LAN. Unterscheidet sich die vom Server errechnete Zahl von der übermittelten Zahl (negatives Ergebnis), wird die Verbindung sofort abgebrochen.

Das hier beschriebene Secure-ID-Verfahren ist inzwischen bei Fernzugriffen auf Unternehmensnetze weit verbreitet. In der Anfangsphase gab es Schwierigkeiten bei der Zeitsynchronisation zwischen dem Authentifizierungsservern und der Token-Card, wenn ein Server nach einem kurzfristigem Ausfall wieder seinen Dienst verrichtete. Dies ließ sich jedoch nach Installation eines DFC-49 Zeitsignalempfängers beheben.

5.3.2 Speicherkarten und Smart Cards

Der französische Journalist Roland Moreno hat 1968 bei der Patent Erteilung bestimmt nicht geahnt, welchen Siegeszug die Plastikkarte antreten würde, als er die Idee hatte, eine Prozessorschaltung – ausgelegt für bestimmte Anwendungen – in eine Plastikkarte zu integrieren. Bis zu den 70er Jahren konnten Prozessorchipkarten lediglich Daten schreiben und lesen. Mitte der 70er Jahre kam eine Schutzfunktion für die gespeicherten Daten in Form einer PIN-Nummer hinzu, und die zwei Faktoren *Besitz* und *Wissen* sicherten die Nutzung der Chipkarte. Der PIN-Schutz beinhaltet einen Zähler für Fehleingaben des Nutzers, der nach einer dreimaligen Falscheingabe unweigerlich zur Sperrung der Karte führt. Dieser Kartentyp wird als *intelligente Speicherchipkarte* bezeichnet. Allerdings bietet die PIN-Absicherung in Form eines verkürzten Passwortes nur einen geringen Schutz. Eine wesentliche Verbesserung wird von den biometrischen Verfahren erwartet, sobald diese praxistauglich sind. In den 80er Jahren wurden in Frankreich mit der „carte bleu“ Plastikkarten in großem Umfang eingeführt. Heutzutage sind auf Basis der Speicherchipkarte bereits mehrere hundert Millionen Karten hergestellt worden, die auf verschiedensten Gebieten zur Anwendung kommen.

Neben der Speicherung persönlicher Daten, die auch in Magnetstreifenkarten möglich waren, werden Chipkarten durch den Einbau eines Mikroprozessors zu regelrechten Minicomputern erweitert. Die Leistungsfähigkeit der Karten (Smart Cards) ermöglicht Verschlüsselungsaktivitäten. Damit können Verfahren wie DES oder RSA für Authentifizierungszwecke zum gesicherten Transport von Daten zwischen Karte und Terminal und zum Berechnen von digitalen Signaturen vorgenommen werden.

Chipkarten und Smart Cards haben die Größe einer Standard EC-Karte ($85,60 \times 53,98 \times 0,76$ mm). Sie haben, im Gegensatz zur reinen Magnetstreifenkarte, eine integrierte Schaltung zur Informationsspeicherung mit einer Eingabemöglichkeit und je nach Kartentyp mehr oder weniger weitreichende Funktionalität. Tab. 5.1 zeigt die unterschiedlichen Technologien und die verschiedenen Eigenschaften.

Weiterhin lassen sich Chipkarten in mehrere technische Kategorien einteilen, die je nach Verwendungszweck unterschiedliche Kosten verursachen. Je nach verwendeter Speichertechnologie sind Chipkarten nur lesbar (ROM), einmal beschreibbar (EPROM) oder wiederholt beschreibbar (EEPROM). Tab. 5.2 gibt einen Überblick der jeweiligen technischen Kategorien und Ausprägungen. Für einfache Chipkarten (Speicherkarten) reicht es aus, wenn die vorhandenen Bits sequentiell abgebucht werden. Sobald das letzte Bit beschrieben ist, ist die Karte verbraucht und verliert ihre Funktion (Telefonkarte). Derartige Karten benötigen keine weitreichende Intelligenz, eine einfache Logik reicht vollkommen aus, um Bits abzubuchen. Nachfolgend wird auf die *intelligente Prozessorchipkarte* (Smart Card) eingegangen, da dieser Typ im IT-Sicherheitsbereich zur Anwendung kommt. Ein Zugriff zu den Speicherbereichen ist ausschließlich über die CPU möglich. Das Betriebssystem (OS) der Chipkarten-CPU ist im ROM abgelegt und kann je nach Kartentyp um Funktionen im EEPROM erweitert werden. Smart Cards haben eine 8-Bit CPU, zwischen 128 und 256 RAM, bis 24 KB ROM und zwischen 1 und

Tabelle 5.1: Kartentechnologien und Aufbau einer Chipkarte

Kartentechnologie	**Speicherplatz**	**Sicherheit des Speichers**	**Kosten**
Magnetstreifenkarte	$\leq$ 350 Bytes (R/W)	keine	Karte sehr kostengünstig Leser moderat Leser/Schreiber teuer
Chipkarte	bis 20 Kbytes (WORM oder R/W)	Zugriff über Logik eingeschränkt, aktive Aufgaben (Verschlüsselung möglich)	Karte moderat bis teuer Leser = Schreiber sehr kostengünstig
Laserkarte	1 MB (WORM)	keine	Karte kostengünstig Leser/Schreiber sehr teuer

Tabelle 5.2: Technische Kategorien und Ausprägungen der Chipkarte

Chipkartenkategorie	**Ausprägung**
Interface	elektrisch, induktiv
Speichertechnologie	ROM, PROM, EEPROM
Intelligenz	Logik, CPU

16 KB EEPROM. Gehobene Smart Cards führen zusätzlich RSA-Operationen mit Schlüssellängen von 512 bis 1024 Bit mit einem Krypto-Coprozessor durch.

Eine Reihe von Normen beschreiben die Smart Card-Funktionalität. Darüber hinaus haben einige Hersteller Quasistandards geschaffen, wie z.B. Microsoft mit der PC/SC-Initiative oder auch SUN mit der Java-Card-Spezifikation. Richtungsweisend ist jedoch die ISO 7816-Norm, die aus mehreren Teilen besteht. In Bezug auf Sicherheitsaspekte sind jedoch nur folgende normierte Befehle interessant:

Verify: Dieser Befehl erlaubt es, gespeicherte Daten mit den zur Karte geschickten Daten zu vergleichen. Damit sind Passwort oder PIN-Mechanismen möglich. Durch den Fehlbedienungszähler (FBZ) kann verhindert werden, dass die PIN bzw. das Passwort erraten werden.

External Authenticate/Internal Authenticate: Erlaubt die Authentifizierung der Karte durch einen Challenge-Response-Mechanismus. Dabei wird in einem ersten Schritt ein Challenge-Wert vom Terminal (Interface-Device oder Host) übermittelt. Mit einem gespeicherten Schlüssel wird dann ein Response ermittelt, die es wiederum dem Terminal ermöglicht, eine Prüfung vorzunehmen. Im zweiten Schritt wird ein Terminal-Response-Wert an die Karte zurückgeschickt, mit dem die Karte dann überprüfen kann, ob das Terminal die Karte erkannt hat. Erst nach positiver Antwort beider Schritte kann der Status auf „authentifiziert“ abgeändert werden.

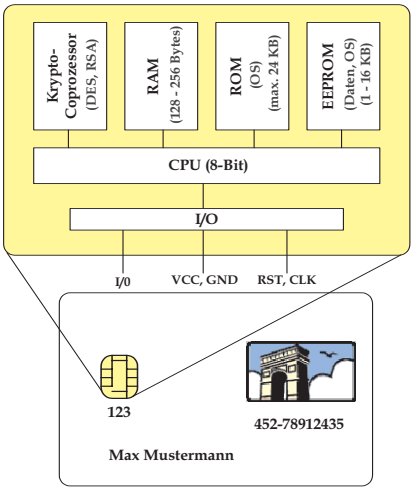


Abb. 5.7: Grundlegender Aufbau einer Chipkarte

Smart Cards gelten als fälschungssicher und schützen die abgelegten Daten vor dem Zugriff unbefugter Dritter. Damit eignen sich Smart Cards als sicheres Medium für persönliche Schlüssel und X.509 Zertifikate. Insbesondere der sehr sicherheitskritische private Schlüssel zum Signieren von Daten mittels eines Public-Key-Verfahrens (Abschn. 4.7) lässt sich vor unberechtigtem Zugriff geschützt ablegen. Ein entscheidender Vorteil der Karte liegt darin, dass symmetrische und asymmetrische Verschlüsselungen vorgenommen werden können, ohne das geheime Schlüssel über die Ein-/Ausgabeschnittstelle (I/O) das System verlassen können. Verglichen mit einer Schlüsselspeicherung auf einem Rechner sind die Schlüssel auf der Chipkarte wesentlich weniger angreifbar. Die Vorteile der heutigen Smart Cards lassen sich wie folgt zusammenfassen:

- Hohe Sicherheit als Speichermedium für sensible Daten
- Hohe Sicherheit beim Ausführen kryptographischer Operationen
- Schnelle Identifikation des Nutzers mittels PIN
- Multifunktionale Nutzung
- Ablegen von Rechten, Profilen und Schlüsseln auf der Karte

Die Nachteile liegen im Wesentlichen in den Kosten und im administrativen Aufwand:

- Spezielle Lesegeräte sind erforderlich
- Verlust der Karte oder Vergessen der PIN

- Administrativer Aufwand und sichere Logistik für das Ausstellen der Karte
- Keine zentrale Erneuerung von Rechteprofilen, z.B. beim gleichzeitigen Einsatz mehrerer Smart Cards

Dennoch überwiegen die Vorteile gegenüber den Nachteilen, so dass ein Einsatz der Smart Card-Technologie oder auch der Token-Card bei einem Remote-Access-VPN auf jedem Fall einem einfachen Passwort bzw. einer PIN/TAN-Lösung vorzuziehen ist.

5.4 Authentifizierungsverfahren in der Anwendung

Die folgenden Authentifizierungsverfahren finden weite Verbreitung bei der VPN-Technologie. Dabei weisen das auf eine PPP-Verbindung aufsetzende PAP- und CHAP-Protokoll sowie RADIUS und TACACS+ gewisse Gemeinsamkeiten auf. Hiervon setzt sich das Kerberos-Authentifizierungsverfahren deutlich ab, das in seinen Grundideen wesentlich früher entwickelt wurde. Es wird am Schluss dieses Kapitels behandelt.

5.4.1 Die PPP-Verbindung als Voraussetzung für PAP und CHAP

Als Voraussetzung für eine Authentifizierung mit dem PAP- oder dem CHAP-Protokoll muss eine serielle Punkt-zu-Punkt-Verbindung (PPP) zwischen beiden Kommunikationspartnern aufgebaut werden, also beispielsweise zwischen einem heimischen privaten ISDN-Router und dem Zugangsserver eines Unternehmens oder Zugangsrouter eines ISP.

Das Point-to-Point Protocol (PPP) bietet die Möglichkeit, IP-Datagramme über eine serielle Leitung zu schicken. PPP ist gemäß IETF im [RFC 1661] spezifiziert. Allerdings diskutieren eine Reihe weiterer RFCs für das PPP-Protokoll die unterschiedlichen Aspekte wie z.B. PPP-Authentifizierung, IP/AppleTalk/IPX over PPP und auch PPP als Multiprotokoll. Auf diese Erweiterungen bzw. Ergänzungen wird hier nicht näher eingegangen.

PPP ist eine Standardmethode, mit der Protokollinformationen innerhalb der Network Layer über eine PPP-Verbindung gekapselt übertragen werden können. PPP besteht im Wesentlichen aus drei Komponenten:

- Einem Verfahren zum Einpacken von Datagrammen über eine serielle Leitung
- Einem *Link Control Protocol* (LCP) zum Aufbau, Konfigurieren und Testen der Layer-2-Verbindung (Data-Link-Layer)
- Einer Familie von *Network Control Protocols* (NCPs) zur Etablierung und Konfiguration verschiedener Network Layer-Protokolle

Zum Aufbau einer Kommunikation über eine Punkt-zu-Punkt-Verbindung sendet jeder Endpunkt der PPP-Leitung zunächst LCP-Pakete, um eine Datenverbindung während der Verbindungsaufbauphase zu konfigurieren und zu testen. PPP sendet nach Aufbau der Datenverbindung NCP-Pakete auf Layer-2, um eines oder mehrere der möglichen Netzwerk-Layer-Protokolle auszuwählen und zu konfigurieren. Anschließend können Datagramme über die Verbindung gesendet werden. Die Verbindung bleibt solange erhalten, bis eines der LCP- oder NCP-Pakete die Verbindung explizit schließt. Eine Verbindung kann auch vom Netzwerkadministrator oder von einem Zeitzähler terminiert werden.

Tabelle 5.3: Das PPP-Modell in Anlehnung an das Internet-Schichtenmodell

PPP-Modell	**Internet-schichtenmodell**
Protokolle höherer Schichten	Layer-3 bis Layer-5
Network Control Protocol (NCP) Beispiele sind: BCP - Bridge Control Protocol IPCP - Internet Control Protocol IPXCP - Internetwork Packet Exhange Control Protocol	Layer-2
Link Control Protocol (LCP)	
High-Level Data Link Control (HDLC)	
Physical Layer (ISDN, V.24, PSTN)	Layer-1

In Anlehnung an das OSI-Schichten-Modell und das daran orientierte Internetschichtenmodell (Tab. 2.2) ist das PPP-Modell entstanden (Tab. 5.3). Eine PPP-Session wird in drei Phasen aufgebaut:

Phase-1: Aufbau einer PPP-Leitung, indem LCP-Pakete zur Konfiguration und zur Verbindungsprüfung ausgetauscht werden.

Phase-2 : Die LCP-Pakete enthalten ein Konfigurationsfeld, in dem Parameter zur größtmöglichen Übertragungseinheit der *Maximum Receive Unit* (MRU) sowie zur Kompression und zur Authentifizierung gesetzt werden können. Diese werden zwischen den Peers ausgehandelt.

Phase-3 : Findet eine *(optionale)* Authentifizierung statt, muss sie abgeschlossen sein, bevor eines der Network Layer-Protokolle (NCP) aktiviert wird. Je nach gesetzten Parametern kann entweder das PAP- oder das CHAP-Protokoll verwendet werden.

Nachfolgend werden die beiden in Frage kommenden Authentifizierungsprotokolle beschrieben. Dabei wird eine eingeleitete PPP-Verbindungsaufbauphase vorausgesetzt.

5.4.2 Password Authentication Protocol (PAP)

Ein in der VPN-Technologie weit verbreitetes Verfahren ist das PAP-Protokoll. Es wird häufig zum Verbindungsaufbau zwischen einem Netzbetreiber (ISP) und einem Endgerät eingesetzt. PAP ist ein einfaches Authentifizierungsprotokoll, das durch Benutzerkennung und Passwort zur Berechtigungsüberprüfung einer sich einwählenden Person dient. Abb. 5.8 zeigt die Arbeitsweise des PAP-Protokolls. PAP ist Bestandteil des PPP-Protokolls und gemäß IETF in [RFC 1334] beschrieben. Das Verfahren arbeitet entweder nach dem Zwei-Wege-Handshake, bei dem der Client nach dem Verbindungsaufbau seine Benutzerkennung und sein Passwort unverschlüsselt an den Server sendet, der die Verifikation durchführt, oder nach dem Ein-Wege-Handshake. Bei Übereinstimmung antwortet der Server mit einer Bestätigung und gibt den Zugang zum Netz frei. Bei fehlerhafter Eingabe wird die Verbindung unterbrochen.

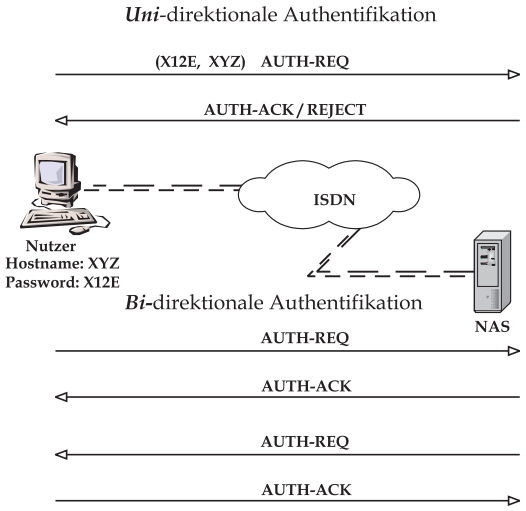


Abb. 5.8: Unidirektionale und bidirektionale Authentifizierung mittels PAP

Obwohl das PAP-Protokoll für einen Zwei-Wege-Handshake einsetzbar ist, zählt es nicht zu den sicheren Protokollen, da beide Kommunikationspartner ihre Kennung und Passwort im Klartext über das Netz senden (Abb. 5.8). Auch gegen einen Missbrauch *(Replay Attack)* ist das PAP-Protokoll nicht gerüstet. Ähnlich verhält es sich mit dem CHAP Protokoll, das nachfolgend vorgestellt wird. Es bietet, anders als das PAP-Protokoll, ein Drei-Wege-Handshake.

5.4.3 Challenge Handshake Authentication Protocol (CHAP)

Das CHAP-Protokoll ist ein weiteres Protokoll, das in der Aufbauphase einer PPP-Verbindung der wechselseitigen Authentifizierung beider Kommunikationssys-

teme dient. Das CHAP-Protokoll verzichtet auf das direkte Senden eines Passworts und nutzt stattdessen ein dreistufiges Authentifizierungsprotokoll, in dem mehrfach eine Frage/Antwort-Sequenz *(challenge-response)* ausgetauscht wird. Bei CHAP wird üblicherweise MD5 als Einweg-Hash-Funktion eingesetzt – ähnlich wie beim eingangs beschriebenen S/Key-Verfahren – um gegen spezielle Angriffe gewappnet zu sein. Die Abfolge der Frage /Antwort-Sequenz wird bei CHAP vom Authentifizierungsserver ausgelöst und nicht vom Remote-Computer wie bei PAP. Folgende Sequenzen werden (Abb. 5.9) zwischen beiden *Peers* für einen vollständigen Verbindungsaufbau ausgetauscht:

1. Der Authentifizierungsserver (R1) sendet eine Nachricht zum Remote-Computer (R2) mit der Aufforderung, sich zu authentifizieren.
2. Die Peer-Instanz (R2) schickt ihrerseits eine Aufforderung nebst Challenge (C) zum Server (R1), sich gegenüber der Peer-Instanz (R2) ebenfalls zu authentifizieren und schickt gleichzeitig seine Kennung (R2) mit.
3. Der Server (R1) sucht in seiner Datenbasis den zur Kennung (R2) gehörigen Schlüssel.
4. Mittels MD5 wird ein Hash-Wert gebildet, bestehend aus (C), dem Schlüssel, bzw. dem Passwort (hier: xyz), das der Datenbasis entnommen wurde.
5. Dieser Hash-Wert wird nebst Kennung von (R1) zum Remote-Computer (R2) geschickt.
6. Nach Ankunft der Werte wird im Remote-Computer (R2) in der lokalen Datenbasis der zur Kennung (R1) gehörige Schlüssel bzw. das Passwort gesucht.
7. Nach Ermittlung des Passwortes (hier: xyz) und des ursprünglich ausgesandten (C) wird mit der gleichen Hash-Funktion (MD5) ebenfalls ein Hash-Wert gebildet.
8. Der Vergleich des von (R1) geschickten Hash-Wertes mit dem bei (R2) selbst gebildeten Hash-Wert zeigt, ob eine Übereinstimmung existiert oder nicht.
9. Die Eingangswerte (Challenge und Passwort) bei (R1) und (R2) sind nur identisch, wenn der gleiche Hash-Wert ermittelt wurde. Eine erfolgreiche Authentifizierung ist somit durchgeführt und die ursprüngliche PPP-Verbindung kann mit dem Austausch von NCP-Paketen fortgesetzt werden.

Eine Authentifizierung kann allerdings nur dann erfolgreich durchgeführt werden, wenn vorab auf einem anderen Wege die Datenbanken auf beiden Seiten (R1, R2) mit den entsprechenden Passwörtern der jeweiligen Kennungen versehen wurden. Das CHAP-Protokoll ist gemäß IETF im [RFC 1994] beschrieben und wird nicht nur zu Beginn einer PPP-Session eingesetzt, sondern periodisch aufgerufen. Abb. 5.9 illustriert die oben aufgeführte Authentifizierung der Schritte 1 - 9. Obgleich CHAP gegenüber PAP einige Vorzüge aufzuweisen hat, ist es kaum für größere Unternehmen geeignet, da es schlecht skalierbar ist. Ebenso muss, da keine Geheimnisse (hier: xyz) über das öffentliche Netz geschickt werden, eine entsprechend große Datenbank gepflegt werden. Bei großen Unternehmen mit

einer größeren Anzahl an Telearbeitern erfordert dies einen beträchtlichen Wartungsaufwand. PAP und CHAP haben den Nachteil, dass Passwörter auf Nutzer-

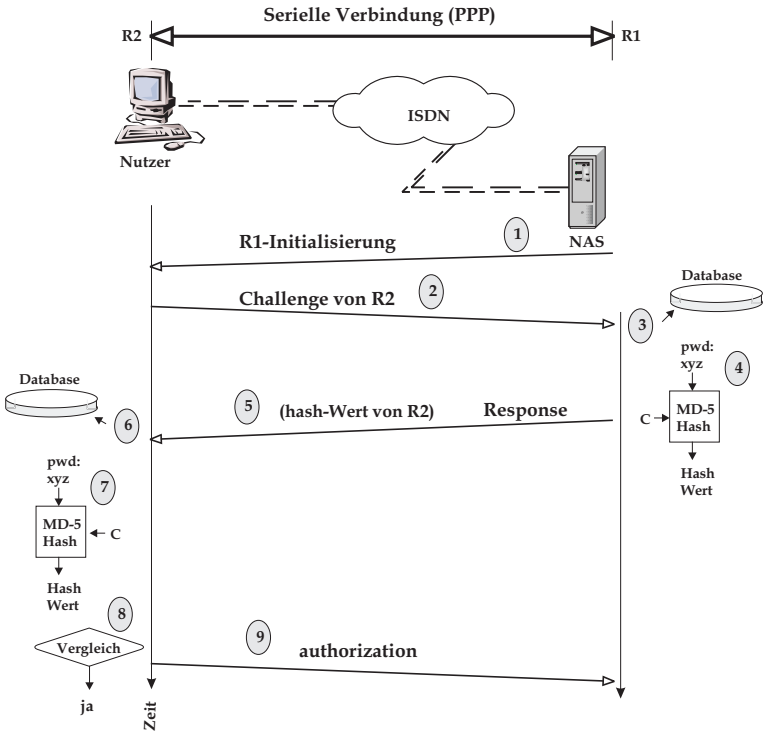


Abb. 5.9: Dreistufige Authentifizierung mittels CHAP

und Serverseite in Datenbanken abgelegt werden. Gerät einer der Computer unter Kontrolle eines unbefugten Dritten, ist das Passwort kompromittiert. Weiterhin lassen sich mit PAP und CHAP keine unterschiedlichen Netzwerkrechte *(Privilegien)* vergeben. Diese Schwierigkeit tritt auf, wenn mehrere Telearbeiter in einem Büro (SOHO) mit einem ISDN-Router, der zur gemeinsamen Nutzung ausgelegt ist, eine Verbindung zum Unternehmen aufbauen.

5.4.4 Die AAA-Sicherheitsarchitektur

Die AAA-Architektur ist als Framework zu verstehen, mit dem drei unabhängige Sicherheitsfunktionen in übereinstimmender Weise konsistent konfiguriert werden können. Die Architektur bietet eine modulare Zusammenstellung der A-Sicherheitsdienste mit den Vorteilen einer erhöhten Flexibilität, Kontrollier- und Skalierbarkeit. Weiterhin werden standardisierte Authentifizierungsmethoden wie RADIUS, TACACS+ und Kerberos unterstützt. Ebenso ist ein Multiples Backup-

System definiert. Aktiviert wird die AAA-Architektur auf einem der genannten Server durch ein spezielles Kommando. Explizit werden unter der AAA-Architektur folgende Services verstanden:

Authentifizierung: Hierunter werden im Allgemeinen Methoden einer Nutzeridentifizierung für Netzwerk bzw. für Netzwerkdienste zusammengefasst. Dazu gehören einfache Anmelde- und Passwort-Dialogverfahren sowie Challenge-Response-Verfahren, außerdem ein Nachrichtentransport, der – je nach gewähltem Sicherheitsprotokoll – auch verschlüsselt durchgeführt werden kann.

Autorisation: Sie arbeitet mit einer Reihe von Attributen, die beschreiben, welche Rechte einem Nutzer innerhalb eines Netzwerkes eingeräumt sind. Dies können Remote-Access-Rechte, inklusive Einmal-Zugriff bzw. für bestimmte Dienste gesondert erteilt, sein. Hierzu zählen Nutzerberechtigungslisten und -Profile, Gruppenzugehörigkeiten sowie die IP, IPX, ARA oder Telnet-Berechtigung. Die Attribute werden im Autorisationsprozess mit Werten, die in einer Datenbank gehalten werden und für jeden Nutzer definiert sind, mit den aktuellen Anmeldedaten verglichen, um Berechtigungen und Restriktionen abzuprüfen. Die dazu notwendige Datenbank kann lokal im Zugangsserver oder in einem Router plaziert oder auf einem RADIUS- bzw. TACACS+ Server installiert sein. Remote-Sicherheitsserver wie RADIUS und TACACS+ autorisieren nutzerspezifische Rechte mit geeigneten *attribute-value* (AV)-Paaren.

Accounting: Es ermöglicht die Zusammenstellung von Daten, die zur Rechnungsstellung, zur Auditierung und zum Reporting geeignet sind. Dazu gehören die Verbindungszeiten eines Nutzers und die exakten Start- und Beendigungszeiten der PPP-Verbindungen, außerdem die Ausführungskomandos und die Anzahl der übertragenen Bytes einer Verbindung. Mit einem Accounting-Verfahren ist es möglich, die Netzwerkauslastung festzustellen und die von den Nutzern häufig angeforderten Dienste zu erkennen. Ist ein AAA-Accounting aktiviert, schickt der Netzzugangsserver je nach Konfiguration entsprechende Berichte über die Nutzeraktivitäten an den RADIUS- bzw. an den TACACS+ Server. Jeder Accounting-Datensatz (Record) schließt dabei die AV-Paare für eine spätere Auswertung ein.

Eine typische AAA-Infrastruktur besteht aus AAA-Servern, die untereinander in Verbindung stehen und ein spezielles AAA-Protokoll zur Kommunikation benutzen. Entsprechende Clients nehmen in einem Request/Response-Verfahren Kontakt mit einem AAA-Server auf. Die IETF hat seinerzeit die Arbeitsgruppe *AAAarch Research Group* eingerichtet, um ein solch theoretisches Framework zu definieren. Die Abb. 5.10 zeigt die Systemarchitektur eines allgemeinen, applikationsunabhängigen AAA-Systems. Die AAA-Funktionalität wird in zwei Bereiche unterteilt, der eine beinhaltet den applikationsspezifischen Teil (ASM), der andere einen allgemeinen Teil, der für alle Anwendungen gedacht ist (Policy Repository). Darüber hinaus besitzen AAA-Server Proxy-Fähigkeiten, da sie in der

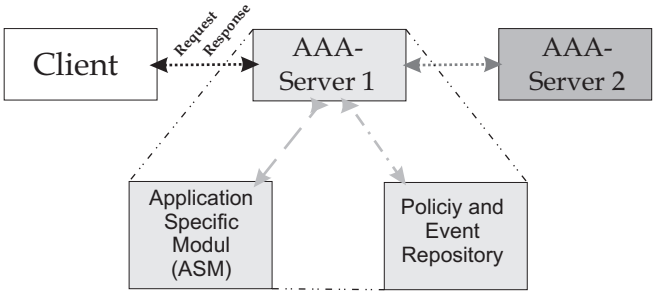


Abb. 5.10: Darstellung einer allgemeinen AAA Systemarchitektur

Lage sind, Anfragen weiterzuleiten, die nicht selbst beantwortet werden können. Häufig wird der installierte AAA-Service um eine Sicherheitsfunktion ergänzt. Durch die zentrale Verwaltung aller relevanten Daten in einer einzigen gesicherten Datenbank ist es wesentlich einfacher, ein Netz zu verwalten.

TACACS+ ist wie RADIUS und Kerberos eines der Protokolle, mit denen AAA-Informationen zwischen einem *Network Access Server* (NAS) und dem Zentralen Server ausgetauscht werden können. Alle drei Protokollvarianten spielen für die VPN-Technologie eine Rolle und sind Gegenstand der nächsten Abschnitte.

5.4.5 Remote Authentication Dial-In User Service (RADIUS)

Das RADIUS-Protokoll, das von der Firma Livingsten entwickelt wurde, ermöglicht sowohl eine Authentifizierung und eine Autorisation als auch ein Accounting (AAA-Service). Inzwischen ist es ein offenes Protokoll und wird durch die IETF weiterentwickelt. Eine Referenzimplementierung ist frei zugänglich und kann bei Bedarf verändert werden.

Anders als die auf Peer-Instanzen beruhenden PAP- und CHAP-Verfahren entspricht die RADIUS-Lösung einer vollständigen Client-Server-Architektur und ist damit vom Ansatz her wesentlich flexibler. Weiterhin authentifizieren sich Client und Server jeweils gegenseitig. Dies wird erreicht, indem Client und Server ein gemeinsames Geheimnis – ein *shared secrect (S)* – einsetzen.

Eine Kommunikation zwischen dem Netzwerk-Zugangsserver[7] (NAS), der als Client agiert, und dem RADIUS-Server basiert auf dem verbindungslosem UDP-Protokoll. Verbindungsprobleme *(Time-out, Retransmission)* zwischen Client (NAS) und Server (RADIUS-Server) werden somit vom Server abgefangen und nicht vom Protokoll. Der RADIUS-Server stellt einen Dämon-Prozess dar und kann sowohl auf UNIX als auch auf WinNT installiert werden.

[7] Der *Network Access Server* (NAS) arbeitet sonst üblicherweise als Server für den allgemeinen Netzwerkzugang.

Das Zusammenspiel der Komponenten ist in Abb. 5.11 skizziert. Ein Remote-Client nimmt zunächst Kontakt über eine DFÜ-ISDN-Verbindung mit dem NAS-Eingangsmodem (z.B. ADSL) auf. Der Kontakt kann abgelehnt oder akzeptiert werden. Bei Erfolg nimmt der NAS-Client seinerseits eine UDP-Verbindung mit dem RADIUS-Server auf, um eine AAA-Anfrage durchführen zu lassen. Dabei muss eine Authentifizierung nicht zwingend auf dem RADIUS-Server erfolgen. Dieser kann sich – wenn vorhanden – an einen zentralen Authentifizierungsserver, wie z.B. einen Kerberos-Server, DCE, Token-Server oder ein RACF-System, wenden. Um Angriffen vorzubeugen, werden die zu überprüfende Nutzerkennung und das Passwort verschlüsselt verschickt. Je nach Resultat wird der anfängliche Verbindungsaufbau vom Remote-Client zu einem gewünschten Applikationsserver fortgesetzt oder nicht. Neben der erfolgreichen Authentifizierung des Nutzers können auch Filteroptionen an das NAS weitergeleitet werden. Diese können z.B. Rechtebeschränkungen für bestimmte Netzwerkressourcen beinhalten wie die Nutzeranforderung hinsichtlich bestimmter Protokolle, z.B. TCP/IP und/oder das Internet Packet Exchange (IPX). Hauptaufgabe einer

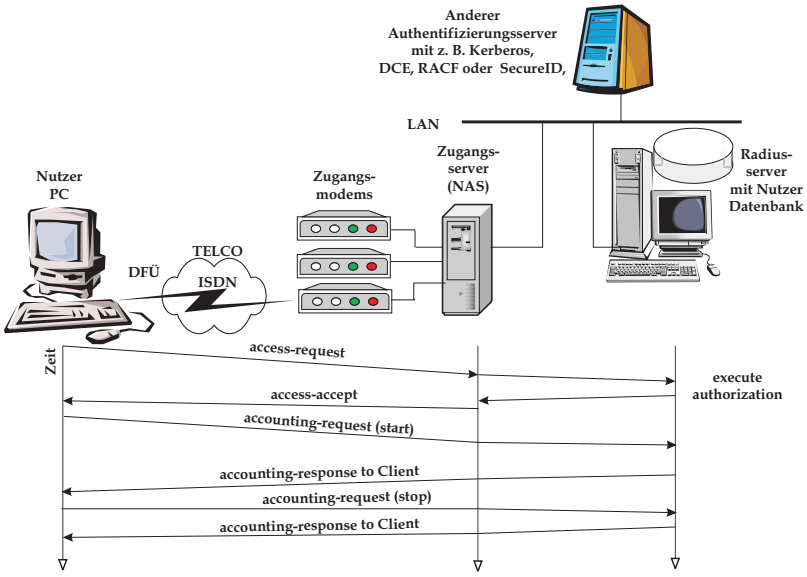


Abb. 5.11: Autorisation mit gleichzeitigem Accounting mittels RADIUS

RADIUS-Lösung ist es, einen gesicherten Netzwerkzugang und einen wirksamen Schutz gegen Zugriffe von unbefugten Dritten zu bieten. Weiterhin wird ein Protokoll unterstützt, das ein Frame-Format gemäß UDP/IP bietet. Der Server ist üblicherweise ins firmenseitige Netzwerk eingebunden und kann als Proxy-Client auch für andere Authentifizierungszwecke genutzt werden. Der Client ist dann regulär an der Schnittstelle des Einwahlservers zum öffentlichen Netz installiert. Wird ein von Cisco vertriebener Einwahlserver (z.B. aus der Serie AS-5x00) ein-

gesetzt, der gleichzeitig Modemzugänge bietet, ist der RADIUS-Client ab der Betriebssystemversion IOS 11.1 enthalten.

Die Aufgabe des RADIUS-Clients besteht darin, Nutzerinformationen (Kennung und Passwort) zum korrespondierenden RADIUS-Server zu schicken und nach Erhalt der Authentifizierungsinformation zu reagieren. Die zentrale Aufgabe im Authentifizierungsprozess obliegt also dem RADIUS-Server. Er ist auch für eine funktionierende geschützte Verbindung zum Client hin zuständig und dafür, dass die ausgewerteten Informationen für den weiteren Verbindungsaufbau des Remote-Nutzers eingesetzt werden. Zum Schutz der UDP/IP-Verbindung bzw. der ausgetauschten Nutzerkennung und des Passwords wird eine symmetrische Verschlüsselung eingesetzt.

Weiterhin pflegt der RADIUS-Server nur *eine* zentrale Datenbank mit allen berechtigten Benutzern und den zugeordneten Diensten. Gerade dies ist für große Netze sehr interessant, falls sie mit mehreren verteilten Netzwerkzugangsservern arbeiten. Die Nutzer sind somit nicht an einen bestimmten Einwahlpunkt gebunden, sondern können sich an geographisch unterschiedlichen Lokationen einwählen, da ihr Profil zentral gespeichert wird. Laut IETF, die 1996 in der eigens eingerichteten Arbeitsgruppe für RADIUS das Protokoll weiterentwickelt, hat das RADIUS-Protokoll inzwischen den Status als *Proposed Standard* für [RFC 2138] und für das Accounting-Verfahren [RFC 2139] den Status als *Informational Standard* erlangt. Obgleich TACACS+ wesentlich vielseitiger als RADIUS ist, wie in Abschn. 5.4.6 ausgeführt wird, bevorzugen gerade Internet Service Provider (ISP) RADIUS als AAA-Protokoll, da es mit weniger CPU-Leistung auskommt und geringere Speicherkapazitäten benötigt. RADIUS kann sowohl eine Layer-2-Tunnelverbindung – im Compulsory und im Voluntary Mode – als auch eine PPP-Verbindung authentifizieren und stellt für die VPN-Technologie eine interessante Komponente dar. In Kapitel 7 sind weitere Ausführungen hierzu zu finden.

5.4.6 Terminal Access Controller Access Control System

Ganz ähnlich wie RADIUS arbeitet das Terminal Access Controller Access Control System (TACACS) auch in einer Client-Server-Architektur. Es ist ebenfalls ein typisches Industrie-Standardprotokoll und 1993 durch die IETF in dem [RFC 1492] spezifiziert worden. Eine Authentifizierungsanfrage wird, vergleichbar mit RADIUS, zu einem zentralen TACACS-Server geschickt. Der zentrale TACACS-Server kann eine eigene Datenbank nutzen oder auf externe Datenbanken zurückgreifen.

Neben der reinen TACACS-Lösung hat Cisco eine Extended TACACS, als XTACACS bezeichnet, die mit zusätzlichen Eigenschaften ausgestattet ist. Eine weitere Variante stellt die TACACS+ Lösung – ebenfalls von Cisco – dar, bei der es ein separater Zugriffserver (TACACS+) es ermöglicht, die Dienste zu Authentifizierung, Autorisation und Accounting unabhängig und getrennt voneinander auszuführen. Dies erhöht die Flexibilität erheblich, gerade für die Autorisation, die die Nutzerzugriffsprofile verwaltet, die dynamisch verändert werden können.

Weiterhin wird – anders als bei RADIUS – eine TCP/IP-Verbindung zwischen Client und Server aufgebaut. Nur im Originalprotokoll TACACS wird ein UDP-Verbindung eingesetzt. Neben diesen Eigenschaften bietet TACACS+ einen spezifischen Service für Router an, auf den hier aber nicht näher eingegangen werden soll. Der am meisten genutzte Dienst ist die PPP-Unterstützung für das IP und die Exec-Shell zur Kommunikation mit der Routershell.

Da TACACS+ eine komfortable Lösung darstellt und häufig vorzufinden ist, werden nachfolgend die Vorzüge von RADIUS und TACACS+ diskutiert.

5.4.7 Vergleich zwischen RADIUS und TACACS+

Tab. 5.4 zeigt die Eigenschaften von RADIUS und TACACS+. Da RADIUS eine verbindungslose UDP/IP-Verbindung aufbaut, ist es gegenüber TACACS+ hinsichtlich der Zuverlässigkeit benachteiligt. TCP/IP bietet eine verbindungsorientierte Kommunikation. Dies muss RADIUS durch eigene programmierbare Variable z.B. für das *Time-out* und *retransmission* ergänzen, um den Best-Effort-Pakettransport zu kompensieren. Die TCP-typischen Vorteile werden jedoch nicht erreicht. TACACS+ bietet die Möglichkeit, das gesamte Paket zu verschlüsseln und

Tabelle 5.4: Vergleich zwischen Radius und TACACS+

RADIUS	**TACACS+**
nutzt UDP	setzt TCP/IP ein
verschlüsselt nur das Passwort in einer AAA-Anfrage	verschlüsselt das gesamte Paket für eine AAA-Anfrage
kombiniert Authentifizierung und Autorisation	nutzt eine vollständige AAA-Architektur, die die AAAs trennt
entspricht einem Industrie-Standard	proprietär, CISCO-firmenspezifisch
unterstützt kein ARA Zugriff, Netbios Frame Control Protocol, NASI und X.25 PAD-Verbindungen	bietet die volle Multiprotokollunterstützung
bietet einem Nutzer keine Unterstützung zur Befehlskonfiguration von Routern	bietet zwei Möglichkeiten zur Befehlskonfiguration von Routern an

für den Debug-Prozess das Paket in Klartext zu übertragen. Im regulären Datenverkehr ist das Paket verschlüsselt.

Bei RADIUS ist die Authentifizierung mit der Autorisation gekoppelt und schickt bei einer erfolgreichen Authentifizierung *(access-accept)* automatisch auch die Autorisation *(Rechteprofil im Firmennetz)* zum Fernnutzer *Remote-Client*.

TACACS+ folgt dagegen vollkommen der AAA-Architektur, die eine Trennung der drei As *(Authentifizierung, Autorisation, Accounting)* vorgibt. Es ist z.B. möglich, Kerberos zur Authentifizierung einzusetzen und TACACS+ für Autorisation und Accounting. Nachdem der NAS mittels Kerberos-Server eine Authentifizierung durchgeführt hat und außerdem z.B. Autorisationsinformationen vom TACACS+

Server benötigt, müssen diese nur einmal abgeprüft werden, da der NAS nur eine erfolgreiche Authentifizierung weitergibt. Außerdem wirkt sich die Entkoppelung der drei As auf eine im Bedarfsfall zu wiederholende Rechteüberprüfung innerhalb einer Session ressourcenschonend aus.

Im Gegensatz zu TACACS+ unterstützt RADIUS nicht das *AppleTalk Remote Access* (ARA) Protokoll, das NetBIOS *Frame Control Protocol*, das *Novell Asynchronous Services Interface* (NASI) oder eine X.25 PAD-Verbindung. Das Router-Management von RADIUS ist ungeeignet, bestimmte Kommandos auf einem Router zu unterbinden und auch nicht flexibel genug, einen Terminalservice zu bieten. Hier liefert TACACS+ Möglichkeiten, entweder auf Nutzer- oder auf Gruppenebene, Privilegien einzurichten. Weiterhin ist der RADIUS-Standard nicht so interoperabel wie gewünscht, da etliche Hersteller in den RADIUS-Clients nicht alle bzw. unterschiedliche RADIUS-Attribute – von denen derzeit 45 definiert sind – implementiert haben. Allerdings gibt es auch Hersteller, die die RADIUS-Attribute erweitert haben. Bei einer Verwendung ist eine Interoperabilität nicht mehr gewährleistet.

5.4.8 DIAMETER

Das RADIUS-Protokoll, das sich inzwischen breitflächig durchgesetzt hat, ist bezogen auf die sich abzeichnenden Roaming-Möglichkeiten, die die UMTS/GPRS- und WLAN-Technologie ermöglicht, eingeschränkt. Abb. 5.11 illustriert ein typisches Remote-Dial-In-Verfahren gemäß dem RADIUS Protokoll.

WLAN Roaming-Szenarien, die es mit nur einer Nutzeridentifikation erlauben, WLAN-Hotspots mehrere verschiedener Anbieter zu nutzen, benötigen eine unterbrechungsfreie Session (*Seamless Roaming*) über mehrere Access-Point-Betreiber (Provider) hinweg. Das RADIUS-Protokoll ist AAA geeignet, jedoch muss beim Wechsel des Zugangsnetzes immer wieder eine neue Verbindung aufgebaut werden. Es ist nicht in der Lage, ein *Seamless Roaming* zu bieten. Damit ist es ungeeignet, eine nahtlose Integration von UMTS/GPRS-Technologien und Mobile-IP (vgl. Abschn. 2.3.1) in diesen Szenarien zu ermöglichen. Somit müssen RADIUS Infrastrukturen an roamingunterstützende AAA-Protokolle wie DIAMETER angepasst werden. Abb. 5.12 zeigt in sechs Schritten wie sich ein Nutzer (User) sich über einen Interims-Provider (Visit ISP) hinweg bei seinem eigentlichen Provider ins (3GG/WLAN) Netz einbucht.

DIAMETER bietet neben der Möglichkeit, ein Roaming zu gewährleisten, z.B. die Einrichtung eines Failover, das bei RADIUS nicht vorhanden ist. Außerdem ist die Transmission-Sicherheit nur rudimentär, denn die Vertraulichkeit pro Paket ist nicht gegeben, wenn das *attribute-hiding* Flag gesetzt ist (vgl. Tab. 5.4.7). DIAMETER besteht aus zwei Hauptkomponenten, dem Basisprotokoll und dem CMS Security Module [RFC 3588]. Mit diesem werden alle Tripel-A Funktionalitäten bereit gestellt. Das CMS Modul bietet die notwendigen Mittel, um eine Ende-zu-Ende Sicherheit herzustellen. Außerdem werden die von allen Implementationen zu unterstützenden Funktionalitäten und Message-Formaten definiert. Anhand von Attribute Value Pairs (AVP) werden Informationen ausgetauscht.

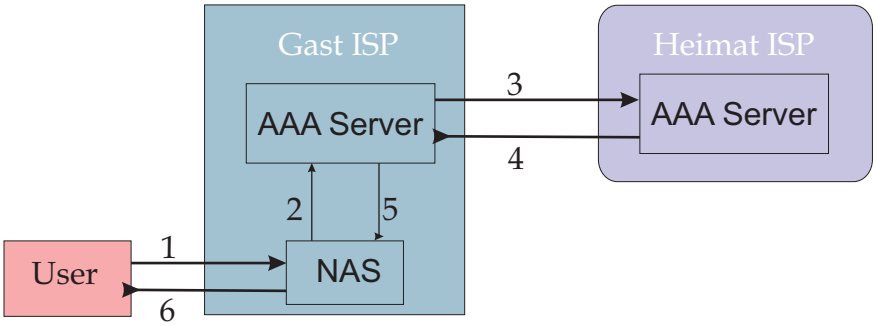


Abb. 5.12: Schematische Darstelllung eines Mobile Dial-In mittels DIAMETER

Dennoch wurde das DIAMETER-Protokoll nicht völlig neu entworfen. Es stellt im Kern eine Weiterentwicklung des RADIUS-Protokoll dar. Die Unzulänglichkeiten von RADIUS wurden eliminiert und neue Bestandteile hinzugefügt. Das Basiskonzept von DIAMETER beruht auch auf einen AAA-Dienst dar, der nun beliebig erweiterbar ist und damit für zukünftige Zugangstechnologien gerüstet ist. Mächtig wird DIAMETER durch die Applikationen, wie z.B. NASREQ, ROAMOPS und Mobile-IP. Zusammenfassend können die Eigenschaften des

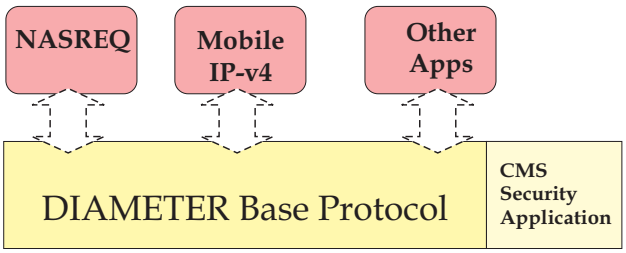


Abb. 5.13: DIAMETER-Architektur

DIAMETER-Protokolls wie folgt beschrieben werden [Ventura 2002]:

SCTP-Protokoll ersetzt das UDP-Protokoll: Im Gegensatz zum UDP-Protokoll (RADIUS) ist das Stream Transmission Control Protocol (SCTP) ein sicheres Transportprotokoll. Der Dienst ähnelt den Möglichkeiten, die auch TCP bietet, jedoch ist SCTP um einige Punkte erweitert worden [RFC 2960]. Weiterhin liefert SCTP eine Flusssteuerung *(congestion control)* und einen Mechanismus zur Stauvermeidung *(congestion avoidance)*. Ebenso liefert es Signalisierungsmeldungen über IP-basierte Netze. Interessant im Fall von DIAMETER ist die „multi home“ -Fähigkeit, indem verschiedene IP-Adressen gleichzeitig unterstützt werden.

Keep-alive Nachrichten eingerichtet: Mit dieser Eigenschaft ist es möglich zu registrieren, wenn eine Peer-Instanz ausgefallen ist. Einher geht damit eine Fehlerüberbrückung *(failover functionality)*, die langen Ausfallzeiten entgegen wirkt – falls ein alternativer Server erreichbar ist.

Peer-to-Peer (P2P)-Verbindung ersetzt das Client/Server-Konzept: Damit teilen alle Beteiligten einen Teil der Ressourcen, indem die Kommunikation direkt erfolgt. Das Adresssystem basiert nicht auf DNS. DIAMETER ist somit in der Lage, als *Client* und als *Server* zu dienen.

Zeitstempel implementiert: Mit dieser Einrichtung werden *Replay-Attacken* entgegen gewirkt. Damit ist jede Nachricht zeitpunktbezogen und kann z.B. bei doppelter Versendung unterschieden werden.

Erweiterungsmöglichkeit vorgeplant: Das Protokoll bietet genügend Platz für herstellerspezifische Einstellungen und Attribute, so dass dennoch die Interoperabilität nicht leidet.

IPSec und SSL/TLS hinzugefügt: Anders als bei RADIUS, bei dem die Übertragungssicherheit von den gewählten Passwörtern der Kommunikationspartner abhängt, ist bei DIAMETER eine sichere Übertragung z.B. zwischen zwei DIAMETER Knoten bezüglich der Integrität und Vertraulichkeit möglich.

End-to-End Sicherheit ermöglicht: Mit dem CMS Modul wird eine *Hop-by-Hop*-Authentifizierung durchgeführt. Dies bedeutet, das der angeforderte Dienst eines Servers eine sichere Verbindung mit dem Home-Server aufbaut. Die IETF hat zwei Techniken vorgeschlagen, wie ein sicherer Nachrichtentransport gewährleistet werden kann. Zum einen wurden digitale Signaturen und entsprechende Zertifikate zur Authentifizierung und Integrität, zum anderen wurden asymmetrische Verschlüsselungsverfahren eingesetzt.

5.4.9 Kerberos

Kerberos[8] ist ein auf symmetrischen Verschlüsselungsverfahren basierter Netzwerk-Authentifizierungsdienst für Client-Server-Anwendungen. Kerberos wird zu den starken Authentifizierungsmechanismen (Abschn. 5.2) gezählt. Es garantiert *optional* die Integrität und Vertraulichkeit des Datenaustausches zwischen Client und Server. Es genügt ebenso den Anforderungen des *Triple-A*-Framework. Es arbeitet auf fixen UDP- und TCP-Ports und zählt zu den Firewall-freundlichen[9] Protokollen.

[8] Der Name Kerberos kommt ursprünglich aus der griechischen Mythologie und bezeichnet den dreiköpfigen Wachhund, der den Eingang zur Unterwelt (*Hades*) bewacht. Dieser Name wurde wohl nicht ganz zufällig für ein Teilprojekt des vom MIT als *Athena* bezeichneten Projekts gewählt, das Mitte der 80er Jahre durchgeführt wurde.

[9] Der Begriff Firewall-freundlich hat sich umgangssprachlich eingebürgert, wenn eine HTTP-Verbindung als Ersatzverbindung eingesetzt werden kann und somit keine Modifikationen an den Firewall-Filterregeln erforderlich werden.

Von Bedeutung sind gegenwärtig die Versionen 4 und 5. In der Praxis ist Version 4 (Patchlevel-10) weit verbreitet – nicht zuletzt durch die bessere Performance und einfachere Handhabung gegenüber der aktuellen Kerberos V5 Release 1.1.2. Die IETF hat Kerberos V5 im [RFC 1510] im Jahr 1993 spezifiziert. Mittlerweile ist eine eigene Arbeitsgruppe für Kerberos *(KRB-WG)* eingerichtet worden, die etliche Vorschläge zur Erweiterung bzw. Ergänzung von Kerberos erarbeitet hat. Allerdings ist Version 4 auf TCP/IP beschränkt und lässt als Verschlüsselungsverfahren nur DES zu. Version 5 bietet gegenüber Version 4 eine größere Funktionalität und kompensiert einige Unzulänglichkeiten[10] der Vorgängerversion. Weiterhin lassen sich neben DES andere Verschlüsselungsverfahren und Netze mit Version 5 bedienen. Ebenso ist in Version 5 neu hinzugekommen, dass die *Lebenszeit* eines Tickets frei einstellbar ist.

Eine Kerberos Version-5-Implementierung ist im Betriebssystem Windows 2000 von Microsoft erfolgt. Im Zusammenspiel mit dem Windows-2000-Server wird eine Nutzeranmeldung und Applikationsnutzung in einer Domäne ausschließlich mittels Kerberos erreicht. Für einen Fernzugriff *(Remote Access)* bei einer B2B- oder B2C-Anwendung wird auf eine PKI-Lösung zurückgegriffen. Microsoft hat die Kerberos V5 etwas modifiziert[11], die Hintergründe der Modifizierung jedoch nicht offengelegt [RFC 3244]. Zur Microsoft-Kerberos-Lösung äußerte sich Bruce Schneier in seinen monatlichen Crypto-Nachrichten sehr kritisch [Crypto-Gram 03-2000]. Die Vorbehalte wurden in den folgenden Ausgaben kontrovers diskutiert [Crypto-Gram 04-2000], [Crypto-Gram 05-2000] und [Crypto-Gram 06-2000].

Weiterhin setzt Microsoft das symmetrische RC4-Verfahren der Firma RSA Security Inc. für den amerikanischen Markt mit einer Voreinstellung von 128 Bit ein, für den internationalen Markt dagegen nur mit 56 Bit. Es kann allerdings auch DES verwendet werden, wenn die RC4-Voreinstellung dafür entsprechend geändert wird.

Das Kerberos-Protokoll ist ein *Trusted Third Party Authentication Protocol*. Somit setzt die Kommunikation zwischen zwei Partnern ein Vertrauensverhältnis gegenüber einer dritten Instanz voraus. Dies ist der Kerberos-Server[12](KDC). Der Kerberos-Server (Abb. 5.14), der im Prinzip als Schlüsselverteiler agiert (*Key Distribution Center*, KDC), kann logisch in zwei Teile untergliedert werden: in den Authentifizierungsserver (AS) und den *Ticket Granting Server* (TGS). Beide Server bedienen sich einer Datenbasis, die ebenfalls im KDC vorhanden ist. In ihr hält der KDC alle Namen und geheimen Schlüssel *(Secret Keys)* seiner *Principals*[13] – speziell Nutzer der Applikationsserver – bereit. Die Grundidee von Kerberos ist

---

[10] So ist z.B. in der Kerberos-Version 4 eine Integritätssicherung bei DES mit dem nicht standardisierten PCBC-Modus eingesetzt worden, der einen Sicherheitsmangel enthält.

[11] Es ist das *Data-Authorization-Field*, das Microsoft nutzt, jedoch keine andere Kerberos-Implementierung (z.B. bei UNIX). Damit wird es für andere Anbieter unmöglich sein, eine direkte Windows-2000-Client-Unterstützung anzubieten.

[12] Das zugrunde liegende Verfahren basiert teilweise auf dem Needham-Schroeder-Protokoll.

[13] Unter *Principals* sind im Kerberos Sprachgebrauch die Nutzer zu verstehen.

im Wesentlichen, Passwörter nicht über das Netz zu schicken. Die Kenntnis des geheimen Schlüssels wird folglich als Identitätsnachweis betrachtet.

Eine typische Kerberos-Umgebung, auch als *Realm* bezeichnet, beinhaltet einen Kerberos-Server, eine Anzahl von Clients und eine Anzahl von Applikationsservern mit den folgenden beiden Randbedingungen:

- Der Kerberos-Server muss von allen Nutzern die Kennung (ID) nebst allen Passworten, die mit einem Hash-Wert versehen sind, in seiner Datenbank gespeichert haben.
- Der Kerberos-Server muss mit jedem Server einen gemeinsamen (symmetrischen) Schlüssel besitzen. Alle Server müssen bei dem Kerberos-Server registriert sein.

Abb. 5.14 zeigt in sechs Schritten, wie die Anmeldung eines Nutzers bei einem Applikationsserver unter Ausnutzung eines Kerberos-Berechtigungsverfahren durchgeführt wird.

Schritt 1: Ein Nutzer (C) mit der Identität (ID_c) meldet sich an seinem Computer an und fordert einen Dienst vom (KDC), indem zunächst eine (ID_{tgs}) Nachricht, (Ticket Anforderung) zum (AS) geschickt wird. Die Nachricht (C $\rightarrow$ AS) beinhaltet einen Zufallswert ($Nonce_1$), einen Zeitstempel (TS_1) und die Adresse (AD_c) von (C). Nebenbei könnten noch eine Reihe von Flags gesetzt werden. Die Nachricht hat die Form:
[C $\rightarrow$ AS: Options, ID_c, $Realm_c$, ID_{tgs}, TS_1, $Nonce_1$]

Schritt 2: Im (AS) wird die Anfrage und die Nachricht mit den Daten in der Datenbank geprüft und ein Ticket Granting Ticket ($Ticket_{tgs}$) sowie ein Session Key ausgestellt. Das Resultat wird mit dem geheimen Schlüssel des Nutzers ($E_{KC}(K_{c,tgs})$) verschlüsselt, ebenfalls mit einer Zeitmarke (TS_2) und dem Zufallswert ($Nonce_1$) versehen und mit einer eigenen Kennung (ID_{tgs}) an den Nutzer (C) zurückgeschickt. Mit dem empfangenen Zeitstempel (TS_1) konnte der (AS) zuvor eine Zeitsynchronisation vornehmen.
[AS $\rightarrow$ C: $Realm_c$, ID_c, $Ticket_{tgs}$, E_{KC} $\langle$ $K_{c,tgs}$, TS_2, $Realm_{tgs}$, ID_{tgs} $\rangle$]
Das Ticket setzt sich aus mit E_{Ktgs} verschlüsselten Komponenten zusammen:
$Ticket_{tgs}$ = E_{Ktgs} $\langle$ Flags, $K_{c,tgs}$, $Realm_c$, ID_c, AD_c, TS_2 $\rangle$

Schritt 3: Die eingetroffene Nachricht am Computer des Nutzers (C) wird nach einer Passwortabfrage entschlüsselt. Anschließend schickt Nutzer (C) das erhaltene Ticket ($Ticket_{tgs}$), das verschlüsselte Komponenten, seine Kennung (ID_c) und einen Zeitstempel (TS_3) enthält, die im $Authenticator_c$ untergebracht sind, sowie die Kennung des Applikationsservers (ID_v) zum Ticket Granting Server (TGS). Die Nachricht hat folgenden Aufbau:
[C $\rightarrow$ TGS: Options, ID_v, TS_3, $Nonce_2$, $Ticket_{tgs}$, $Authenticator_c$]

Schritt 4: Mit dem geheimen Schlüssel (E_{Ktgs}), den (AS) und (TGS) beide kennen, ist die eingetroffene Nachricht im (TGS) zu entschlüsseln. Mit dem Session Key ($K_{c,tgs}$) kann zweifelsfrei die Echtheit der Nachricht von (C) nachgewiesen werden. Daraufhin entschlüsselt (TGS) mit dem Session Key den

$Authenticator_c$. Nun stellt der (TGS) für den Nutzer (C) ein Ticket für den Applikationsserver (SV) aus und schickt eine entsprechende Nachricht an den Nutzer (C):
[TGS $\rightarrow$ C: $Realm_c$, ID_c, $Ticket_v$, $E_{kc,tgs}$ $\langle$ $K_{c,v}$, Times, $Nonce_2$, $Realm_v$, ID_v $\rangle$]
Das Ticket setzt sich aus mit E_{kv} verschlüsselten Komponenten zusammen:
$Ticket_v$ = E_{kv} $\langle$ Flags, $K_{c,v}$, $Realm_c$, ID_c, (AD_c), Times $\rangle$
Der Authenticator hat die Form:
$Authenticator_c$ = $E_{Kc,tgs}$ $\langle$ (ID_c), $Realm_c$, TS_1 $\rangle$

Schritt 5: Nach der letzten vom (TGS) erhaltenen Nachricht liegen alle Anmeldeparameter vor. Jetzt schickt Nutzer (C) eine Nachricht zum Applikationsserver (SV), um einen Dienst anzufordern. Die Nachricht hat den Aufbau:
[C $\rightarrow$ SV: Options, $Ticket_v$, $Authenticator_c$]
Der $Authenticator_c$ setzt sich aus mit $E_{Kc,v}$ verschlüsselten Komponenten zusammen:
$Authenticator_c$ = $E_{Kc,v}$ $\langle$ (ID_c), $Realm_c$, TS_2, Subkey, Seq-Nr. $\rangle$
Der Subkey kann wahlweise zur Verschlüsselung der Session beim Applikationsdialog eingerichtet werden. Die Seq-Nr., ein optionales Feld, liefert Sequence-Nummern für den Dialog.

Schritt 6: Abschließend schickt der Applikationsserver (SV) folgende Nachricht zur Eröffnung des Applikationsdialog zum Nutzer (C):
[SV $\rightarrow$ C: $E_{Kc,v}$ $\langle$, Subkey, Seq-Nr. $\rangle$]

Die Schlüssel der Nutzer werden aus deren Passwörtern unter Verwendung einer geeigneten Einweg-Hash-Funktion *(string-to-key)* abgeleitet. Aus Sicherheitsgründen werden die in der Datenbasis abgelegten *Secret Keys* zusätzlich mit einem Master Key verschlüsselt. Da Kerberos die geheimen Schlüssel seiner Nutzer kennt, kann er Nachrichten erstellen, die einen Principal (Nutzer) von der Identität seines Kommunikationspartners überzeugen. Um die Identität eines Principals nachzuweisen, werden neben den Tickets spezielle Authentikatoren, die zusammengefasst als *Credentials* bezeichnet werden, eingesetzt. Diese werden ausnahmslos verschlüsselt verschickt. Als Verschlüsselungsverfahren wird DES in der Kerberos-Version 4, andere Verfahren in der Version 5 eingesetzt. Als Betriebsmodi der Blockchiffren wird in der Version 5 CBC eingesetzt (Abschn. 4.2.1).

Tickets werden ausschließlich vom KDC erstellt und erfüllen die Aufgabe, die Identität des Principals, für den das Ticket ausgestellt wurde, sicher zum Server zu übertragen. Jedes Ticket gilt generell nur für ein Principal, der allerdings das Ticket mehrmals verwenden kann.

Authentikatoren werden ausschließlich von den Principals erzeugt und gelten – im Gegensatz zu den Tickets – genau einmal. Somit muss der Principal (Client) für jede Nutzung eines Servers einen neuen Authentikator erstellen. Authentikatoren werden genau für zwei Zwecke erzeugt: sie enthalten den Namen des Nutzers und der Realm, die mit einem Sitzungsschlüssel chiffriert wurden, und sie enthalten einen Zeitstempel, der ein Wiedereinspielen *(Replay-Attacken)* von

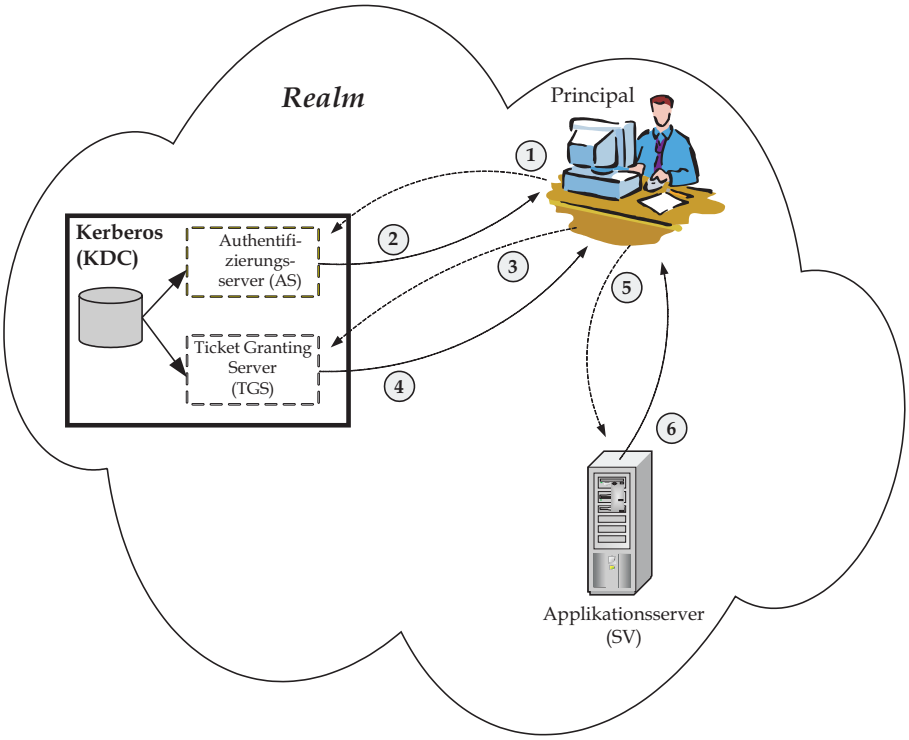


Abb. 5.14: Authentifizierung und Freigabe des Zugriffs auf einem Applikationsserver durch einen Kerberos-Server (KDC)

abgelauschten Ticket-Authentikator-Paaren verhindert. Allerdings wird eine Toleranz (Unschärfe) von einigen Minuten im Zeitvergleich zugelassen. Dennoch ist es erforderlich, dass alle Maschinen einer Realm ihre Uhren hinreichend gut synchronisieren. Weiterhin sind in der Kerberos V5 so genannte Nonce eingeführt worden. Diese dienen ebenfalls zur Unterbindung von Replay-Attacken, da ein Nonce nur einmal verwendet wird und einen zufällig ermittelten Wert beinhaltet. Zur Unterscheidung mehrerer im Netz kursierender Nonce werden sie mit Indices versehen.

Kerberos hat viele Kritiker, nicht zuletzt deshalb, weil das Protokoll etlichen Revisionen unterworfen wurde. Weiterhin stellt die Datenbank mit den geheimen Schlüsseln *aller* Nutzer ein gewisses Sicherheitsrisiko dar, so dass im Umgang mit dem Kerberos-Server eine besondere Sorgfalt gelten muss. Die Datenbank muss physikalisch sicher untergebracht werden und sollte nur ausgewählten Personen zugänglich sein. Außerdem sollte der Computer mit der Datenbank keine weiteren Aufgaben erfüllen, insbesondere nicht als NFS-Server oder -Client eingesetzt werden. Ebenso sollte der Fernzugriff über die bekannten UNIX-r-Utilities, SSH, Telnet etc. unterbunden werden. Weiterhin wird als Schwachstelle bezeich-

net, dass das Kerberos-Master-Passwort der Authentifikationsdatenbank in einem File auf der Kerberos-Servermaschine abgelegt werden muss, um bei einem automatischem Reboot oder Systemabsturz verfügbar zu sein. Die Negativliste könnte um etliche Punkte – z.B. das Problem der Ticketlebenszeit oder das Proxy-Problem – ergänzt werden.

Aktuell arbeitet die von der IETF eingesetzten Arbeitsgruppe (KERB-WG) an Verbesserungen. Eine ganze Reihe von Vorschläge liegen derzeit zur Diskussion vor. So wurde durch das [RFC 2623] die Adaption zu NFS Version 2 und 3 hinzugefügt. Weiterhin wurde das Kerberos-Protokoll erweitert, um den Einsatz für Telnet Sessions zu ermöglichen. Ebenso wurde TLS als Sicherheitsprotokoll eingeführt. Weitere Schritte sind Kerberos für die Public-Key-Kryptographie tauglich zu gestalten.

5.5 Übungen

1. Welches sind die Kerngrößen, die für Authentifizierungsverfahren bestimmend sind?
2. Welche zwei großen Unterscheidungen sind hinsichtlich der Authentifizierung bezogen auf Informationssysteme zu treffen?
3. Mit welchen Mitteln kann aus einer einfachen ungeschützen Authentifizierung eine einfache geschützte Authentifizierung erreicht werden?
4. Welches ist der Unterschied zwischen einer Zwei-Wege- und Zwei-Faktoren-Authentifizierung?
5. Welche Rolle spielt die Zeit bei einer Authentifizierung?
6. Worin unterscheiden sich PAP und CHAP?
7. Welches sind die Vorteile von Kerberos gegenüber PAP/CHAP?
8. Welche Rolle spielt das Needham-Schroeder-Protokoll bei Kerberos?
9. Welches sind die Grundideen des Tripel-A-Modells?
10. Welche Implementierungen gibt es zu Tripel-A für die mobilen Netze?
11. Was beinhalten die AVP's beim DIAMETER-Protokoll im Fall einer Mobile-IP-Applikation?
12. Was zeichnet Kerberos gegenüber RADIUS und TACACS+ aus?

6 Varianz der VPN-Typen

In Abschn. 6.1 werden drei wesentliche Einsatzmöglichkeiten von VPN-Technologien für unterschiedliche Geschäftsvorfälle beschrieben. Abschn. 6.2 behandelt die Randbedingungen für den Einsatz eines VPN und stellt den Bezug zu der in Abschn. 3.2.6 diskutierten Sicherheitsphilosophie her.

Die elektronischen Unternehmensgrenzen (Perimetergrenzen) lösen sich zusehens auf. Dieser Prozess wird – je nach Geschäftsanforderung – unterstützt durch ein vom Unternehmen selbst realisiertes VPN, durch das VPN eines Netzanbieters (NSP)[1] oder eines reinen Internetanbieters (ISP)[2].

Infonetics Research schreibt in ihrem 1997 erschienenen VPN-Report, dass mit einem VPN eine Kosteneinsparung von 20% bis 47% gegenüber herkömmlichen Weitverkehrsverbindungen erreicht werden kann. Noch größer sind die Kosteneinsparungen (60% - 80%) bei einem Remote-Access-VPN. Damit verspricht die VPN-Technologie den Unternehmen eine Verminderung des zunehmenden Kostendruckes, der auf der IT lastet und hält für jeden Geschäftsvorfall eine adäquate Lösung parat. Abb. 6.1 zeigt die drei wesentlichen Anwendungsfälle heutiger VPN-Lösungen:

Intranet-VPN: Dieser VPN-Typ verbindet Außenstellen und entfernt gelegene Büros über eine geteilte, meist öffentliche Infrastruktur mit einer Zentrale. Über diese Infrastruktur werden dezidierte Verbindungen eingerichtet. In den entfernt angebundenen Außenstellen und Büros sind die gleichen Geschäftsprozesse möglich wie im privaten Netzwerk des Unternehmens. Eine Kommunikation findet unter sicheren Randbedingungen statt. Gesonderte Einwahlmechanismen können bei geeigneter Architektur wegfallen.

Extranet-VPN: Es ermöglicht eine Anbindung von Zulieferern, Partnern und eventuell eigenen Kunden sowie anderen am Intranetzugang der Firma interessierten Gruppen. Eine Verbindung erfolgt über eine geteilte öffentliche Infrastruktur. Relevante Geschäftsprozesse sind wie im privaten Netzwerk der Firma möglich, allerdings innerhalb vorgegebener Sicherheitsrichtlinien und QoS-Anforderungen. Eine spezielle Einwahl ist auf jeden Fall erforderlich.

Remote-Access-VPN: Entfernte technische Außendienstmitarbeiter, Vertriebsmitarbeiter, Heimarbeiter und eventuell kleine Büros wählen sich über öffentliche Wählleitungen, z.B. ISDN oder PSTN, ins Firmennetz ein. Es wird

---

[1] Ein Network Service Provider (NSP) bietet seinen Kunden eine dezidierte IP-Bandbreite auf seinem privaten Backbone an, vielfach auf Grundlage eines Asynchronous Transfer Modus (ATM) oder auf Basis der Frame-Relay-Technik an. Häufig wird darüber hinaus den Kunden auch ein Internetzugang bereit gestellt.

[2] Ein Internet Service Provider (ISP) bietet seinen Kunden ausschließlich einen Internet-Zugang an.

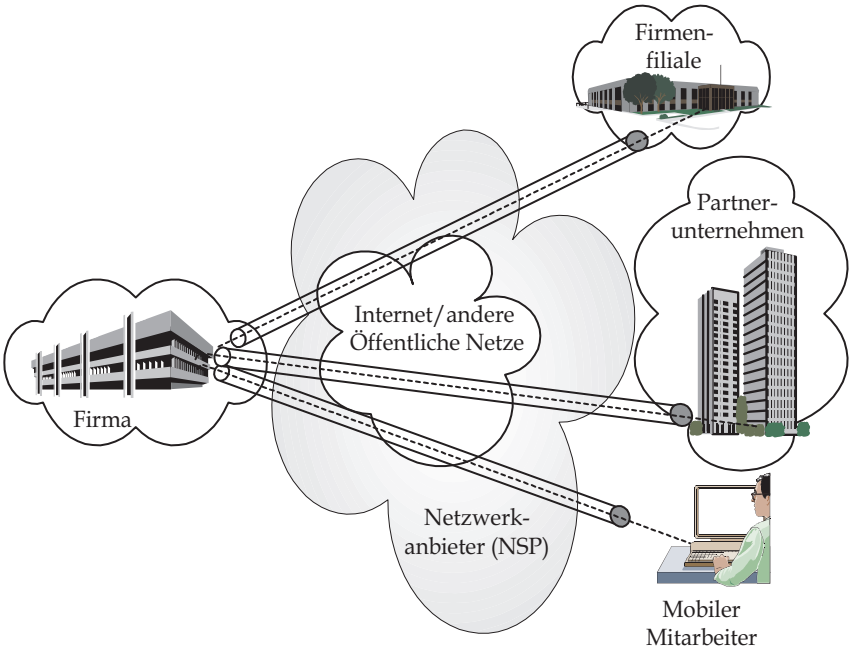


Abb. 6.1: VPN-Anwendungsspektrum

ihnen ein Rechteprofil für den Zugriff auf Netzwerkressourcen und Applikationen eingeräumt. Die Mitarbeiter können dieselben Geschäftsprozesse ausführen, als ob sie ihren Computer im Firmennetzwerk bedienten. Eine spezielle Einwahl ist auf jeden Fall erforderlich.

Natürlich können diese drei VPN-Typen gleichzeitig und vermischt eingerichtet werden. Es gibt die Möglichkeit, den jeweiligen VPN-Typ durch einen Netzanbieter (NSP) realisieren zu lassen oder nur den reinen Internetanschluss von einem (ISP) zu beziehen, um in Eigenregie ein eigenes VPN aufzubauen, zu betreiben und zu warten.

Dabei ist bei den drei VPN-Typen offen, welche Art von VPN-Technologie eingesetzt wird. Es kann ein Secure VPN, ein Trusted VPN (Extranet) oder aus einer Hybrid VPN-Technologie bestehen.

6.1 VPN-Einsatzmöglichkeiten

Obgleich die VPN-Technologien nahezu standardisiert sind, unterstützen nicht alle Produkte am Markt alle VPN-Typen. Solange nur eine Technologie zum Einsatz kommt, ist dies nicht kritisch. Dennoch sind für eine geeignete VPN-Lösung folgende Gesichtspunkte zu beachten. Die VPN-Lösung sollte:

- auf die Geschäftsprozesse abgestimmt sein,
- eine hinreichende Kommunikationssicherheit bieten,
- ausreichende Performance liefern und
- interoperabel zu den bestehenden Systemen sein.

Den größten Mehrwert kann ein Unternehmen erreichen, wenn sich eine vorhandene Lösung bei Veränderungen – z.B. Geschäftsprozessen – flexibel erweitern bzw. neuen Technologien anpassen lässt. Immer mehr Produkte ermöglichen diese Flexibilität.

Nahezu alle IPSec-basierten VPN beruhen derzeit auf eine IPv4-Umgebung, die in absehbarer Zeit nicht mehr das dominante Protokoll im Internet sein wird; Version IPv6 gewinnt zunehmend an Bedeutung. Somit ist es heute schon wichtig, dass die ausgewählten Lösungen kompatibel bzw. an die künftige IPv6-Version anpassungsfähig sind. Allerdings spielt, um eine gelungene VPN-Implementierung zu erreichen, neben der Technik auch die Erfahrung des beratenden Unternehmens eine große Rolle.

Häufig wird die Kommunikationssicherheit (Kapitel 3) als ein gravierendes Problem beim Einsatz eines VPN hervorgehoben. Es gibt heute ausgereifte kryptographische Absicherungsmöglichkeiten (Kap. 4), die stets aktuell gehalten werden und die auf künftige Gegebenheiten erweitert werden (Abschn. 4.2.5). Bei einer sorgfältigen Planung und einer gut abgestimmten Sicherheitspolitik sowie ausreichenden Sicherheitsmaßnahmen spielt die Kommunikationssicherheit eher eine untergeordnete Rolle. Im Prinzip sollten zwei unterschiedliche Vertrauensmodelle bei einer VPN-Planung berücksichtigt werden. In dem einen Modell vertraut das Unternehmen a priori *nicht* dem Netzanbieter – vor allem dann, wenn das VPN über Netze mehrerer Anbieter geführt werden soll, was im Rahmen der Globalisierung keine Seltenheit mehr ist. So gilt z.B. das *Layer-2-Tunneling-Protokoll* allein schon lange nicht mehr als sicher. Deshalb hat die IETF empfohlen, den Tunnelverkehr mittels IPSec zu verschlüsseln. Somit muss eine Firma, die auf das Layer-2-Tunneling-Protokoll setzt, entsprechende eigene Maßnahmen ergreifen. In Abschn. 7.2.3 wird näher auf das Layer-2-Tunneling-Protokoll (L2TP) eingegangen.

Im Alternativmodell traut das Unternehmen dem Netzanbieter (NSP) zu, ein fremdgewartetes, sicheres VPN zu unterhalten. Dies ist vergleichbar mit der Bereitstellung von öffentlichen Frame-Relay- oder auch ATM-Diensten eines Netzanbieters, wenn man von der zukünftigen MPLS-Technologie und den optischen Netzen absieht. In diesem Modell vertraut das Unternehmen darauf, dass keine IP-Pakete fehlgeleitet, verändert, belauscht oder analysiert werden. Ebenso wird den Firewallaktivitäten – z.B. funktionierende Filterlisten oder Firewall-Monitoring – des Netzanbieters vertraut.

Ausgehend von den sieben Schichten des OSI-Referenzmodells (Abb. 2.2) können verschiedene Sicherungsmaßnahmen auf den verschiedenen Ebenen zur Absicherung unterschiedlicher VPN-Typen installiert werden – je nachdem welches

Ziel und welches Vertrauensmodell verfolgt wird. Generell lassen sich aus einem VPN-Blickwinkel die sieben Schichten auf drei VPN-Ebenen reduzieren (Abb. 6.2):

- VPN auf der Applikationsebene in den Schichten (5 - 7),
  - Ein VPN auf Layer-5 kann eine sichere Kommunikation auf der Session-Ebene über einen Proxy-Dienst aufbauen, indem TCP verwendet wird. Diese Architektur ist gut geeignet, um mit Partnernetzen zu kommunizieren. Der VPN-Client arbeitet auf der Transportschicht problemlos mit den Computern des Partnernetzes zusammen. Ebenso überwindet auf dieser Ebene der VPN-Client auf einfache Weise die Firewall des Partner-Extranetzes, was bei einem VPN auf Layer-3 schwieriger ist. VPN auf Layer-5 sind jedoch nicht in der Lage, RPC-basierte Dienste abzufangen, so dass ein mobiler Nutzer keine File- und Druckerdienste ausführen kann, wie es für einen entfernten LAN-Zugriff üblich ist. Allerdings können alle auf TCP-aufbauenden Anwendungsprotokolle wie HTTP, FTP oder Telnet eingesetzt werden, ohne dass in bestehenden Anwendungen Änderungen auf den Partnercomputern vorgenommen werden müssen.
- VPN auf der Transport-/Netzwerkebene in den Schichten (3 - 4),
  - Ein Layer-4-VPN dient der sicheren Kommunikation auf der Transportschicht. Diese Art VPN ist gut geeignet für die sichere Kommunikation von zwei oder mehreren Netzwerken, die eine sichere Verbindung für E-Commerce-Anwendungen benötigen.
  - Ein Layer-3-VPN bietet die Möglichkeit, neben TCP/IP, auch Protokolle wie RPC und UDP einzusetzen. Derartige VPN-Lösungen werden vornehmlich für ein Remote-Access-VPN eingesetzt und bieten dem Nutzer ein breites Anwendungsspektrum. Allerdings ist das Supportaufkommen nicht zu unterschätzen.
- VPN auf der Sicherungs-/Bitübertragungsebene in den Schichten (1 - 2)
  - VPN auf den unteren Schichten besitzen gegenüber VPN der höheren Schichten den Vorteil, dass wesentlich einfacher Quality of Service-Garantien (QoS) verbindlich erteilt werden können. Vorteile liegen in der Skalierbarkeit und im VPN-Management.

In diesem Kontext wird auf die VPN-Technologie sowohl auf der Applikationsebene als auch auf der Transport/Netzwerk- und der Sicherungs-/Bitübertragungsebene eingegangen. Die technischen Voraussetzungen werden in den nächsten Kapiteln behandelt.

In den drei Ebenen (Applikationsschicht, Transport-/Netzwerkschicht und Link- bzw. Physikalische-Ebene) lassen sich die wesentlichen Protokolle und Sicherungsmechanismen einordnen, mit denen sich die vollständige Absicherung eines VPN und damit auch des sonstigen Datenverkehrs erreichen lässt. Da

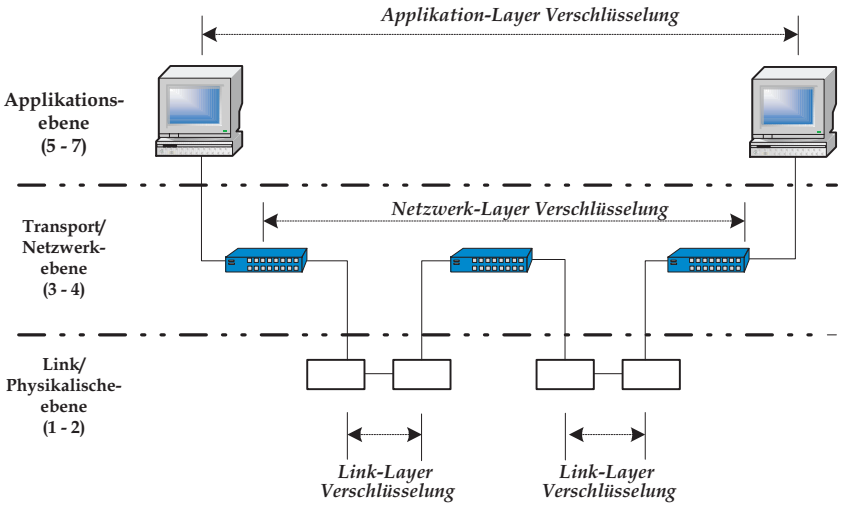


Abb. 6.2: Einordnung der VPN ins Schichtenmodell

die VPN-Technologie in direktem Zusammenhang mit der vertraulichen Datenübertragung steht, haben sich im Laufe der Zeit in den drei Ebenen unterschiedliche Absicherungsmechanismen mit unterschiedlichen Zielsetzungen herauskristallisiert. Abb. 6.3 zeigt die Protokolle und Verfahren zur Absicherung der unterschiedlichen VPN-Lösungen auf den Schichten (1 - 7). Hervorzuheben ist die Absicherung auf der Netzwerkebene oder speziell die IP-Absicherung. Eine effektive Absicherung wird in Abschn. 7.4 mit der Diskussion über IPSec vorgestellt.

Einige der modernen kryptographischen Sicherungsmechanismen lassen sich in der Anwendungsebene finden, z.B. in Secure MIME (S/MIME) oder Pretty Good Privacy (PGP). Die gängigen für ein VPN geeigneten Sicherheitstechnologien sind:

- IP Paket Filtertechniken
- Network Address Translation (NAT)
- IP Security Architecture (IPSec)
- SOCKS
- Secure Socket Layer (SSL)
- Application Proxyies
- Firewall-Systeme
- Kerberos, RADIUS, DIAMETER, TACACS+ und andere Authentifizierungssysteme

- Antivirus, Content-Überprüfung und Intrusion Detection Systeme (IDS)

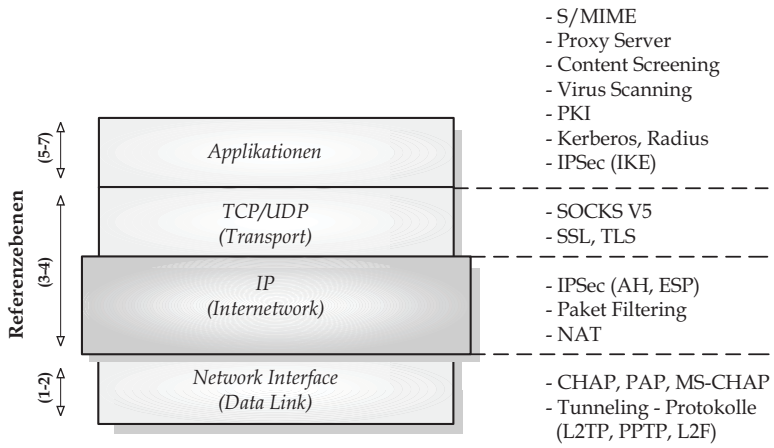


Abb. 6.3: Typische Absicherungsmechanismen für VPN-Lösungen auf unterschiedlichen Schichten

Abb. 6.3 zeigt die Technologien bezogen auf die Internet-Schichtenansicht. Die mittlere Schicht (Transport-/Netzwerkschicht) ist hervorgehoben, weil sie eine bedeutende Rolle in der VPN-Technologie spielt. Aufgrund der zahlreichen Möglichkeiten ist es interessant zu wissen, wie sich die einzelnen Technologien ergänzen, überlappen oder ob sie für bestimmte Absicherungen einfach nicht geeignet sind.

Der Vergleich in Tabelle 6.1 berücksichtigt wiederum die speziellen Anforderungen eines VPN und ermöglicht den Entwurf einer ersten Sicherheitsarchitektur. Das gewünschte Sicherheitsniveau lässt sich einfach nivellieren. Details werden im Kapitel 10 behandelt. In der ersten Spalte von Tab. 6.1 sind die wesentlichen Lösungen, Protokolle und Mechanismen aufgelistet, in der ersten Zeile die typischen Sicherungsmöglichkeiten. Wie der Matrix zu entnehmen ist, bietet eine IP-Filterung nur die Möglichkeit einer Zugriffskontrolle und einer UDP-Unterstützung. Im Gegensatz dazu bietet IPSec die weitreichendsten Möglichkeiten, jedoch keine Session-Überwachung. Es wird deutlich, dass eine Kombination der unterschiedlichen Möglichkeiten ratsam ist. Um das gewünschte Sicherheitsniveau zu erreichen, sollte eine entsprechende Sicherheitsstrategie vorhanden sein. An dieser Stelle sei darauf hingewiesen, dass es nicht sinnvoll ist, ein Sicherheitsniveau anzustreben, wenn vorher nicht festgelegt wurde, was vor wem zu schützen ist (Kap. 3).

6.1.1 Intranet-VPN (Site-to-Site)

Kennzeichnend für ein Intranet-VPN ist, dass es verschiedene Standorte derselben Firma verbindet. Dies ist eines der einfachsten und häufigsten VPN-Szen-

Tabelle 6.1: Vergleich charakteristischer Sicherheitstechnologien für VPN-Lösungen

Lösung	Zugriffskontrolle	Verschlüsselung	Authentifizierung	Integritätsprüfung	Schlüsselaustausch	Verbergen der internen Adresse	Schutz gegen Wiedereinspielen	Session-Kontrolle	UDP-Unterstützung
IP-Filter	Ja	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja
NAT	Ja	Nein	Nein	Nein	Nein	Ja	Nein	Ja (Verbindung)	Ja
L2TP	Ja (Verbindung)	Ja (PPP-Link)	Ja (call)	Nein	Nein	Ja	Nein	Ja (call)	Ja
IPSec	Ja	Ja (Paket)	Ja (Packet)	Ja (Paket)	Ja	Ja	Ja	Nein	Ja
SOCKS	Ja	Optional	Ja (client/user)	Nein	Nein	Ja	Nein	Ja (Verbindung)	Ja
SSL	Ja	Ja (Daten)	Ja (system user)	Ja	Ja	Nein	Ja	Ja	Nein
Appl.-Proxy	Ja	normal nicht	Ja (user)	Ja	normal nicht	Ja	normal nicht	Ja (Verbindung, Daten)	normal nicht
AAA-Server	Ja (Verbindung)	einige	Ja (user)	Nein	normal nicht	Nein	Nein	Nein	Ja

arien, die heutzutage anzutreffen sind. Abb. 6.1 zeigt das typische Beispiel der Anbindung einer Filiale (oberer Teil der Abbildung) an die Firmenzentrale (unten im Bild).

Am Aufbau eines Site-to-Site-VPN sind zwei VPN-Gateways/Firewall-Systeme beteiligt. Die Verschlüsselung der Daten erfolgt nur auf dem Weg zwischen den beiden VPN-Gateways; der Weg durch das lokale Netz vom Gateway zum Endgerät bleibt unverschlüsselt. Das VPN ist somit für Endgeräte transparent und sie benötigen keine zusätzliche VPN-Client-Software. Abb. 6.4 zeigt eine typische Konfiguration. Hier zielt eine VPN-Absicherung darauf, dass unbefugte Dritte nicht in das Intranet eindringen können, und dass die Daten, die über das Internet oder über das IP-Netz eines Providers (ISP) geführt werden, auf dem Übertragungswege für unbefugte Dritte unbrauchbar sind.

Eine Möglichkeit, ein *Site-to-Site*-VPN zwischen einer Zentrale und einer Niederlassung einzurichten, besteht darin, lediglich einen Internetanschluss bei einem ISP zu mieten und auf beiden Seiten Firewall-Systeme bzw. Router mit integrierter Firewall-Technologie oder spezielle IPSec-Gateways an der Schnittstelle zum Internetanschluss einzurichten. Dieses Szenario benötigt keine zusätzliche IPSec-Technologie, wenn die Firewall bzw. der spezielle Router die für IPSec notwen-

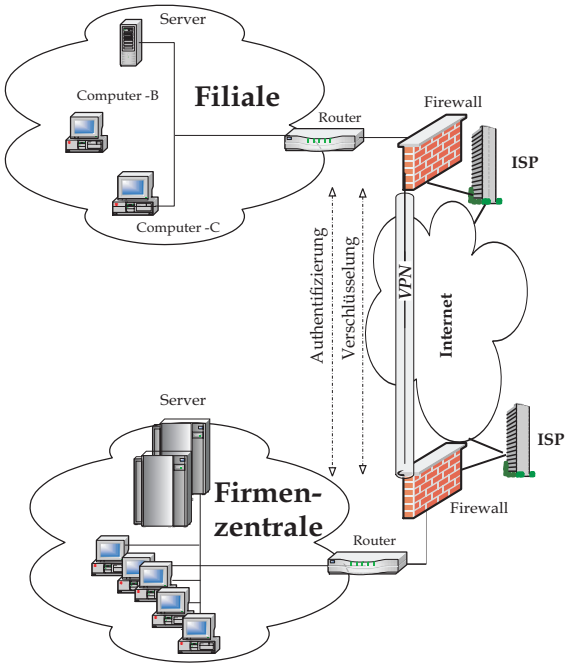


Abb. 6.4: Beispiel eines typischen Intranet-VPN

digen Schritte durchführt. Kapitel 7 geht detailliert auf diese Techniken ein. Mit dieser Lösung können vertrauliche Informationen – ohne Zugriff oder Kenntnisnahme von unbefugten Dritten – verschickt werden. Die Firewall hält dabei wirksam Angriffe ab.

6.1.2 Extranet-VPN (End-to-End)

In einem Extranet werden virtuelle Verbindungen zwischen den Sites mehrerer Firmen, die unterschiedliche Interessen haben können, verknüpft. Ein sehr eindrucksvolles Beispiel ist in Abbildung 1.4 illustriert. Es zeigt das Branchennetz der Automobilindustrie, das mit dem ENX-Projekt ein europaweites Extranet eingerichtet hat. Dabei haben die beteiligten Organisationen (Hersteller/Zulieferer) unterschiedlich beschränkte Zugriffe auf das Extranet. Es lassen sich weitere Vorteile für ein Extranet-VPN aufzählen:

- Eine weitgefächerte Erreichbarkeit des Unternehmens
- Eine größere zeitliche Effizienz der Geschäftsprozesse
- Ein besserer Kundenservice

- Eine bessere Zusammenarbeit innerhalb des Unternehmens
- Eine Verbesserung der Zusammenarbeit innerhalb der Wertschöpfungskette im Bereich der Zulieferer *(Supply Chain)*
- Eine frühere Investitionsrückgewinnung *(Return of Investment)*

Ein Extranet kann über das Backbone eines einzigen Netzbetreibers geschaltet sein. Es können jedoch auch mehrere Netzbetreiber und sogar autonome Systeme hinzugezogen werden, wenn dies für die Zusammenschaltung erforderlich ist. Somit existiert ein gravierender Unterschied zum Intranet-VPN, in dem Zugangskontrollmechanismen den beschränkten Zugriff der unterschiedlichen Organisationen regeln. Diese Zugangskontrolle wird häufig mit Firewall-Systemen, mit Zugriffslisten *(Access Lists)* in den jeweiligen Routern oder mit richtlinienbasierte Kontrollen *(Policy-based Access Controls)* realisiert. Diese Kontrollen können mit speziellem Equipment firmenseitig oder auf der Netzbetreiber-Seite durchgeführt werden. Abb. 6.5 zeigt ein typisches Extranet-VPN zwischen einem Hersteller und einem Zulieferer.

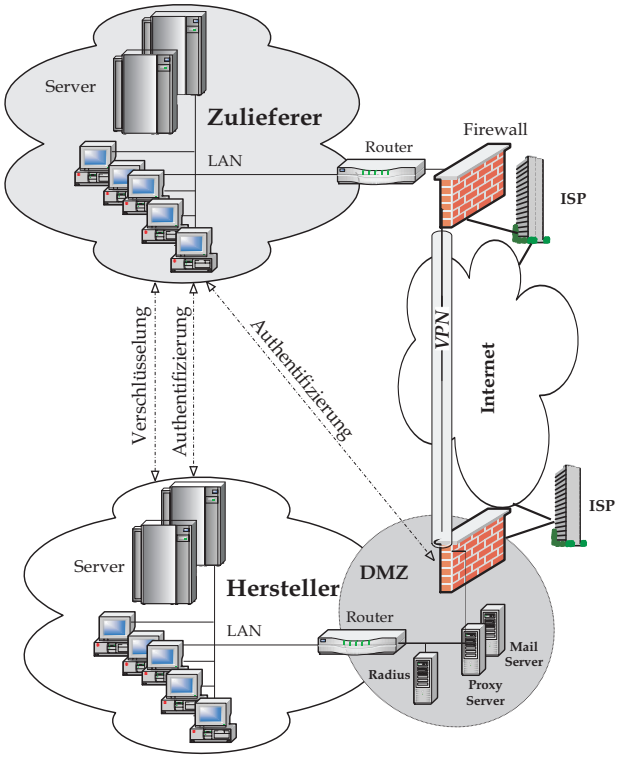


Abb. 6.5: Beispiel eines Extranet-VPN

In einem End-to-End-VPN erfolgt die Verschlüsselung häufig direkt zwischen zwei Endgeräten über den gesamten Kommunikationsweg hinweg. Beide Seiten sind mit einer VPN-Client-Software ausgestattet und müssen die öffentlichen Schlüssel aller Kommunikationspartner kennen. Bei der Kommunikation über das Internet benötigt jeder VPN-Client eine offizielle feste IP-Adresse. Ein VPN dieser Kategorie kann z.B. zwischen dem Arbeitsplatzrechner einer Zulieferfirma und der Produktionsfirma, die mit dem Zulieferer zusammenarbeitet, geschaltet sein. Dabei kann eine Kommunikationsverbindung direkt zum Intranet-Server des Herstellers eingerichtet werden. Häufig entsteht eine Ende-zu-Ende-Verbindung.

Die Authentifizierung des Arbeitsplatzrechners bei einem Verbindungsaufbau wird zuerst an der Firewall bzw. an dem Router des Herstellers und anschließend am Server im Intranet des Herstellers durchgeführt. Eine Berechtigungsvalidierung findet für einen Verbindungsaufbau seitens des Zulieferers an zwei Punkten statt. Wie der hierzu notwendige Tunnel eingerichtet wird, hängt stark von den QoS-Anforderungen der Beteiligten ab. Im einfachsten Fall kann z.B. ein IPSec-VPN über das Internet geschaltet werden. Die Datenpakete, die ausgetauscht werden, werden für unbefugte Dritte unbrauchbar übertragen.

6.1.3 Remote-Access-VPN (End-to-Site)

Ein End-to-Site-VPN ist eine Mischung aus den ersten beiden Varianten. Sie dient dem Aufbau von Remote-Access-VPN, wenn ein externer Client eine verschlüsselte Verbindung zum Firmennetz benötigt. Die Verschlüsselung erfolgt vom Client zum VPN-Gateway, wobei derzeit noch alle Clients mit einer VPN-Client-Software ausgestattet werden müssen[3], da das IP selbst erst ab der Version IPv6 eine Verschlüsselungsmöglichkeit besitzt. Die klassische Anwendung eines Remote-Access-VPN ist die Anbindung von Außendienstmitarbeitern. Z.B. bei Versicherungsunternehmen ergreifen die Versicherungsvertreter die Initiative, um mit dem Firmennetz eine Verbindung herzustellen. Abb. 6.1 zeigt im oberen rechten Teil den Verbindungsaufbau eines VPN mit einem mobilen Endgerät (Laptop) mittels DFÜ über den Internetzugang eines Providers (ISP) ins LAN seines Unternehmens. Meistens wird DHCP eingesetzt, so dass eine reguläre Firewall die IP-Adresse nicht zuordnen kann. Eine andere Möglichkeit ist die Einwahl[4] in das IP-Netz eines Providers; an der Firmen-Firewall muss dann eine zweite Authentifizierung durchgeführt werden.

Die Kontaktaufnahme mit einem Firmennetzwerk von einem außerhalb gelegenen Standort ist so neu nicht. Seit geraumer Zeit können sich Firmenmitarbeiter

[3] In jüngster Zeit wird dieser Zugriff häufig mit einem TLS/SSL-VPN geregelt. Dann ist keine Client-Software notwendig.

[4] Dies geschieht oftmals über eine separate 800-Telefonnummer. Die Einwahl ist dann durch ein allgemeines Passwort für die ganze Firma geschützt.

via Modem ins Firmennetz einwählen – allerdings mit einer inzwischen überholten Übertragungsleistung. Diese Möglichkeit fordert den Unternehmen die Installation von Modempools, entsprechende Räumlichkeiten und geschultes Personal ab. Mit einem Remote-Access-VPN fallen diese häufig aufwändigen Rand-

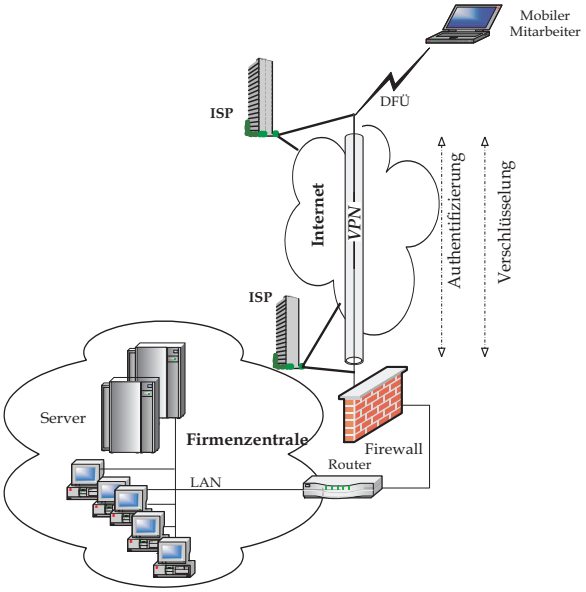


Abb. 6.6: Schematische Darstellung eines Remote-Access-VPN

bedingungen weg und ermöglichen eine Kostenreduktion bei gleichzeitigem Übertragungs- und Informationsgewinn für die Außendienstarbeiter des Unternehmens. Im Gegensatz zu einer Modemverbindung wird bei einem Remote-Access-VPN die Kommunikationsverbindung zu einem Internet Service Provider aufgebaut. Heutige Betriebssysteme wie Windows 2000 oder Linux sind hierfür ausreichend vorbereitet. Auch mit preiswerten ISDN-Routern, wie z.B. von DrayTek, Netgear, AVM etc. kann eine Verbindung aufgebaut werden. Verwendete Protokolle sind L2TP, L2F, PPTP oder IPSec. Diese werden im Kapitel 7 ausführlich behandelt.

Ein Tunnelaufbau mittels Authentifizierung und Datenverschlüsselung wird in einem zweiten Schritt zwischen der Firewall des Unternehmens und dem einwählenden Computer, z.B. einem Laptop, aufgebaut (Abb. 6.6). Im Prinzip gibt es für solch ein Szenario zwei Möglichkeiten, um ein Remote-Access-VPN aufzubauen:

Client-initiiert: Über die Einwahlsoftware auf dem Laptop des Außendienstmitarbeiters wird eine sichere IP-Verbindung zum Internet Service Provider aufgebaut und zum Unternehmensnetz weitergeleitet.

Server-initiiert: Vom Client-Rechner (Laptop) wird eine nichtsichere Verbindung zum ISP aufgebaut und erst der Network Access Server (NAS) stellt anschließend eine sichere Verbindung über das öffentliche Netz zwischen Client-Rechner und NAS her.

Beide Varianten habe ihre Vor- und Nachteile, die je nach Anforderung mehr oder weniger ins Gewicht fallen. Bei der zweiten Lösung fällt wesentlich weniger Aufwand für Installation, Wartung und Update-Service an. Beispielsweise kann bei einer umfangreichen Laptop-Basis mit etlichen hundert oder gar tausend Geräten ein erheblicher Aufwand und Kostenblock entstehen, wenn zuvor eine Modemeinwahl möglich war, die nun im Zuge eines Remote-Access-VPN ausgetauscht werden soll. Allein die Installation der Client-Software ist eine logistische und technische Herausforderung, wenn außerdem die künftige Authentifizierung mittels Smart Card erfolgen soll – ganz abgesehen davon, dass zuvor eine Public-Key-Infrastruktur (PKI) im Unternehmen aufgebaut werden muss.

6.2 Eckpunkte für den Einsatz eines VPN

Vor der Planung eines VPN muss man sich über einige Randbedingungen im Klaren sein. Der zentrale Anschluss eines VPN in das Firmennetz erfolgt durch ein spezielles VPN-Gateway, eine Firewall oder durch einen Router. An diesem Anschlusspunkt muss eine VPN-Sicherheitspolitik umgesetzt werden, die mit dem vorhandenen IT-Sicherheitskonzept in Einklang stehen muss. Nachfolgend werden zu diesem Anschlusspunkt einige Überlegungen angestellt.

6.2.1 VPN-Sicherheitspolitik

Bevor via VPN ein Zugang zum Firmennetz eingerichtet wird, ist es sinnvoll, einige grundsätzliche Überlegungen zum Thema Kommunikationssicherheit anzustellen (siehe auch Kapitel 3). Ausgehend von der Überlegung, dass ein verschlüsselter VPN-Tunnel nicht ohne weiteres kompromittiert werden kann, sind die beiden Endpunkte eine nicht zu unterschätzende Gefahrenzone, wenn keine speziellen Maßnahmen, wie z.B. in Kapitel 5 beschrieben, vorgenommen wurden. Nie kann sich ein Kommunikationspartner vollkommen sicher sein, dass kein unbefugter Dritter eine Verbindung aufbaut. Weiterhin kann es bei der heutigen Virenflut nur zu leicht passieren, dass ein „Wurm“ oder „Trojaner“ seine zerstörerischen Aktivitäten selbst über eine verschlüsselte Verbindung entfaltet – obwohl gerade die Transparenz für die Anwendungen einer der Pluspunkte eines VPN ist.

Von einem Laptop aus können sich Würmer über das VPN ins Firmennetz einschleusen und durch die Windows-Dateifreigaben meist unbemerkt weiterverbreiten. Ähnliches gilt für Trojanische Pferde.

Solche Risiken lassen sich nicht völlig ausschließen, können aber durch ein konkretes Sicherheitskonzept minimiert werden. Grundsätzlich muss das VPN-Gateway gegen Angriffe von außen geschützt werden. Es gelten die gleichen Regeln wie beim Betrieb einer Firewall: Außer den notwendigen Diensten – z.B. der PPTP- bzw. IPSec-Server und SSH für die Fernwartung – muss alles abgeschaltet werden. Die Umsetzung dieser Beschränkungen erfolgt beim Unternehmen, nicht beim auf dem Notebook installierten Client.

Während ein einfaches Netzwerksicherheitskonzept beschreibt, welcher Netzverkehr wohin erlaubt ist und welcher unterbunden werden soll, beschreibt ein VPN-Sicherheitskonzept mehr die Absicherungscharakteristik eines spezifischen Verkehrsprofils. Damit bildet es eine Ergänzung zum regulären Netzwerksicherheitskonzept. Es betrachtet ein spezielles Netzsegment wesentlich detaillierter, wird allerdings durch den Rahmen des Netzwerksicherheitskonzepts eingegrenzt. In einem VPN-Sicherheitskonzept ist beschrieben, durch welche Absicherungsmaßnahmen das Kommunikationsaufkommen, das durch das VPN geleitet wird, zu schützen ist:

- Wie sollen Quell- und Zielports geschützt werden?
- Welche Sicherheitsprotokolle (Tab. 6.1) sollen grundsätzlich auf welcher Ebene (Abb. 6.2) eingesetzt werden?
- Wie sehen die Sicherheitsanforderungen für die Authentifizierung, Verschlüsselung, Schlüsseltransport, Schlüssellänge sowie Lebenszeit der Schlüssel etc. aus?

Dabei können VPN-Sicherheitsrichtlinien für einzelne Geräte, Verbindungen oder zentrale Lösungen installiert werden. Vorzuziehen ist allerdings immer eine zentralisierte Einrichtung, wenn es sich um eine umfangreiche Menge von Sites oder um eine größere Anzahl von Fernzugriffen handelt, die es zu betreuen gilt. Cisco [Halpern et al. 2004] schlägt hierzu beispielsweise die SAFE-Lösung[5] vor, die im Wartungsaufwand gegenüber einer Einzellösung erhebliche Vorteile bietet.

6.2.2 VPN und Firewall

Werden die derzeit gängigen VPN-Gateway-Lösungen eingehender betrachtet, so lassen sie sich grob in vier Varianten einstufen. Und auch hier gilt: Die Lösung gibt es nicht, sondern alle Varianten haben ihre Berechtigung und sind in der Praxis vorzufinden. Das Rahmenwerk für die Freiheitsgrade unterschiedlicher Konstellationen ist das Sicherheitskonzept, das von der Sicherheitsarchitektur und von der im Unternehmen vorherrschenden Sicherheitsphilosophie geprägt ist (Abschn. 3.2.6).

[5] Die Fa. Cisco bietet im Rahmen der hauseigenen Blueprint-Serie SAFE eine komplette Beschreibung, konkret für kleine mittelständische, große und sehr große Firmen, zur Einrichtung eines sicheren VPN.

Die einzige Verbindung zum Internet soll ausschließlich über die Firewall erlaubt sein und deshalb soll ein VPN-Gateway hinter der Firewall platziert werden (Abb. 6.7). Allerdings ist diese Konstellation mit einigen Nachteilen verbunden:

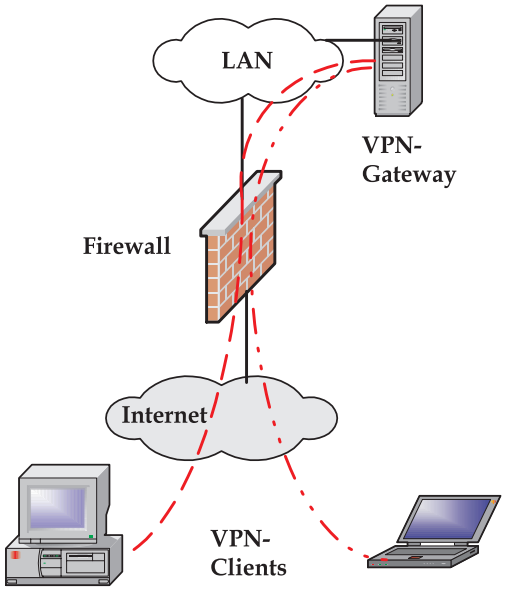


Abb. 6.7: Das VPN-Gateway ist hinter der Firewall positioniert

1. Die Firewall kann eingehende verschlüsselte Pakete, die für das VPN-Gateway bestimmt sind, nicht ausreichend analysieren und filtern.
2. Die Firewall kann nicht erkennen, an welche Rechner oder Ports die verschlüsselten Pakete gerichtet sind.
3. Virenfilter und Mail-Gateways haben Schwierigkeiten, mit dieser Konstellation umzugehen.
4. Gewöhnlich treten Probleme mit dem Network Address Translation (NAT) bzw. Masquerading mit einer Firewall auf, wenn z.B. ein IPSec-VPN-Gateway mit einem Authentication Header (AH) betrieben wird. Wird ausschließlich ein AH verwendet, darf aufgrund der vorgenommenen Prüfsumme nachträglich an den IP-Paketen nichts verändert werden. Dies jedoch passiert bei NAT.

Bei IPSec-Installationen (Abschn. 7.4) wird der Hash-orientierte Authentication Header (AH) allerdings seltener eingesetzt. Häufiger ist die Verschlüsselung mit Encapsulation Security Payload (ESP). Und auch hier gibt es Probleme, denn etliche kostengünstige ISDN-Router bzw. DSL-Router mit eingebauter NAT-Funktion können mit ESP oft nicht umgehen. Genaue Ausführungen zu IPSec werden

in Kap. 7 diskutiert. Gleiches gilt für das von PPTP verwendete Generic Routing Encapsulation (GRE).

Wesentlich weniger problembehaftet ist die Konstellation, bei der ein VPN-Gateway in Form einer IPSec-Lösung direkt in die Firewall integriert ist (Abb. 6.8). Hierzu existieren mittlerweile etliche Herstellerlösungen. Bei dieser Konstellation konzentriert sich z.B. für den Administrator der Aufwand in Wartung und Pflege allein auf die Firewall. Und somit reduziert sich neben den Anschaffungskosten auch die Anzahl der zu betreuenden Computer. Dennoch rät das Bundesamt für

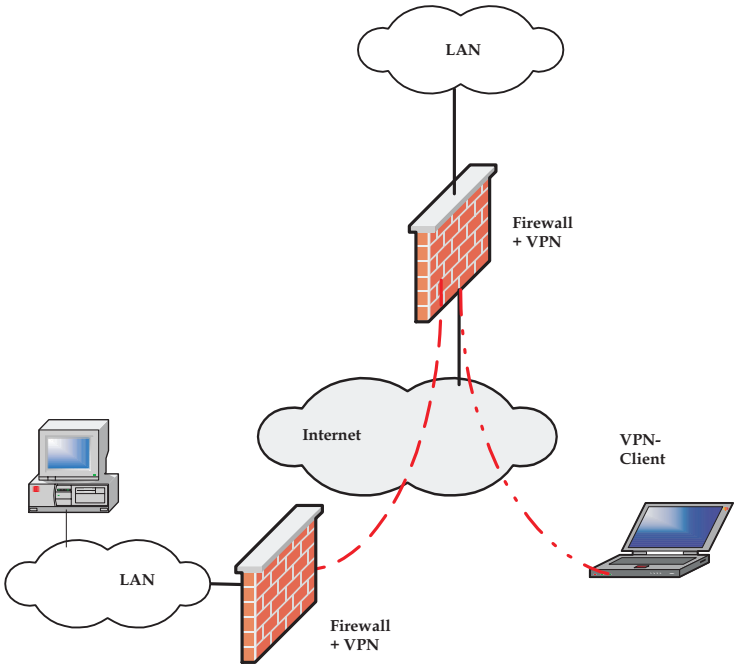


Abb. 6.8: Das VPN-Gateway und die Firewall befinden sich auf demselben Computer

Sicherheit in der Informationstechnik (BSI) nachdrücklich von diesen als *All-in-One* bezeichneten Lösungen ab. Begründet wird dies damit, dass jeder zusätzliche Dienst auf einer Firewall die Sicherheit beeinträchtigen kann. Häufig weisen gerade offene VPN-Ports in der Praxis eine gewisse Angriffsschwäche gegenüber den gefürchteten *Denial-of-Service-Attacken* (DOS) auf. Z.B. bei der Checkpoint-Lösung (Firewall-1) sowie bei der Nachfolger Version NG ist eine VPN-Lösung (Modul) direkt in der Firewall implementiert. Ein VPN-Client (Secure Remote-Verschlüsselungsclient) kann eine gesicherte Remote-Kommunikation über das Internet aufnehmen. Weiterhin kann eine LAN-to-LAN-Kopplung über das Internet durch die Absicherung zweier Firewall-Systeme erreicht werden. Eine vergleichbare Konstellation ist auch bei etlichen Routern möglich. Hier werden dann Anpassungen bzw. Konfigurationsänderungen an der Firewall bzw. am Router

notwendig. Folgende Änderungen müssen vorgenommen werden:

- Das IP-Forwarding muss freigeschaltet (erlaubt) werden
- Der UDP-Port 500 für das Schlüsselmanagement (IKE) muss geöffnet werden
- Die Protokollnummern 50 und 51 für (ESP) und (AH) müssen geöffnet werden
- Der UDP-Port 1701 für L2TP und L2F muss geöffnet werden
- Die IP-Protokollnummer 47 (GRE) und der TCP-Port 1723 für PPTP muss geöffnet werden

Sicherheitstechnisch ist es daher sinnvoll, das VPN-Gateway völlig aus dem Einflussbereich des LAN und der Firewall zu entfernen. Ideal ist es das VPN-Gateway in die ohnehin oft schon vorhandene demilitarisierte Zone (DMZ) zu integrieren.

Eine Minimalkonstellation zeigt Abb. 6.9: Hier wird die Firewall mit einer zusätzlichen Netzwerkkarte (Interface) ausgerüstet und an diese das VPN-Gateway angeschlossen. Zusätzlich benötigt die Firewall noch spezielle Regelerweiterungen, mit denen der Netzwerkverkehr über das Interface zum VPN-Gateway geleitet wird. Obwohl diese Konstellation in die richtige Richtung weist,

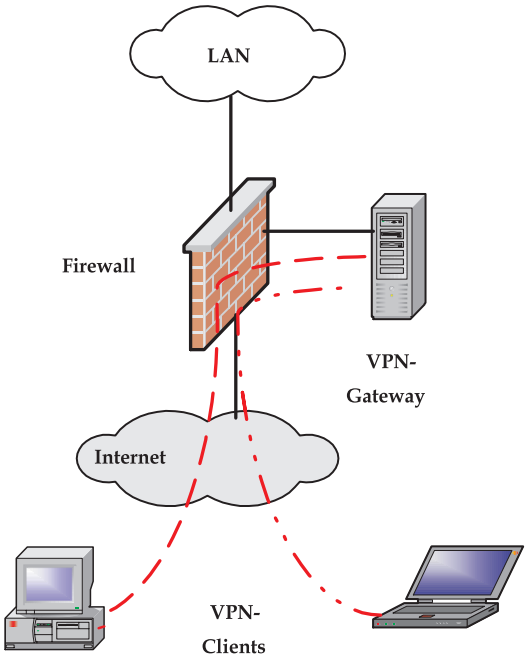


Abb. 6.9: Das VPN-Gateway ist über eine Netzwerkkarte mit der Firewall verbunden und steht in der DMZ

gibt es Anlass zur Kritik. Die verschlüsselten IP-Pakete, die zum VPN-Gateway umgeleitet und dort entpackt werden, werden anschließend direkt in das LAN eingespeist. Folglich müssen alle Prüfungen, die sonst auf der Firewall durchgeführt werden, auf dem VPN-Gateway vorgenommen und somit an zwei Orten bzw. auf zwei Rechnern (Firewall, VPN-Gateway) Filterregeln eingerichtet und gepflegt werden. Hierbei können den oftmals überlasteten Administratoren gefährliche Fehlkonfigurationen unterlaufen. Natürlich ist diese Gefahr immer gegeben, doch sollte eine Konstellation bevorzugt werden, die möglichst einfach und stringent zu handhaben ist.

Als derzeit ideal hat sich jene Konstellation herauskristallisiert, bei der ein Router mit Paketfilterregeln, die den ein- und ausgehenden Verkehr überwachen, vorgeschaltet ist. Hinter diesem Router, der nur bestimmte IP-Pakete aus dem Internet an das Gateway weiterleitet, findet gleichzeitig das VPN-Gateway Schutz (Abb. 6.10). Außerdem stellen spezielle Filterregeln sicher, dass niemand von außen IP-

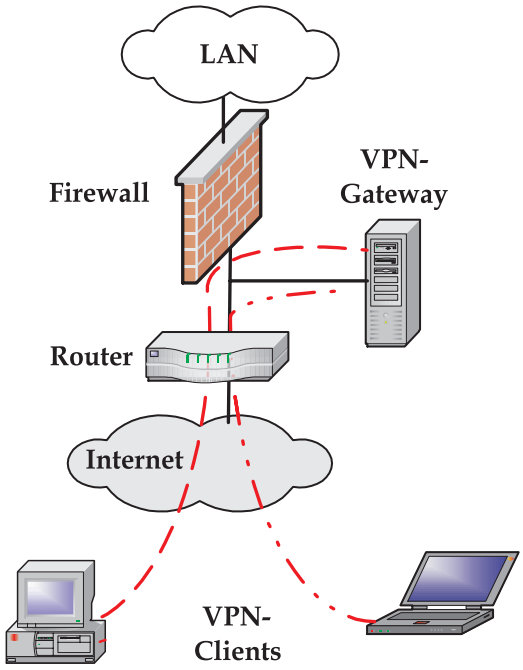


Abb. 6.10: Das VPN-Gateway befindet sich vor der Firewall in einer DMZ und wird über einen zusätzlichen Router angesprochen

Pakete einschleusen kann, die nur scheinbar aus den VPN-Netzen kommen. Ein weiterer großer Vorteil dieser Konstellation besteht darin, dass die bereits vom VPN-Gateway entschlüsselten IP-Pakete noch die Firewall passieren müssen, um ins Firmen-LAN zu gelangen. Damit wird sichergestellt, dass die lokalen Sicherheitsregeln nicht unterlaufen werden. Auch kann der Zugriff von außen über das

VPN auf bestimmte Rechner und Ressourcen beschränkt und E-Mails auf Viren untersucht werden.

6.2.3 VPN und Router

Router können – genauso wie Firewall-Systeme – zum Aufbau eines VPN eingesetzt werden, wenn sie ein entsprechend ausgelegtes Betriebssystem haben. Im Gegensatz zu Site-to-Site-VPN, die Daten auf physikalischer Ebene zwischen zwei Geräten Punkt-zu-Punkt verschlüsseln, ist der Einsatz von IPSec-VPN problematischer.

Zurückzuführen ist das auf die mangelnde Spezifikation des IPSec-Protokolls im Bereich der Remote-Nutzer-Authentifizierung und der Client-Konfiguration. Remote-Nutzer-Authentifizierung und Datenkompression werden derzeit von vielen Herstellern noch proprietär gehandhabt. Damit sind diese wichtigen Funktionen in einem heterogenen Umfeld oftmals nicht nutzbar, weil nicht jedes Gerät diese Eigenschaften auf gleiche Weise umgesetzt hat. Wichtige Funktionen wie automatische Konfiguration sind in einem heterogenen Netz nicht möglich. Der Administrator kann zwar in einigen Fällen detaillierte Rechteprofile bis zum Endanwender weiterleiten, doch gilt dies meist nur, wenn durchweg Komponenten nur eines Herstellers verwendet werden. Folglich muss manuell konfiguriert werden, was sich auf die Skalierbarkeit nachteilig auswirkt. Dies ist bei der Betreuung einer großen Anzahl von Geräten nicht mehr machbar.

6.2.4 Quality of Service in VPN

Die Frage nach einer garantierten Dienstgüte, z.B. der Quality of Service (QoS), ist für ein Overlay-Netz, welches mit Tunneltechniken oder allein mit IPSec verkapselten IP-Paketen aufgebaut wird, zunächst negativ zu beantworten, sofern das darunter liegende Netz (z.B. Internet) nach dem Best-Effort-Prinzip arbeitet.

6.2.5 Diffserv in VPN

Allerdings ist es, wie in Abschn. 2.3.4 über DiffServ diskutiert, dennoch möglich, ein IPSec-basiertes End-to-End-VPN mit Dienstgüten zu realisieren. Das erweiterte TOS-Feld im IPv4-Protokollkopf und das *Traffic-Class-Octet* im IPv6-Protokollkopf, das gemäß Diffserv als *DS-Field* bezeichnet wird und ein Per-Hop-Behavior (PHB) ermöglicht, lässt in den dafür ausgelegten Netzknoten eine Steuerung nach Dienstgüten und zuvor festgelegten Service Level Agreements (SLA) zu.

Der Einsatz von DiffServ in IPSec-VPN ist im Wesentlichen darauf zurückzuführen, dass IPSec das DS-Feld im Protokollkopf nicht nutzt und auch nicht in kryptographische Berechnungen, z.B. bei einer Hash-Wert-Bildung zur Integritätssicherung, einschließt. Somit hat eine Modifikationen des DS-Felds

zugunsten einer Steuerung nach Dienstgüten auf einen Netzknoten, der Teil eines IPSec-Tunnels ist, keine Auswirkungen. Im Tunnel-Mode des IPSec-Frameworks wird zusätzlich am Tunnelanfang ein IP-Header *(Outer-Header)* gebildet, der den eigentlichen IP-Header des Senders (Host) einkapselt *(Inner-Header)*. Nähere Ausführungen finden sich in Abschn. 7.4 über IPSec. Die Arbeitsweise des DS-Felds in einem IPSec-Tunnel verläuft nach folgendem Schema:

1. Der Netzknoten zu Beginn eines IPSec-Tunnels verpackt gemäß IPSec das IP-Paket des Senders und setzt das DS-Feld im Outer-Header gemäß den vorab eingestellten SLA-Werten der lokalen DS-Domain.
2. Das gesicherte (gekapselte) IP-Paket durchläuft nun das DS-fähige Netzwerk. Passierte Zwischenknoten modifizieren das DS-Feld.
3. Am Tunnelende angelangt, werden die Tunnelpakete im letzten Netzknoten entfernt und somit die originalen (ursprünglichen) Informationen im IP-Header des Senders zur Weiterleitung wiederhergestellt.
4. Falls die letzte DS-Domain des originalen IP-Datagramms sich von der DS-Domain des IPSec-Tunnelanfangs unterscheidet, wird am Tunnelende im letzten Netzknoten das DS-Feld des originalen IP-Paketes den herrschenden SLA-Bedingungen angepasst. Damit übt der letzte Netzknoten die Eigenschaft eines *DS-Ingress-Node* aus.
5. Nach Verlassen des IPSec-Tunnels – falls das IP-Paket weiterhin in einem DS-fähigen Netzwerk zur Zieladresse weitergeleitet werden muss – modifizieren die Zwischenknoten das originale IP-Paket.

6.2.6 Beispiel einer komplexen VPN-Architektur

In diesem Abschnitt wird eine VPN-Architektur diskutiert, die *on the wild* existiert, d.h. diese Architektur wird in einer realen Umgebung operativ eingesetzt, gewartet, gepflegt und weiterentwickelt. Die Verwaltung und Betreuung der VPN-Plattform wird von einem Drittanbieter (IT-Dienstleister) durchgeführt. Die VPN-Plattform wird als Remote-Access-Plattform von vier Finanzdienstleistern zur Einwahl (Fernzugriff) in das jeweilige Unternehmensnetz genutzt. Beabsichtigt ist, mit dem VPN eine Ende-zu-Ende Sicherheit (Vertraulichkeit) zu ermöglichen sprich eine verschlüsselte Verbindung zwischen dem VPN-Client eines Nutzers und dem VPN-Gateway zu etablieren. Ebenso soll eine starke Authentifizierung mittels Zertifikaten vorgenommen werden. Das VPN bietet Fernnutzern die Freiheit, sich von jedem Festnetz- bzw. Internetanschluss in das jeweilige Firmennetz einzuwählen.

Die Abb. 6.11 skizziert die Remote-Access-VPN-Plattform aus Sicht der Kommunikationsobjekte. Eine funktionale Betrachtung der Einwahl eines Fernnutzers geschieht wie folgt:

- Ein Fernnutzer wählt sich mit seiner eigens installierten Software (NCP-Client) z.B. über eine Wählverbindung auf den Access-Router der VPN bzw. RAS-Plattform ein (vgl. linke obere Bildhälfte). Es handelt sich bei dem VPN um eine L2Sec-Implementierung der Fa. NCP aus Nürnberg (vgl. Abschn. 7.2.4 und Abb. 7.11).
- Das VPN-Gateway ist in der Beispielarchitektur hinter der Firewall platziert, so dass die verschlüsselten Pakete von der Firewall durchgelassen werden. Damit kann die Firewall lediglich Ports und IP-Adressen filtern und nicht Paketinhalte.
- Am VPN-Gateway wird der VPN-Tunnel terminiert und die Pakete entschlüsselt. Da die Höhe der Last zeitlichen Schwankungen, z.B. je nach Tageszeit und Wochentag, unterworfen ist, ist es erforderlich mehrere VPN-Gateways parallel zu betreiben. Damit wird die Last der einzelnen Gateways aufeinander abgestimmt. In der Abb. 6.11 ist dies durch die hintereinander geschachtelte schematische Darstellung der VPN-Gateways angedeutet. Sind die Pakete des Fernnutzers entschlüsselt, werden diese in die eigentliche DMZ an den RADIUS-Server weitergeleitet.
- Der RADIUS-Server führt im Wesentlichen ein Accounting durch, um auf der mandantenfähigen Plattform, für den Betreiber der Plattform eine verursachergerechte Abrechnung zu erstellen. Nach Erfassung der relevanten Abrechnungsparameter, wird das eingangene Paket weitergeleitet.
- Am LADAP-Server (DirX) findet eine Zertifikatsüberprüfung und eine Rollen- und Berechtigungsprüfung statt. Im Rahmen der Zertifikatsprüfung wird u.a. eine mögliche Revokation des Zertifikats abgeprüft.
- Nach Durchlaufen der Prüfungen werden die Pakete in einem GRE-Tunnel zu den Partnernetzen bzw. zu den Routern am Ausgang der Plattform geschickt. Je nach Zugehörigkeit des Fernnutzers wird eine Tunnlerichtung vorgegeben.
- Zwischen den Routern am Ausgang der Plattform und den Firewall-Systemen (unterer Teil der Abb. 6.11) ist keine Absicherung hinsichtlich der Vertraulichkeit vorgesehen. Die Partnernetze gelten a priori als vertrauenswürdig. Damit ist der Fernnutzer schließlich in sein Firmennetz gelangt und kann seine Geschäftsvorfälle bearbeiten.

Aus Sicht des Wartungspersonals sind die hierzu erforderlichen Komponenten in der rechten Hälfte der Abbildung dargestellt. Denn neben der eigentlichen Bereitstellung der Funktionalität, ist es ebenso zwingend die Perimeterkomponenten auf den neuesten sicherheitstechnischen Stand (Patch) zu halten. Jedoch sind auch reguläre Updates der verschiedenen Hersteller zu berücksichtigen.

Dies Beispiel illustriert, wie ein Zusammenspiel derjenigen Komponenten, die in den vorangegangenen Kapiteln diskutiert wurden, in einer mandantenfähigen Plattform zum Einsatz kommen. Oftmals ist es einfacher, nur einzelne Komponenten isoliert zu betrachten. Doch erst das Zusammenspiel und die Beherrschung

des Zusammenspiels der Komponenten einer komplexen Infrastruktur ist eine nicht zu unterschätzende Aufgabe für den Betrieb einer solchen Plattform.

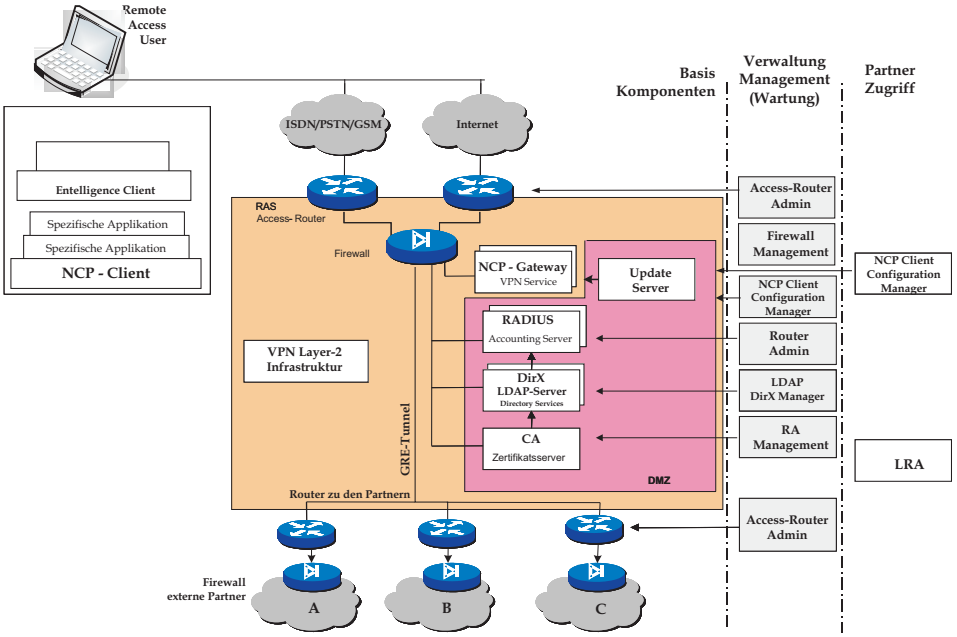


Abb. 6.11: Mandantenfähige Remote-Access-VPN-Plattform für die Einwahl von ungefähr 6000 Nutzern

Natürlich stellt die Architektur einige Herausforderungen an den Architekten der Plattform. So muss die Plattform mit zunehmender Anzahl der Nutzer mitwachsen (vgl. Abschn. 9.2). Neben den rein technischen Aspekten sind z.B. nachprüfbare Leistungsparameter, derer die Zuverlässigkeit anhand und Verfügbarkeit der VPN-Plattform gemessen werden kann, für die einzelnen Mandanten wichtig. Der Abschnitt 9.2.3 beschäftigt sich ausgiebig mit diesem Thema.

6.2.7 Ausblick

Bezogen auf das OSI-Referenzmodell lassen sich gemäß Abb. 6.2 drei unterschiedliche VPN-Layertypen definieren. Es sind die VPN der Anwendungsebene (Application Layer), der Transport- und Netzwerkebene (Network Layer) sowie der Netzwerkverbindungsebene (Link/Physical Layer).

Neben den oben aufgezeigten Varianten der VPN-Layertypen, gibt es zwei grundsätzliche Ansätze (Secure, Trusted) ein VPN zu implementieren, sowie ergänzend eine Mischform (Hybridform). Im ersten Ansatz (Eigenrealisierung) wird das (Secure, Trusted) VPN vom Unternehmen in Eigenregie betrieben. Im zweiten An-

satz, in der reinen Provider-Lösung oder Hybridform, wird ein VPN durch einen Netzanbieter vollständig bzw. teilweise implementiert.

Tab. 6.2 zeigt, welche VPN-Services zu welcher Architektur und Technologie zuzuordnen sind. Weiterhin wurde eine Abgrenzung der Architektur und Technologie eines Remote-Access-VPN gegenüber einem Intra- und Extranet-VPN vorgenommen. Der Architektur- bzw. Technologie-Einsatz kann in Bezug auf Fremdleistung, Hybrid-Form und Eigenrealisierung betrachtet werden.

Die in Tab. 6.2 aufgezeigten Tunneltechnologien stehen im Kap. 7 im Vordergrund. Die WAN-Technologien (Frame Relay, ATM, MPLS) werden im Kap. 8 behandelt.

Tabelle 6.2: VPN-Services, Architekturen und Technologien auf Netzwerk- und Protokollebene

Service	**Architektur**	**Technologien**
Access-VPN	Vom Endgerät aufgebaut und vom Netzzugang (NAS) initiiert	L2F/L2TP, IPSec, PSTN, xDSL, Mobile-IP, Kabel
Intranet und Extranet-VPN	IP-Tunnel Virtual Circuit MPLS	GRE, IPSec Frame Relay, ATM IP oder IP-over-ATM

Beide Ansätze bzw. Anwendungsszenarien haben ihre Besonderheiten, Vorzüge und Nachteile im Betrieb. Diese und die Entscheidung, welche Lösung (Site-to-Site, End-to-Site, End-to-End) mit einem Netzwerkanbieter bzw. in Eigenregie verwirklicht werden sollte und welche Kriterien dabei zu beachten sind, werden im Kap. 9 behandelt.

6.3 Übungen

1. Auf welche drei grundsätzlichen Strukturen lassen sich die unterschiedlichen VPN-Architekturen zurückführen. Wie lautet die Begründung für diese drei Strukturen?

2. Welche drei Architekturen gibt es, um ein VPN-Gateway in Bezug zu einer Firewall zu platzieren?

3. Welche Vor- bzw. Nachteile haben die drei Architekturen hinsichtlich einer zentralen Administration der Perimeterkomponenten?

4. Wie könnten in den jeweils drei Architekturen des Abschn. 6.2.2 starke Authentifizierungen vorgenommen werden *(a)* und welche Protokolle müssten dazu eingesetzt werden *(b)*?

5. Welche Vorteile bietet eine demilitarisierte Zone (DMZ) gegenüber anderen Perimeterarchitekturen, die ein VPN-Gateway beinhalten?

6. Welche Anforderungen (QoS) müssten an ein VPN gestellt werden, wenn es Sprache in verschlüsselter Form übertragen soll *(a)* und wie könnte dies realisiert werden *(b)*?

7. Wie wird in der Beispielarchitektur (Abb. 6.11) die Authentifizierung bei der VPN-Einwahl eines Nutzers durchgeführt?

8. Wozu dient der GRE-Tunnel in der Beispielarchitektur (Abb. 6.11)?

9. Welchen Sinn haben die Firewall-Systeme (Abb. 6.11) im Bereich der Partner-Anbindung?

10. Was könnte die Erklärung sein, warum in der Beispielarchitektur (Abb. 6.11) sowohl RADIUS als auch Software-Zertifikate (X.509 v3) eingesetzt werden?

11. Ist es für einen mobilen Nutzer der Plattform auch möglich, sich über ein Roaming-unterstützendes Verfahren einzuwählen *(a)*? Falls nein, warum nicht *(b)* und wie müsste die Beispielarchitektur nachgebessert werden *(c)*?

12. Was könnte ein technischer Grund dafür sein, das bei dieser VPN-Plattform IPSec nicht eingesetzt wurde bzw. werden konnte?

13. Wie und welche Messgrößen müssten definiert werden, um die Leistungsfähigkeit der Plattform zu dokumentieren?

7 Secure VPN

Der Hauptgrund für den Einsatz von Secure VPN liegt darin, das Unternehmen über das Internet sensitive Informationen übertragen wollen, ohne dabei befürchten zu müssen, das diese Informationen unbefugte Dritte lesen können. Jede Information, die über das Secure VPN geht, ist in geeigneter Weise verschlüsselt und integritätsgesichert. Somit ist ein unbefugter Dritter, der den Verkehrfluss des Secure VPN mitschneidet (*captured*), nicht in der Lage – auch unter Einsatz von erheblicher Rechenleistung – den Verkehrsfluss zu entschlüsseln noch diesen unbemerkt zu verändern.

Zu den wesentlichen Protokollen der Secure VPN-Technologie gehören:

- IPSec mit geeigneter Verschlüsselung, im Transport- oder im Tunnelmodus.
- IPSec innerhalb einer L2TP-Verbindung
- SSL 3.0 bzw. TLS mit geeigneter Verschlüsselung

Diese Protokolle und deren Einsatz in unterschiedliche Szenarien bilden den Schwerpunkt dieses Kapitels.

Nach Einführung des zentralen Begriffs der Tunnel-Technologie (Abschn. 7.1), wird auf die unterschiedlichen Secure VPN-Architekturen eingegangen. Es wird detailliert IPSec diskutiert, das auch das komplizierte und noch nicht vollständig spezifizierte Remote-Access-Verfahren einschließt.

Im Laufe der Zeit sind mehrere ähnliche Tunnelprotokolle entwickelt worden, von denen in der Praxis hauptsächlich die nachfolgenden vier häufig vorzufinden sind:

1. Das Point-to-Point Tunneling Protocol (PPTP) von Microsoft, das im Grunde eine Erweiterung des Point-to-Point-Protokolls (PPP) darstellt. Unterstützt werden die Protokolle IP, IPX, NetBIOS und NetBEUI. Im Bereich der Fernein-wahl hat das PPTP ein größere Bedeutung erlangt.
2. Das Secure Socket Layer Protocol (SSL) bzw. das Transport Layer Protocol (TLS) hat sich als gesichertes Applikationskommunikationsprotokoll etabliert und wird vielfältig in Verbindung mit Homebanking oder zur Absicherung in der B2C-Kommunikation eingesetzt. Eine Variante zum SSL/TLS-Protokoll bildet das L2Sec-Protokoll, das als Alternative zu IPSec eingesetzt werden kann, wenn Komponenten auf dem Verbindungsweg nicht IPSec-fähig sind.
3. Das Internet Protocol Security (IPSec), das gemäß der Internet Engineering Task Force (IETF) in mehreren RFCs spezifiziert wurde, stellt den Standard für die Maschinenkommunikation (Router-Router-Kopplung) dar. Weiterhin

kann es nun im Bereich der Ferneinwahl – nach jüngsten Modifikationen der Spezifikation – eingesetzt werden.

4. Das Layer-2-Tunneling Protocol (L2TP), das aus zwei unterschiedlichen Entwicklungen hervorging und durch die IETF spezifiziert wurde, ist in den neueren Windows-Betriebssystemen implementiert worden.

Das umfassensde, aber auch das mit einem hohen Komplexitätsgrad behaftete Protokoll, das mehr einem Framework gleicht, ist IPSec. Es enthält für die heute wichtigsten VPN-Eigenschaften – Verschlüsselung und Tunneling – eigene weitreichende Spezifikationen. Weiterhin trifft es Vorkehrungen für die Benutzerberechtigung sowie für das Schlüsselmanagement und die Datenkompression. Hinzugekommen sind jüngst die Anpassungen bezügl. NAT, die im Remote-Access-Einsatz notwendig wurden.

Microsoft hat PPTP im Windows NT-4.0 Server implementiert und damit eine relativ große Marktdurchdringung erreicht. PPTP ist jedoch in seinen Möglichkeiten eingeschränkter als IPSec. Weiterhin hat ein Konsortium von Softwareherstellern PPTP mit einem ähnlichen Protokoll, dem Layer-2-Forwarding-Protocol (L2F), von CISCO kombiniert. Als Resultat entstand das L2TP Protokoll, welches von der IETF ebenfalls zum Standard erhoben wurde [RFC 2661].

7.1 Tunneling

Tunneling ist ein Konzept, mit dem beliebige Datenpakete über ein *(unsicheres)* Transitnetz im Huckepackverfahren sicher weitergeleitet werden können.

Als Analogie sei hier die Überwindung der Straße von Dover (Englischer Kanal) durch einen Eisenbahntunnel zwischen Frankreich und England herangezogen. Fahrzeuge, die auf die Insel möchten, werden auf der französischen Seite (Tunneleingang) auf die Bahn verladen und auf der englischen Seite (Tunnelausgang) wieder entladen. Ähnlich wie getunnelte IP-Pakete, können die Fahrzeuge Geschwindigkeit und Richtung im Tunnel nicht mehr selbst bestimmen.

Das Tunneling-Verfahren ist ein allgemein anerkanntes Verfahren zum Transport von IP-Paketen über andere Netze, beispielsweise IP-over-ATM, IP-over-Frame-Relay. Es wird auch verwendet, wenn IPv6 Pakete über ein IPv4 ausgelegtes Teilnetz geführt werden sollen. Eine Workstation bzw. ein Quellrechner verschickt das ganze Originalpaket als Nutzlast (*Payload*) eines anderen Protokolls. Dieser auch als *Encapsulation* bezeichnete Vorgang erzeugt einen zusätzlichen Protokollkopf *(Header)*, den so genannten Tunnel-Header, der dem Originalpaket vorangestellt wird. Abb. 7.1 zeigt, wie ein IP-Paket – mit Angabe der Quelle (A) und Ziel (B) nebst Nutzdaten verschickt – von einem Computer der Filiale durch ein VPN zur Firmenzentrale gelangt. Solange das IP-Paket durch den Tunnel transportiert wird, übernimmt der zusätzliche Header mit Quelle (1) und Ziel (2) die Weiterleitung. Während der Weiterleitung kann das ursprüngliche

Paket, je nach Tunneleigenschaft, sogar verschlüsselt werden. Im Zielrechner *(Sicherheitsgateway-2)* wird der Tunnel-Header entfernt und das Originalpaket ist wiederhergestellt. Dieser Mechanismus wird als Decapsulation bezeichnet. Aus Sicht einer Workstation bleiben in einem Netz existierende Tunnel unsichtbar. Sie werden von den VPN-Gateways virtuell in IP-Hops übersetzt. Der Anfangspunkt eines Tunnels wird dort definiert, wo der zusätzliche IP-Header hinzugefügt wird. Dies gilt ebenso für den Endpunkt des Tunnels, der sich dort befindet, wo der IP-Header wieder entfernt wird.

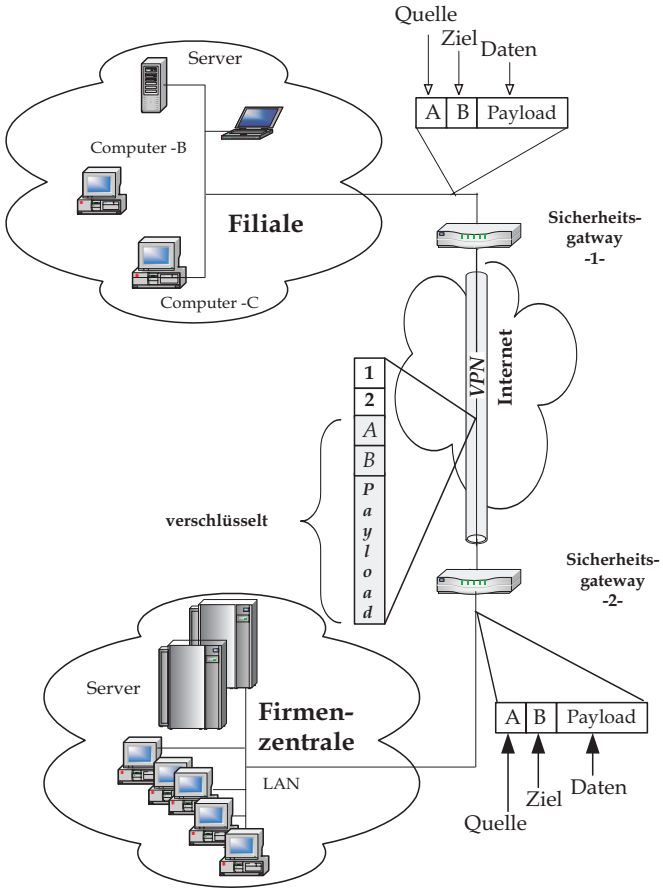


Abb. 7.1: IP-Paket-Transport zwischen Filiale und Firmenzentrale mittels Tunnel durch das Internet

Der General Routing Encapsulation (GRE)-Tunnel

Mit dem General Routing Encapsulation (GRE)-Protokoll wurde 1994 eine erste Standardisierung für Tunneling-Verfahren vorgenommen [RFC 1701, RFC 1702].

Dabei handelt es sich mehr um einen generellen Vorschlag als um ein eigentliches Protokoll, wie z.B. bei IPSec (Abschn. 7.4). Nach diesem Vorbild sind andere Tunneling-Protokolle, wie z.B. PPTP, ATMP von Ascend und BayDVS von Bay Networks, aufgebaut worden. Unter anderem sind auch Elemente von GRE in IPSec eingeflossen.

Grundsätzlich werden drei Abschnitte im GRE-Paket unterschieden:

1. Der GRE-Header (Protokollkopf)
2. Der eigentliche Netzwerk-Protokollkopf *(Delivery Header)*
3. Die Nutzlast *(Payload)*

Als Nutzlast *(Payload)* kann nahezu jedes beliebige Paket aus höheren Protokollschichten eingesetzt werden. Im GRE-Header werden Informationen über die verwendeten Tunnel- und Verschlüsselungsalgorithmen hinterlegt. Der Netzwerk-Protokollkopf speichert das Tunnelziel außerhalb des GRE-Tunnels.

Für Service-Anbieter, die ein gemanagtes IP-VPN über ein IP-Netzwerk als Produkt anbieten, hat das GRE-Protokoll signifikante Vorteile gegenüber einem IPSec-Tunnel. Zum einen kann ein fein abgestimmter Quality of Service (QoS) auf Applikationsebene erreicht werden, da die im Tunnel liegenden Router Header-Informationen auswerten können. Zum anderen sind die IPSec-Header-Informationen nicht sichtbar und somit auch nicht auswertbar. Weiterhin ist bei der GRE-Lösung der Datenverkehr durch die Ende-zu-Ende-Kontrolle an einen getrennten Kanal *(Out-Band)* gebunden. Hat allerdings ein Kunde einen höheren Sicherheitsbedarf, so ist es für den Provider möglich, *on demand* auf Applikationsebene eine Absicherung mittels Verschlüsselung anzubieten, z.B. für eine sichere Verbindung via Webbrowser. Die am meisten verbreitete Implementierung des GRE-Protokolls findet zwischen zwei Routern *(Point-to-Point)* statt, die manuell konfiguriert werden müssen. Deshalb wird das GRE-Protokoll als Tunneltechnik langfristig an Bedeutung verlieren.

7.2 Layer-2-Techniken

Der Begriff Layer-2 bezieht sich auf die Schicht 2 des OSI-Referenzmodells (Abb. 6.2). Layer-2-Tunneltechniken haben gegenüber Layer-3-Verfahren den systemimmanenten Vorteil, dass sie multiprotokollfähig sind, also neben IP auch z.B. IPX, SNA und Netbios übertragen. Weiterhin haben tiefere Schichten Vorteile bezüglich Wartung und Betreuung. Dabei bildet ein Layer-2-Tunnel quasi einen *virtuellen Kanal*, der sich unter jeder IP-Plattform einrichten lässt. Auch gibt es keine Probleme, wenn die IP-Router zwischen VPN-Klienten und Gateways eine *Network Address Translation* (NAT) vornehmen.

In der Regel wird ein Point-to-Point-Protokoll (PPP) im Tunnel über ein anderes Netzwerk, meist sogar über IP, unterhalten. Dies klingt zunächst kompliziert

und nach großem Verwaltungsaufwand *(Overhead)*, jedoch lassen sich etliche sinnvolle Eigenschaften aufzählen, die für diese Variante sprechen. Die Vielfalt und die Möglichkeiten des Internets wären stark eingeschränkt, wenn die Layer-2-Techniken nicht zur Verfügung stehen würden.

Alle Layer-2-Techniken liegen als Vorschläge bzw. als RFCs durch die IETF der Öffentlichkeit vor und können über das Internet bezogen werden. Tab. 7.1 gibt einen Überblick über die Access Tunneling-Protokolle, wie die Layer-2-Techniken häufig bezeichnet werden. Jede der in der Tab. aufgeführten Technologien hat

Tabelle 7.1: Vergleich der Layer-2-Techniken

Eigenschaften	**PPTP**	**L2F**	**L2TP**
Standard/Status	RFC 2637 (informell)	RFC 2341 (informell)	RFC 2661 (Standard)
Medium	IP/GRE	IP/UDP, FR, ATM	IP/UDP, FR, ATM
Private Adresszuweisung	ja	ja	ja
Multiprotokoll Unterstützung	ja	ja	ja
Kanäle	Eingang und Ausgang	Eingang	Eingang und Ausgang
Protokoll	Kontrolle über TCP Port 1723	Kontrolle über UDP Port 1701	Kontrolle über UDP Port 1701
Verschlüsselung	Microsoft PPP (Encryption MPPE)	PPP Encryption (MPPE); IPSec optional	PPP Encryption (MPPE/ECP); IPSec optional
Authentifizierung	PPP-Authentifizierung (user)	PPP-Authentifizierung (user); IPSec optional (Paket)	PPP-Authentifizierung (user); IPSec optional (Paket)
Tunnelmodus	typischerweise voluntary Tunnel-Modus	compulsory Tunnelmodus	voluntary & compulsory Tunnel-Modus
Mehrere Kanäle pro Tunnel	nein	ja	ja
PPP multilink-Unterstützung	nein	ja	ja

Stärken und Schwächen und je nach Anwendungsszenario ist eine geeignete Technologie auszuwählen. Nähere Ausführungen zu den Informationen in Tab. 7.1 sind in den nachfolgenden Abschnitten zu finden.

Mithilfe einer Erweiterung des PPP-Protokolls lassen sich Sicherheitsmechanismen und Layer-2-VPN-Tunneleigenschaften vereinen. Derzeit gibt es die folgenden Ansätze:

- Erweiterung der PPP-Authentication Phase (PAP/CHAP) und
- Erweiterung von PPP durch das Encryption Control Protocol (ECP).

PAP/CHAP wurden bereits in Abschn. 5.4.1 in Zusammenhang mit den Authentifizierungsverfahren und dem PPP-Protokoll diskutiert. Weiterhin kann

das Secure-Socket-Layer-Handshake-Protokoll (SSL) als Absicherung einer PPP-Verbindung eingesetzt werden wie [RFC 2716] beschreibt. Die Firma NCP bietet auf Basis dieser Technologie ihren Kunden VPN-Lösungen an (vgl. Abb. 6.11).

7.2.1 L2F

Das Layer-2-Forwarding (L2F)-Verfahren wurde etwa zur gleichen Zeit wie das PPTP-Verfahren gemeinsam von den Firmen Cisco, Northern Telekom und Shiva entwickelt. Inzwischen ist die Bedeutung von L2F zugunsten von L2PT und PPTP stark zurückgegangen. PPTP ist eine Technologie, die bevorzugt für den Zugriff eines Außendienstmitarbeiters bzw. eines Heimarbeitsplatzes über ein öffentliches Netz in das firmeneigene Intranet verwendet wird, da nur ein Kanal pro Tunnel existiert. Eigenschaften wie Vertraulichkeit und Wartungsmöglichkeiten sind bereits in der Verbindung enthalten.

Cisco reichte das Verfahren bei der Internet Engineering Task Force (IETF) als Vorschlag ein. Unter [RFC 2341] ist L2F als Standard verabschiedet worden. Genau wie das PPTP-Protokoll (Abschn. 7.2.2) ermöglicht L2F den Aufbau eines VPN über ein öffentliches Netz, wie z.B. das Internet, indem ein Tunnel zwischen dem Arbeitsplatzrechner und einem Server im unternehmenseigenen Lokal Area Network (LAN) aufgebaut wird. Dabei ist die Protokollfreiheit größer als bei PPTP, weil L2F nicht an das Internet-Protokoll (IP) gebunden ist (Tab. 7.1). Es kann mit Frame Relay, ATM oder auch mit der inzwischen veralteten FDDI-Technik zusammenarbeiten. Damit ist das Anwendungsspektrum wesentlich breiter als bei PPTP. Für L2F ist eine Wählverbindung bis zum Point-of-Present (PoP) eines Internet Service Providers (ISP) notwendig. Bei dieser kostengünstigen Variante muss der Endnutzer bei einer Einwahl nur den Ortstarif zahlen.

Weiterhin unterstützt L2F mehr als eine Verbindung gleichzeitig – ein weiterer Vorteil gegenüber PPTP. L2F erreicht diese Eigenschaft, indem in der aufgebauten Tunnelverbindung mehrere logische Kanäle geschaltet werden können. Interessant ist dies vornehmlich für kleinere Lokationen, die nur mit einer Wählverbindung, wie z. B. ISDN oder über das analoge Telefon (PSTN), ans öffentliche Netz angebunden sind. Eine ISP benötigt somit wenige bzw. nur eine Verbindung zum Gateway des Unternehmens.

Abb. 7.2 stellt einen L2F-Tunnel zwischen einem Client und einem LAN dar. Der L2F-Tunnel existiert nur zwischen PoP und dem Sicherheitsgateway (Router, Firewall, VPN-Gateway) und dem Netzzugangsserver (NAS) des Unternehmens. Zur Client-Authentifizierung wird, genau wie bei PPTP, das Point-to-Point-Protokoll (PPP) verwendet. Außerdem kann TACACS+ und RADIUS zur Authentifizierung eingesetzt werden. Um eine Verbindung zum Unternehmen herzustellen, muss bei L2F eine Authentifizierung an zwei Schnittstellen vorgenommen werden: zuerst bei der PoP-Einwahl des Internet-Service-Anbieters (ISP), anschließend am Sicherheitsgateway des Unternehmens.

Datenpakete werden bei L2F durch den virtuellen Tunnel zwischen den Endpunkten einer PPP-Verbindung ausgetauscht. L2F vollzieht dies auf einer unteren

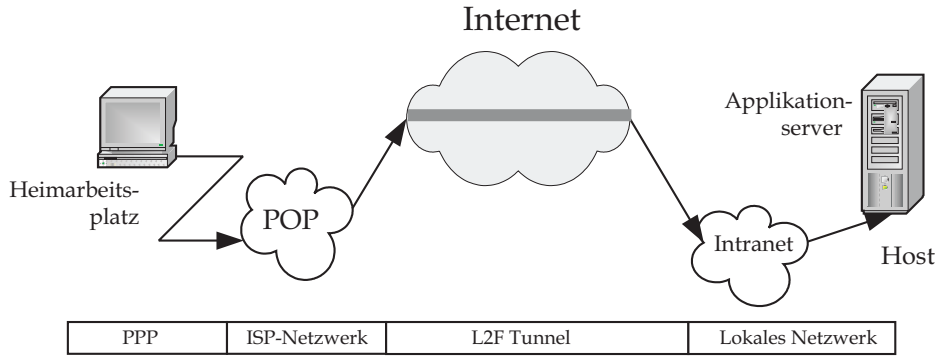


Abb. 7.2: Skizzierung eines L2F-Tunnels vom PoP zum VPN-Gateway eines Unternehmens

Protokollebene. Bei einem Layer-2-Frame, das beim PoP vom Heimarbeitsplatzrechner eintrifft, wird das Frame/Transparency Byte entfernt, anschließend in den Tunnel geschickt *(Encapsulation)* und über das öffentliche Netz (Internet) oder den IP-Backbone des ISP bis zum NAS weitergeleitet. Beim Sicherheitsgateway (Tunnelende) des Unternehmens, also an der Schnittstelle zum lokalen Netzwerk, wird nach Prüfung das Layer-2-Frame entgegengenommen, die Tunnelhülle entfernt und weiterverarbeitet. Vorteilhaft kommt die Eigenschaft von L2F als Layer-2-Protokoll zum Tragen, da es nicht nur IP sondern auch andere Protokolle, wie z.B. IPX oder NetBUI, transportieren kann. Mit L2F lässt sich ein Ende-zu-Ende-VPN aufbauen. L2F biete eine zuverlässige, sichere und skalierbare Lösung für VPN und hatte seinen technologischen Höhepunkt gegen Ende der 90er Jahre.

7.2.2 PPTP

Das Point-to-Point-Tunneling-Protokoll (PPTP) entstand in der Zusammenarbeit der Firmen Microsoft, 3COM, ECI Telematics, Ascend Communications und US Robotics. Es stellt eine Erweiterung des Point-to-Point-Protokolls (PPP) dar (Abschn. 5.4.3) und ist als Access-Technologie relativ weitverbreitet. Gerne wird es für einen Internetzugang im Endanwenderbereich eingesetzt. So ist dieses Protokoll bereits Bestandteil der Microsoft Betriebssysteme Windows NT, Windows 98 und Windows 95.

PPTP ermöglicht den Fernzugriff *(Dial-In)* auf ein Unternehmens-LAN über das Internet technologisch einfacher zu gestalten. Dies gelingt durch eine Erweiterung des PPP-Protokolls. Sie wird erreicht, indem PPP mit einem GRE-Header gekapselt und mit einem zusätzlichen Tunnel-IP-Header versehen wird. Die Einbindung des GRE-Headers bietet dabei die Möglichkeit, andere Protokolle als IP, wie z.B. IPX und NETBUI, zu übertragen. Damit ist PPTP vielfach einsetzbar.

Durch den Einfluss von Microsoft ist PPTP in allen neueren Windows-Betriebssystemen enthalten. Eine enge Anbindung zu Windows NT ist durch die Authentifi-

zierungsmechanismen PAP und CHAP sowie deren für Windows NT modifizierte und verbesserte Version MS-CHAP gegeben.

Allerdings stellten [Schneier et al. 1999] erhebliche Sicherheitslücken in MS-CHAP Vers. 1 und Vers. 2 fest. Deshalb ist bei einer Nutzung von PPTP empfehlenswert, gerade diese Versionen nicht einzusetzen. Darüber hinaus ist es schwierig, Anwendungen zu finden, die außerhalb der Microsoft-Welt, also z.B. das Betriebssystem LINUX/UNIX, PPTP nutzen.

Um die Vertraulichkeit einer PPP-Verbindung abzusichern, hat Microsoft eine spezielle Verschlüsselung, die Microsoft *Point-to-Point Encryption* (MPPE), entwickelt. MPPE arbeitet ideal mit MS-CHAP zusammen und stützt sich auf den MD4 Hash-Algorithmus. Er wird während einer MS-CHAP-Authentifizierung eingesetzt, um einen sicheren Schlüsselaustausch für eine PPP-Session zu erzielen. Eine PPP-Session wird beim MPPE-Verfahren mit RC4, also nur mit einem unzureichenden 40-Bit Schlüssel für den nicht amerikanischen Markt, abgesichert. Dieser geringe Verschlüsselungsschutz kann heute als fahrlässig bezeichnet werden.

PPTP wird durch die folgenden Merkmale charakterisiert:

- Bevor eine PPP-Verbindung aufgebaut werden kann, muss von einem Eingangskonzentrator (PAC) und einem Endpunkt (PNS) eine entsprechende virtuelle TCP-Verbindung aufgebaut werden. Sie wird als Kontrollverbindung des Tunnels genutzt. Dabei verhält sich ein PPTP-Tunnel wie eine *Out-Band*-Lösung.
- Ein PPTP-Tunnel kann nur auf Anforderung von einem Endgerät *(Dial-In)* initiiert werden.
- Zwischen Eingangskonzentrator (PAC) und Ausstiegspunkt (PNS) kann jeweils nur ein Tunnel aufgebaut werden, der eine Kontrollverbindung besitzt.
- Über eine logische PPP-Verbindung kann protokollunabhängig kommuniziert werden. Dabei sind alle Protokolle nutzbar, die von PPP unterstützt werden, also z.B. IP, IPX oder NetBUI.
- Zur Authentifizierung wird auf die PPP unterstützenden Mechanismen zurückgegriffen: das Password Authentification Protocol (PAP) und das Challenge Handshake Authentification Protocol (CHAP) sowie die Microsoft Variante MS-CHAP.
- PPTP greift auf die eher schwachen Sicherheitsmechanismen von Microsoft MPPE zurück.

In Abb. 7.3 ist das Prinzip eines PPTP-Tunnels dargestellt. Die zum eigentlichen Tunnel parallel verlaufende Linie skizziert das *Out-Band*-Verfahren. Kontrollinformationen und Datenpakete werden getrennt über das Netz geleitet. Die Kontrollverbindung (Signalisierung) lässt sich in Analogie zu ISDN mit dem D-Kanal, die Datenübertragung mit dem B-Kanal vergleichen. In einigen älteren

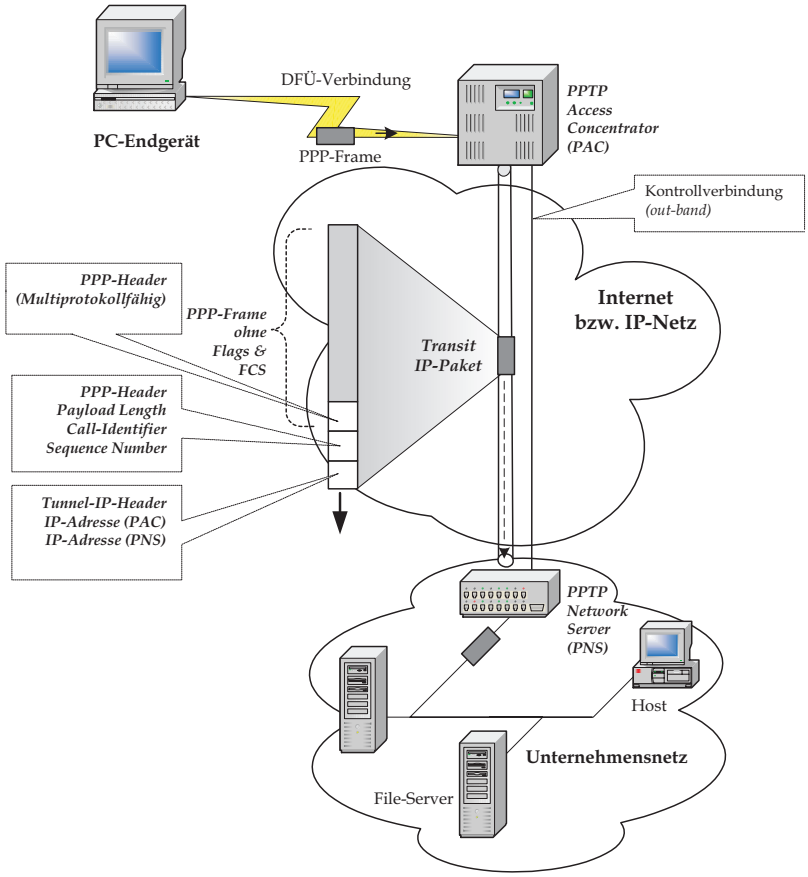


Abb. 7.3: Skizze eines PPTP-Tunnels zwischen Zugangsrouter (PAC) und Unternehmensgateway (PNS)

Veröffentlichungen finden sich noch die Bezeichnungen LCP und NCP. Neuerdings wird der PPTP Access Concentrator einheitlich mit PAC für den Tunneleinstieg am Point-of-Present (PoP) bezeichnet. Der PPTP-Network-Server ist in (PNS) abgeändert worden und stellt den Tunnelausstieg dar.

Dem eigentlichen Datagramm werden drei Header vorangestellt (Abb. 7.4): Als erstes kommt der PPP-Header, der als Frame einige Erweiterungen erfahren hat (Abschn. 5.4.1); anschließend der GRE-Header, der neben der Datenfluss- und Kollisionskontrolle hauptsächlich für die Kapselung der PPP-Pakete zuständig ist. Der GRE-Header stellt eine vereinfachte Version des GRE-Protokolls dar. Der eigentliche Header, der Tunnel-IP-Header, wird wie der GRE-Header nur für die Tunnelstrecke benötigt. Am Ende des Tunnels wird dieser Header ebenso wie der GRE-Header entfernt. Damit wird deutlich, dass das Kernstück einer PPTP-Verbindung auf ein GRE-Protokoll zurückzuführen ist.

Abb. 7.4 zeigt den GRE-Header und seine Felder im Header. Die ersten Bits zeigen an, ob bestimmte nachfolgende Felder belegt sind oder nicht, wie z.B. die Sendefolgenummer (Sequence Number) oder die Empfangsfolgenummer (Acknowledge Number, Ack).Falls die zuvor genannten Nummern (S=1, A=1) vorhanden sind, erfolgt eine Datenflusskontrolle nach dem Sliding-Window-Prinzip[1]. Die CALL-ID gibt im Header die Identifikation der PPP-Verbindung im Tunnel an. Der Protokoll-Type (PT=x880B) teilt mit, dass ein PPP-Frame als Nutzlast befördert wird. Die Größe der Nutzlast wird in der Payload Length hinterlegt. Für

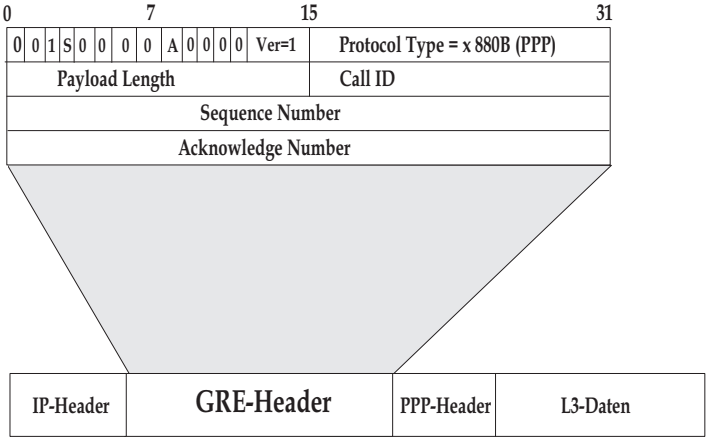


Abb. 7.4: GRE-Header bestehend 32-Bit-Worten

einen Tunnelaufbau und -abbau werden jeweils vorab etliche PPTP-Nachrichten zwischen PAC und PNS ausgetauscht, bevor der eigentliche Tunnel bereitsteht bzw. wieder vollständig abgebaut ist. Die Tunnelkontrolle mittels Kontrollverbindung verläuft in einer *Out-Band*-Kontrollverbindung und damit getrennt zum eigentlichen Tunnel.

Abb. 7.5 ist in zwei Betrachtungsbereiche unterteilt. In der oberen Hälfte werden die Kommunikationsobjekte skizziert. In der unteren Hälfte wird eine komplette PPTP-Verbindungssession, die mit dem Aufbau einer Kontrollverbindung beginnt, gezeigt. Eine TCP-Verbindung wird als Basis für die Kontrollverbindung zwischen PAC und PNS eingesetzt. Sie kann sowohl vom PAC als auch vom PNS aufgebaut werden. Initiiert wird die Kontrollverbindung in diesem Fall vom PAC durch die *Start-Control-Connection-Request*-Nachricht (Start-CC-Request). Gleichzeitig werden Informationen über den Zugang (PSTN/ISDN), die maximale Anzahl der möglichen PPP-Verbindungen und die DNS-Namen vom PAC und PNS

[1] Das Sliding-Window-Prinzip erlaubt der Sendeeinheit, eine bestimmte Anzahl Pakete, entsprechend der Fenstergröße, abzusenden, ohne dass ein Acknowledgement zurückgekommen ist. Die Einheiten treffen versetzt ein (vgl. Abb. 2.8).

mitgeliefert. Als Antwort trifft die *Start-Control-Connection-Reply*-Nachricht (Start-CC-Reply) am PAC ein. Die Zeit verläuft vertikal in der Abb. 7.5.

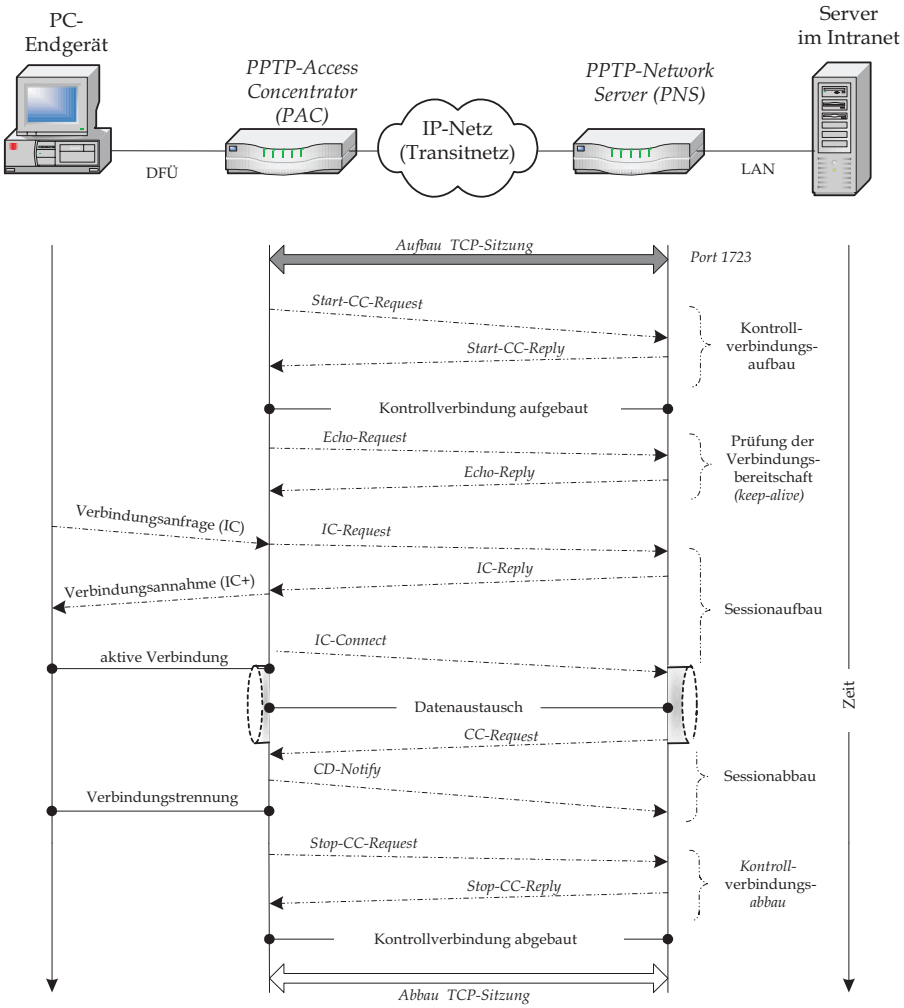


Abb. 7.5: Austausch von Kontrollnachrichten, die zum PPTP-Tunnelaufbau erforderlich sind

Um theoretischen Kollisionen bei gleichzeitigen Aufbauanforderungen vom PAC und vom PNS entgegenzuwirken, ist ein spezieller Echo-Mechanismus *(Echo-Request/Echo-Reply)* vorgesehen. Falls keine Nutzdaten ausgetauscht werden, tritt alle 60 Sekunden der Echo-Mechanismus in Kraft. Damit wird die Bereitschaft beider Kommunikationspartner (PAC/PNS) kontrolliert. Wird beispielsweise ein *Request* nicht beantwortet, wird die Kontrollverbindung mittels *Stop-Control-Connection-Request* geschlossen; mitgeliefert wird dabei eine Information über den

Grund des Verbindungsabbruchs. Bleibt die Kontrollverbindung aufgrund des Echo-Mechanismus erhalten, ist die Verbindung im Status *(Idle)*, um weitere Verbindungsanfragen von einem Endgerät abzuwarten. Kommt eine Verbindungsanfrage (IC) beim PAC an, wird diese sofort als *Incoming Request* (IC-Request) zum PNS geschickt und ein *Incoming Reply* (IC-Reply) abgewartet (Session-Aufbau). Trifft dieser Reply ein, kann die Verbindung zum PC-Endgerät angenommen und aufgebaut werden. Bei Ankunft eines *Incoming-Control-Connect* (IC-Connect) beim PNS können dann mittels Tunnel Datenpakete ausgetauscht werden (Abb. 7.5).

Ist der Datenaustausch beendet, wird durch ein *Clear-Connection-Request* (CC-Request) eine Verbindungstrennung eingeleitet und mit einem *Clear-Disconnect-Notify* (CC-Notify) abgeschlossen (Session-Abbau). Trifft ein *Stop-Control-Connection-Request* (Stop-CC-Request) ein, wird diese Aufforderung zum Verbindungsabbau mit einem *Stop-Control-Connection-Reply* (Stop-CC-Reply) beantwortet. Damit gehen die Kontrollverbindungselemente im PAC und PNS in einen Wartezustand *(Idle)* über. Abschließend wird die verbliebene TCP-Verbindung abgebaut.

Das PPTP-Protokoll ist nur beim PAC und beim PNS installiert. Kein anderes System nimmt von dieser Verbindung Kenntnis. Bei einem Fernzugriff werden an ein PC-Endgerät – außer ein geeignetes Betriebssystem – keine gesonderten Anforderungen gestellt.

Neben der bisher betrachteten nutzerinitiierten dynamischen *Dial-In*-Verbindung kann eine Verbindung (auf Anfrage des Fernnutzers) auch von einem Netzwerkzugangsserver (NAS) aufgebaut werden. Diesen vordefinierten Tunnelweg *(Compulsory Tunnel)* durch das Internet kann das PC-Endgerät nicht verlassen, denn dieser hat statische Eigenschaften. Diese Art der Zugriffsvariante ermöglicht einem Unternehmen eine wesentlich bessere Zugriffskontrolle gegenüber dem *Dial-In*-Verfahren. Beim dynamischen *Dial-In* kann der Nutzer mit seinem PC-Endgerät neben dem Zugangsserver des Unternehmens noch beliebig viele andere Adressen im Internet ansteuern und genießt mehr Freiheiten als beim statischen *Dial-In*. Welches Art der Zugriffsvariante ein Unternehmen für seine Fernnutzer wählt, hängt vom angestrebten IT-Sicherheitsniveau und von den getroffenen IT-Sicherheitsrichtlinien ab.

Der vordefinierte (statische) Tunnelweg (Compulsory Tunnel) hat den Vorteil, mehrere Verbindungen über einen Tunnel führen zu können. Dies reduziert die benötigte Bandbreite, denn der Kontrollverbindungsaufwand (Overhead) für einen einzigen vordefinierten Tunnelweg ist wesentlich geringer als der Aufwand für mehrere beliebig aufgebaute Tunnelverbindungen (Voluntary Tunnel). Ein Nachteil besteht allerdings darin, dass die Signalisierung im Out-Band-Verfahren außerhalb des Tunnels verläuft und somit Angriffsmöglichkeiten bietet. Weiterhin erfordern statische Tunnel (Compulsory Tunnel) ein entsprechendes Equipment, wenn nicht eine manuelle Konfiguration erfolgen soll. Folglich erhöht die Compulsory Tunnel-Technologie unweigerlich den Wartungs- und Betreuungsaufwand.

Ein interessanter Ansatz für Unternehmen wäre, die Vorteile einer dynami-

schen *Dial-In*-Verbindung (geringer Wartungs- und Betreuungsaufwand) mit den Vorteilen einer statischen *Dial-In*-Verbindung (weitreichende Kontrolle) zu verknüpfen. Dies lässt sich mittels RADIUS-Server realisieren, der in das System integriert wird. Die Konfigurationsdaten auf den RADIUS-Server können zentral verwaltet werden und für eine Session können diese ad hoc *(on-the-fly)* umgesetzt werden.

Im Wesentlichen erfordert eine PPTP-Verbindung drei Komponenten:

1. Einen Netzwerk-Access-Server (NAS)
2. Einen PPTP-Server und
3. Einen PPTP-Client

Obgleich sich der PPTP-Server meist im Unternehmen befindet und vom firmenseitigen Netzwerkadministrator gewartet wird, kann dieser auch im Verantwortungsbereich eines ISP liegen, wenn nicht ein spezieller PPTP-Client auf dem PC-Endgerät installiert werden muss. Dann wird vom ISP außer dem Betreuungsaufwand für den NAS keinerlei PPTP-spezifische Unterstützung bzw. Service benötigt.

7.2.3 L2TP

Das L2TP-Protokoll ist das prominenteste Protokoll der Layer-2-Technologie. Es gibt etliche Hersteller, die Produkte auf der Basis von L2TP anbieten, und es ist als Industriestandard anerkannt nicht zuletzt, weil Cisco maßgeblich zur Entwicklung beigetragen hat. Voraussichtlich wird die Verbreitung von L2TP weiter zunehmen, da es Bestandteil von Windows 2000 und auch Windows XP geworden ist und somit in der Bürokommunikation weitflächig eingesetzt werden kann.

L2TP ist eine Mischform seiner beiden Vorbilder bzw. Konkurrenzprodukte L2F und PPTP; es verknüpft die Leistungsfähigkeit des L2F-Protokolls mit den Vorteilen des PPTP-Protokolls. Eine typische Anwendung ist die Einwahl eines Endgerätes ins firmeneigene Intranet über einen Remote-Access-Zugang. Der Zugang zum Unternehmen erfolgt nicht über eine Telefonverbindung, sondern über die Ortsvermittlung zum Zugangspunkt (PoP) eines Internet Service Providers (ISP). Vom PoP wird eine Verbindung zum Sicherheitsgateway der Firma mittels Point-to-Point-Protokoll (PPP) aufgebaut:

- Vor dem Aufbau einer PPP-Verbindung muss von einem Eingangskonzentrator (LAC) und einem Ausstiegspunkt (LNS) eine Kontrollverbindung errichtet werden. Dabei verhält sich ein L2TP-Tunnel wie eine *In-Band*-Lösung. Über dieselbe Verbindung gehen Daten wie Management- und Wartungsinformationen.

- Ein L2TP-Tunnel kann entweder auf Anforderung von einem Endgerät *(Dial-In)* oder als Mandanten-Tunnel *(Dial-Out)* initiiert werden. Weiterhin ist der L2TP-Tunnel für den Nutzer des Endgerätes transparent und erfordert keine zusätzlichen Installationen außer der ISDN/PSTN-Einwahlmöglichkeit zum PoP.
- Zwischen Eingangskonzentrator (LAC) und Ausstiegspunkt (LNS) können mehrere Tunnel aufgebaut werden, die ihre eigenen Kontrollverbindungen besitzen. Außerdem können über einen L2TP-Tunnel mehrere logische PPP-Verbindungen aufgebaut werden.
- Über jede logische PPP-Verbindung kann unabhängig von den anderen PPP-Verbindungen kommuniziert werden. Dabei sind alle Protokolle nutzbar, die von PPP unterstützt werden, z.B. IP, IPx, NetBUI, AppleTalk und SNA.
- Zur Authentifizierung kann auf die von PPP unterstützten Verfahren zurückgegriffen werden: *Password Authentification Protocol* (PAP) und das *Challenge Handshake Authentification Protocol* (CHAP) (vgl. Abschn. 5.4.1).
- L2TP hat keine eigenen Sicherheitsmechanismen. Es kann jedoch Verfahren nutzen, wie z.B. IPSec zur Verbindungsabsicherung oder TACACS+ und RADIUS zur Authentifizierung.

Um die aufgezählten Punkte näher zu erläutern, ist in Abb. 7.6 ein L2TP-Tunnel skizziert, in dem ein PPP-Frame in unterschiedlichen (drei) Verbindungsbereichen dargestellt ist. Ein PPP-Frame wird per Datenfernübertragung (DFÜ) zum LAC des Netzwerkanbieters übertragen. Dabei agiert der LAC als Konzentrator, der mehrere logische PPP-Verbindungen gleichzeitig über ein und denselben L2TP-Tunnel führen kann. Als typisches Paket ist ein Transitpaket ohne Flags und Prüfsumme (*Frame Check Sequence)* in einem L2TP-Tunnel vergrößert dargestellt. Vor dem Datagramm sind vier weitere Protokollköpfe (Header) platziert: der Tunnel-Header, der den Eingang (LAC) und Ausgang (LNS) bestimmt, nachfolgend ein UDP-Header, ein L2TP-Header und ein PPP-Header. Da mehrere logische PPP-Verbindungen über einen Tunnel möglich sind, zieht jede Verbindung eine Session-Identifikation *(Session-ID)* und eine Tunnel-Identifikation *(Tunnel-ID)* nach sich, die im L2TP-Header eingetragen sind.

Ähnlich wie bei PPTP werden bei L2TP zwei Arten von Nachrichten *(messages)* übertragen: die Kontrollnachricht *(control message)* und die Datennachricht *(data message)*. Allerdings werden im Gegensatz zu PPTP beide Nachrichten in ein und derselben Verbindung geführt. Falls der Tunnel über ein abgegrenztes IP-Netz des Providers aufgebaut wurde, werden beide Nachrichten im selben IP-Paket übertragen. Die Kontrollnachrichten sind dann für Tunnelauf- und -abbau sowie für die Tunnelwartung zuständig. Sie steuern auch die Übertragungsrate und die Buffer-Parameter, um die PPP-Pakete einer speziellen Session beeinflussen zu können. Um eine möglichst hohe Übertragungsgeschwindigkeit zu errei-

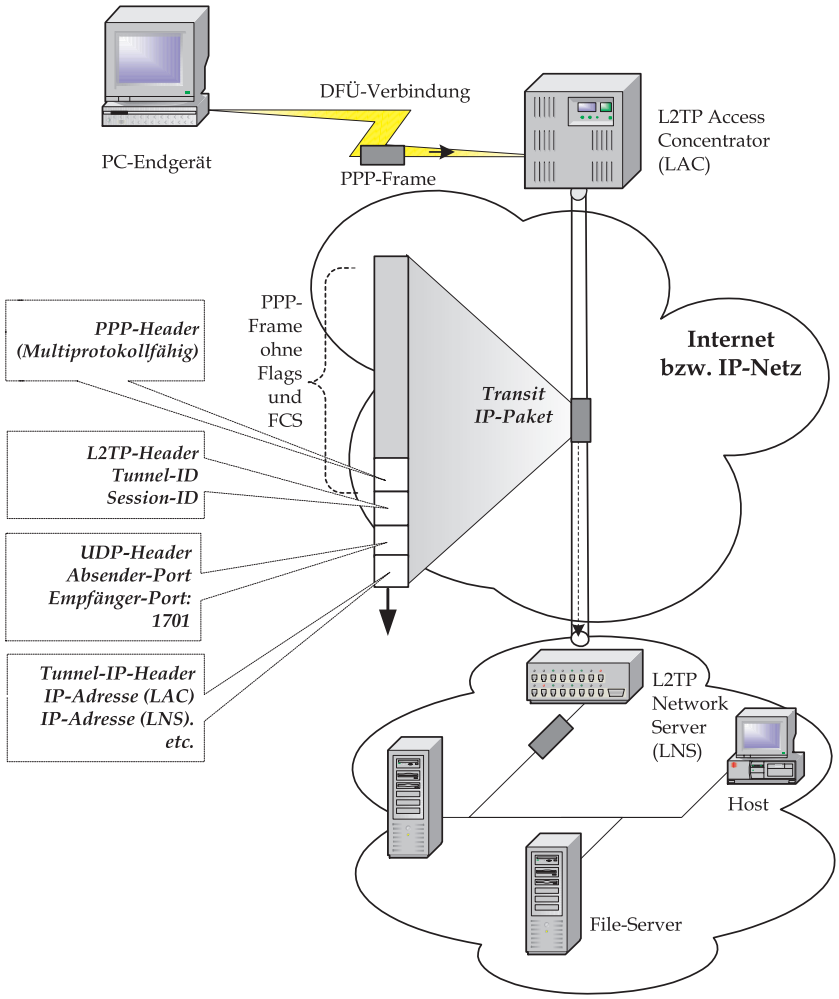


Abb. 7.6: Skizze eines L2TP-Tunnels

chen, wird die Protokollverwaltung (Overhead) mit einem speziellen Kompressionsverfahren reduziert. Außerdem hält die aktive Flusskontrolle den Netzwerkverkehr gering und vermeidet weitestgehend Kollisionen im Netz.

Die Protokoll-Unabhängigkeit von L2TP erfordert, dass sich im PPP-Header Angaben über den Protokolltyp (IP, IPX, NetBUI, SNA) befinden. Die Daten-Nachrichten regeln die Datenübertragung im Tunnel. Im Prinzip kann ein vollständiger Tunnelauf- und -abbau von beiden Seiten, also vom Endgerät als auch vom Netzwerk-Server erfolgen. Der Tunnelaufbau durch das Endgerät wird häufig als ankommender Anruf (Voluntary Tunnel) oder auch als *Dial-In* bezeich-

net und stellt den typischen Verlauf eines dynamischen Fernzugriffs *(Remote Access)* auf das Firmennetzwerk dar (vgl. Abschn. 6.1.3 und Abb. 7.6). Die zweite Möglichkeit des Tunnelauf- und -abbaus – auch als verpflichtender Anruf (Compulsory Tunnel)T oder als *Dial-Out* bezeichnet – erfordert den Kontrakt mit einem Netzwerkbetreiber und die Bereitstellung einer Dienstleistung in Form einer Verbindung zwischen dem Netzwerkserver (LNS) und dem L2TP-*Access Concentrator* (LAC). Ein LAC ist üblicherweise durch eine Software-Komponente in einem Zugangsrouter realisiert, der wiederum durch eine Authentifizierungskomponente im Zugangspunkt (PoP) abgesichert ist.

Abb. 7.8 zeigt eine ähnliche Betrachtung des Datenaustausches wie Abb. 7.6 zwischen einem PC-Endgerät und einem Local Area Network (LAN). Jedoch wird in Abb. 7.8 auf die Übertragungs- und Kontrollperspektive näher eingegangen. Abb. 7.7 verdeutlicht die Struktur einer Kontrollnachricht. Abb. 7.8 illustriert im unteren Bildteil einen vollständigen Verbindungsaufbau mit der vorab ausgehandelten Kontrollverbindung, die Datenübertragung im L2TP-Tunnel und den Abbau der jeweiligen Verbindungen. Der Zeitablauf ist durch die vertikalen Linien angedeutet. Er ist nicht maßstabsgetreu dargestellt, sondern soll lediglich den prinzipiellen zeitlichen Ablauf skizzieren.

Eine Kommunikation zwischen LAC und LNS findet mittels Kontrollnachrichten statt, die mit den L2TP-Paketen übertragen werden. Im L2TP-Header wird zur Unterscheidung das T-Feld mit T=1 als Kontrollnachricht und T=0 als Nachricht mit Daten gekennzeichnet. Die Kontrollnachrichten mit T=0 zeigen den in Abb. 7.6 typischen Datenübertragungszustand eines PPP-Frame ohne Flags und Prüfsummen (FCS). Mit T=1 wird im L2TP-Header gekennzeichnet, dass eine Kontrollnachricht (Abb. 7.7) vorliegt. Neben der *message type ID* (MT) sind es vor allem die *Attribute Value Pair* (AVP), die die Kontrollnachricht bestimmen und die im unteren Teil der Abbildung detaillierter dargestellt sind. AVPs werden durch den Typ von Steuerungsangaben *(Attribute Type)* und durch die Steuerungswerte *(Attribute Value)* bestimmt. Das Mandatory-Bit (M) signalisiert mit M=1, dass ein AVP vorhanden ist.

Das Hidden-Bit gibt mit H=1 Auskunft, dass das Attribute Value verschlüsselt ist. Die Länge eines AVP wird mit dem Length-Bit gekennzeichnet. Die Vendor-ID (z.B. ID = 43 steht für 3COM) gibt gemäß [RFC 1700] Auskunft über den Anbieter.

Im L2TP-Header – im oberen Teil der Abbildung detaillierter skizziert – sind alle relevanten Informationen für die Verbindung zwischen LAC und LNS zu finden. Weiterhin ist der Typ der Nachricht durch das T-Feld gekennzeichnet. Da einige Header-Informationen optional sind, werden nach dem T-Feld jeweils diejenigen Bits gesetzt, also z.B. L,S,O =1, bei denen Informationen in den dafür vorgesehenen Feldern abgelegt sind.

Die x-Bits sind für mögliche zuknüftige Funktionen reserviert. Ebenso sind Tunnel-Identifikation (Tunnel-ID) und Session-Identifikation (Session-ID) fixiert. Die Länge der Nachricht ist dem Length-Field zugeordnet, falls L=1 gesetzt ist. Die optionalen Nummernfelder (Ns, Nr) geben Auskunft über die Sendefolge- und Empfangsfolgenummer der zu erwartenden Nachricht, falls S=1 ge-

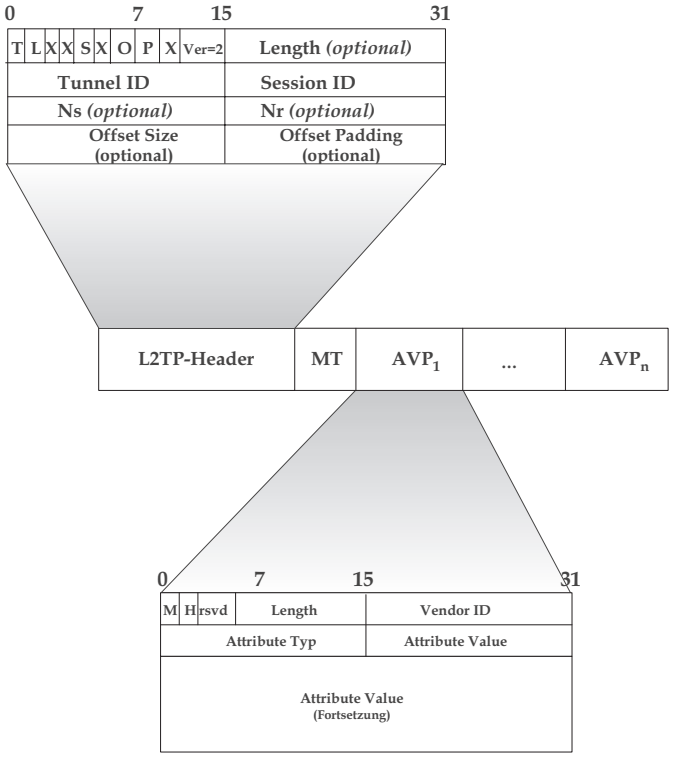


Abb. 7.7: Zusammensetzung einer Kontrollnachricht (T-Bit=1)

setzt ist. Beim Aufbau einer Kontrollverbindung werden zwischen LAC und LNS in einem Frage-und-Antwort-Verfahren die Nachrichten *Start-Control-Connection-Request* (SCCRQ) und die *Start-Control-Connection-Reply* (SCCRP) ausgetauscht. Eine Kontrollverbindung ist erst dann aufgebaut, wenn vom LAC die Nachricht *Start-Control-Connection-Connected* (SCCCN) mit einer *Zero-Length-Body-Nachricht* (ZLB-Nachricht) beantwortet wurde. Dabei besteht die ZLB-Nachricht nur aus dem aus vier 32-Bit-Worten bestehenden L2TP-Header.

Falls zeitweise keine Daten ausgetauscht werden, wird ungefähr alle 60 Sekunden eine Verbindungsbereitschaft mit Hello und einer ZLB-Nachricht *(Keep-Alive-Statement)* in Form einer positiven Quittung periodisch beantwortet. Bis ein Tunnel auf- und wieder abgebaut ist, werden etliche L2TP-Nachrichten ausgetauscht, die über L2TP-Datenpakete transportiert werden. Man unterscheidet drei L2TP-Nachrichten. Die kürzeste, die als Quittung genutzt wird, ist die ZLB-Nachricht. Weiterhin werden L2TP-Kontrollnachrichten benötigt, die bestimmte Steuerungsangaben in den Attribute-Value-Pair (AVP) weiterleiten. Die AVP beinhalten Informationselemente in den Kontrollnachrichten. Dabei existieren eine Vielzahl dieser AVP, von denen einige zwingend *(mandatory)* und andere optional sind

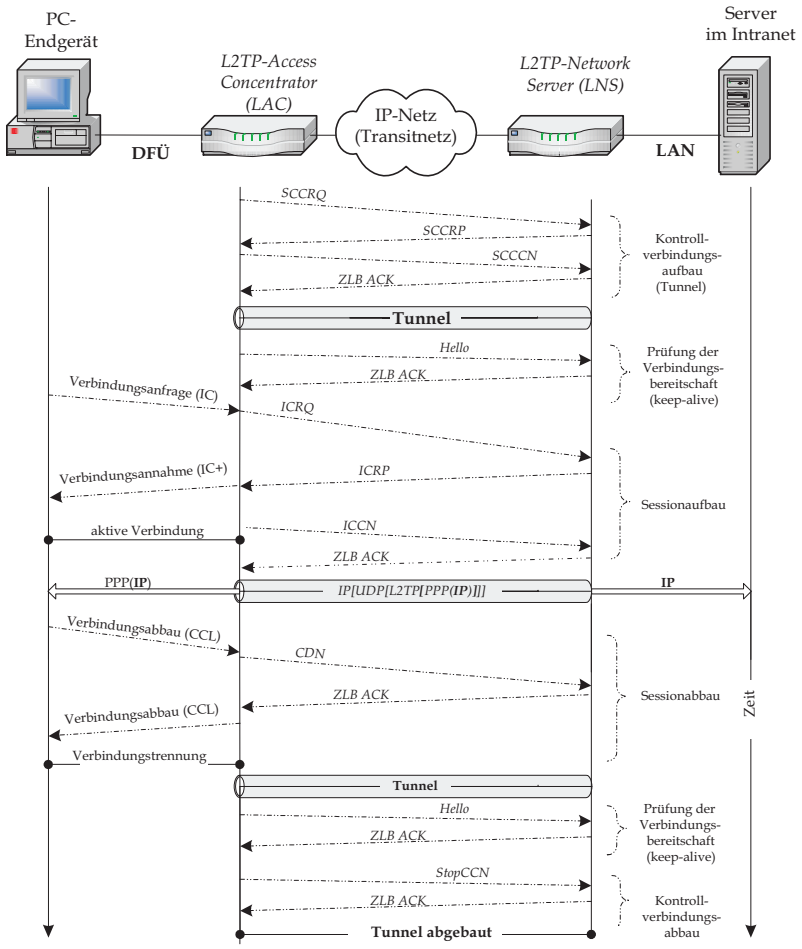


Abb. 7.8: Auf- und Abbau einer Kontrollnachricht (T-Bit=0)

[RFC 2661].

Ankommender Anruf als Fernzugriff (Dial-In)

Abb. 7.8 illustriert ferner, wie auf eine Verbindungsanfrage (IC) von einem PC-Endgerät für einen Zugriff auf das Firmennetzwerk (LAN) am Zugangsrouter (LAC) des Netzwerkbetreibers registriert wird. Der IC löst den Aufbau der eigentlichen Tunnel-Session – mit der später Nutzdaten übertragen werden können – zum Netzwerkserver (LNS) durch die ICRQ-Nachricht *(Incoming-Call-Request)* aus. Dabei wird eine Sitzungsnummer, die sich mittels AVP übertragen werden, zugewiesen. Erst nachdem beim LAC die ICRP-Antwortnachricht *(Incoming-Call-Reply)* vom LNS eingetroffen ist, wird durch die Rufannahme (IC+) die Be-

reitschaft zum Aufbau einer aktiven Verbindung zwischen PC-Endgerät und LAC signalisiert. Dieser Zustand wird durch die ICCN-Nachricht *(Incoming-Call-Connection)* sofort vom LAC zum LNS weitergeleitet. Als Reaktion wird eine Quittung (ZLB-Nachricht) geschickt und eine PPP-Verbindung zwischen dem PC-Endgerät und dem Netzwerkserver im Unternehmen kann aufgebaut werden. IP-Pakete wechseln die Lokationen und ein Datenaustausch wird praktiziert. Ist der Datenaustausch zwischen PC-Endgerät und Firmennetzwerk abgeschlossen, beendet der Fernnutzer des PC-Endgerätes die Verbindung mit einer CCL-Nachricht *(Clear-Call-Message)*.

Da über einen Tunnel mehrere logische PPP-Verbindungen gleichzeitig unterhalten werden können, ist ein Verbindungsabbruch nicht mit einem Tunnelabbruch gleichzusetzen. Wird allerdings die letzte logische PPP-Verbindung abgebaut, wird auch der Tunnel abgebaut. Empfängt der LAC den Verbindungsabbruch mittels eines *Clear-Calls*, sendet er eine *Call-Disconnect-Notify* (CDN-Nachricht) zum LNS. Diese Nachricht enthält in den AVP Angaben über die Abbruchursache. Durch die ZLB-Nachricht bestätigt der LNS die empfangene CDN-Nachricht des Verbindungsabbruchs. Sofort werden die Vereinbarungen zwischen LAC und LNS aufgelöst. Dies kommt einem Tunnelabbau gleich. Hat der LAC dem PC-Endgerät durch das *Clear-Call*-Signal den Verbindungsabbau mitgeteilt, wird die aktive Verbindung über das Zubringernetz (analog/digital) abgebaut.

Abgehender Anruf vom Netzwerk-Server (Dial-Out)

Der umgekehrte Vorgang – also der Aufbau eines Tunnels vom LNS zum LAC – wird als verpflichtender Anruf *(compulsory)* bezeichnet und im Prinzip spiegelbildlich zum oben beschriebenen Ablauf (Abb. 7.8) gehandhabt. Eine OCRQ-Nachricht *(Outgoing-Call-Request)* wird als Kontrollverbindung verschickt, die vom LAC mit der OCRP-Nachricht *(Outgoing-Call-Reply)* beantwortet wird. Die zugewiesene Sitzungsidentifikation wird dem L2TP-Header übergeben und dort in der *Session ID* hinterlegt. Entsprechend wird vom LAC eine abgehende Verbindung über das Zubringernetz zum PC-Endgerät errichtet, die dann bei Verbindungserfolg mit der OCCN-Nachricht *(Outgoing-Call-Connected)* zum LNS gesendet wird. Nach der anschließend beim LAC eintreffenden ZLB-Quittung *(ZLB-ACK)* sind alle notwendigen Vereinbarungen getroffen.

Vertraulichkeit bei der Datenübertragung in einem L2TP-Tunnel

Wie den Ausführungen zum L2TP-Protokoll zu entnehmen ist, sind keine Mechanismen vorgesehen, die die Vertraulichkeit der übertragenden Daten sichert. Nur beim Aufbau der Kontrollverbindung *Start-Control-Connection-Request* (SCCRP) und der darauf folgenden *Start-Control-Connection-Reply* (SCCRP) der Gegenseite ist es möglich *(optional)*, nach dem Challenge-Response-Verfahren mit dem CHAP-Protokoll (Abschn. 5.4.3) eine beidseitige Authentifizierung vorzunehmen.

Das L2TP-Protokoll ist zwar eine kostengünstige Lösung für den Fernzugriff auf ein Unternehmensnetz, doch müssen hinsichtlich der Vertraulichkeit etli-

che Bedenken angemeldet werden, wenn keine zusätzlichen Sicherungsmaßnahmen getroffen werden. Ein L2TP-Tunnel agiert, indem ein L2TP-Frame in einem UDP-Paket gekapselt transportiert wird. Dabei definieren die Quell- und Ziel-IP-Adressen den Beginn und das Ende des Tunnels. Um die Vertraulichkeit zu gewährleisten, kann bei der Datenübertragung ergänzend IPSec eingesetzt werden (Abb. 7.6). Die PPP-Arbeitsgruppe der IETF hat einen Vorschlag ausgearbeitet, wie mit IPSec die Vertraulichkeit für einen L2TP-Tunnel erreicht werden kann. Der Einsatz des IPSec-Protokolls kann eine sichere End-to-End-Verbindung zwischen dem PC-Endgerät und dem Unternehmensnetzwerk ermöglichen [RFC 3193]. IPSec liefert u.a. eine Authentifizierung der einzelnen im Tunnel transportierten Pakete und eine Integritätsprüfung der Pakete mittels Prüfsummen. Weiterhin bietet es die Möglichkeit die Datagramme zu verschlüsseln. Darüber hinaus existiert mit IKE/ISAKMP ein Automatismus zur Schlüsselerzeugung -verwaltung und zum -austausch. Die IETF hat eine dringende Empfehlung ausgesprochen, IPSec bei Verwendung eines L2TP-Tunnels im Internet zur Absicherung beim Ende-zu-Ende-Datenverkehr zur Wahrung der Vertraulichkeit einzusetzen. Auf IPSec wird in Abschn. 7.4 detaillierter eingegangen. Hier wird IPSec als Absicherungskomponente in L2TP-Anwendungen eingesetzt.

Im ersten Anwendungsszenario wird eine Client-Lösung (vgl. Abb. 7.9) eines *Dial-In* und *Dial-Out* betrachtet. Hierzu ist ein L2TP-fähiger Client am Endgerät erforderlich. Dieser fungiert gleichzeitig als LAC.

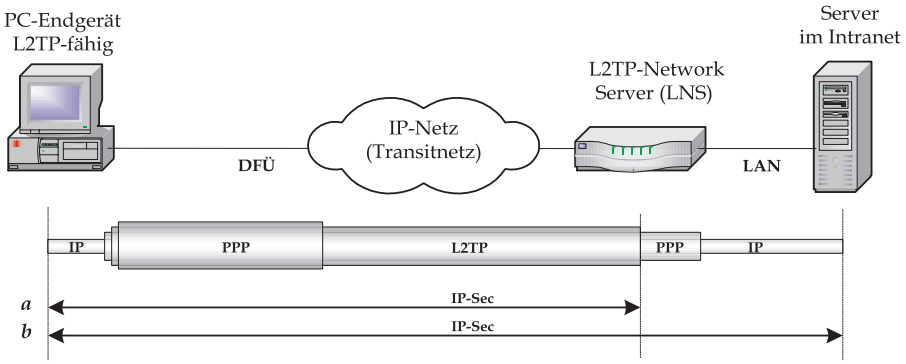


Abb. 7.9: Mit IPSec gesichertes L2TP-VPN eines L2TP-fähigen Clients

Abb. 7.9 zeigt in der oberen Hälfte der Abbildung die Kommunikationsobjekte. In der unteren Hälfte der Abb. 7.9 sind beide IPSec-Varianten, eine L2TP-Verbindung abzusichern, durch Linien skizziert. Bei Variante *(a)* reicht die Absicherung bis zum Sicherheitsgateway bzw. LNS. Um eine Ende-zu-Ende-Absicherung zu verwirklichen (vgl. Variante *(b)*), müssen beide Endgeräte, auch der Server im Intranet, IPSec-fähig sein.

Inzwischen gehört der L2TP-Client bereits zum Lieferumfang einiger Betriebssysteme, z.B. Windows 2000 (W2K) und Windows XP (WXP). Gerade die Möglich-

keiten, die sich mit dem Betriebssystem Windows 2000/XP und dem Windows-2000/2003-Server bieten, lassen diese Variante für viele Firmen interessant erscheinen. Jedoch bietet auch das Linux-Betriebssystem mit der von John Gilmore initiierten FreeS/WAN-Lösung eine ähnliche Absicherung.

Zweiter Anwendungsfall für das IPSec ist die typische Netzwerkbetreiber-Lösung (Abb. 7.10). Hier befinden sich LAC und LNS im ausschließlichen Einflussbereich des Betreibers. Allerdings unterscheidet man bei dieser Variante zwischen *Dial-In* und *Dial-Out*. Wie in Abb. 7.9 sind in Abb. 7.10 die unterschiedlichen Einsatzvarianten von IPSec durch die ausgezogenen Linien skizziert. Variante *(a)* zeigt die IPSec-Verschlüsselung zwischen einem LAC und einem LNS. In diesem Szenario muss sich der Anwender auf die Dienstleistung des Netzwerkbetreibers und auf die mit ihm vereinbarten Verträge *(Service Level Agreements)* und ihrer Einhaltung hinsichtlich einer Datenabsicherung verlassen.

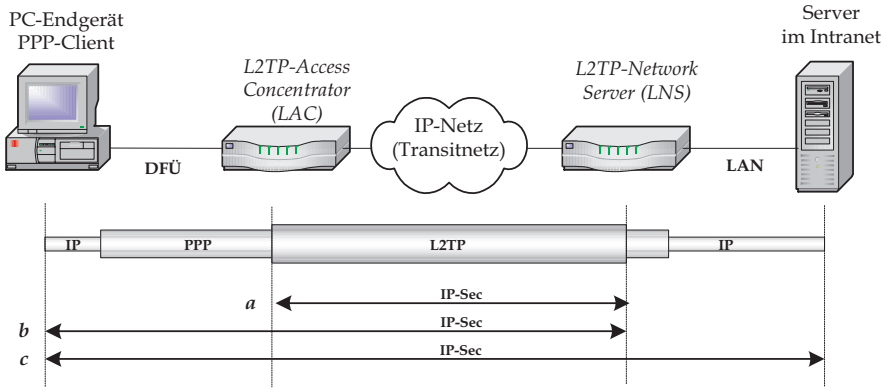


Abb. 7.10: Mit IPSec gesichertes L2TP-VPN eines PPP-fähigen Clients

Bei Variante *(b)* endet die IPSec-Verschlüsselung direkt am LNS; somit bewegen sich die IP-Pakete im Netzwerk des Unternehmens unverschlüsselt. Variante *(c)* setzt einen IPSec-fähigen Server voraus, mit dem eine Ende-zu-Ende-Kommunikation aufgebaut werden kann.

Für das PC-Endgerät ist lediglich ein PPP-fähiger Client notwendig, der sich automatisch installiert, wenn die DFÜ-Einrichtung im Windows-2000/XP-Betriebsystem aktiviert wird. Somit stellt der zweite Anwendungsfall eine interessante und für den Endanwender einfach einzurichtende VPN-Möglichkeit dar.

7.2.4 SSL over L2TP oder L2Sec

Die L2Sec-Lösung ist mittels des [RFC 2716] standardisiert. L2Sec beschreibt eine interessante VPN-Variante, die sich mit der Implementierung der Firma NCP großer Beliebtheit erfreut. L2Sec kann als Kombination von L2TP-Tunnel und

SSL/TLS-Authentifizierung aufgefasst werden. Im Kern handelt es sich um eine gesicherte PPP-Verbindung in Form einer *Dial-In*-Lösung. Das PPP-Protokoll bildet als Punkt-zu-Punkt-Verbindung dabei die Grundlage, bezogen auf die Ebene-2 im OSI-Referenzmodell. Es ist vielfältig einsetzbar (vgl. Abschn. 7.2.2 und Abschn. 7.2.3). Das PPP-Protokoll kann außerdem in Verbindung mit Frame Relay genutzt werden [RFC 1973]. Da im PPP-Protokoll bereits ein Verbindungskontrollmechanismus *(Link Control Protocol*, LCP) enthalten ist, kann – ergänzt durch einen Authentifizierungsprozess *(Extensible Authentication Protocol*, EAP) [RFC 2284] und dem TLS-Protokoll [RFC 2246] auf OSI-Schicht 7 – eine vertrauliche Kommunikation eingerichtet werden.

Die L2Sec-Lösung ist interessant, denn es vermeidet einige Unzulänglichkeiten von IPSec. Denn IPSec setzt bereits während der Aufbauphase eine gültige IP-Adresse voraus (vgl. Abb. 7.4.8). Gerade für den Aufbau einer sicheren Datenkommunikation ist eine angemessene Authentifizierung während des Verbindungsaufbaus wichtig. Dies gewährleistet L2Sec: Die Tunnelelemente von L2TP sowie das erweiterte Authentifizierungsprotokoll (EAP) und die Verschlüsselungseigenschaften von TLS/SSL wurden verschmolzen, so dass das L2TP-EAP-TLS-Protokoll [RFC 2716] entstand. Die nachfolgende Abb. 7.11 zeigt schematisch den Ablauf. Allerdings gibt es hinsichtlich der Protokollverwaltung einen Nachteil bei L2Sec: sie ist aufwändiger als bei IPSec. Auch gibt es keine Einzelabsicherung von Prozessen oder Ports, da bei L2Sec alle Pakete getunnelt sind und der Tunnel als Ganzes abgesichert wird.

Nachdem verschiedene Sicherungsmöglichkeiten einer PPP/L2TP-Verbindung diskutiert wurden und auf IPSec verwiesen wurde, wird nachfolgend auf IPSec und die Layer-3-Techniken eingegangen. Dabei werden unter anderem Mechanismen wie Transport- und Tunnelmodus und der überaus wichtige Schlüsselaustausch (IKE/ISAKMP) behandelt.

7.3 Layer-3-Techniken

Zu den Layer-3-Techniken, die in der VPN-Technologie Verwendung finden, zählt das IPSec-Protokoll sowie das unterstützende Schlüsselaustauschprotokoll (IKE). IKE ist oberhalb der Layer-5 im OSI-Referenzmodell einzuordnen. Dennoch existiert eine enge Beziehung zwischen beiden Protokollen. IPSec setzt symmetrische kryptographische Schlüssel ein, um einen IP-Pakettransport gemäß den IuK-Schutzzielen (vgl. Abschn. 3.1) abzusichern. Allerdings besitzt IPSec keinerlei Mechanismen, um die notwendigen Schlüssel für die Kommunikationspartner zu erzeugen oder zu verteilen. Diese Rolle übernimmt das Schlüsselmanagement mittels IKE. In Abschn. 7.4.9 wird ausgeführt, wie IKE den initiierten IPSec-Verbindungsaufbau mit eigenen Sicherheitsmaßnahmen ausstattet, um die für IPSec notwendigen kryptographischen Schlüssel zur Authentifizierung und Verschlüsselung zu verteilen.

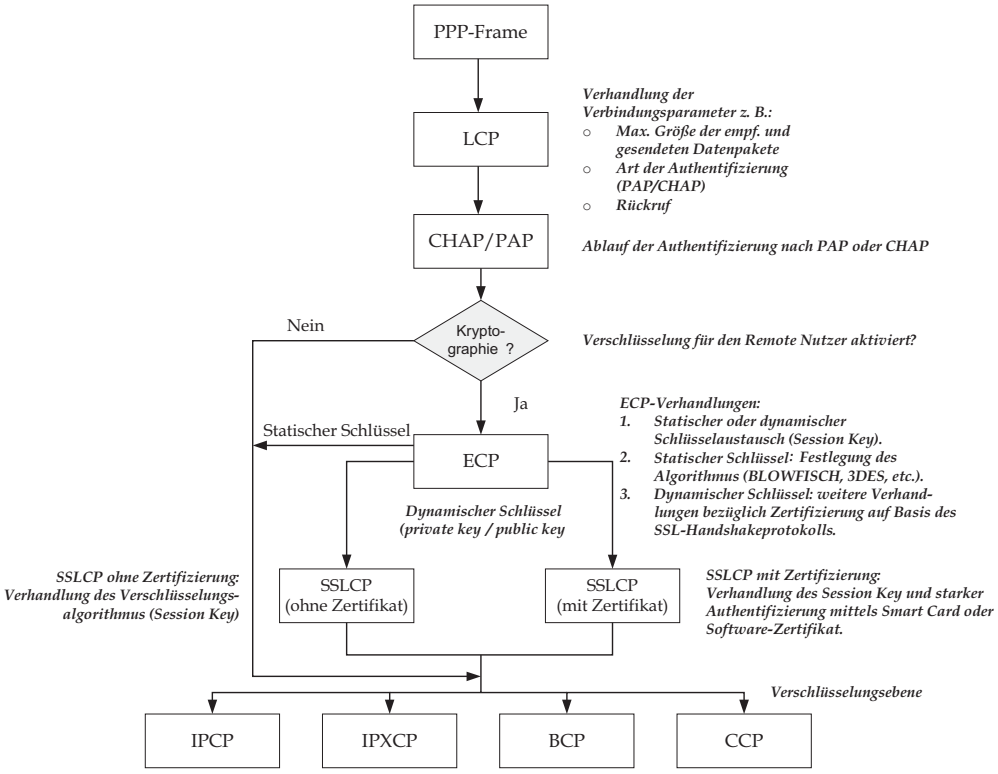


Abb. 7.11: Funktionsdiagramm einer SSL-over-L2TP (L2Sec) Verbindung

IKE entstand aus der Kombination von ISAKMP/Oakley, wie in frühen Veröffentlichungen das Schlüsselmanagement noch bezeichnet wird. Das *Internet Security and Key Management Protocol* (ISAKMP) ist ein Rahmenwerk für Authentifizierungsverfahren und Schlüsselaustausch (vgl. Abschn. 7.4.12). Ergänzend hierzu beschreibt das *Oakley Protocol* (Oakley) verschiedene Techniken des Schlüsselaustausches (vgl. Abschn. 7.4.13).

7.4 Sicherheitsstandard für das Internet (IPSec)

IPSec stellt, bezogen auf das OSI-Referenzmodell, *den* Sicherheitsstandard auf Layer-3 dar. IPSec ist standardisiert gemäß IETF, mit dem herstellerübergreifend ein sicherer und geschützter Datenaustausch durch das IP ermöglicht werden kann. Die Normungsaktivitäten laufen seit 1995 unter Führung von Jeffrey Schiller und Marcus Leech. Die IPSec-Arbeitsgruppe ist innerhalb der IETF der *Security Area* untergliedert.

Zum Transport der nach IPSec modifizierten IP-Pakete sind zwei unterschiedliche Arbeitsmodi – der Transportmodus und der Tunnelmodus – definiert worden. Beide unterscheiden sich im Wesentlichen durch den Aufbau der Paketergänzungen und durch ihre Einsatzmöglichkeiten.

Neben den Arbeitsmodi ist der Schlüsselaustausch (vgl. Abschn. 7.4.9) und das Schlüsselmanagement (vgl. Abschn. 7.4.12 und Abschn. 7.4.18) von großer Bedeutung. Außerdem soll nach neuesten Vorschlägen ein zentrales Schlüsselmanagement mit Kerberos (Abschn. 5.4.9) einsetzbar sein.

Mit IPSec ist es möglich, die folgenden IuK-Schutzziele (vgl. Abschn. 3.1) bei einer Datenübertragung in einem offenen Netz umzusetzen:

Integrität: Die Daten (IP-Pakete) werden vor Verfälschung während des Transports gesichert, indem ein verschlüsselter Hash-Wert in das Datenpaket aufgenommen wird, der vom Empfänger im Nachhinein verifizieren werden kann.

Authentizität: Die Echtheit der IP-Pakete wird durch Integritätsbedingungen erfüllt, die auch für die Absenderadresse bindend sind.

Vertraulichkeit: Die Datenpakete können mittels kryptographischer Verfahren, wie z.B. mit DES im CBC-Modus, vor unbefugten Dritten während einer Datenübermittlung verborgen werden. Dabei ist es unbedeutend, ob die Daten auf dem Quell- und auf dem Zielrechner unverschlüsselt vorliegen.

IPSec beeinflusst weder die Kommunikationsprotokolle noch die Anwendungsprogramme, so dass eine Zusammenarbeit über verschiedene IP-Netze nicht beeinträchtigt wird. IPSec ist im TCP/IP-Schichtenmodell unterhalb der Transportschicht angesiedelt und setzt auf die Internet-Schicht (IP) auf. Abb. 7.12 zeigt das OSI-Referenzmodell, das TCP/IP-Schichtenmodell und die Einordnung von IPSec ins TCP/IP-Schichtenmodell.

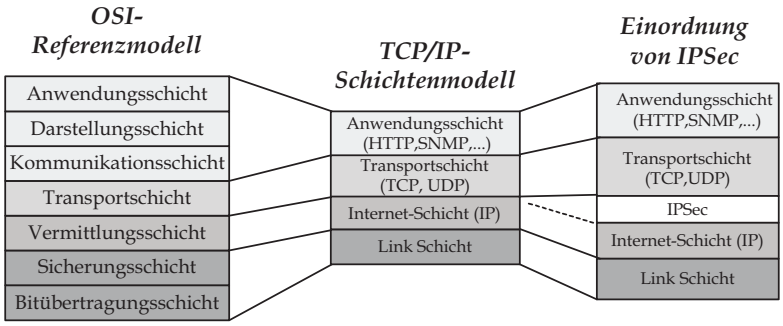


Abb. 7.12: Einordnung von IPSec in Schicht 3 des TCP/IP-Schichtenmodells

Mit IPSec kann jeglicher Datenverkehr, wie z.B. TCP, UDP, ICMP, HTTP, FTP, SNMP, Telnet etc. geschützt werden. IPSec wird jedoch nicht gänzlich kritiklos

gesehen. Einer der größten Vorwürfe, mit denen IPSec konfrontiert wird, ist die überwältigende Komplexität der IPSec-Normenspezifikation und die des Protokolls selbst, wie bei [Ferguson und Schneier 1999] zu lesen ist. Dabei standen kryptographische Untersuchungen im Mittelpunkt dieser Veröffentlichung. Die Autoren wiesen allen maßgeblichen Komponenten Sicherheitsschwächen nach. Dennoch kommen sie zu dem Ergebnis, dass IPSec besser als PPTP und L2TP ist und es derzeit keine Alternative zu IPSec gibt. Vielfach wird in der Literatur die Diskussion IPSec kontra SSL/TLS geführt; auf diese wird im Abschn. 7.5.2 näher eingegangen wird. Auch andere Autoren [Kurtz et al. 2001] haben sich jahrelang mit IPSec beschäftigt und kommen zu einem ähnlichen Ergebnis wie [Ferguson und Schneier 1999]. Sie bezweifeln sogar, dass überhaupt jemand IPSec mit seinen vielfältigen Details vollständig verstehen wird.

IPSec kam offensichtlich durch eine ungünstige Konstellation zustande: es ist das typische Ergebnis eines Komitees, das naturgemäß auf die unterschiedlichen Interessen aller Beteiligten Rücksicht nehmen muss. Schneier schlägt deshalb zur Verbesserung zukünftiger Internetsicherheitsstandards ein regelrechtes Ausleseverfahren vor, so wie es bei dem kryptographischen Standard AES für die US-Bundesbehörden vom NIST durchgeführt wurde (Abschn. 4.2.5).

Allerdings lässt sich das Argument der Komplexität und des wenig durchsichtigen Protokolls auch umkehren: ein unbefugter Dritter hat demnach dieselben Schwierigkeiten, wenn er am UDP-Port (UDP 500) IKE-Elemente ausliest. Trotzdem ist das undurchsichtige Protokoll *(security by obscurity)* kein stichhaltiges Argument, wie die Geschichte der Kryptographie[2] immer wieder gezeigt hat. Dennoch müssen sich die heutigen Nutzer von IPSec vollständig auf die Implementierungen der Hersteller verlassen. Microsoft hat IPSec in Windows 2000/Windows XP implementiert und es wird wohl nur eine Frage der Zeit sein, bis diese Implementierung nachhaltig geprüft wird. Es wird sich dann zeigen, wie gut die Implementierung wirklich ist.

7.4.1 Das Ziel von IPSec

Zu Beginn des Internets fand eine Kommunikation in offenen Systemen ohne jegliche Absicherung statt (Abschn. 2.2.1). Dies wurde zunächst nicht als nachteilig empfunden, da am Datenaustausch über das Internet nur ein kleiner wissenschaftlich geprägter Personenkreis teilnahm. Mit zunehmender Kommerzialisierung des Internets änderten sich die Sicherheitsanforderungen grundlegend. Als weitsichtige Reaktion hat seinerzeit die IETF eine Arbeitsgruppe *(IP Security Working Group)* ins Leben gerufen, die sich mit der Absicherung des IP-Protokolls beschäftigt. Die Vorschläge [RFC 1825] bis [RFC 1829], die im Wesentlichen auf die Arbeiten von R. Atkinson aus dem Jahre 1995 zurückgehen, sind mittlerweile obsolet. Die frühen Arbeiten von Atkinson legten die Grundstruktur von IPSec fest. Im November 1998 sind neuere Vorschläge [RFC 2401] bis [RFC 2412] und [RFC

[2] Vgl. Abschn. 4.1.2, dort das Theorem von Kerkhoff.

2451] als Standards verabschiedet worden. Dennoch wird weiterhin an IPSec gearbeitet, um das Protokoll an neuen Erfordernissen anzupassen. Beispiele hierfür sind: IKEv2[3], Einbettung von AES als zwingende Verschlüsselungskomponente, Übermittlung des ESP[4]-Protokoll mittels UDP-Pakete (UDP-Encapsulation ESP Header).

Das IP-Paket, das eine fundamentale Rolle in der Kommunikation von IP-Netzwerken spielt, enthält Informationen über die IP-Adresse des Absenders und des Ziels sowie Informationen über die Nutzlast (Payload), die transportiert wird (Abschn. 2.3). IPSec definiert zwei weitere Protokollköpfe (Header) für IP-Pakete, um eine Authentifizierung und eine Verschlüsselung zu erreichen: den *Authentication Header* (AH) und den *Encapsulation Security Payload* (ESP).

Wesentliche Aspekte der IP-Absicherung zielten nach Vorstellung der IETF-Arbeitsgruppe nicht auf das IPv4-Protokoll, sondern auf das nachfolgende IPv6-Protokoll ab. Dieses Protokoll trug zeitweise den Arbeitstitel Next Generation Protocol (IPng), bis der Name IPv6 offiziell vergeben wurde. Allerdings zieht sich eine flächendeckende Einführung von IPv6 länger als erwartet hin. So wurde für IPv4 eine Zwischen- bzw. Übergangslösung entwickelt. Nachträglich wurde IPSec für das IPv4-Protokoll als optionaler Protokollkopfbestandteil angepasst. Für IPv6 sind diese Bestandteile immanent. Damit ist IPSec für IPv4 nutzbar und Netzwerkapplikationen können spezielle TCP/IP-Stacks bedienen. Je flächendeckender IPv6 eingesetzt wird – UMTS[5] wird diesen Prozess beschleunigen –, desto schneller werden die Zwischenlösungen verschwinden.

IPSec nutzt nahezu alle aktuellen kryptographischen Techniken, um die IuK-Schutzziele (Abschn. 3.1) Vertraulichkeit, Integrität und Authentifizierung zu gewährleisten. Dabei wurde auf eine möglichst große Flexibilität bei der Erreichung der Schutzziele Wert gelegt, indem Kombinationen der Schutzziele zugelassen wurden. Weiterhin wurde bei der ursprünglichen Definition von IPSec weitsichtig vereinbart, eine Unabhängigkeit gegenüber kryptographischen Techniken festzuschreiben.

Der Vorteil der Unabhängigkeit gegenüber kryptographischen Techniken zeigt sich z.B., nachdem DES durch den AES-Algorithmus abgelöst worden ist (Abschn. 4.2.5). Denn es ist relativ einfach, Ersatzlösungen in IPSec einzubringen, wie die neuesten IPSec-Vorschläge zeigen. Derzeit können folgende Verfahren zur Absicherung der Kommunikation verwendet werden:

- Das Diffie-Hellman-Verfahren für den symmetrischen Schlüsselaustausch zwischen zwei Kommunikationspunkten *(peers)* über ein öffentliches Netz

---

[3] In dem Vorschlag: draft-ietf-ipsec-ikv2-17.txt, wird gegenüber IKEv1 ein Änderung hinsichtlich NAT Traversal, Extensible Authentication und Remote Address vorgenommen. Bei Verabschiedung würden die RFCs 2407, 2408 und 2409 obsolet werden.

[4] Diese Änderung führt zu der Abkehr von dem Protokoll 50, das momentan für eine ESP Übermittlung notwendig ist. Gleichzeitig wird das AH-Protokoll im Rahmen von IPSec abgewertet, indem es nur noch als „MAY“ und nicht mehr als „Should“ deklariert wird.

[5] In der neuen Mobilfunkübertragungstechnik nach dem UMTS-Protokoll ist IPv6 ein wesentlicher Bestandteil.

- Asymmetrische Schlüsselverfahren *(Public-Key-Kryptographie*), um eine sichere gegenseitige Identifizierung der Kommunikationspartner zu erreichen; damit wird eine *Man-in-the-middle*-Attacke (Abb. 3.4) wirkungsvoll unterbunden
- DES oder andere blockorientierte Verschlüsselungsalgorithmen im CBC-Mode, die die Nutzlast des IP-Paketes absichern können
- Zur Sicherung der Integrität bzw. der Authentizität dienen die Verfahren HMC [RFC 2857], MD5 [RFC 1828] und SHA [RFC 2404, RFC 2405]
- Digitale Zertifikate können zur Validierung der öffentlichen Schlüssel eingesetzt werden

Das Hauptentwicklungsziel von IPSec besteht darin, den IP-Paketaustausch in Kommunikationsnetzen abzusichern. Im Kern sollten die bekannten Schwächen des IP-Protokolls, die eine Verfälschung und ein Abhören während der Übertragung zulassen, wirkungsvoll unterbunden werden. Gleichzeitig lassen sich auf Basis von IPSec die unterschiedlichen VPN-Architekturen *Site-to-Site* (Abschn. 6.1.1), *End-to-End* (Abschn. 6.1.2) und *End-to-Site* (Abschn. 6.1.3) effektiv schützen. IPSec wurde daher mit einer geeigneten Architektur ausgestattet. Jedoch hat es im *End-to-Site*-Definitionsbereich etliche Freiheitsgrade gegeben. Die im März 2000 mit der Lösung beauftragte IETF-Arbeitsgruppe *(IP Security Remote Access Working Group, IPSRA)* wurde inzwischen, durch die IETF-Arbeitsgruppe *IKEv2 Mobility and Multihoming (MobIKE)* ersetzt. Denn der Technologietrend bei *End-to-Site*-VPN in Richtung Mobilität ließen eine reine Arbeitsgruppe für Fernzugriffe als nicht mehr zielführend erscheinen.

Die IPSec zugrunde liegende Architektur weist einen modularen Charakter auf, so dass die drei Hauptbestandteile von IPSec – das AH-Protokoll, das ESP-Protokoll und das Schlüsselmanagement *(Key-Management)* – nahe zu beliebig (sinnvoll) zusammen eingesetzt werden können. Die Verschlüsselungstechniken, die Authentifizierungstechniken sowie der Umgang mit den Schlüsseln sind von den dazugehörigen Protokollen und Schlüsselmanagement getrennt gehalten. Dabei kommt dem Schlüsselmanagement, z.B. beim Einsatz von IKE, eine zentrale Aufgabe zu, wenn zwei Kommunikationspartner gesichert Daten austauschen wollen. Weiterhin muss für den Zeitraum der Kommunikation sichergestellt werden, dass beide Kommunikationspartner dieselben kryptographischen Techniken, z.B. Schlüssellänge, Intervall des Schlüsselwechsels und gleiche Authentifizierungsmethoden etc., anwenden. Dies wird mittels eines temporären, nur für den Zeitraum der Kommunikation gültigen Vertrag bzw. durch eine Vereinbarung (Security Association) erreicht. Da die Spezifikation von IPSec neben den bevorzugten Algorithmen und Verfahren auch andere zulässt, ist zur Vereinfachung und zur Verwaltung der möglichen Parameter mit der Security Association (SA) ein Standard geschaffen worden, der mit Domain of Interpretation (DOI) bezeichnet wird.

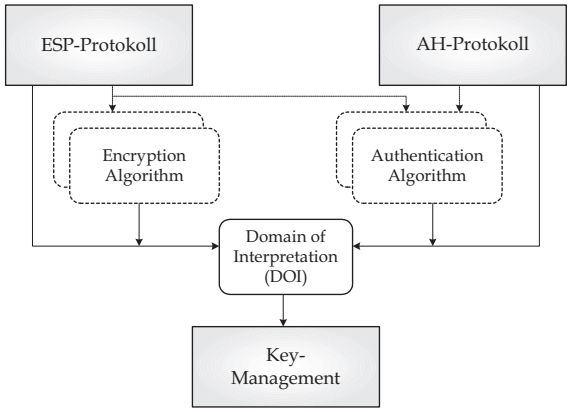


Abb. 7.13: Die der IPSec-Spezifikation zugrunde liegende Architektur [RFC 2411]

7.4.2 Die IPSec-Sicherheitsvereinbarungen (SA)

Bevor zwei der drei Hauptkomponenten – das AH-Protokoll und das ESP-Protokoll – näher erläutert werden, wird der dritte zentrale Bestandteil von IPSec, die *Security Association* (SA), dargestellt. Dies erleichtert das Verständnis beim Aufbau einer IPSec-Verbindung. Wollen zwei Kommunikationspartner (Peer-Instanzen) mit IPSec abgesichert Daten austauschen, müssen *vorab* Sicherheitsvereinbarungen ausgehandelt werden. Denn IPSec bietet neben den Voreinstellungen einen weiten Raum für individuelle Anpassungen. Unter anderem muss festgelegt werden, welches Verschlüsselungsverfahren für die Nutzlast eingesetzt werden soll. Ebenso muss der Schlüsselaustausch und der Schlüsselwechsel ausgehandelt werden.

Jede Kommunikationsrichtung zwischen Sender und Empfänger erfordert eine eigene Security Association, da diese unidirektional ist, ebenso die Protokolle AH und ESP innerhalb einer IPSec-Verbindung. Dies gilt auch, wenn für die Authentifizierung und für die Verschlüsselung dieselben Algorithmen eingesetzt werden. Werden das AH-Protokoll und das ESP-Protokoll zusammen eingesetzt, wird dies als *SA-Bundle* bezeichnet. Eine Security Association beinhaltet alle wichtigen Elemente zum Aufbau einer gesicherten Kommunikationsverbindung. Sie steht damit in engem Zusammenhang mit dem anfänglich notwendigen Schlüsselaustausch (Abschn. 7.4.9). Weiterhin legt die SA den Arbeitsmodus fest, der entweder aus dem Transport- oder dem Tunnelmodus oder aus beidem bestehen kann.

Eine SA für eine gesicherte IPSec-Kommunikation ist für folgende Regelungen verantwortlich:

- Arbeitsmodus des Authentifizierungsalgorithmus, der im AH-Protokoll festgelegt ist; hierzu werden außerdem die Schlüssel definiert.

- Arbeitsmodus des Verschlüsselungsalgorithmus für das ESP-Protokoll, wie z.B. CBC. Weiterhin werden die dazugehörigen Schlüssel, wie z.B. der Initialisierungsvektor, definiert.
- Spezifizierung einer möglichen kryptographischen Synchronisation und Einsatz von kryptographischen Maßnahmen.
- Vorgabe, welches Protokoll, welcher Algorithmus und welcher Schlüssel zur Authentifizierung benutzt werden.
- Vorgabe, welches Protokoll, welcher Algorithmus und welcher Schlüssel für eine vertraulichen Kommunikation eingesetzt werden.
- Vorgabe, wie häufig die eingesetzten Schlüssel ausgetauscht werden sollen.
- Spezifizierung des Authentifizierungsalgorithmus und Arbeitsmodus.
- Spezifizierung der zeitlichen Gültigkeit aller Schlüssel.
- Spezifizierung der zeitlichen Gültigkeit der SA.
- Bekanntgabe der SA-Quelladresse.

Eine SA ist gleichbedeutend mit einem sicheren Kanal durch ein unsicheres öffentliches Netz zu einem bestimmten Kommunikationspartner, zu einer Gruppe von Kommunikationspartnern oder zu anderen Netzwerk-Ressourcen. Es entspricht einem mit der Gegenseite ausgehandelten Kontrakt. SA sind unidirektionale (simplex) Verbindungen, die zum Datentransport vom Sender zum Empfänger ausgerichtet sind. Für den Rücktransport der Daten muss eine weitere SA ausgehandelt werden. Um diesen Aufgaben zu genügen, ist eine bestimmte Parameterform für die unidirektionale Verbindung zwischen zwei IPSec-Systemen, z.B. Host-1 und Host-2, festgelegt worden. Die Parameter einer SA sind gekennzeichnet durch das folgende Tripel:

SA $= \langle$ **Security Parameter Index, IP Destination Address, Security Protocol** $\rangle$

Die einzelnen Parameter bedeuten:

Security Parameter Index (SPI): Dies ist ein 32-Bit-Wert (0-255), um verschiedene SA zu unterscheiden, die die gleiche Zieladresse und das gleiche Sicherheitsprotokoll (AH oder ESP) haben. Der SPI-Wert ist im Header des dazugehörigen Sicherheitsprotokolls (Abb. 7.14 und 7.15) eingebettet. Die SPI-Werte von 0-255 entsprechen den Bestimmungen der *Internet Assigned Numbers Authority* (IANA). Ein SPI hat ausschließlich lokale Bedeutung und wird bei der Festlegung einer SA definiert.

IP Destination Address: Die Zieladresse kann prinzipiell eine *Unicast*, *Broadcast* oder auch *Multicast*-Adresse sein. Derzeit wird nur eine *Unicast*-Adresse unterstützt.

Security Protocol: Es bestimmt, ob das AH-Protokoll oder das ESP-Protokoll eingesetzt werden.

Die Werte des Parametertripels müssen eine Teilmenge der Menge aller *zugelassenen* Werte bilden. Die Menge aller *zugelassenen* Werte für den IP-Verkehr (z.B. TCP, UDP, ICMP), die den Regelungen genügen, ist in einer speziellen Datenbank bzw. Tabelle, der *Security Policy Database* (SPD), abgelegt. Aus ihr werden mittels Selektoren bestimmte, für eine SA gültige Parameter übernommen und in eine temporäre Datenbank, die *Security Association Database* (SAD), hinterlegt. Abb. 7.18 zeigt die Datenbanken bei einer SA-Initiierung.

Security Policy Database (SPD): Eine SPD definiert die Menge der Services, die für einen IP-Verkehr angeboten wird. Die Menge der Services ist abhängig von Faktoren wie z.B. Quelle und Ziel sowie vom *In-Bound* oder *Out-Bound* des Verkehrs. Ebenso ist eine nach Verkehrsart sortierte Liste mit Policy-Einträgen vorhanden. Die Einträge bestimmen, welcher IP-Verkehr nach IPSec wie behandelt wird, welcher nicht und welche IP-Pakete sofort verworfen werden. Als Analogien können Firewall-Filterregeln oder Routertabellen betrachtet werden.

Security Association Database (SAD): In einer SAD befinden sich die konkreten Parameter für eine unidirektionale SA: die Parameter für den AH- und ESP-Algorithmus und die dazu gehörigen Schlüssel sowie Sequenznummern, Arbeitsmodi der Protokolle und zeitliche Gültigkeit der SA. Für einen *Out-Bound*-Prozess bestimmt die Konfiguration des SPD-Eintrags, welchen Einschränkungen ein SAD-Parameter ausgesetzt ist. Damit bestimmt die SPD die Freiheitsgrade einer SA für ein bestimmtes ausgehendes IP-Paket. Für einen *In-bound*-Prozess startet die SA eine Abfrage, wie mit einem Paket verfahren werden soll und legt diese Information in der SAD ab. Alle ankommenden IP-Pakete konsultieren daraufhin mittels Security Parameter Index (SPI) nur noch die SAD (Abb. 7.14).

Je nach IPSec-Implementierung und Herstellerlösung kann die Benutzerfreundlichkeit der Bedieneroberfläche recht unterschiedlich ausfallen – und damit auch die Bearbeitung der Datenbank- bzw. Tabelleneinträge.

7.4.3 IPSec-Authentifizierung mittels AH-Header

Der AH-Header, ein spezieller Protokollkopf, ist für die Authentifizierung im IPSec-Protokoll zuständig und wurde im [RFC 2402] spezifiziert. Der AH-Header ist zwischen dem ursprünglichen IP-Header und anderen Layer-3-Elementen, wie z.B. TCP, eingebettet. Die Nutzdaten (Payload) bleiben jedoch unberührt, sie werden in ihrem ursprünglichen Zustand belassen. Die Funktion des AH-Headers besteht darin, mögliches IP-Spoofing oder Session-Hijacking-Angriffe wirkungsvoll zu unterbinden. Eine Eigenschaft, die z.B. SSL/TLS-VPN nicht bieten können (vgl. Abschn. 7.5.2).

Die Eigenschaften des AH-Headers lassen sich wie folgt zusammenfassen:

- Datenintegrität wird unterstützt und ein Wiedereinspielen *(Replay Attack)* von verschickten Datenpaketen unterbunden.
- Hash-Funktionen (HMAC) werden mit gleichen (symmetrischen) Schlüsseln eingesetzt.
- Starke kryptographische Verfahren werden eingesetzt, die nur eine moderate Prozessorlast erfordern.
- Das IP-Datagramm wird nicht verschlüsselt, folglich ist keine Vertraulichkeit der Nutzlast gegeben.
- Es wird kein variabler IP-Header benötigt, um Prüfwerte der Integrität (ICV), wie z.B. TOS, Flags, Fragment Offset, TTL und ein Head-Checksum, zu bestimmen.

Durch den AH-Header wird ein IP-Paket um 24 Byte vergrößert (Abb. 7.14) und kann als Wert zur Durchsatzberechnung, zur Fragmentierung und zur MTU-Berechnung benutzt werden. Der AH-Header enthält fünf Felder, die von Be-

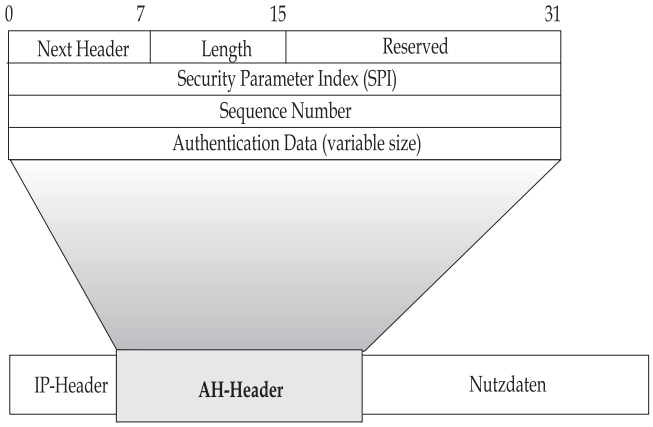


Abb. 7.14: Der Authentication-Header (AH) garantiert die Integrität einzelner IP-Pakete [RFC 2402]

deutung sind, und außerdem ein reserviertes Feld für zukünftige Erweiterungen. Abb. 7.14 zeigt den AH-Header mit allen Feldern:

- Das 8 Bit umfassende *Next-Header-Field* (z.B. TCP, UDP, ICMP), das bei allen IP-Pakten vorhanden ist
- Das nächste 8-Bit-Feld bezeichnet die Länge des AH-Headers
- Der 32 Bit große *Security Parameter Index* (SPI)
- Eine 32 Bit *Sequence Number* (Sequenz-Nummer), die mehrmalig vergeben werden kann

- Abschließend stehen die eigentlichen, mittels HMAC-Operation gebildete Authentifizierungsdaten

Derzeit sind für den AH-Header folgende Hash-Algorithmen vorgesehen:

- *zwingend (must):*
  - HMAC-SHA-1 [RFC 2404] oder
  - NULL [RFC 2410]
- *sollte (should+):*
  - AES-XCBC-MAC-96 [RFC 3566]
- *könnte (may):*
  - HMAC-MD5-96 [RFC 2403]

Der AH-Header kann sowohl im Transport- als auch im Tunnelmodus eingesetzt werden. Er kann aber auch eigenständig oder zusammen mit dem ESP-Header genutzt werden, je nachdem, welcher Grad der Absicherung eines IP-Paketes erreicht werden soll. Es gilt zu beachten, dass die Hash-Algorithmen die Übertragungsgeschwindigkeit unterschiedlich beeinflussen.

Nach den jüngsten Entwicklungen der IETF-Arbeitsgruppe scheint die Bedeutung des AH-Protokoll zugunsten des ESP-Protokoll zurückzugehen.

7.4.4 IPSec-Vertraulichkeit mittels ESP-Header

Das zweite für IPSec wichtige Protokoll ist das *Encapsulating Security Payload*-Protokoll (ESP). Es ist durch die IETF im [RFC 2406] spezifiziert. Eine Anwendung von ESP garantiert die Vertraulichkeit der zu übertragenden Nutzlast, die mit einem reversiblen kryptographischen Verfahren behandelt wird. Im Gegensatz zum AH-Header ist ein ESP-Header in der Lage, sowohl eine Verschlüsselung als auch eine Authentifizierung durchzuführen. Der Encapsulating Security Payload-Header ist als ein Frame zu verstehen, in dem die eigentlichen Nutzdaten zwischen dem ESP-Header und dem ESP-Trailer eingebettet sind (Abb. 7.15). Der ESP-Header enthält neben dem ESP-Trailer und dem ESP-Authentication-Field sechs wichtige Felder, die im unteren Teil der Abbildung skizziert sind. Außerdem enthält der ESP-Header einen Initialisierungsvektor (IV) (vgl. Abschn. 4.2.1), der für die Blockverkettung des einzusetzenden Verschlüsselungsverfahrens zuständig ist. Weiterhin können – je nach blockorientierten Verschlüsselungsverfahren – Füllzeichen (Padding) notwendig werden, damit eine bestimmte Blockgröße, meist am Ende eines Textes, nicht unterschritten wird. Die Pad Length gibt die Anzahl der Füllzeichen an. Das 8-Bit-Feld Next-Header zeigt den nachfolgenden Header, wie z.B. TCP, UDP oder ICMP, an. Analog zum AH-Header sind die 32-Bit-Felder Security Parameter Index (SPI) und das 32-Bit-Feld der Sequenz-Nummer vorhanden.

Derzeit sind folgende Verschlüsselungsverfahren vorgesehen:

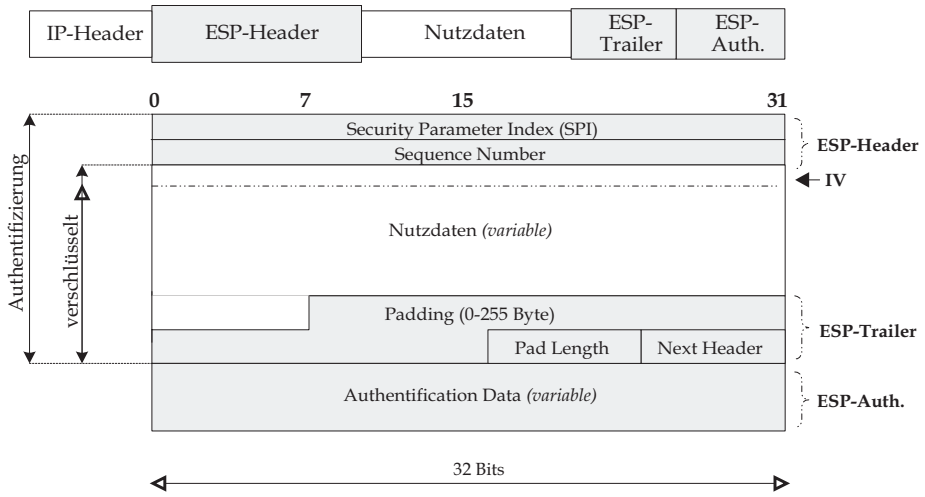


Abb. 7.15: Encapsulation Security Payload (ESP), spezifiziert nach [RFC 2406]

- *zwingend:*
  - TripleDES-CBC [RFC 2451] oder
  - NULL [RFC 2410]
- *optional:*
  - CAST-128 [RFC 2451]
  - RC5 [RFC 2451]
  - IDEA [RFC 2451]
  - Blowfish [RFC 2451]
  - AES-CBC mit 128-Bit Schlüsseln [RFC 3602]
  - AES-CTR [RFC3686]

Erfreulich ist, das nach jüngsten Vorschlägen der Algorithmus DES-CBC nach [RFC 2405] nicht mehr eingesetzt werden soll. Als Hash-Algorithmen sind vorgesehen:

- *zwingend (must):*
  - HMAC-SHA-1 [RFC 2404] oder
  - Null [RFC 2410]
- *sollte (should+):*
  - AES-XCBC-MAC-96 [RFC 3566]
- *könnte (may):*
  - HMAC-MD5-96 [RFC 2403]

Interessant ist das späte Hinzufügen der NULL-Funktion gemäß [RFC 2410]. Sie kann entweder nur für die Verschlüsselung oder nur für die Integritätsprüfung, also auf keinen Fall gemeinsam angewendet werden. Die NULL-Funktion wurde durch die unterschiedlichen Verschlüsselungsmethoden und ihren Arbeitsmodi erforderlich. So bringt z.B. DES mit dem Arbeitsmodus CBC (DES-CBC) durch die Verkettung innerhalb von CBC schon eine Integritätsprüfung mit (Abschn. 4.2.1 und Abb. 4.3). Mit der NULL-Funktion kann die ESP-Integritätsprüfung ausgeschaltet werden, um einen unnöntigen Verwaltungsaufwand zu vermeiden.

Wird allerdings ein Verschlüsselungsverfahren benutzt, welches keine Integritätsprüfung beinhaltet oder in einem Blockmodus ohne Integritätsprüfung arbeitet, z.B. im einfachen ECB-Modus (Abschn. 4.2.1, Abb. 4.1), ist es sinnvoll, eine eigene Integritätsprüfung im ESP-Header zur Verfügung zu stellen. Weiterhin wird häufig ein Initialisierungsvektor (IV) benötigt, der, wenn er im Klartext übertragen wird, ebenfalls einer Integritätsprüfung unterzogen werden sollte.

Der ESP-Header kann im Transport- und im Tunnelmodus betrieben werden. Ebenso kann er eigenständig oder zusammen mit dem AH-Header eingesetzt werden, je nachdem, welcher Grad der Absicherung für ein IP-Paket vorgesehen ist. Hieraus ergeben sich verschiedene Varianten, die allerdings vor dem Hintergrund einer Reduzierung der Übertragungsleistung zu betrachten sind.

Es stellt sich die Frage, warum IPSec [RFC 2401] zwei Möglichkeiten einer Authentifizierung vorsieht, zumal jeweils die gleichen Algorithmen im AH-Header und im ESP-Header eingesetzt werden können. Abgesehen davon, dass beide Authentifizierungsmöglichkeiten einen unterschiedlichen Wirkungskreis haben, scheint eine Redundanz vorzuliegen. Ausführungen hierzu fehlen in der Spezifikation [RFC 2401]. Jedoch lassen sich einige Überlegungen in diesem Kontext anstellen.

7.4.5 Transport- und Tunnelmodus

Die grundlegende Idee beim Entwurf von IPSec war, jedes IP-Paket auf dem Übertragungswege einerseits mittels Authentifizierung und Integritätsmechanismen vor Verfälschung zu schützen, andererseits eine Vertraulichkeit der IP-Pakete durch Verschlüsselungsmethoden zu erreichen. Hierzu werden die zu übertragenden IP-Pakete (IPv4, IPv6) um zusätzliche Angaben (Abschn. 7.4.3 und 7.4.4) erweitert. Je nach Anwendungsszenario stehen die Erweiterungen zur Verfügung, um das Original IP-Paket abzusichern. Um jede denkbare Verbindungsvariante zu ermöglichen, sind die zwei Betriebsarten, der Transportmodus und Tunnelmodus, entwickelt worden.

Transportmodus

Im Transportmodus wird durch IPSec nur die Nutzlast des zu transportierenden IP-Paketes verschlüsselt. Der Original-IP-Kopf bleibt erhalten und ein IPSec-Kopf wird hinzugefügt. Von Vorteil ist die geringe Anzahl Bytes, die hinzugefügt wird.

Ein Angreifer kann zwar den verschlüsselten Datenverkehr im VPN lesen, jedoch nicht die Datagramminhalte verstehen. Er kann lediglich feststellen, welcher Host Daten austauscht.

Abb. 7.16 skizziert in der Bildmitte die Kommunikationsobjekte Host-1/Host-2, die über ein IP-Netz miteinander vertrauliche Daten austauschen wollen. Oberhalb und unterhalb der Skizze sind schematisch mögliche Absicherungsszenarien mittels Transportmodus dargestellt. Für die Absicherung zweier Host-Systeme, z.B. Host-1 und Host-2, ohne Beteiligung von Sicherheitsgateways gibt es laut [RFC 2401] folgende Empfehlung: Es sollte nur der Transportmodus und die gemeinsame Nutzung von AH-Header und ESP-Header in der Reihenfolge (siehe AH/ESP-Transport), wie in Abb. 7.16 gezeigt, eingesetzt werden. Ergänzend ist in der Abbildung ein IPv4-Paket skizziert, um zu verdeutlichen, wie unterschiedlich die Erweiterungen (AH, ESP) sich auf das ursprüngliche IPv4-Paket auswirken. Nach einer Erweiterung des IP-Paketes mit IPSec bleibt der ursprüngliche IP-Protokollkopf mit seiner Quell- und Zieladresse durch eine ESP-Erweiterung unberührt (siehe ESP-Transport in Abb. 7.16). Die Nutzlast – es ist TCP als höheres Schichtenprotokoll als Beispiel eingezeichnet – wird verschlüsselt. Zusätzlich wird die Integrität der verschlüsselten Nutzlast sichergestellt. Allein bei einer AH-Header-Erweiterung ist die Integritätsprüfung eines empfangenen IP-Paketes gegenüber einem herkömmlichen IPv4 Paket beim Host-2 möglich (siehe AH-Transport in Abb. 7.16). Keine Modifikation des Paketes und damit keine Modifikation am eingezeichneten höheren Schichtenprotokoll TCP am Host-2 bleibt unerkannt. Ein mögliches Mitlesen der im Klartext verschickten Nutzlast (TCP) kann allerdings nicht unterbunden werden.

Durch die empfohlene Kombinationsreihenfolge der Header – erst AH und dann ESP – bedeutet für die Vertragsaushandlung Security Association (SA) für den Aufbau einer (Out-Bound) Verbindung, dass zunächst die innere SA (ESP) abgeschlossen sein muss, bevor die äußere SA (AH) ausgehandelt werden kann. Beim In-bound-Verkehr wird umgekehrt vorgegangen: Zuerst wird eine SA für die AH-Erweiterung ausgehandelt und anschließend eine SA für die ESP-Erweiterung. So wird ein System, hier z.B. Host-2, (zeitlich) von der Last einer Dechiffrierung befreit, wenn im Fall einer fehlgeschlagenen Integritätsprüfung das angekommene Paket ignoriert wird.

Tunnelmodus

Der Tunnelmodus hat die zusätzliche Aufgabe, die Quell- und Zieladresse auf dem Übertragungsweg – explizit im öffentlichen Netzbereich bzw. im IP-Transitnetz – zu schützen. Damit wird das IPSec-Paket im Umfang größer als im Transportmodus. Allerdings besteht der nicht zu unterschätzende Vorteil, dass IPSec lediglich in den Gateways implementiert sein muss und nicht in den lokalen Netzen (LAN). Ein Angreifer hat nur die Möglichkeit, die Anfangs- und Endpunkte des IPSec-Tunnels festzustellen.

Der Tunnelmodus kann jedoch nur eingesetzt werden, wenn entsprechende Einrichtungen bzw. Sicherheitsgateways den öffentlichen Netzbereich bzw. Transit-

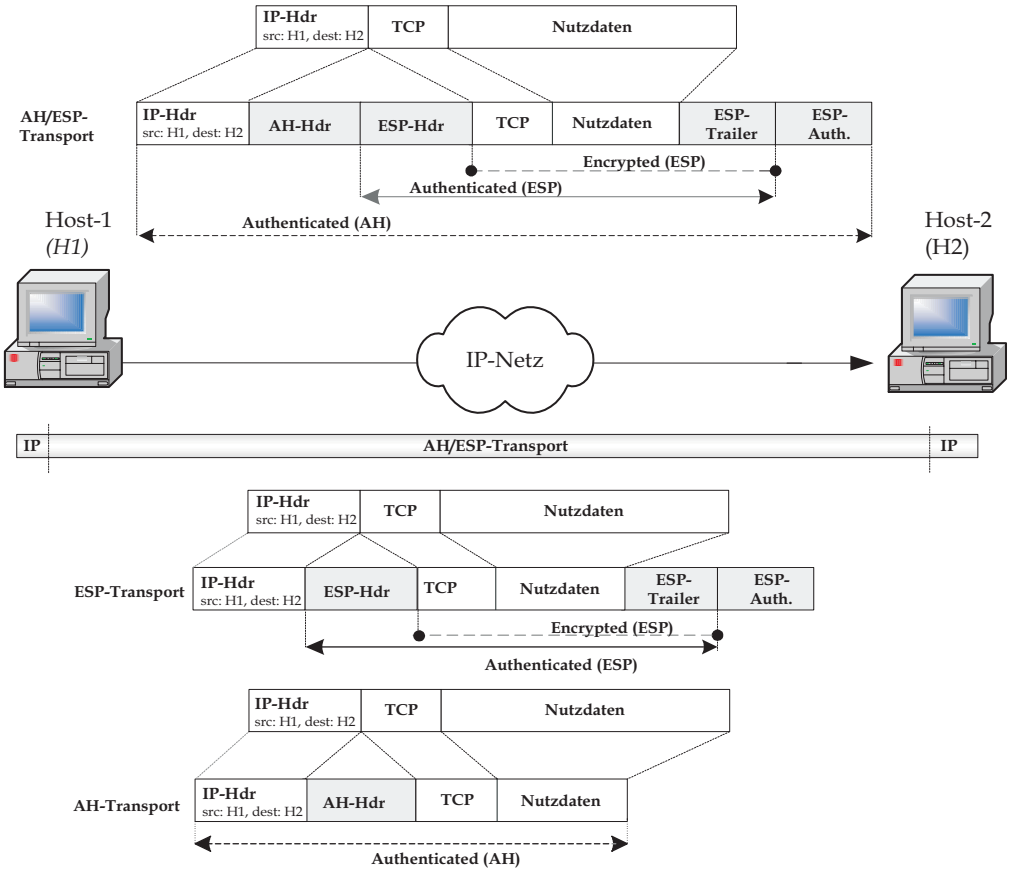


Abb. 7.16: IPSec-Verbindung mittels Transportmodus zwischen Host-1 und Host-2

bereich eingrenzen. Zu den Sicherheitsgateways können speziell ausgestattete Router oder auch Firewall-Systeme eingesetzt werden.

Abb. 7.17 zeigt eine Möglichkeit, wie unter sinnvollen Randbedingungen eine gesicherte Kommunikationsverbindung zwischen den beiden Host-Systemen (H1, H2) und den beiden Gateways (G1, G2) aufgebaut werden kann. Dabei kommt die Verbindung auf Betreiben von H1 zustande. Ein wichtiges, durch die Spezifikation vorgegebenes Kriterium lautet, dass IPSec im Tunnelmodus betrieben werden muss[6], sobald ein Sicherheitsgateway auf dem Verbindungsweg genutzt wird. Allerdings sind keinerlei Beschränkungen hinsichtlich einer Schachtelungstiefe vor-

[6] Es gibt allerdings eine Ausnahme, wenn zu Wartungszwecken das Sicherheitsgateway selbst mit SNMP oder auch ICMP angesprochen werden muss. In diesem Fall kann der Transportmodus verwendet werden. Während dieses Zeitraums kann das Sicherheitsgateway den Tunnelmodus nicht unterstützen.

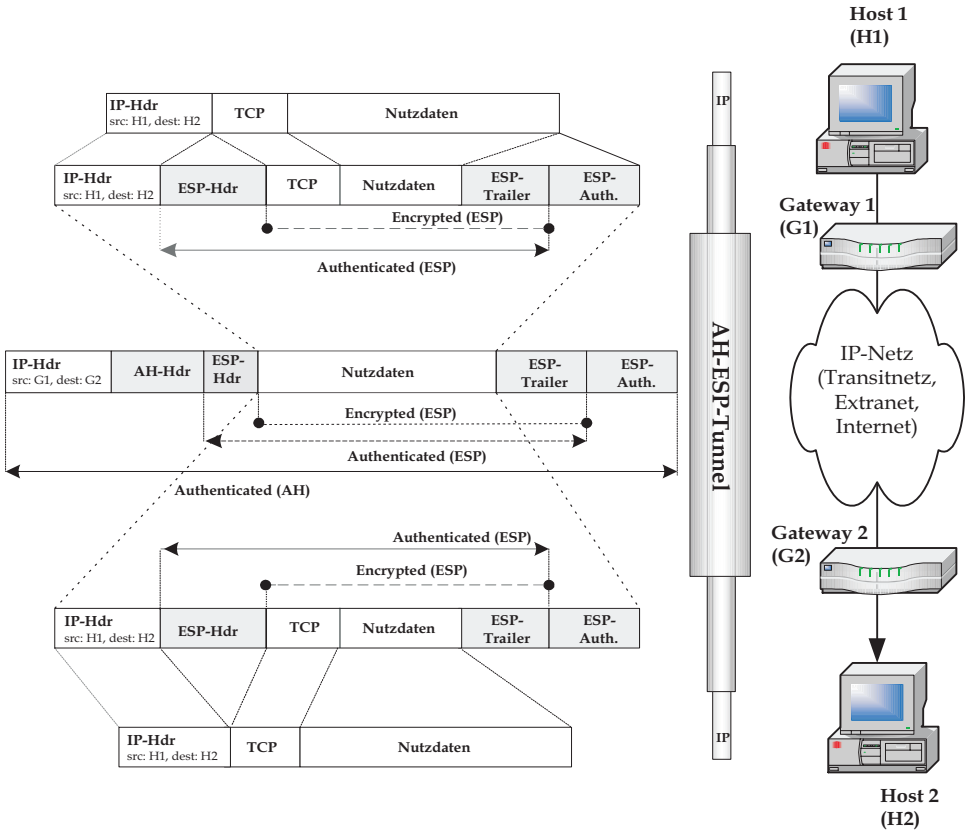


Abb. 7.17: IPSec-Verbindung mittels Tunnelmodus zwischen den Hosts (H1, H2)

gegeben. Dennoch ist aus Geschwindigkeitsgründen eine Schachtelungstiefe von mehr als drei Stufen wenig sinnvoll.

7.4.6 Kombinationen von Security Associations

Die beiden Protokolle AH und ESP sowie die beiden Arbeitsmodi (Transport, Tunnel) mit den verschiedenen Verschachtelungsvarianten ermöglichen viele Kombinationen und Verschachtelungen, die auch zu unsinnigen und ungeeigneten Absicherungen führen können. Um diese Variantenvielfalt noch komplexer zu gestalten, besteht laut Spezifikation die Möglichkeit, die Endpunkte einer Security Association (SA) für den AH-Header (SA-AH) und für den ESP-Header (SA-ESP) unterschiedlich zu gestalten, um z.B. nur Teilstrecken zu bedienen.

Abb. 7.18 zeigt im oberen Teil der Abbildung die Host-Systeme H1 und H2 sowie die Gateways G1 und G2. Unterhalb der Kommunikationsobjekte sind drei

unterschiedliche Tunnelverbindungen skizziert. Die beiden Gateways G1 und G2 stellen im Fall-1 einen einfachen Router dar. In den anderen Fällen sind die Gateways G1 und G2 gleichbedeutend mit Sicherheitseinrichtungen wie z.B. Firewall-Systeme. Abb. 7.18 zeigt eine Auswahl an notwendigen und sinnvollen Schachtelungstiefen, doch laut Spezifikation ist die Schachtelungstiefe nicht begrenzt. Im unteren Teil der Abbildung sind die Protokollkopferweiterungen in sinnvollen Zusammenstellungen skizziert.

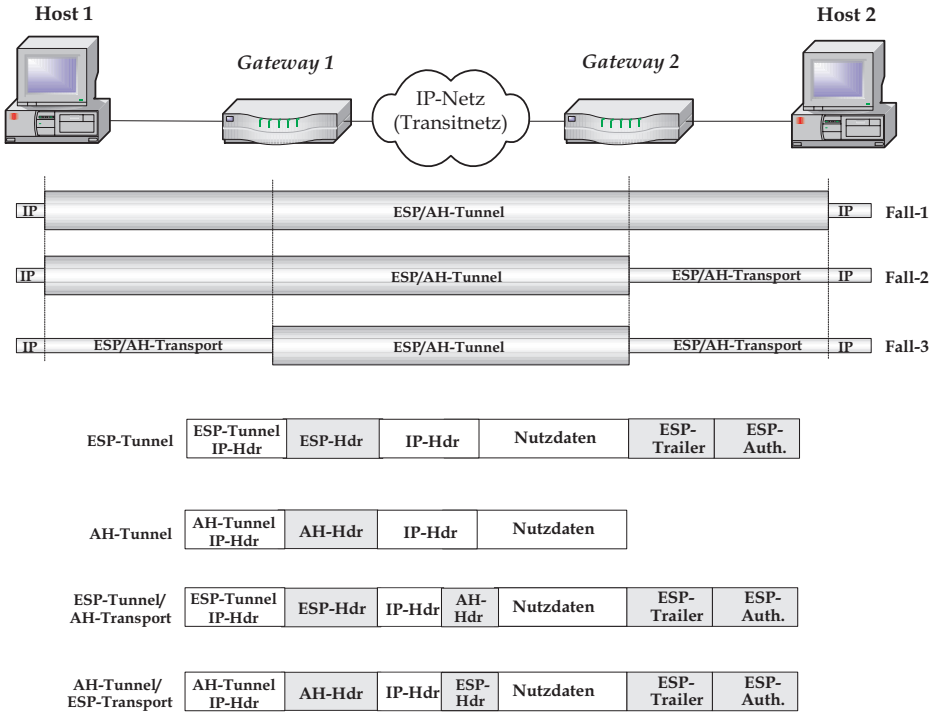


Abb. 7.18: IPSec-Verbindung zwischen zwei Gateways (G1,G2) sowie Hosts (H1,H2)

In der folgenden Beschreibung der Fälle 1 - 3 ist ein vorausgegangener Schlüsselaustausch mittels IKE (Abschn. 7.4.7) abgeschlossen. Ebenso wird angenommen, dass beide Kommunikationspartner geeignete sichere Sitzungsschlüssel ausgetauscht haben. Außerdem wird nur von einer SA-Vertragsaushandlung von Host-1 ausgegangen. Somit können bei einer SA-Vertragsaushandlung die folgenden Kombinationen auftreten:

Fall-1: Die Gateways stellen Router dar, so dass zwischen den beiden Host-Systemen jeweils ein SA-AH-Tunnel oder ein SA-ESP-Tunnel ausgehandelt werden kann. Ebenso können geschachtelte Tunnel mittels SA-AH und SA-ESP und unter Einsatz des Transportmodus aufgebaut werden. (Der reine Transportmodus wurde bereits in Abb. 7.16 dargestellt.)

Fall-2: In diesem Szenario gewinnt eine Mischform Bedeutung. Ein Tunnel wird von einem Host nur bis zum Ende des Gateways G2 aufgebaut. Damit können reine SA-AH und SA-ESP-Vertragsaushandlungen erfolgen, aber auch die einfachen Kombinationen SA-AH-ESP oder SA-ESP-AH sind möglich. In der Verbindung zwischen dem zweiten Gateway (G2) und Host-2 (H2) kann wiederum ein Transportmodus eingesetzt werden.

Fall-3: Dieser Fall stellt eine einfache jedoch typische VPN-Situation dar: nur zwischen den beiden Sicherheitsgateways G1 und G2 existiert eine gesicherte Verbindung. Diese kann z.B. mittels Firewall-System eingerichtet werden oder auch durch eine Absicherung am Access Concentrator eines ISP. Ausschließlich zwischen G1 und G2 wird eine SA-AH oder SA-ESP aufgebaut. Verschachtelte Konstruktionen sind nicht erforderlich, da das gesamte Paket im Tunnel gesichert wird. Außerhalb der Gateways kann wiederum der Transportmodus Verwendung finden.

7.4.7 Initiierung einer Security Association

Bei den bisherigen Betrachtungen und Szenarien wurde davon ausgegangen, dass sich die Kommunikationspartner gegenseitig identifiziert haben und vorab ein Schlüsselaustausch beider Systeme erfolgte. Wie dieser anfängliche Schlüsselaustausch mit dem Aufbau einer SA-Vertragsaushandlung in Verbindung steht, soll jetzt beschrieben werden. In Abschn. 7.4.9 wird der Schlüsselaustausch detailliert behandelt.

Bevor zwischen zwei Host-Systemen ein aktiver IP-Paket-Austausch stattfinden kann, müssen entsprechende SA vereinbart werden. Abb. 7.19 zeigt eine vollständige Vertragsaushandlung zweier Hosts in sechs Schritten. Die vertikalen Linien stellen Zeitachsen dar. Jedes der beiden Host-Systeme H1 und H2 hat eine eigene SPD, die vom Systemadministrator vorab konfiguriert wurde und alle generellen Einträge beinhaltet. Für eine später erstellte SA bzw. einen SA-Verbund werden konkrete Eintragungen in die dafür zuständige SAD vererbt. Jeder Eintrag in der SPD definiert die Art des Datenverkehrs und wie dieser im System zu behandeln ist, außerdem, auf welche Art und Weise der Datenverkehr geschützt werden soll und zu welchem Zweck dieser Schutz zu erfolgen hat.

Ein Schlüsselaustausch nach IKE verläuft in zwei Phasen, wie Abb. 7.19 durch die ineinander liegenden Pfeile illustriert. Die erste Phase (IKE-Control Channel) dient dem Aushandeln von Authentifizierungsmethoden und Verschlüsselungsverfahren, die für eine SA-Vereinbarung gelten sollen. Die zweite Phase (IKE-SA) dient zur Anwendung der in Phase 1 ausgehandelten Verfahren und Methoden, um eine Absicherung der SA-Vereinbarung zu erreichen.

Soll z.B. eine mit IPSec geschützte TCP-Verbindung von Host H1 zum Host H2 ausgehandelt werden, muss für jede Übertragungsrichtung eine SA vereinbart werden, da sich jede TCP-Verbindung aus zwei unidirektionalen und entgegengerichteten virtuellen Verbindungen zusammensetzt. Der in Abb. 7.19 gezeigte Verbindungsablauf erfolgt in sechs Schritten:

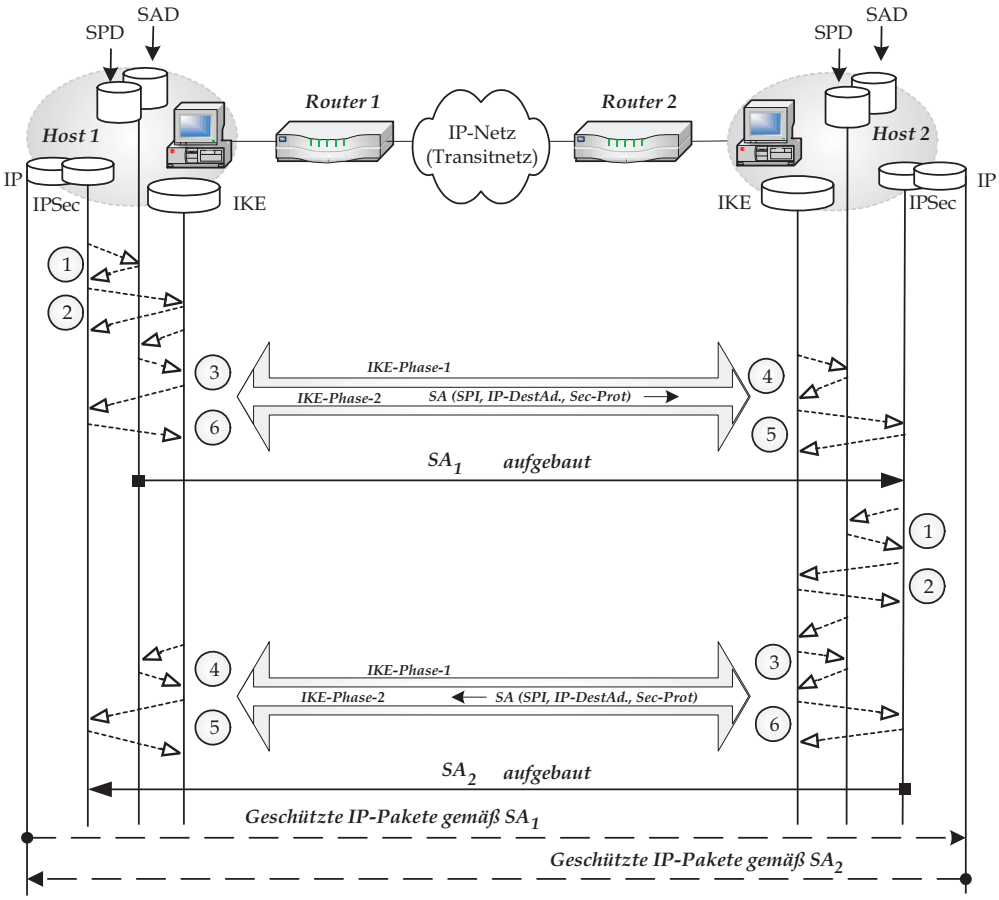


Abb. 7.19: SA-Initiierung zwischen zwei Host-Systemen (H1,H2) mittels IKE-Schlüsselaustausch

1. Das aktive IPSec-Modul in H1 erfragt in der Tabelle bzw. Filterliste für den Out-Bound-Verkehr der SPD, ob die zu übertragenden IP-Pakete für diese TCP-Verbindung überhaupt abgesichert werden müssen. Trifft dies zu, wird in der SAD überprüft, ob schon eine SA existiert, auf die das Verbindungsprofil passt. Falls nein, kann z.B. IKE eingesetzt werden.
2. Das IPSec-Modul befiehlt dem IKE-Modul, mit dem Zielrechner H2 Sicherheitsparameter auszuhandeln (Abschn. 7.4.9).
3. Das IKE-Modul befragt die SPD des Rechners H1 über einzuhaltende Sicherheitsrichtlinien für einen Out-Bound-Verkehr und übergibt eine entsprechende Anforderung (Abschn. 7.4.9) an das IKE-Modul im Rechner H2 (IKE-Phase-1). Um unmittelbar nach Eintreffen der Anforderung von H1 eine SA in H2 einzurichten, überprüft das IKE-Modul von H2 in seiner SPD, ob und welche

In-bound-Verkehrsrichtlinien gemäß IPSec zugrunde gelegt werden müssen. Ist dies der Fall, wird in der SAD verifiziert, ob schon eine SA mit dem Profil existiert.

4. Falls nein, wird eine SA mit einem Werte-Tripel ⟨ SPI; IP-DA; Sec-Prot ⟩ ausgehandelt (IKE-Phase-2). Die Aushandlung, die zu einem mehrfachen Werteaustausch führen kann, erfolgt unter Einbeziehung der Schritte 5 und 6. Dabei erfolgt die wechselseitige Übertragung der Werte verschlüsselt, da bereits die IKE-1 Phase abgeschlossen ist.
5. Die angebotenen Werte werden zwischen dem IKE- und dem IPSec-Modul des Hosts H2 ausgetauscht.
6. Die angebotenen Werte werden zwischen dem IKE- und dem IPSec-Modul des Hosts H1 ausgetauscht.

Damit ist die SA_1 zwischen Host H1 und H2 komplett. Die zweite für TCP erforderliche Verbindung wird, ausgehend vom Host H2, in Gegenrichtung mittels einer eigenen SA_2 nach dem gleichen Muster mit den Schritten 1 - 6 ausgehandelt. Anschließend können geschützte IP-Pakete, die den Sicherheitsrichtlinien der SPD (In-Bound, Out-Bound) des jeweiligen Hosts genügen und beiden Rechnern bekannt sind, ausgetauscht werden.

In den angeführten Beispielen wird unterstellt, dass eine feste Zuordnung der IP-Adressen möglich ist, auch wenn es sich bei dem Szenario um einen Fernzugriff handelt, wie in Abschn. 6.1.3 beschrieben. Für einen reinen mobilen Nutzer (Road Warrior), der z.B. abends von einem Hotel aus Zugang ins Firmennetz erlangen will, sieht dies schwieriger aus, wenn die Kommunikationsverbindung mittels IP-Sec abgesichert werden soll.

7.4.8 IPSec und Remote Access

Aus den vorangegangenen Betrachtungen zu IPSec wurde deutlich, wie mit IPSec eine Kommunikationsverbindung für die drei VPN-Architekturen (Intranet/Extranet/Access, vgl. Abschnitte 6.1.1, 6.1.2 und 6.1.3) abgesichert werden kann. Für einen Fernzugriff (Remote Access) ergibt sich allerdings eine besondere Situation: Soll ein Fernzugriff von einem mobilen Computer in das firmeneigene LAN erfolgen und wurde mittels dynamischer Adresszuweisung (DHCP) eine IP-Adresse vom Internet Service Provider (ISP) bei der Einwahl in den PoP zugewiesen, entsteht ein IP-Adressierungskonflikt.

Mittels IKEv1 kann vielleicht eine Security Association (SA) für den In-bound-Verkehr – also eine Kommunikationsverbindung von außen in das Firmen-Netzwerk (LAN) gerichtet – für die Werte des bezeichneten SA-Tripels ⟨ Security Parameter Index (SPI), IP Destination Address, Security Protocol ⟩ (Abb. 7.19) ausgehandelt werden. Jedoch spätestens für einen Out-Bound-Verkehr gelingt es nicht, die IP-Adresse (IP Destination Address) des mobilen Computers, die vom

ISP als DHCP vergeben wurde, zu ermitteln und eine Out-Bound-SA auszuhandeln.

IPSec oder vielmehr die wichtige Verbindungsaufbaukomponente (SA) ist an eine feste IP-Zieladresse geknüpft, die es jedoch bei einer dynamischen IP-Adresszuweisung durch einen ISP nicht gibt. So scheitert beispielsweise ein Verbindungsaufbau für eine TCP-Verbindung, wie in Abb. 7.19 dargestellt, wenn Host H1, durch einen mobilen Computer ersetzt wird.

Es ergeben sich einige fundamentale Unterschiede, die für die IPSec-Nutzung bedeutsam sind, wenn, wie oben erwähnt, mittels eines Dial-In über das Netz eines Internet Service Providers (ISP) ein Zugriff mittels DHCP erfolgen soll.

Für den Authentifizierungsprozess ist es unumgänglich, dass der Nutzer des mobilen Computers am Prozess beteiligt werden muss. Dieser Prozess muss also zwischen dem mobilen Nutzer und dem Firmennetzwerk erfolgen und darf nicht bei der IP-Adresse des ISP enden. Für einen Remote Access, der mittels IPSec abgesichert werden soll, müssen einige Randbedingungen erfüllt sein. Außerdem müssen, falls das Firmennetzwerk eine gewisse Größe und Komplexität überschritten hat, häufig mehrere Firmeneinwahlpunkte unterstützt werden. Auch muss oftmals auf Altlasten Rücksicht genommen werden. Etliche Systeme basieren auf einer Abfrage der Nutzerkennung, Hardwarekennung, Zeit-Token, IP-Adresse etc., die meistens erst bei einem Fernzugriff via ISP vorliegen, wenn eine Verbindung zum Firmennetz erfolgreich eröffnet wurde. Weiterhin muss gewährleistet sein, dass eine klare Zugriffstrennung bei einem Fernzugriff erfolgt, wenn mehrere Nutzer den gleichen mobilen Computer benutzen.

IPSec weist im Zusammenhang mit einem Remote Access eine Reihe von Unzulänglichkeiten auf:

1. Wenn Pre-shared Keys, Main Mode und dynamische IP-Adressen genutzt werden, müssen die Pre-shared Keys für alle IPSec-Clients gleich sein.
2. IPSec unterstützt nicht die traditionell beim Fernzugriff eingesetzten unidirektionalen Authentifizierungsmethoden RADIUS (PAP/CHAP), Secure-ID oder OTP.
3. Die IP-, DNS- und WINS-Adresszuweisungen vom VPN-Gateway zum Client sind innerhalb des IKEv1-Protokolls nicht spezifiziert. Die privaten IP-, DNS- und WINS-Adressen müssten in jedem IPSec-Client fest konfiguriert werden.
4. Bei größeren Remote-Access-Netzen mit mehr als 300 Teilnehmern können Ressourcen-Probleme am Gateway auftreten. Falls IPSec-Clients ihre PPP-Verbindung zum Provider unterbrechen und dabei unter Umständen ihre eigene Security Association (SA) löschen, kann ein offener Verbindungsteil im VPN-Gateway zurück bleiben.
5. Zwischen IPSec-Client und VPN-Gateway darf kein IP-NAT-Verfahren eingesetzt werden, da der IPSec-ESP-Header nicht über genügend Informationen verfügt. Setzt beispielsweise ein Filial-Router IP-NAT bei der Einwahl zum

Provider ein, muss sich der Tunnelendpunkt im Router befinden. Das heißt, es findet nur eine Authentifizierung des LAN statt, jedoch keine persönliche Authentifizierung der Teilnehmer am Arbeitsplatzrechner. Vor allem beim Einsatz von digitalen Zertifikaten mittels einer PKI muss der Tunnelendpunkt im Rechner in der Außenstelle liegen.

6. In großen Remote-Access-Installationen ist die Konfiguration und Administration der SPD-Einträge *(Security Policy Database)* sowohl auf Clientseite als auch im Zentralsystem sehr aufwändig.

Mittlerweile gibt es Ansätze, diese Unzulänglichkeiten zu beseitigen. In den nachfolgenden Abschnitten sind die derzeitigen Entwicklungen beschrieben.

Cisco schlägt im Draft XAUTH (Extended Authentication) eine Lösung für die ersten beiden Punkte vor. Die Lösung scheint in der Praxis befriedigend angenommen zu werden. Jedoch ist das IKE-Protokoll erweitert worden und folgt nicht mehr vollständig den RFCs der IETF. Cisco hat XAUTH in eine Reihe von VPN Gateways eingebaut. Ein entsprechender Draft für die Zuweisung von IP-, DNS- und WINS-Adressen (wie im Punkt 3 aufgezeigt) liegt bisher noch nicht vor. Um das in Punkt 4 benannte Problem zu lösen, gibt es einen Vorschlag, der einen Pollingmechanismus beschreibt. Mit diesem Verfahren soll signalisiert werden, dass eine Security Association nicht mehr aktiv ist. Pollingmechanismen führen allerdings zu einem Problem, wenn der Client im Shorthold-Modus arbeitet. Denn dann bleibt die Layer-2-PPP-Verbindung zum Provider immer bestehen. Das Übersetzungsproblem der Netzwerkadressen zwischen IPSec-Client und VPN-Gateway (Punkt 5) soll der neue Draft NAT Traversal 28/2-2001 der Firma SSH lösen. Damit Geräte, die Network Address Translation (NAT) einsetzen, kommunizieren können, wird jedes IPSec-Paket zusätzlich in einen IP- und UDP- Header verpackt. Punkt 6 wird davon allerdings nicht berührt, er hängt von der Software-Implementierung der SPD ab. Doch dies ist eine herstellerabhängige Lösung, von denen es inzwischen mehrere am Markt gibt. Um weiteren proprietären Lösungen entgegenzuwirken, hat die IETF die Weiterentwicklung von IKE im Jahr 2001 begonnen. Im Abschn. 7.4.9 werden die aktuellen Lösungsvorschläge diskutiert.

Ein anderer interessanter Ansatz, um die in den Punkten 1 bis 5 aufgezeigten Probleme zu lösen, ist im [RFC 2888] beschrieben, und zwar mit IPSec-over-L2TP (Secure Remote Access with L2TP). IPSec-over-L2TP verlangt keine Änderungen an den [RFC 2401 bis 2409] und dürfte deshalb auf breite Zustimmung treffen. [RFC 2888] sieht vor, dass zunächst ein Layer-2-Tunnel zwischen VPN-Client und VPN-Gateway aufgebaut und anschließend eine Standard-PPP-Verbindung ohne erweiterte Sicherheitsfunktionen – im Gegensatz zu PPP-EAP-TLS – eingerichtet wird. Über diese werden die IKE-Verhandlungen (Handshake) und die IPSec-Datenpakete übertragen (Punkte 1 bis 3). Trennt der Client die Layer-2-Verbindung zum Provider, wird der Tunnel automatisch abgebaut und die IPSec-SA können gelöscht werden (Punkt 4). Mit Punkt 5 (IP-NAT) gibt es, wie eingangs beschrieben, bei einem L2TP-Tunnel keine Probleme.

IPSec über Layer-2-Tunneling (SSLoL2TP)

Doch [RFC 2888] weist einige Nachteile auf: Einmal der vergrößerte Overhead, also L2TP- und IPSec-Haeader, außerdem die Komplexität, die auf die Kombination von Layer-2-Tunneling und IPSec zurückzuführen ist. Ein dritter Nachteil ist, dass die privaten IP-Adressen unverschlüsselt übermittelt werden, weil IPSec erst nach Aufbau des Tunnels und dem anschließenden PPP-Handshake aktiv wird. In der Praxis hat sich jedoch gezeigt, dass der Overhead bei IPSec-over-L2TP entweder durch PPP- oder IP-Kompression (IP-comp) auf IPSec-Ebene begrenzt werden kann. Wie komplex die Implementierung ausfällt, hängt davon ab, über welches Fachwissen ein Hersteller in Bezug auf die Layer-2-Technik verfügt. Ob die privaten IP-Adressen unverschlüsselt über das Netz geleitet werden sollen, obliegt dem Betreiber eines VPN.

IPSec ist ein Standard mit ausgezeichneten Sicherheitsmechanismen. Er eignet sich vor allem für VPN-Szenarien, in denen mit festen IP-Adressen gearbeitet wird, etwa im Business-to-Business-Bereich. In diesen Fällen lassen sich durchaus VPN-Gateways verschiedener Hersteller einsetzen. Allerdings können Probleme beim Einsatz von digitalen Zertifikaten auftreten.

7.4.9 Schlüsselaustausch für IPSec (IKE)

Ein Schlüsselmanagement (Internet-Key-Exchange-Management) als Teil von IPSec erfordert die Erstellung und Verteilung von geheimen Schlüsseln. Die Herausforderung besteht darin, vier Schlüssel für eine gesicherte Kommunikation zwischen zwei Applikationen, für den Hin- und Rückweg für die beiden Protokolle AH und ESP, auszutauschen. Dabei schreibt die IPSec-Architektur zwingend zwei grundsätzliche Verfahren vor:

Manueller Austausch: Ein Systemadministrator muss z.B. in der Lage sein, jedes der eigenen Systeme mit den dazugehörigen Schlüsseln und die Schlüssel des kommunizierenden Systems manuell zu bedienen. Dies ist allerdings nur für kleinere Systeme oder für Testzwecke praktikabel.

Automatischer Austausch: Ein System erzeugt und verteilt auf Anforderung eine Security Association (SA), die Konfiguration und geeignete Schlüssel an das dazugehörige Management.

Ein manueller Schlüsselaustausch wurde in der Praxis z.B. 1996 bei dem von der RSA Data Security Inc. initiierten Interoperabilitätstest unterschiedlicher IPSec-Herstellerlösungen eingesetzt. Diese Initiative, die sich zum Ziel gesetzt hatte, einen sicheren Weitverkehrsbereich Secure-WAN aufzubauen, wird als S/WAN-Gruppe, oder neuerdings auch als Free-S/WAN bezeichnet. Eine der ersten Implementierungen der Free-S/WAN-Gruppe wurde auf dem Betriebssystem Linux durchgeführt. Bis Ende 1997 wurden noch alle Tests mit manuell erstellten

Schlüsseln vorgenommen. Obgleich ein manueller Schlüsselaustausch für kleinere Netze noch praktikabel erscheint, ist es erforderlich, ein automatisches Verfahren zu haben, welches Session-orientierte Schlüssel im einfachen Umgang für größere Umgebungen bereitstellt.

Neben Free-S/WAN existieren zwei weitere freie Implementierungen von IPSec. Seit dem Linux Kernel 2.6 ist IPSec bzw. ISAKMP und RACOON Bestandteile des Betriebssystems[7] geworden. RACOON ist eine asiatische Implementierung – die unter dem Namen KAME bekannt ist – von IPSec. RACOON ist wesentlich schlanker als ISAKMP, jedoch auch weniger umfangreich in seinen Parametern. Für den praktischen Einsatz von IPSec ist das Buch von [Spengenberg 2004] sehr zu empfehlen. Ebenso hat IPSec außerhalb der Open-Source-Welt Eingang in Windows-Betriebssysteme[8] gefunden. Weiterhin sind DSL-Router auch schon im unteren Preissegment mit IPSec ausgestattet. Oftmals wird dann nicht die ganze Palette der IPSec-Möglichkeiten unterstützt, sondern nur ein Teil, wie z.B. nur der Tunnelmodus (ESP).

Das durch die IPSec-Spezifikation empfohlene Schlüsselaustauschverfahren ist das Internet-Key-Exchange-Verfahren (IKE), das im [RFC 2409] definiert ist. Es ist aus einer Kombination des ISAKMP- und dem Oakley-Protokoll entstanden. Das Internet Security Association and Key Management Protocol (ISAKMP) bietet eine Rahmen- und Paketstruktur (Abschn. 7.4.12) für unterschiedliche Authentifizierungs- und Schlüsselaustauschverfahren [RFC 2408]. Dagegen unterstützt das Oakley-Protokoll (Abschn. 7.4.13) verschiedene Möglichkeiten einer Schlüsselverteilung.

Die IPSec-Protokolle AH und ESP erfordern, dass alle Kommunikationsteilnehmer bereits geheime symmetrische Schlüssel ausgetauscht haben und verlangen von einem robusten Schlüsselmanagement, dass es folgende Herausforderungen erfüllt:

- Es muss unabhängig sein von speziellen kryptographischen Verfahren.
- Es muss unabhängig sein von speziellen Austauschverfahren.
- Es muss eine Authentifizierung der Schlüsselmanagement-Elemente vornehmen.
- Es muss eine SA über ein unsicheres Netz aufbauen können.
- Es muss effizient mit Ressourcen umgehen können.
- Es muss ad hoc sowohl eine Host-, als auch eine Session-Anforderung für eine SA-Verbindung in Einklang bringen.

---

[7] ISAKMP und RACOON lassen sich relativ einfach über Parameter steuern, die in einer ASCII-Datei gespeichert werden.

[8] Der IPSec-Stack in den Windows-Betriebssystemen, wie z.B. Windows XP, lässt sich über die Microsoft Management Console (MMC) bedienen. Allerdings gibt es auch spezielle Tools, die die Bedienung vereinfachen.

Mit IKE ist ein Verfahren entwickelt worden, das den genannten Anforderungen nachkommt. Grundsätzlich ist IKE durch die folgendenden sieben Eigenschaften geprägt:

1. Es bestimmt für die beteiligten Kommunikationsteilnehmer, welche Protokolle, Algorithmen und Schlüssel zu verwenden sind.
2. Es wird sichergestellt, dass von Beginn an *(Startbedingung)* mit der richtigen Person bzw. Applikation ein Schlüssel ausgehandelt wird.
3. Es wird ein sicheres Schlüsselmanagement (Schlüsselwechsel und -erneuerung) für die ausgehandelten Schlüssel gewährleistet.
4. Es wird ein sicherer Schlüsselaustausch zugesichert.
5. Es ist über den UDP-Port 500 nutzbar.
6. Es bietet ein Zwei-Phasen-Konzept (Kontroll- und Datentransferkonzept).
7. Es lässt vier unterschiedliche Authentifizierungsverfahren zu.

Entscheidend für einen sicheren Datenaustausch mit einem entfernt gelegenen Host ist die Start- bzw. die Authentifizierungsphase, die in Punkt 7 angesprochen wurde. Hier bietet IKE drei Verfahren:

1. Vorab ausgetauschte Schlüssel (Pre-shared Keys, PSK)
2. Digitale Signaturen (Digital Signatures RSA, DSS)
3. Asymmetrische Schlüsselverfahren nach RSA (RSA Public Key Encryption) und überprüfte asymmetrische Schlüsselverfahren gemäß RSA (Revised RSA Public Key Encryption)

Seit dem die PKI-Technologie (vgl. Abschn. 4.7) und sich die damit verbundenen Zertifikate gemäß X.509 v3 (vgl. Abschn 4.7.1) allgemein in der Wirtschaft etabliert hat, liegt seit Sommer 2004 ein IETF-Vorschlag vor, wie die PKI-Technologie im Kontext zu IKE/IPSec einzubinden ist. Der Vorschlag berücksichtigt IKEv1 und IKEv2 unter Einbindung des PKIX-Framework.[9]

Jedes dieser drei Verfahren hat seine Vorteile und Anwendungscharakteristik, die je nachdem welche Verbindungsart abgesichert werden soll eingesetzt werden können. Tab. 7.2 vergleicht die Eigenschaften der vier Verfahren. Auf das in Punkt 6 von Seite 246 erwähnte Zwei-Phasen-Konzept wird in den Abschnitten 7.4.10 und 7.4.11 näher eingegangen.

[9] Die PKIX-Arbeitsgruppe der IETF wurde bereits 1995 gegründet. Das ursprüngliche Ziel galt nicht nur den ITU/PKI-Standard für das Internet anzupassen. Darüber hinaus hatte man die Neuentwicklung unter Verwendung von X.509-basierten PKI-Systemen im Fokus.

Tabelle 7.2: Die acht derzeit für die IKEv1-Phase-1 zur Verfügung stehenden Authentifizierungstechniken im Vergleich

Methode	Authentifizierungsverfahren	Vorteile	Nachteile
Pre-shared-Keys	Hash-Wert wird über die ausgetauschten Informationen gebildet	einfache Handhabung	■ Sitzungsschlüssel muss vor einer IKE-Initiierung verteilt werden ■ Es werden ausschließlich IP-Adressen als Identifier benutzt
Digital Signatures (RSA or DSS)	Anwendung der Hash-Funktion über die ausgetauschten Informationen	■ Alternativen zu IP-Adressen sind möglich ■ Partner-Zertifikat wird erst bei IKE-Initiierung benötigt	■ Zertifikatverwaltung etc. erforderlich
RSA Public Key Encryption	Hash-Wert über Nonce, Verschlüsselung mit Public Keys	■ Bessere Sicherheit beim DH-Austausch durch Public Key Verfahren ■ Identifier-Absicherung mittels aggressiven Modus	■ Public Keys (Zertifikate) müssen vor IKE-Initiierung vorliegen ■ Performance intensive Public-Key-Berechnungen
Revised RSA Public-Key Encryption	Hash-Wert über Nonce, Verschlüsselung mit Public Keys	■ Bessere Sicherheit beim DH-Austausch durch Public Key Verfahren ■ Weniger Schlüssel-Berechnungen, da ein Zwischenschlüssel eingesetzt wird	■ Public-Key (Zertifikate) müssen vor IKE-Initiierung vorliegen

7.4.10 IKEv1-Phase-1

Die IETF hat aufgrund der Anforderungen im Bereich des Remote Access – und dies kann sowohl eine WLAN als auch eine 3G (UMTS) Verfahren sein – die Weiterentwicklung von IKE vorgenommen. Eine spezielle Arbeitsgruppe wurde mit dieser Problemstellung beauftragt. Mit IKEv2 soll es einfacher werden für mobi-

le Fernnutzer[10] eine sichere Kommunikationsverbindung über das Internet aufzubauen. Insbesondere soll IKEv2 bei gleichem Sicherheitsniveau wie IKEv1 eine bessere Performance, eine geringere Komplexität im Management sowie eine verbesserte Resistenz gegen Angriffe bieten. Außerdem soll das Network Address Translation (NAT) gelöst werden. Im Gegensatz zu den herstellerspezifischen Lösungen wird somit eine herstellerunabhängige protokollbasierte Lösung geschaffen, die für Interoperabilität sorgt.

In diesem Abschnitt wird zunächst auf IKEv1 und auf die zwei Phasen eingangen. Es folgen Betrachtungen zum Schlüsselmanagement ISKAMP sowie zum Oakley-Schlüsselprotokoll. ISAKMP und das Oakley-Protokoll sind inzwischen feste Bestandteile von IKE. Anschließend wird näher auf IKEv2 eingegangen.

Während der IKEv1-Phase-1[11] werden zwischen den Kommunikationspartnern Angebote über eine ISAKMP-SA wechselseitig ausgetauscht, bis eine Einigung über ein Verfahren erreicht wird. Diese Phase dient zunächst dem Aufbau eines sicheren KontrollKanals (Abb. 7.19). In diesem Abschnitt wird detailliert auf den Austauschvorgang eingegangen. Dabei wird bei einer ISAKMP-SA ein Konsens über eines der gemäß Tab. 7.2 möglichen Verfahren angestrebt.

Während des Austauschvorgangs werden Authentifizierungsmethoden, Hash-Verfahren und Verschlüsselungs- sowie Schlüsselaustauschverfahren ausgehandelt. Anschließend tauschen beide Partner Informationen zur Erzeugung eines gemeinsamen Geheimnisses aus, wie z.B.:

- Cookies, die anschließend die SPIs in der IKEv1-Phase-2 unterstützen,
- Diffie-Hellman-Werte,
- Nonces (Zufallszahlen),
- oder auch eine Identifizierung nach einem asymmetrischen Schlüsselverfahren.

Im Folgenden erzeugen beide Seiten in ihrer sicheren Umgebung gemäß den ausgetauschten Werten die Sitzungsschlüssel, bevor weitere Authentifizierungsmechanismen angewandt werden. Wenn dieser Austauschprozess erfolgreich abge-

---

[10] Unter mobile Nutzer und Fernnutzer bzw. *Mobile User* und *Remote User* werden unterschiedliche Nutzungsszenarien verstanden. Der *Remote User* wählt sich i.d.R. von einem entfernten, jedoch fixen Standort ein. Eine IP-Adresse kann dann beispielsweise von einem ISP über DHCP zugewiesen werden. Dies Szenario beschreibt den klassischen Remote Access-Fall. Unter einem *Mobile User* wird ein Szenario verstanden, bei dem der User sich wie oben beschriebenen über ein ISP einwählt, seinen Standort jedoch während der Sitzung (Session) verlässt. Mit den heutigen 4G-Netzen (UMTS) wird dieses Szenario bald Wirklichkeit werden.

[11] Inzwischen hat die IETF mehrere Vorschläge erarbeitet, um das NAT-Problem bei IPSec zu lösen. Der wohl am vielversprechende sieht eine Überarbeitung des IKE-Protokolls vor. Um eine Abgrenzung zum ursprünglichen IKE [RFC 2409] zu geben, wird nachträglich für IKE eine Versionsnummer eingeführt. IKEv1 bezeichnet die Definition gemäß [RFC 2409]. IKEv2 stellt die überarbeitete Version dar, die ein NAT-Traversal nach [RFC 3947] ermöglicht.

schlossen ist, besitzen beide Seiten die gleichen symmetrischen Schlüssel (vgl. Abschn. 4.2). Diese sind dabei zu keiner Zeit über das dazwischenliegende unsichere Netz transportiert worden.

IKEv1 hält zwei unterschiedliche Modi für die Phase-1 bereit, die auf das ursprüngliche Oakley-Protokoll zurückgehen: der Hauptmodus (*Main Mode*) und der verkürzte *Aggressive Mode*, der durch einen Austausch von nur drei Nachrichten gekennzeichnet ist. Der aggressive Modus ist eine Ausnahme. In der Praxis wird der Hauptmodus am häufigsten eingesetzt.

Für unterschiedliche Anwendungsfälle können die vier in Tab. 7.2 für die IKEv1 Phase-1 zur Verfügung stehenden Authentifizierungstechniken zwischen Host H1 und Host H2 eingesetzt werden. Exemplarisch werden nachfolgend drei Techniken im Main Mode und eine im aggressiven Modus behandelt. Weitere Techniken für den aggressiven Modus sind anschließend leicht ableitbar. Im ers-

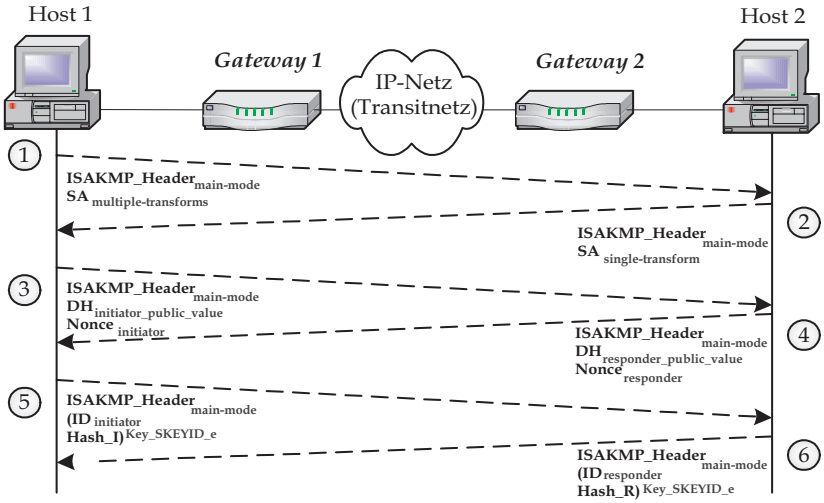


Abb. 7.20: IKEv1-Phase-1 und Austausch von sechs Nachrichten im Main Mode mit Pre-shared Keys

ten Nachrichtenwechsel der Abb. 7.20 (1, 2) zwischen Host H1 und H2 werden so genannte *Transforms* ausgehandelt. Ein *Transform* kann z.B. das Hash-Verfahren HMAC-MD5 für den später zu nutzenden AH-Header oder auch ein Verschlüsselungsverfahren, z.B. DES-CBC, für den in der ISAKMP-SA zu transportierenden ESP-Header sein. Weiterhin werden Cookies erzeugt, um einen möglichen DoS-Angriff (Denial-of-Service-Attacke) wirkungsvoll zu unterbinden. Generell sind jedoch für den Hauptmodus nach einem Nachrichtenaustausch von (3) und (4) alle Schlüsselelemente ausgetauscht, während das ausgehandelte Hash-Verfahren schon beim Nachrichtenaustausch (5) und (6) verwendet wird.

In Abb. 7.21 sind bereits in der Nachricht (3) die Nutzlast der ID und des

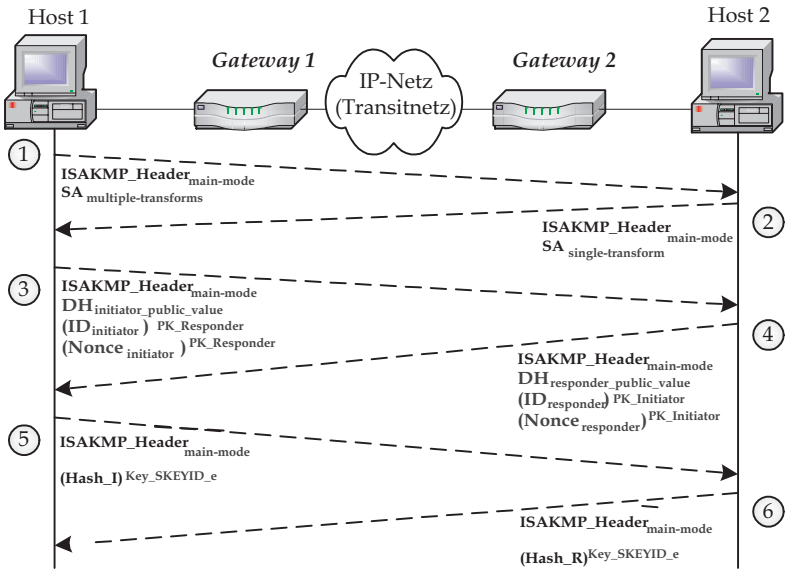


Abb. 7.21: IKEv1-Phase-1 mit Austausch von sechs Nachrichten im Main Mode mit dem Public-Key-Verfahren

Nonce (Zufallswert) mit dem öffentlichen Schlüssel von Host H2 verschlüsselt. In der Nachricht (4) sind entsprechend die Nutzlast der ID und ein Nonce mit den öffentlichen Schlüsseln von Host H1 abgesichert. Wie im Einzelnen das Hash-Verfahren ($Hash_{Initiator}$, $Hash_{Responder}$) aussieht, hängt vom Authentifizierungsprozess ab. So wird, wenn digitale Signaturen verwendet werden, der $Hash_{Initiator}$ und $Hash_{Responder}$ signiert übertragen, so dass der jeweilige andere Host die Signatur überprüfen kann. Bei der Verwendung des Public-Key-Verfahrens sowie bei Pre-shared Keys wird der notwendige Hash-Wert erzeugt und an den anderen Host weitergeleitet. Die Erzeugung des richtigen Hash-Wertes authentifiziert den jeweiligen anderen Host gemäß des Public-Key-Verfahrens bzw. der Pre-shared Keys (PSK).

Abb. 7.22 zeigt den Austausch von digitalen Signaturen in der IKEv1-Phase-1. Dabei ist die in der Nachricht (5) und (6) skizzierte ISAKMP-Payload bereits verschlüsselt. Durch den verkürzten Nachrichtenaustausch im aggressiven Modus gegenüber dem Hauptmodus werden ab der Nachricht (1) die Nutzlast der ID und des Nonce mit dem öffentlichen Schlüssel von Host H2 verschlüsselt. Nachdem die Nachricht bei Host H2 angekommen ist, liegen für H2 alle Schlüsselelemente zur weiteren abzusichernden Kommunikation der Phase-1 vor. Das Gleiche gilt für die Nachricht (2), die von Host H2 zurück an Host H1 geschickt wird, in der die Nutzlast der ID und des Nonce von H2 mit dem öffentlichen Schlüssel von Host H1 abgesichert sind. Damit ist Host H1 in der Lage, eine vertrauliche integritätsgeprüfte Kommunikation mit H2 vorzunehmen. Eine Hash-Wert-Absicherung

kommt für die Nachrichten (2) und (3) zum Tragen.

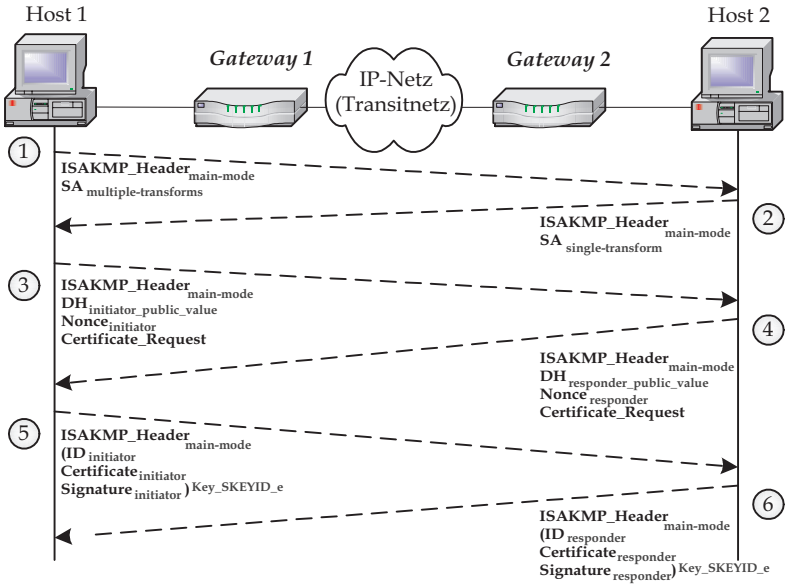


Abb. 7.22: IKEv1-Phase-1 mit Austausch von sechs Nachrichten im Main Mode mit dem digitalen Signatur Verfahren

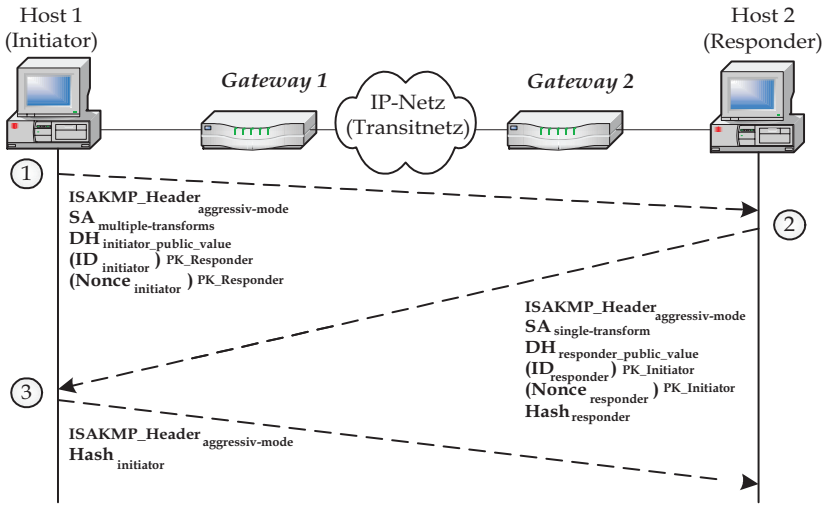


Abb. 7.23: IKEv1-Phase-1 mit Austausch von drei Nachrichten im Aggressive Mode mit einm Public-Key-Verfahren

7.4.11 IKEv1-Phase-2 oder der Quick Mode

Nachdem die Phase-1 komplett abgeschlossen ist, ist es das Ziel der Phase-2, zwischen den Kommunikationspartnern eine ISAKMP-SA zu vereinbaren. Diese Vereinbarung geschieht, ähnlich wie in der Phase-1, durch ein wechselseitiges Anbieten von Techniken und Verfahren zwischen den Kommunikationspartnern. Dies wird üblicherweise durch einen Automatismus abgehandelt, bis eine Einigung über die Authentifizierungsmethoden, Hash-Wert-Bildung und Verschlüsselungsverfahren zu Stande kommt, um IP-Pakete gemäß IPSec-AH und IPSec-ESP abzusichern. Eine Schlüsselvereinbarung erfolgt durch Phase-1. Optional kann allerdings in der IKEv1 Phase-2 nochmals ein Diffie-Hellman-Austausch für eine abgesicherte Weiterleitung vorgenommen werden.

Phase-2 kann mehrere Security Associations in einem Austausch erzielen, indem mehrere SA-Payloads in einer ISAKMP-Nachricht übertragen werden (Abschn. 7.4.12). Beispielsweise kann es nötig sein, eine FTP-Session kryptographisch stärker abzusichern als die der Telnet-Session. Dennoch kann es sein, dass die Schlüssel für die Telnet-Session häufiger auszutauschen sind als die der FTP-Session. Im üblichen Quick Mode der Phase-2 werden drei Nachrichten mit jeweils drei unterschiedlichen Hash-Werten ausgetauscht, um sicherzustellen, dass es sich um die originären Kommunikationspartner handelt. Zufallswerte bzw. so genannte Nonce werden im Nachrichtenaustausch (1) und (2) vorgenommen. Ein Diffie-Hellman-Schlüsselaustausch wird ebenfalls während des Nachrichtenaustauschs in (1) und (2), wenn die Option (PFS) gesetzt wurden, vorgenommen.

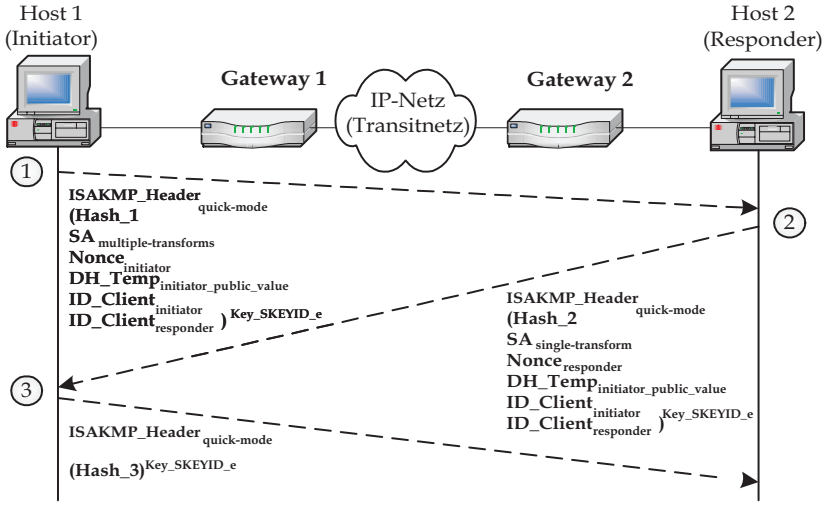


Abb. 7.24: IKEv1-Phase-2 im Quick Mode, der durch die Verschlüsselung (SKEYID_e) resultierend aus der IKEv1-Phase-1 abgesichert ist

Der Quick Mode ist im Grunde keine selbstständige Phase, da die Schlüssel (SKEYID_e) aus der IKEv1-Phase-1 verwendet werden. Doch jede übertragene

Payload ist integritätsgesichert und bis auf den ISAKMP-Header verschlüsselt. Die Reihenfolge der Payloads nach dem ISAKMP-Header ist vorgeschrieben. So muss nach dem ISAKMP-Header zwingend die HASH-Payload und dann die SA-Payload folgen.

Sind Phase-1 und Phase-2 erfolgreich abgeschlossen, können die beiden Host-Systeme H1 und H2 eine gesicherte Kommunikation gemäß den Sicherheitsvereinbarungen (Policys) mit entsprechenden Verkehrsprofilen durchführen.

7.4.12 Das Internet Security Association and Key Management Protocol (ISAKMP)

ISAKMP wurde von der IETF im [RFC 2408] spezifiziert und bietet ein breites Spektrum an Möglichkeiten, um eine Security Association (SA) zu erzeugen, auszuhandeln und zu modifizieren. Es stellt neben dem Oakley-Protokoll die zweite Grundlage für IKEv1 dar. Auf ISAKMP gehen das Zwei-Phasen-Konzept, die Paketformate und die Modi (Main Mode, Aggressive Mode, Quick Mode) zurück, während das Prinzip des Schlüsselaustauschs auf dem Oakley-Protokoll basiert. Der Schlüsselaustausch findet sich in der Key Exchange Payload (KE) innerhalb von ISAKMP wieder.

ISAKMP schreibt kein spezielles Managementverfahren vor, sondern hier wird eine Rahmenstruktur, wie ein Schlüsselmanagement auszusehen hat, spezifiziert. Allerdings werden Paketformate definiert, die als ISAKMP-SA bezeichnet werden. In den Abb. 7.20 bis 7.22 sind drei Zwei-Wege-Verfahren zwischen Host H1 als Sender einer SA und dem Empfänger H2 dargestellt. In allen Schritten (1 - 6) ist stets ein ISAKMP-Header führend vor eine Nutzlast (Payload) gestellt. Eine ISAKMP-Payload wird genutzt, um Schlüssel auszutauschen und Authentifizierungsdaten etc. zu übertragen. Dabei entspricht das Format der Nutzlast ebenfalls einer Rahmenstruktur (Generic Payload Header), die von speziellen Protokollen unabhängig ist.

Abb. 7.25 zeigt einen ISAKMP-Header und exemplarisch drei von derzeit zwölf möglichen Payload-Typen (SA-Payload, Proposal-Payload, Transform-Payload). Dabei werden die verwendeten Payload-Typen nach dem ISAKMP-Header angehängt. Eine Reihenfolge ist nicht vorgegeben, da Identitätsparameter weitergereicht werden.

Beginnend mit dem ISAKMP-Header wird in dem Next-Payload-Feld die darauffolgende Payload benannt, hier z.B. die SA-Payload. Dieses Verfahren zieht sich bis zur letzten Payload durch. Es findet eine Art Verkettung statt. Das Length-Feld im ISAKMP-Header kennt allerdings die Länge der gesamten Nachricht einschließlich aller Payload-Typen, die angehängt wurden.

In den Cookie-Feldern, (H1) und (H2) in Anlehnung an die Abbildungen 7.20 bis 7.22, befinden sich jeweils 64-Bit lange Informationen, z.B. zum Aufbau einer ISAKMP-SA. Das 8-Bit lange Flag-Feld gibt entweder an, ob alle dem ISAKMP-Header folgenden Payload-Typen verschlüsselt sind, oder es wird angezeigt, dass

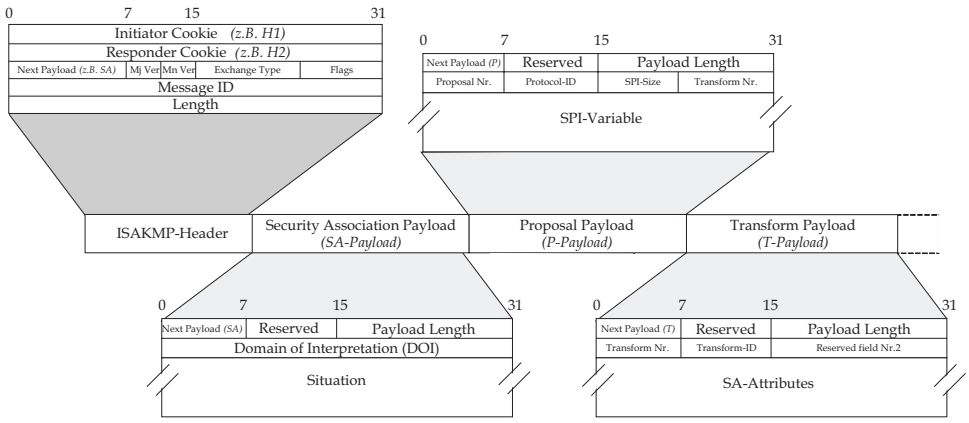


Abb. 7.25: ISAKMP-Header mit drei exemplarisch dargestellten Payload-Typen

erst verschlüsselt wird, nachdem ein ISAKMP-SA vollständig eingerichtet ist. Wird das Authentication-Only-Bit im Flag-Feld gesetzt, kommuniziert dies mit der Status-Information aus der Notify-Payload *(N-Payload)* und zeigt an, dass die ISAKMP-SA integritätsgesichert, jedoch nicht verschlüsselt übertragen werden.

Das Exchange-Type-Feld im ISAKMP-Header-Feld birgt ebenfalls eine Rahmenstruktur, allerdings für die Exchange-Nachrichten. Es werden fünf Exchange-Typen unterschieden, die den Hintergrund zu der Anzahl der auszutauschenden Nachrichten bilden: Base-Exchange, Identity-Protection-Exchange, Authentication-Only-Exchange, Aggressive-Exchange und Informational-Exchange. Für IKEv1 haben sich aus diesen die drei bereits genannten Typen (Main Mode, Aggressive Mode, Quick Mode) entwickelt. So wurde beispielsweise der Main Mode aus der Identity-Protection-Exchange abgeleitet. Eine untergeordnete Rolle spielen die beiden 4-Bit-Felder: MjVer und MnVer, die zur einfacheren Unterscheidung eine Hauptversionsnummer (*Major Version*) und eine Nebenversionsnummer (*Minor Version*) bilden.

Die zwölf möglichen Payloadfelder, die einem ISAKKMP-Header nachgestellt werden können und in ihrer Form einem Generic Payload Header entsprechen, werden nun eingehender beschrieben:

SA-Payload: Die Security Association Payload wird zu Beginn einer ISAKMP-SA eingesetzt. Sie dient der Vereinbarung von Sicherheitsattributen und definiert die Domain of Interpretation (DOI) sowie die Situation, unter der die Vereinbarungen stattfinden. So beschreibt z.B. der DOI-Wert (1), gemäß der IANA Namenskonvention, dass die IPSec DOI zur Anwendung kommt. Im Situation-Field werden Informationen an den Empfänger weitergeleitet, mit denen die Policy abgleichen kann, in welcher Form mit der anfragenden ISAKMP-SA weiter verfahren werden soll [RFC 2407]. Hierzu gehören drei *Sit*-Felder *(Sit_Identiy-Only, Sit_Secrecy, Sit_Integrity)*.

P-Payload: Die Proposal-Payload beinhaltet Protokoll-Informationen, die für eine SA-Vereinbarung benutzt werden sollen: die Proposal-Nr. und die Protokoll-ID, z.B. für IPSec-ESP, IPSec-AH oder auch TLS bzw. OSPF. Ebenfalls übertragen wird der Security Parameter Index (SPI) und dessen Größe sowie die Transformations-Nr. für ein Proposal, da in einer P-Payload dem Empfänger mehrere Proposals angeboten werden können. Z.B. kann in einer P-Payload als Protokoll-1 IPSec-ESP mit der Transform-1 für 3DES und der Transform-2 für DES und im Protokoll-2 IPSec-AH mit der Transform-1 für SHA angeboten werden. Der Empfänger hat somit die Möglichkeit, 3DES und SHA-1-96 oder DES und SHA-1-96 zu wählen.

T-Payload: Die Transform-Payload definiert die Absicherungsart des Kommunikationskanals für das anzuwendende Protokoll. Die Transform-Nr. bezeichnet die in dieser Payload genannten Kombinationsmöglichkeiten des Attributfeldes, z.B. 3DES für IPSec-ESP oder HMAC-SHA-1-96 für IPSec-AH.

KE-Payload: In der Key Exchange Payload sind mehrere unterschiedliche Schlüsselaustauschtechniken gemäß [RFC 2408] zugelassen. So sind z.B. die Oakley-Technik, Diffie-Hellman sowie RSA-Schlüssel möglich. Im Key-Exchange-Data-Field sind alle Daten für einen Session Key enthalten, die für den tatsächlich eingetragenen Schlüsselaustauschalgorithmus erforderlich sind.

ID-Payload: Die Identification-Payload enthält eine IPv4- oder eine IPv6-Adresse und wird genutzt, um die Identität der Kommunikationspartner zu übertragen. In Abb. 7.23 wäre dies die IP-Adresse von H1 und H2.

CERT-Payload: Die Certificate-Payload überträgt das zu nutzende Zertifikat. Es existieren derzeit zehn Zertifikatstypen: PKCS #7 in Verbindung mit dem X.509-Zertifikat, PGP-Zertifikat, DNS Signed Key, Signaturen nach dem X.509-Zertifikat, Schlüsselaustausch nach dem X.509-Zertifikat, Kerberos Token, Certificate Revocation List (CRL), Authority Revocation List (ARL), SPKI Certificate, X.509-Zertifikatsattribute. Zu jedem Zeitpunkt eines ISAKMP-Austauschs muss eine Zertifikatsanforderung möglich sein.

CR-Payload: Sie sollte in einen Austausch eingegliedert werden, wenn kein geeigneter Directory-Server (z.B. Secure DNS) zur Verfügung steht. Auf eine CR-Payload muss der Kommunikationspartner mit einem in der CERT-Payload genannten Zertifikate antworten.

HASH-Payload: Diese enthält Daten der Hash-Funktion, die durch einen ISAKMP-SA-Austausch angefallen sind. Weiterhin kann diese Payload genutzt werden, um die Integrität einer ISAKMP-Nachricht bzw. die Authentizität der Kommunikationspartner sicherzustellen.

SIG-Payload: Die Signatur-Payload enthält Daten, die durch die Signaturfunktion über Teile der ISAKMP-Nachricht gebildet wurden. Mit SIG-Payload kann neben der Sicherstellung der Integrität einer ISAKMP-Nachricht mittels Quittung ein Nachweis *(non-reputation services)* über den Erhalt einer ISAKMP erreicht werden.

NONCE-Payload: Enthält Zufallswerte, um ein Wiedereinspielen *(Replay Attack)* zu unterbinden und um gleichzeitig eine bestehende Verbindung anzuzeigen.

N-Payload: Die Notification-Payload enthält Status- und Fehlerinformationen der ISAKMP-SA bzw. die bei der ISAKMP-Vereinbarung aufgetreten sind.

D-Payload: Die Delete-Payload zeigt an, dass eine oder mehrere ISAKMP-SA nicht mehr gültig ist und aus der Datenbank gestrichen werden kann.

Eine *Security Association* kann nicht nur zur Absicherung des IP-Protokolls genutzt werden, sondern auch, um Host-orientierte Zertifikate der unteren Protokollschichten sowie nutzerorientierte Zertifikate für die Protokollschicht der Anwendungsbene, z.B. E-Mail, Remote-Login oder File-Transfer, zu liefern.

Eine große Stärke von ISAKMP liegt in der Unabhängigkeit gegenüber kryptographischen Algorithmen, Schlüsselerzeugungsmechanismen und Sicherheitstechniken. Dieses Flexibilität wird wie folgt deutlich: Zum einen wird eine dynamische Kommunikation ermöglicht, zum anderen können durch die Technologieunabhängigkeit bei zukünftigen Anforderungen neue Technologien hinzugefügt bzw. alte ersetzt werden. Einen weiteren Vorteil bildet die zweistellige Versionsverwaltung (Mj-Ver., Mn-Vers.), mit der unterschiedliche Versionen auseinander gehalten werden können. Bedauerlicherweise ist eine Versionsverwaltung in die Spezifikation von IPSec bisher nicht eingeflossen.

7.4.13 Das Oakley-Schlüssel-Protokoll (Oakley)

Das Oakley-Protokoll ist ein Schlüsselaustausch-Protokoll, dass den Diffie-Hellman-Algorithmus (Abschn. 4.4.1) anwendet. Darüber hinaus bietet es zusätzliche Sicherungsmöglichkeiten, z.B. durch Cookies, und umgeht so einige Schwächen des Diffie-Hellman-Algorithmus. Häufig werden die Schlüsselaustausch-Serien als *Modes* bezeichnet, die jedoch nicht mit den Modi (Main Mode, Aggressive Mode, Quick Mode) des entsprechenden Feldes (Exchange-Typ) im ISAKMP-Header zu verwechseln sind. Oakley liefert die zweite wichtige Komponente für das IKEv1-Verfahren. Die Spezifikation des Oakley-Protokolls kann im [RFC 2412] eingesehen werden.

Den Oakley-Algorithmus kennzeichnen fünf Eigenschaften:

1. Ein als Cookies bezeichneter Mechanismus verhindert DoS-Angriffe (Denial-of-Service-Angriff). Die Bildung der Cookies erfolgt mittels Hash-Wert über die IP-Adresse des Absenders und des Empfängers sowie über den UDP-Port des Absenders und Empfängers und einem lokal gebildeten geheim zu haltenden Wert.
2. Der Algorithmus erlaubt beiden Kommunikationspartnern eine so genannte Parametergruppe zu vereinbaren. Dies sind spezielle globale Parameter, die beim Diffie-Hellman-Schlüsselaustausch eingesetzt werden.

3. Er nutzt Zufallswerte (Nonce), um ein Wiedereinspielen älterer Pakete zu erkennen.
4. Er initiiert den öffentlichen Schlüsselaustausch beim Diffie-Hellman-Verfahren.
5. Er authentifiziert einen Diffie-Hellman-Austausch, um einen Man-in-the-middle-Angriff zu unterbinden.

Erklärungsbedürftig sind die in Punkt 2 angesprochenen Gruppen für den Diffie-Hellman-Austausch. Jede der Gruppen beinhaltet eine Definition von zwei globalen Parametern (p,g) und eine Kennzeichnung des Algorithmus. Bisher sind fünf Gruppen definiert. Die ersten drei gehen auf den klassischen Diffie-Hellman-Algorithmus zurück und beinhalten für die Primzahl (p) und den Generator (g) den Modulo von mindestens 768 Bit, den Default-Wert von 1024 Bit und ein empfohlenes Maximum von 2048 Bit. Die letzten zwei Gruppen beziehen sich auf elliptische Kurven mit einer Gruppe über 2^{155} mit einem (hexadezimalen) Generator für X=7B, Y=1C8 sowie einem (hexadezimalen) Kurvenparameter (A=0,Y=7338F) und 2^{185} mit einem (hexadezimalen) Generator für X=18 und Y=D und (hexadezimalen) Kurvenparameter (A=0,Y=1EE9). Weitere Details sind im [RFC 2409] zu finden.

Abschließend soll für den verkürzten aggressiven Modus, wie er z.B. in Abb. 7.23 dargestellt ist, das Oakley-Schlüsselaustausch-Protokoll detailliert beschrieben werden (Abb. 7.26).

Erster Schritt: Initiator (H1) schickt einen Cookie (CKY_{H1}) (laut der Ausführung unter Punkt 1), die Gruppe (GRP) und die von Host H1 öffentlichen Diffie-Hellman-Schlüssel. Weiterhin beinhaltet die dem Host H2 angebotene Public-Key-Verschlüsselung (PK^{H1}) einen Hash-Wert und ein Authentifizierungsalgorithmus, der für den Austausch benutzt werden soll $(EHAO)$. Ebenso ist in der ersten Nachricht (1) ein Identitätsmerkmal von H1 und H2 (ID_{H1}, ID_{H2}) sowie ein Zufallswert (Nonce) von H1 enthalten (N_{H1}). Zum Schluss signiert H1 mit seinem privaten Schlüssel die beiden Identitätsmerkmale, den Nonce, die Gruppe, die öffentlichen Diffie-Hellman-Schlüssel sowie den angebotenen Algorithmus $(SK_{H1}[...])$.

Zweiter Schritt : Wenn H2 die Nachricht erhält, wird H2 zunächst die Signatur mittels öffentlichen Schlüssel von H1 verifizieren. Bei Erfolg wird ein entsprechender Cookie (CKY_{H2}) von H2 an H1 (CKY_{H1}) in der Nachricht (2) zurückgeschickt *(Acknowledgement)*. Ebenso werden neben dem selbst erzeugten Cookie die eigenen öffentlichen Diffie-Hellman-Schlüssel (PK^{H2}), der jetzt ausgewählte Algorithmus $(EHAS)$ (dieser muss aus der angebotenen Menge stammen) sowie die beiden Identitätsmerkmale (ID_{H2}, ID_{H1}) und beide Nonce (N_{H2}, N_{H1}) in der Nachricht zurückgeschickt. Abschließend signiert H2 – analog zu H1 in der Nachricht (1) – mit seinem privaten Schlüssel $(SK_{H2}[...])$ die beiden Identitätsmerkmale (ID_{H2}, ID_{H1}), die beiden Nonce (N_{H2}, N_{H1}), die Gruppe (GRP), die beiden öffentlichen Diffie-Hellman-Schlüssel (PK^{H2}, PK^{H1}) und den ausgewählten Algorithmus $(EHAS)$.

Dritter Schritt: Bei Erhalt der Nachricht muss H1 die Signatur mit dem öffentlichen Schlüssel von H2 verifizieren. Die beiden erhaltenen Zufallswerte (Nonce) garantieren, dass nicht ältere Pakete wiederverwendet wurden. Um den Austausch zu vervollständigen, muss H1 mit der Nachricht (3) H2 die Gelegenheit geben, zu überprüfen, ob H1 auch tatsächlich die öffentlichen Schlüssel von H2 bekommen hat.

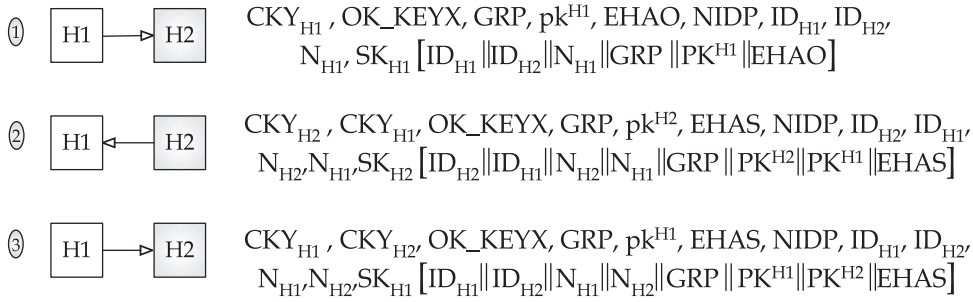


Abb. 7.26: Beispiel eines aggressiven Oakley-Schlüsselaustauschs

7.4.14 IKEv2 - Schlüsselaustausch der nächsten Generation

IPSec und damit auch das Schlüsselmanagement IKE wurde zu einer Zeit entworfen, als ein Fernzugriff (Remote Access) von wechselnden Standorten z.B. über DHCP oder UMTS und ein Network Address Translation (NAT) noch nicht opportun war. Um diesen und weiteren Anforderungen z.B. einer herkömmlichen EAP-Authentifizierung (*legacy authentication*) gemäß [RFC 3748] gerecht zu werden, wurde das Protokoll IKE – genau genommen IKEv1 – überarbeitet. Seit dem Jahr 2001 beschäftigt sich eine spezielle IETF-Arbeitsgruppe mit der Weiterentwicklung von IKE. In mehreren Konsolidierungsrunden wurde ein weitreichender Vorschlag erarbeitet. Damit erlangt die bisher ungenutze Versionierung im ISAKMP-Header (vgl. Abb. 7.25) eine neue Bedeutung. Denn IKE in der bisherigen Entwicklung IKEv1 ist nicht kompatibel zur Weiterentwicklung. In dem IETF-Vorschlag zu IKEv2 wird das RFC für ISAKMP [RFC 2408], für IKEv1 [RFC 2409] und das RFC für die Internet DOI [RFC 2407] mit verarbeitet.

Die Weiterentwicklung zu IKEv2 wird durch den Versionsindex 2 verdeutlicht. Doch gibt es eine Reihe von Gemeinsamkeiten, u.a. dass IKEv2 über denselben UPD-Port wie IKEv1 geführt werden kann. Ein IKE-Dienst[12] muss nun sowohl auf

[12] Als IKE-Dienst wird z.B. Racoon oder ISKAMP auf der UNIX/Linux-Plattform eingesetzt. Auf der Windows-Plattform, wird kein eigenständiger Dienst eingerichtet. Ein Konfiguration geschieht im einfachsten Fall über die Microsoft Management Console (MMC), über die alle erweiteren Einstellungen vorgenommen werden.

den UDP-Port 500 – wie bisher – als auch auf den neu hinzugekommenen UDP-Port 4500 lauschen. Der UDP-Port 4500 ist für gekapselte ESP- und IKE-Pakete reserviert. Einhergehend mit den strukturellen Protokolländerungen hat sich das Vokabular geändert. In IKEv1 wurden die Phasen 1 und 2 definiert. In IKEv2 wird die IKE-Phase-1 durch den initialen Nachrichtenaustausch IKE_SA_INIT und IKE_AUTH sprachlich ersetzt. Die IKE-Phase-2 wird durch den Begriff CREATE_CHILD_SA ausgetauscht. Damit wird den strukturellen Protokolländerungen gleichfalls ein deutliches sprachliches Gewicht verliehen. Als explizites Szenario ist in der Überarbeitung von IKEv2 die Einwahl eines mobilen Endgerätes, das hinter einem Knotenpunkt, der ein NAT durchführt, aufgenommen worden. Mit IKEv2 wird einem mobilen User, der sich in diesem Szenario stationär aufhält, die Möglichkeit eingeräumt, sich über einen Provider bzw. Drittanbieter in das Firmennetzwerk mittels einem gesicherten IPSec-VPN einzuwählen. Dabei können NAT-Barrieren ohne Probleme überwunden werden.

In der Abb. 7.27 ist im oberen Teil der Grafik das Einwahlszenario abgebildet. Im unteren Teil sind die IKEv2-Nachrichten auf der Zeitachse (vertikal) aufgetragen. Dabei handelt es sich um einen prinzipiellen Nachrichtenaustausch, der ggf. durch bestimmte IKEv2-Nachrichten ergänzt werden kann (z.B. NAT Detection, *control message*, Cookies, EAP etc.).

Eingeleitet wird der IPSec-Tunnelaufbau von dem Laptop, der sich über ein öffentliches Netz in das Firmennetz mittels IPSec-VPN einwählen will. Bei der verwendeten Notation entspricht HDR dem IKEv2-Header, wie er in der Abb. 7.28 skizziert ist. Dieser enthält die IPSec SPI's, Versionsnummern und verschiedene Flags. Die SAi1-Payload beinhaltet die kryptographischen Algorithmen, die der Initiator unterstützt. Der Index (i) bezeichnet jeweils den Initiator und (r) entsprechend den Responder. Die KE-Payload beinhaltet die angebotenen Diffie-Hellman-Werte. Mit Ni ist der Nonce bzw. Zufallswert vom Initiator benannt (IKE_SA_INIT_1).

Der Tunnelendpunkt (Responder) antwortet auf die Anfrage, indem ein geeignetes angebotenes kryptographisches Protokoll in der SAr1-Payload zurückgeschickt wird. Es wird weiterhin ein Diffie-Hellman-Wert und ein Nonce (Nr) mitgeliefert. Die in eckigen Klammern angegebenen Payloads sind generell optional; in diesem Fall wird mit [CERTREQ] vom Tunnelendpunkt die Möglichkeit eingeräumt, Zertifikate einzusetzen (IKE_SA_INIT_2).

Zu diesem Zeitpunkt haben beide Seiten genügend Informationen (Schlüsselmaterial), um die nachfolgenden Pakete vertraulich behandeln zu können. Allerdings bleiben die Header (HDR) unverschlüsselt. Durch ein SecureKEYSEED (SK_e, SK_a) – in der Grafik durch SK{...} dargestellt – wird angedeutet, dass die in den Klammern befindlichen Komponenten verschlüsselt sind. Mit der IDi-Payload schickt der Initiator seine Identität dem Tunnelendpunkt. Dieser korrespondiert direkt mit der AUTH-Payload (IKE_AUTH_1).

In der gleichen IKEv2-Nachricht kann wiederum optional ein Zertifikat [CERT] oder eine Zertifikatsanforderung [CERTREQ] geschickt werden. Falls ein Zertifikat [CERT] mitgeschickt wird, müssen in der AUTH-Payload die öffentlichen

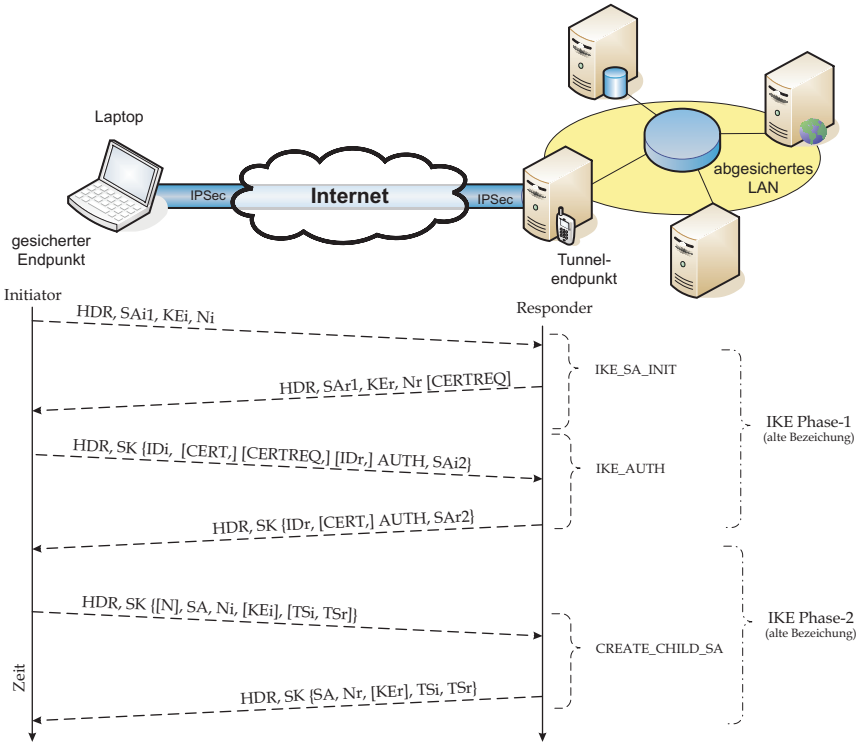


Abb. 7.27: Beispiel eines Remote Access mittels IKEv2 und IPSec-Tunnel

Schlüssel (Public Keys) enthalten sein. Die optionale IDr zeigt die vom Initiator zur Kommunikation erwünschte Identität des Responders an. Diese Eigenschaft ist hilfreich, wenn z.B. der Responder mehrere Identitäten bei gleicher IP-Adresse hat. Für einen Tunnelendpunkt ist dies oftmals der Fall. Den Beginn einer Vereinbarung zur Security Association (SA) wird durch eine SAi2-Payload erreicht. Der Tunnelendpunkt (Responder) antwortet mit der gewünschten IDr, eventuell wird ein Zertifikat mitgeschickt bzw. die öffentlichen Schlüssel des Responders. Damit wird eine Authentifizierung und eine gesicherte Integrität der zweiten Nachricht – durch den Index 2 in der Abb. 7.28 angedeutet – erreicht (IKE_AUTH_2).

Bevor eine CREATE_CHILD_SA initiiert wird, müssen alle Signaturen und Authentifizierungen positiv abgeschlossen sein und die ID-Payloads müssen mit den entsprechenden Schlüssel der AUTH-Payload korrespondieren. Anschließend kann eine CHILD_SA, die wiederum an ein Nachrichtenpaar (request/responds) geknüpft ist, aufgebaut werden. Der Initiator sendet eine IKEv2 Nachricht bestehend aus einem unverschlüsselten Header (HDR) und einer verschlüsselten Payload SK{...}. Neben den optionalen Möglichkeiten Diffie-Hellman-Werte [KEi] mit dem aus den oben bekannten Nonce [N] erneut auszutauschen, werden SA-

Parameter in der SA-Payload verschickt. Die Verkehrsparameter [TSi,TSr] werden über die TS-Payload verschickt. Die TS-Payload erlaubt Endpunkten, Informationen aus den gegenseitigen SPDs auszutauschen. Dies kann beispielsweise in einem Fall zu einer SPD-Konsistenzprüfung führen, in einem anderen Fall zu einem dynamischen Parameteraustausch der SPD. Jede TS-Payload enthält eine Reihe von TS-Parametern (Selektoren), die einen IP-Adressraum, einen Port-Range und eine IP-Protokoll ID bedeuten können. Damit ist eine CHILD_SA erfolgreich aufgebaut und die Kommunikationsverbindung entsprechend den Sicherheitsanforderungen (Policy) des Unternehmens abgesichert. Jetzt kann ein geschützter Datenaustausch beginnen.

An der rechten Seite der Abb. 7.28 sind die neuen (IKEv2) und alten (IKEv1) Bezeichnungen zu sehen. In der IKEv2-Fassung werden die Nachrichten jeweils als Paar aufgefasst und behandelt. So entspricht z.B. das Paar IKE_SA_INIT / IKE_AUTH der alten IKEv1 Phase-1 Bezeichnung. Es werden i.d.R. vier IKEv2-Nachrichten ausgetauscht, die jedoch – wie oben erwähnt – ergänzt werden können. Die alte IKEv1 Phase-2 ist durch die CREATE_CHILD_SA abgelöst worden. Eine CHILD_SA besteht wiederum aus zwei Nachrichten, die bereits durch kryptographische Protokolle gesichert werden.

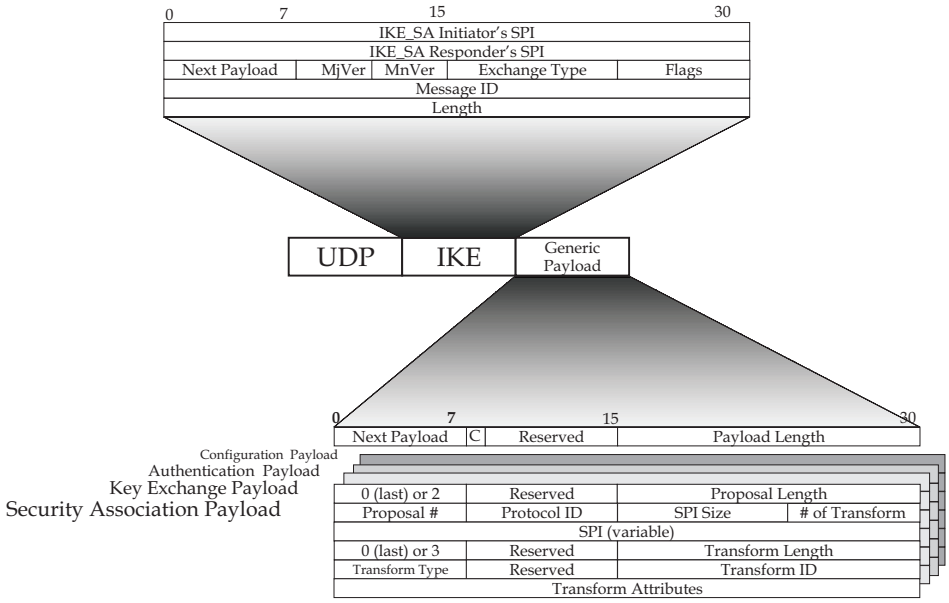


Abb. 7.28: Schematische Darstellung eines IKEv2-Headers gefolgt von einer Generic Payload

In der Abb. 7.28 ist der Protokollaufbau dargestellt. Jede IKEv2-Nachricht beginnt mit einem IKEv2-Header und folgt direkt einem UDP-Header. Im oberen Bildteil ist der IKEv2-Header detaillierter skizziert. Je nach Bedarf und Anforderungen

können verschiedene IKE-Payloads folgen. Dies wird durch die „Next Payload“ angezeigt. Dadurch kann ggf. eine Kette von IKEv2-Paylods entstehen. Die Responder SPI zeigt eine Instanz einer IKEv2-Security Association an und enthält keinen Wert beim initialen Kommunikationsaustausch, wie in Abb. 7.27 angedeutet.

Die Versionsverwaltung hat sich gegenüber ISAKMP nicht geändert. Der „Exchange Type“ hat neben reservierten Werten die Werte 34, 35, 36, 37 für eine IKEV2_SA_INIT, IKEv2_AUTH, CREATE_CHILD_SA und INFORMATIONAL vorgesehen. Das „Flags“ -Feld zeigt eine spezielle Einstellung des „Exchange Type“. Es wird der Initiator und Responder einer Nachricht festgelegt. Damit erfolgt die schon mehrfach erwähnte Paarbildung. Die *message ID* wirkt Wiederholungsangriffen entgegen und kann bei Paketverlusten zu einer eindeutigen Retransmission genutzt werden. Das abschließende „Length“-Feld ist ebenfalls gleich gegenüber ISAKMP geblieben.

In dem unteren Teil der Abbildung ist die generisch gehaltene Payload (Generic Payload) dargestellt. Sie ist generisch, da durch das „Next Payload“-Feld der jeweilige Typ bei immer gleicher Struktur festgelegt wird. Zu sehen ist eine Security Association Payload (SA), die z.B. durch die Kennziffer 33 festgelegt ist. Eine SA beinhaltet Proposals, Transforms und Attribute, wie auch schon unter ISAKMP und IKEv1 bekannt. Jedoch ist die Semantik deutlich unterschiedlich, die Bauweise wesentlich kompakter und übersichtlicher. Die Transform Attribute liefern weitere Einstellparameter für die gewählte Transform.

Eine Zuordnung, welche Payload gerade folgt, wird jeweils durch eine Kennziffer bestimmt. In den Hintergrund versetzt sind weitere mögliche Payloads zur Illustration dargestellt. In der Tabelle 7.3 sind die wichtigsten Kennziffern der Next Payload in einer Generic Payload aufgeführt. Die reservierten und zunächst nicht in Gebrauch befindlichen Werte sind dagegen weggelassen.

Um das Beispiel der Abb. 7.28 und der dargestellten Security Association weiterzufolgen, sei noch ein Blick auf die Transfoms und Attribute gerichtet, um einen Eindruck der Bauweise und Schachtelungsmöglichkeiten von IKEv2 zu bekommen. Die Parametervielfalt innerhalb einer SA wird durch die „Protocol ID“ bestimmt. Es können die Werte 1, 2, 3 angenommen werden, die gleichbedeuten sind mit: IKE, AH, ESP. Die Substruktur eines Proposals äußert sich in der „Transform Type“.

Die möglichen Kennziffern sind der Tabelle 7.4 zu entnehmen.

Exemplarisch sind von den fünf möglichen „Transport Type“ der Tabelle 7.4 nur der Type mit der Nummer 1 in der Tabelle 7.5 aufgelistet. Die „Transform Type“ korrespondiert direkt mit der „Transform ID“.

Es existieren noch eine Reihe weiterer Parameter und Einstellmöglichkeiten für die Generic Payload. Jedoch soll an dieser Stelle nicht weiter darauf eingegangen werden.

Zusammenfassend lassen sich die wesentlichen Merkmale für IKEv2 auflisten:

Tabelle 7.3: Wertemenge der Next Payload in einer Generic Payload

Next Payload Type	Notation	Value
Security Association	SA	33
Key Exchange	KE	34
Identification - Initiatior	IDi	35
Identification - Responder	IDr	36
Certificate	CERT	37
Certification Request	CERTREQ	38
Authentication	AUTH	39
Nonce	Ni, Nr	40
Notify	N	41
Delete	D	42
Vendor ID	V	43
Traffic Selector - Initiator	TSi	44
Traffic Selector - Responder	TSr	45
Encrypted	E	46
Configuration	CP	47
Extensible Authentication	EAP	48

Tabelle 7.4: Wertemenge der Transform Type

Description	Transform Type	Used In
Encryption Algorithm (ENCR)	1	(IKE und ESP)
Pseudo-Random Function (PRF)	2	(IKE)
Integrity Algorithm (INTEG)	3	(IKE, AH, optional in ESP)
Diffie-Hellman Group (D-H)	4	(IKE, optional in AH & ESP)
Extended Sequence Numbers (ESN)	5	(optional in AH und ESP)

Tabelle 7.5: Möglichen Werte für den in Tabelle 7.4 dargestellten Transform Type 1 (ENCR)

Name	Number	Defined In
ENCR_DES_IV64	1	[RFC 1827]
ENCR_DES	2	[RFC 2405]
ENCR_3DES	3	[RFC 2451]
ENCR_RC5	4	[RFC 2451]
ENCR_IDEA	5	[RFC 2451]
ENCR_CAST	6	[RFC 2451]
ENCR_BLOWFISH	7	[RFC 2451]
ENCR_3IDEA	8	[RFC 2451]
ENCR_DESIV32	9	
RESERVED	10	
ENCR_NULL	11	[RFC 2410]
ENCR_AES_CBC	12	[RFC 3602]
ENCR_AES_CTR	13	[RFC 3664]

- IKEv2 zeichnet sich durch eine wesentlich kompaktere Bauweise aus. Dies geschieht zum einen durch den vereinheitlichten Nachrichtenaustausch gegenüber IKEv1, indem eine kompaktere Kennzeichnung bzw. Nummerierung der Proposals und Transforms (vgl. Abb. 7.28) vorgenommen wird. Zum anderen ist die Semantik im Fall der Transforms und bei den Attributen optimiert worden. Einhergehend damit gibt es nur noch einen Austauschmodus und nicht mehr wie bei IKEv1 die Alternative zwischen Main Mode und Quick Mode.
- In Ergänzung zum Public-Key-Verfahren kann eine Authentifizierung mittels EAP durchgeführt werden. EAP ist ein asymmetrisches Verfahren und im Grunde für die Authentifizierung eines Nutzers gegenüber einem Server entwickelt worden. EAP kommt – falls eingesetzt – in dem IKE_AUTH-Austausch (vgl. Abb. 7.27) zur Anwendung. Dadurch wird der IKE_AUTH-Austausch durch ein Drei-Wege-Handshake erweitert. Diese Erweiterung ist in der Abb. 7.27 nicht dargestellt.
- Einer der wohl gravierendsten Errungenschaften in IKEv2 ist die Möglichkeit, nicht mit starren IP-Adressen zu arbeiten, sondern es kann nun eine IP-Adresse aus dem Bereich hinter einem Tunnelendpunkt, also hinter dem NAT liegenden IP-Adressbereich (LAN), angefordert werden.
- IKEv2 ist in der Lage, ein NAT-Traversal durchzuführen. Falls auf einer Seite der Kommunikationsendpunkte ein Network Address Translation (NAT) vorgenommen wird. Bei dem initialen IKEv2-Paketaustausch (IKE_SA_INIT) ist die Möglichkeit durch die Payload (NAT_DETECTION_SOURCE_IP / NAT_DETECTION_DESTINATION_IP) gegeben, ein NAT zu entdecken und entsprechend zu reagieren. Denn wenn der Hash-Wert in der Payload (NAT_DETECTION_DESTINATION_IP) nicht mit der Ziel-IP-Adresse übereinstimmt und außerdem ein Port gefunden wird, so muss es sich um ein NAT handeln. Folglich werden im Rahmen der Verbindung Keep-alive-Nachrichten erforderlich. In diesem Fall ist es dann zwingend, den UDP-Port 4500 einzusetzen. Damit werden alle zukünftige IKE- und ESP-Pakete in der zugehörigen IKEv2_SA über den UDP-Port 4500 getunnelt.
- Ein weiterer gravierender Unterschied zwischen IKEv1 und IKEv2 ist, dass der Gültigkeitszeitraum einer Security Association (SA-Lifetime) ebenfalls nicht mehr starr ist. Beide Kommunikationspartner verwalten diesen Zeitraum getrennt und unabhängig voneinander. Einhergehend damit wird ggf. ein erneuter Schlüsselaustausch *(rekeying)* notwendig.
- Durch die Möglichkeit einer parallelen Einrichtung zweier SA mit dem gleichen Kommunikationspartner (*traffic selector*) kann ein Quality of Service (QoS) gemäß [RFC 2983] erreicht werden. Dies bedeutet, dass z.B. multiple ESP und/oder AH-SA mit einer einzigen IKE_SA eingerichtet werden können.
- IKEv2-Nachrichten sind als Paare (request/response) zu verstehen. Für jede IKEv2-Nachricht ist der Initiator für ein Retransmission sowie für ein Time-out

verantwortlich. Denn IKEv2 ist ein verbindungsorientiertes Protokoll. Dennoch ist vorgesehen, dass ein IKEv2-Endpunkt seinen Zustand z.B. die gerade gültige IKEv2_SA und damit auch eine eventuell zugehörige Child_SA komplett vergisst.

Mit dieser mehr als notwendig gewordenen Weiterentwicklung ist IPSec für die nächste Technologie-Innovationen gut gerüstet. Somit stehen gerade für die mehr und mehr aufkommenden mobilen Anforderungen eine Technologie bereit, die das IP weiterhin absichert. Es zeichnet sich bereits heute sehr deutlich ab, dass in absehbarer Zeit eine vollständige Mobilität eines elektronischen Diensteanwenders möglich sein wird. Es wird zukünftig nicht mehr wichtig sein, in welchem Netz sich der Nutzer gerade befindet. Im Hintergrund regeln Protokolle und Authentifizierungsverfahren die notwendigen Abstimmungen mit den unterschiedlichen Netzen und Providern, wie z.B. WLAN, WIMAX, GPRS und UMTS. IPSec wird jedoch weiterhin eine Hauptrolle in der Absicherung der Netze spielen.

Für die uneingeschränkte mobile Nutzung von Diensten über die Provider-Grenzen hinweg sind neue Authentifizierungsverfahren wie z.B. Diameter (vgl. Abschn. 5.4.8) und IKEv2 ebenso notwendig wie die völlige Standortunabhängigkeit eines Nutzers. Dies kann z.B. auch bedeuten, das sich der Nutzer mit hoher Geschwindigkeit, z.B. in einem ICE der Bundesbahn, bewegt. Um diesen Szenarien gerecht zu werden und beispielsweise einem Nutzer, der in seinem Laptop mehrere Netzwerkkarten (NIC) installiert hat, eine reibungslose geschützte Kommunikation zu liefern, wurde das Mobile IKE-Protokoll (MobIKE Protocol) entworfen.

Im nachfolgenden Abschnitt wird auf diese sich abzeichnende Entwicklung näher eingegangen, um anschließend das Thema IPSec und Wireless LAN (WLAN) zu diskutieren.

7.4.15 IPSec, IKEv2 und Roaming-Verfahren

In dem Abschn. 7.4.14 wurde die Möglichkeit vorgestellt mittels IKEv2 für IPSec eine sichere Kommunikationsverbindung – die durch NAT und durch andere Randbedingungen ergänzt wurden – zwischen zwei stationären Endpunkten aufzubauen. Jetzt wird die zusätzliche Möglichkeit diskutiert, das sich die IP-Adressen während eines eingerichteten IPSec-VPN beliebig ändern können.

Der oben angesprochene Nachteil der starren IP-Adressen wird in diesem Abschnitt diskutiert. Es lassen sich drei Szenarien bilden, die der Forderung nach einer Roaming-Möglichkeit von IPSec mehr als sinnvoll erscheinen lassen. Hierzu ist von IETF ein Vorschlag ausgearbeitet worden, der diesen Forderungen nach kommt. Dreh- und Angelpunkt ist das IKE-Protokoll, das den Anforderungen angepasst werden musste. Das angepasste IKE-Protokoll ist als Mobile IKE, oder kurz MobIKE, benannt worden.

Mobility Szenario

In dem ersten Szenario ist ein mobiler Knoten (*mobile node*, MN) bzw. ein Laptop mittels WLAN über ein Security Gateway (GW) verbunden. Weiterhin könnte das Security Gateway ebenfalls eine Verbindung zu einem Unternehmensnetzwerk, zu einem 3GG Netz (UMTS) oder zu einem anderen Netzwerk, unterhalten. Der initiale IKEv2-Austausch verfolgt den Pfad, der als *old path* bezeichnet wird und über den Zwischenrouter Cross-over Router (CR) bis zum Security Gateway führt. Im oberen Teil der Abb. 7.29 ist die Ausgangssituation illustriert. Da es sich um ein WLAN-Verbindung handelt, wird der alte Access Point als Old Access Point (OAR) bezeichnet. Kennzeichnend für dies Szenario ist, dass ein IPSec-Tunnel zwischen dem Laptop und dem Security Gateway besteht. Der

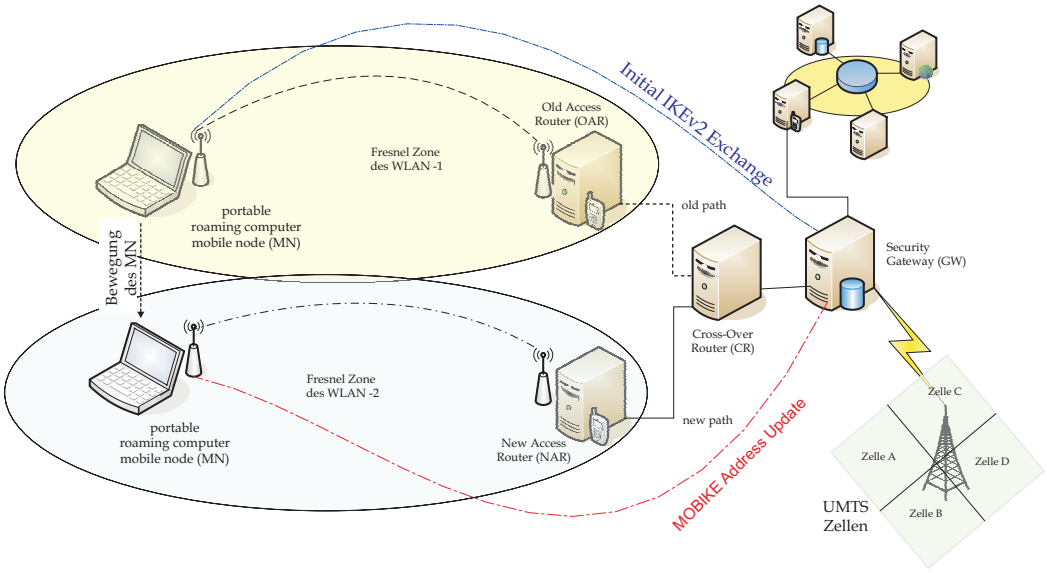


Abb. 7.29: Ein mobiler Knoten bewegt sich zwischen Access Points und weiteren Netzen bei ständiger IPSec-Verbindung

IPSec-Tunnel wird zwar auf dem Security Gateway terminiert, jedoch werden die decapsulierten IP-Pakete an die Zieladresse weitergeleitet. Der Tunnel soll – und das ist die Herausforderung – während des gesamten Szenarios bestehen bleiben und nicht unterbrochen werden.

In dem unteren Teil ist der zweite Teil des Szenarios zu sehen. Der Knoten bzw. Laptop wandert räumlich aus den Empfangsbereich des Access Router hinaus und kommt in den Empfangsbereich[13] eines neuen Access Router (New Access Router, NAR). Dabei erhält der Laptop vom NAR eine völlig neue IP-Adresse, die

[13] Allerdings müssen sich beide Empfangsbereiche über einen gewissen Zeitraum überlappen.

z.B. aus einem anderen Adressraum stammt als die von dem alten Access Router (OAR). Die Aufgabe von MobIKE besteht darin, Sorge dafür zu tragen, dass der IPSec-Tunnel nicht abreißt und von neuem wieder durch ein IKEv2-Austausch aufgebaut werden muss. Diese unterbrechungsfreie Überbrückung von einem Empfangsbereich in den nächsten, so dass dabei die Applikation nicht in Mitleidenschaft gezogen wird, wird oftmals als *Seamless Session* bezeichnet.

Allerdings ist es erforderlich, dass eine Adresserneuerung (MobIKE Address Update) durchgeführt wird. Dabei wird die Adresserneuerung bereits über den neuen Router (NAR) geschickt. Entscheidend für den IPSec-Tunnel und der Aufgabe von MobIKE ist allerdings, dass während sich die Empfangsbereiche noch überlappen, bereits neue Adressen und Informationen frühzeitig ausgetauscht werden. Denn nur so kann ein reibungsloser Übergang erfolgen.

Multihoming Laptop Szenario

Ein anders gelagertes Szenario besteht darin, dass der Laptop zwei Interface-Karten (NIC) besitzt und diese aktiv sind. Die Herausforderung besteht darin, dass sowohl über eine Ethernet-Verbindung – eventuell durch statische IP-Adressvergabe – der Laptop bereits eine IP-Adresse besitzt, als auch über eine Verbindung über die Luftschnittstelle eine IP-Adresse eingerichtet ist. Die Abb. 7.30 stellt dies Szenario dar. Die gestrichelte Linie zeigt die Funkverbindung über die Luftschnittstelle zwischen Laptop (Peer A) und Access Point (Peer B). Über das reguläre Netz (Ethernet) ist Peer (A), dargestellt durch die durchgezogene Linie, über das zwischenliegenden Netzwerk wiederum mit dem Server (B) verbunden, der auch gleichzeitig ein Access Point ist. Weiterhin könnte die WLAN-Karte

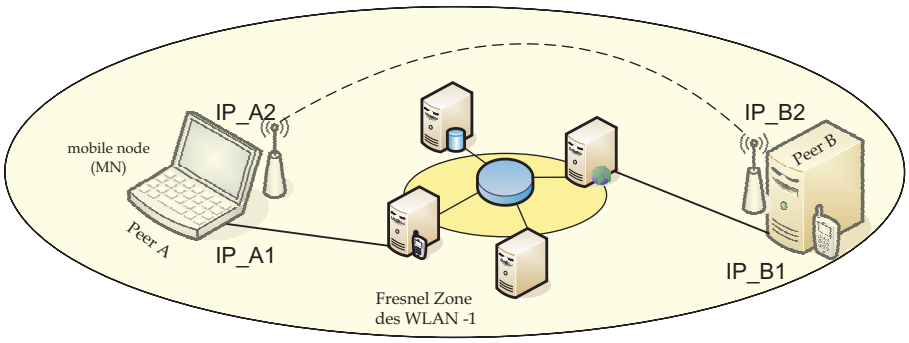


Abb. 7.30: Multihoming Szenario bei mehreren Interface-Karten

oder eine GPRS-Verbindung nicht abgeschaltet sein und über DHCP eine weitere IP-Adresse von dem Server übermittelt bekommen haben. Somit entsteht ein Multihome Peer, der über zwei IP-Adressen mit einem Server verbunden ist.

Realistisch wird dieses Szenario, wenn sich z.B. der Laptop-Nutzer im Büro vom Ethernet Port abkoppelt und während der Fahrt im Bus oder in der Bahn über

eine GPRS-Verbindung weiterhin mit dem Netzwerk des Büros verbunden ist. Zu Hause angekommen, ist der häusliche Access Point der stärkste Sender. Wie im Büro wird eine Ethernet-Kopplung vorgenommen, ohne auf die bestehende aktive WLAN-Verbindung Rücksicht nehmen zu müssen. Somit muss wiederum eine neue IP-Adresszuweisung vorgenommen werden. Entscheidend ist bei diesem Szenario, das der IP-Sec-Tunnel während des Wechsel von einer IP-Adresse zur nächsten, nicht abreißen darf.

Der Nutzer möchte den im Büro etablierten IKE-SA und IPSec-SA zu jeder Zeit aktiv halten, um nicht wieder einen initialen IKEv2-Austausch durchführen zu müssen. Auch in diesem Fall ist ein Seamless Session erwünscht. Dieses Laptop-Szenario könnte verallgemeinert werden, in dem es sich bei den Peers jeweils um zwei Workstations oder Server handelt, die zwei Interface-Karten haben und über ein Netzwerk miteinander verbunden sind. Abb. 7.31 zeigt, wie sich die Szena-

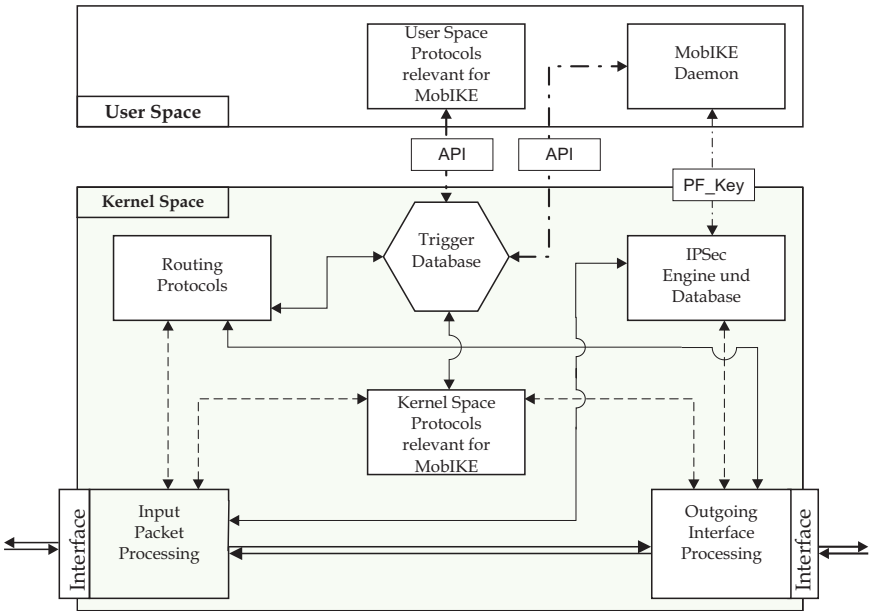


Abb. 7.31: Framework zur Bearbeitung zweier Interface-Karten

rien mit Blick auf das Betriebssystem vom Nutzer aus (*User Space*) und vom darunter liegenden Kernel (*Kernel Space*) aus verhält. Über die Interface – im unteren Teil der Abbildung dargestellt – werden die Datenpakete in das Betriebssystem hinein- und hinausbefördert. MobIKE steht dabei mit der IPSec-Engine in Verbindung und setzt PF-Keys für den initialen Aufbau einer Security Association und Security Policy Database (SPD). Ebenso wird die IPSec-Engine mit IKEv2 und MobIKE interagieren.

Ein herrschender Zustand (aktiver IPSec-Tunnel) hat Auswirkungen auf die ein-

kommenden und ausgehenden Pakete. MobIKE erhält bei diesem Szenario Informationen von anderen Protokollen, die sowohl im User Mode als auch im Kernel Mode arbeiten. Aktuelle Informationen für das MobIKE-Protokoll sind in der dargestellten Datenbank abgelegt.

Mit diesem Vorschlag verfolgt die IETF drei Ziele:

1. Die Möglichkeit, einen Informationsaustausch über die aktuelle IP-Adresse zwischen den beiden Peers einzuräumen.
2. Die Möglichkeit, einen Informationsaustausch über die bevorzugte IP-Adresse eines Peers gegenüber dem anderen Peer einzuräumen.
3. Die Möglichkeit eines Verbindungstests entlang den Routen, um eine Ausnahmesituation zu erkennen, in der dann ggf. in eine gesicherte Rückfallposition gewechselt werden kann.

7.4.16 Zertifikatsbasierte PKI-Authentifizierung für IPSec

In dem Abschnitt über den IPSec-Schlüsselaustausch (vgl. Abschn. 7.4.9) und dem damit verbundenen notwendigen Schlüsselmanagement wurden in der Tabelle 7.2 u.a. Zertifikate nach dem Public-Key-Verfahren aufgeführt. Bisher wurde jedoch auf eine Spezifizierung bzw. Umsetzung sowohl in der Theorie als auch in der Praxis weitgehend verzichtet. Mit diesem Abschnitt wird die in der Tabelle erwähnte zertifikatsbasierte IPSec-Authentifizierung detailliert diskutiert und um eine IETF Spezifikation ergänzt.

Wie eine Zertifikatsverwaltung und ein Public-Key-Management generell agieren und nach welchen Regeln diese funktionieren ist bereits umfassend im Kapitel 4.7 beschrieben worden. Doch bisher hat es kaum bzw. keine Anwendung im Bereich von IPSec-VPN gegeben. Hierfür liegen gute Gründe vor. Zum einen war ein Schlüsselmanagement für IPSec im Fall von Zertifikaten nicht oder nur grob definiert gewesen, zum anderen gab es geeignete Protokolle, die einen Zertifikatsaustausch auf Maschinenebene einfach und effizient vollziehen konnten. Oftmals wurde auch in der Praxis von „Zertifikatsbasierte Benutzer-Authentifizierung ist nur mit aufwändiger und teurer PKI-Software möglich“ gesprochen.

Grundsätzlich ist jedoch die Möglichkeit gegeben, eine IPSec-Authentifizierung mittels X.509-Zertifikaten vorzunehmen. Es liegt der bekannte Patch von A. Steffen[14] vor [Steffen 2002b]. Die Verbreitung von offiziellen X.509-Zertifikaten ist allerdings noch gering. Viele Firmen setzen eigene Certificate Authority (CA) ein. Dabei kommen oftmals selbsterstelle Zertifkate zum Einsatz. Hier hat sich die Zertifikatserstellung gemäß OpenSSL auf der Linux-Plattform weitestgehend durchgesetzt. Eine graphische Oberfläche kann z.B. mit dem auf Perl und

[14] Prof. A. Steffen entwickelte einen Patch, um RSA-basierte Authentifizierung mittels X.509-Zertifikaten vorzunehmen. Eingang hat dieser Patch z.B. in der Linux FreeS/WAN-Plattform gefunden.

GTK-basiertem Werkzeug TinyCA vorgenommen werden. Auf der Serverversion von Windows 2000 ist bereits eine PKI implementiert. Diese kann mittels der Managementkonsole (mmc) durch Laden des entsprechenden Snap-In Module konfiguriert werden [Steffen 2002b].

Als Protokoll zwischen Clients (z.B. Router mit IPSec oder PCs mit Secure VPN-Clients) und einer Zertifizierungsstelle werden typischerweise die PKIX-Protokolle[15] wie in [RFC 2510] und [RFC 2797] beschrieben eingesetzt. Außerdem hat Cisco Systems ein eigenes proprietäres Protokoll entworfen, das einen ähnlichen Funktionalitätsumfang wie die PKIX-Protokolle CMP und CMC hat. Cisco hat diese Alternative *Simple Certificate Enrollment Protocol* (SCEP) genannt. SCEP verwendet für den Austausch der Nachrichten HTTP als Transport-Protokoll. Für die Registrierung bzw. Abfrage von Zertifikaten werden die HTTP Get Messages eingesetzt. Zertifikate sowie Widerrufslisten werden mittels PKCS#7-Formaten ausgetauscht.

Beim Einsatz von X.509-Zertifikaten im Cisco- bzw. Windows-Umfeld kann es zu Fehlkonfigurationen und anderen Problemen kommen. Hier hat sich das Buch von [Aurand 2001] als sehr hilfreich für den Praktiker erwiesen.

Interessant ist die Frage, wie IPSec-VPN z.B. im Bereich eines Extranet eingesetzt werden können, wenn beide Firmen bereits eine Unternehmens-PKI einsetzen. In dem neuen, von Dezember 2004 stammenden Vorschlag der IETF, der sich mit den Anforderungen eines *Public Key Certificate* (PKC)-Management im Zusammenspiel mit unterschiedlichen IPSec-VPN-Produkten und unterschiedlichen PKI-Produkten beschäftigt, könnte die Interoperabilität zwischen unterschiedlichen Herstellerlösungen stark vereinfacht werden. Ziel des Vorschlages ist es, geeignete Schnittstellen und Informationsflüsse zu definieren, um es für Unternehmen einfacher zu gestalten, große und umfangreiche PKI-unterstützende IPSec-VPN zu entfalten. Bei diesen wohldefinierten IPSec-VPN unterstützt eine PKI die Authentifizierung mittels digitaler Signaturen und nutzt beim Aufbau der Security Association das IKE-Protokoll. Die Anforderungen an ein allgmeingültiges PKC umfassen den gesamten Lebenszyklus einer PKI im Zusammenhang mit einer IPSec-VPN-Nutzung: Pre-authentication, PKC-Verteilung, Enrollment-Prozesse (PKC anfordern und zurückziehen), PKC-Erneuerungen, Aktualisieren und Schlüsselerneuerung, Schlüsselzurückziehen, Validierungen und Aktualisierungen der öffentlichen Datenbanken. Damit wird ein VPN-Administrator in die Lage versetzt, dass:

- Authorisierungen entweder direkt oder im Batch-Betrieb von PKC-Erneuerungen, und zwar basierend auf unternehmensspezifischen Richtlinien möglich sind,
- Austeilung von PKI-basierten Identitäten für Nutzer und Computer gleichermaßen, die zu einer IPSec Peer-Instanz gehören. Und dies vor dem Hinter-

[15] Die PKIX-Protokolle gehen auf die Arbeiten der gleichnamigen IETF-Arbeitsgruppe zurück. Diese beschäftigt sich mit der Unterstützung von X.509-basierten PKIs. Dabei werden nicht nur die ITU-Profile behandelt, sondern es werden eigene Standards für das Internet entworfen.

grund einer großen Anzahl von Teilnehmern[16] und IPSec-VPN. Unter dem Begriff Austeilung wird hier die Ausstattung der IPSec-Peers mit gültigen privaten und öffentlichen Schlüsselpaaren verstanden. Dabei wird unter PKC, die von der IETF definierte Public-Key-Technologie und die X.509 v3 (PKIX), die Profile von [CERTPROFILE] und die speziellen Anforderungen von IPSec-PKCs gemäß [IKECERTPROFILE], die für die Tunnelaushandlung im IKE-Protokoll eingesetzt werden (vgl. Tabelle 7.3).

- Einrichten von Sicherheitsrichtlinien und Policys für die korrespondierenden VPN-Gateways oder Nutzer-Authentifizierungen im Fall eines Remote Access (Fernzugriff) und eines Intranet-VPN *(Site-to-Site)*.
- Einrichten von Automatismen für die einfache Verwaltung und Wartung von Zertifikaten (PKC).
- Sicherstellen und zeitlich nahes zur Verfügungstellen von PKC und IKE-Änderungen.

Somit ist ein VPN-Administrator in der Lage, jegliche Konfigurationsmöglichkeiten einer IPSec-Implementierung sowie ein Zertifikatsmanagement mit jeder PKI-Herstellerlösung vorzunehmen.

Abb. 7.32 zeigt eine *Community Realm*, bestehend aus zwei Peerinstanzen im unteren Teil der Grafik. Die graue Einfärbung markiert die Realm. Als Realm wird ein Bereich definiert, der durch eine Policy beherrscht wird. Die Peers sind in diesem Fall zwei Entitys zwischen denen der VPN-Administrator einen IPSec-Tunnel etabliert. Dabei ist die Art der Peer-Kopplung in der Grafik nicht festgelegt. Es kann eine Gateway-to-Gateway-Kopplung genauso wie eine Remote-Host-zu-Gateway-Kopplung sein; oder sogar ein Mix von beiden Möglichkeiten. Die Peers authentifizieren sich gegenseitig durch Anwendung des IKE-Protokolls mittles digitaler Zertifikate, die von ein- und demselben PKI-System stammen. Das dargestellte Framework setzt damit voraus, das alle Komponenten des VPN nur von einer PKC, die zu ein- und derselbem PKI-System gehören, abstammen dürfen. Dies kann bedeuten, das ein IPSec-Peer eine PKC von einer CA akzeptieren muss, die sich ggf. außerhalb seines eigenen PKI-Systems befindet.

Im oberen Teil der Abb. 7.32 ist ein PKI-System dargestellt. Es kann sich um ein öffentliches Trust Center (*managed PKI-Service*) oder um eine PKI handeln, die mit dem VPN-Produkt direkt zusammenhängt. Das PKI-System muss jedoch Mechanismen bereitstellen, die die Aufgaben einer Authorisierungsinstanz für die Administratoren wahrnimmt. Dieser Vorgang wird als RA bezeichnet. Ebenso muss das PKI-System ein geeignetes Repository öffentlich (also im Internet) zur Verfügung stellen, so dass Peer-Instanzen sich über Revokationen von Zertifikaten informieren können. Außerdem ist es erforderlich, dass das PKI-System die

[16] Unter großen Teilnehmeranzahlen werden hunderte oder sogar tausende von gemanagten VPN-Gateways oder Remote-Clients verstanden.

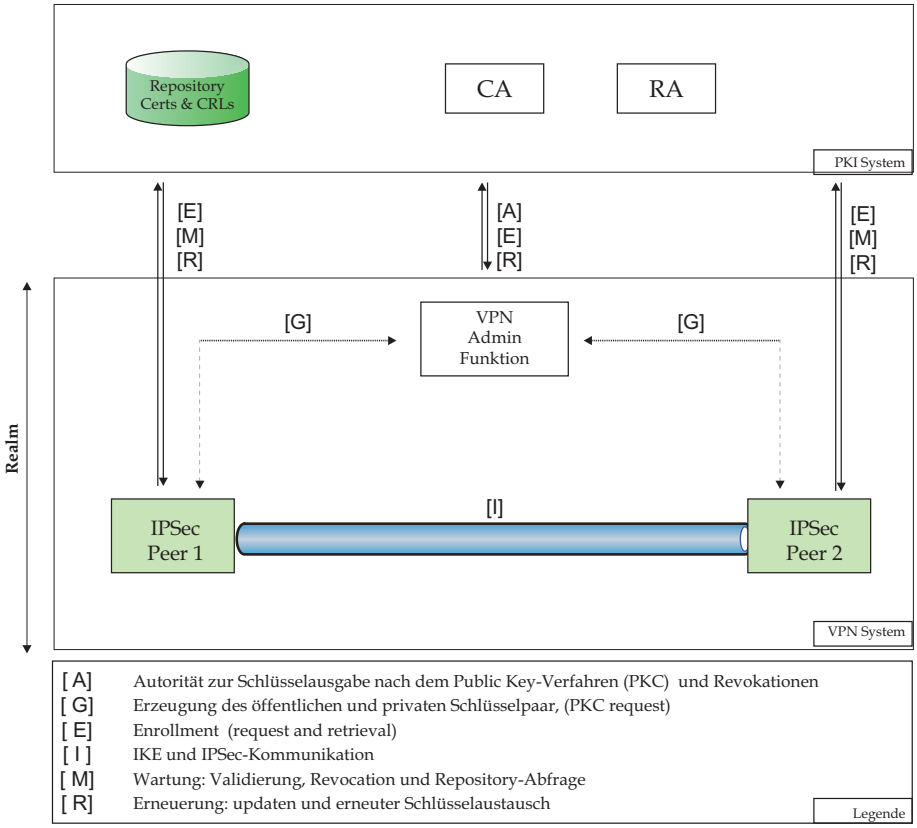


Abb. 7.32: Architektur-Framework für eine VPN-PKI-Interaktion

Kernfunktionalität einer CA leisten kann; also das Erstellen und von privaten und öffentlichen Schlüsselpaaren sowie das Signieren von Zertifikaten.

Dargestellt wird in der Abb. 7.32 der grundsätzliche Aufbau des Frameworks. In der Legende zur Abbildung sind die für die Informationsflüsse verwendeten Buchstaben erklärt. Es wird deutlich, dass es eine Interaktion zwischen allen Akteuren gibt. Aus diesem Framework – und der Gesamtdarstellung – ist nicht so einfach ersichtlich, wie eine spezielle Interaktion aussieht.

Um eine Interaktion exemplarisch herauszugreifen, soll nachfolgend der Informationsfluss in den Schritten von 1 bis 10 zwischen dem Knoten Peer 1, dem Administrator und dem PKI-System illustriert werden. Dabei wird auf die Buchstabenkennung in der Legende der Abb. 7.32 Bezug genommen. Andere Interaktionen können dann nach diesem Vorbild erarbeitet werden.

1. Schritt der Autorisierung [A]. Der Administrator (Admin) übergibt eine Liste von Identitäten (IDs) und Zertifikaten an das PKI-System mit der Bitte um Au-

torisierung der Teilnehmer. Dabei kann die Form der Informationsübergabe der Identitäten auch durch ein auszufüllendes Template, das das PKI-System bereit hält geschehen. Das PKI-System schickt dann eine Liste mit eindeutigen Autorisierungen bezogen auf jeden Teilnehmer (Zertifikatsnummer) und einen One-Time-Token, oftmals als Transportschlüssel bezeichnet, um die Verbreitung (Enrollment) eines jeden Zertifikats sicher zu gewährleisten. Typischerweise wird damit auch gleichzeitig eine Zertifikatspolicy mitgeschickt. In dem in jedem Zertifikat festgesetzt ist, wie lange es gültig ist. Wann die Schlüssel erneuert werden müssen; Schlüssellänge und weitere Parameter sind ebenfalls angegeben.

2. Reaktion auf die Authentifizierungsanfrage [A]. Das PKI-System bestätigt bzw. lehnt die Autorisierung, die im Schritt (1.) angefragt wurde, ab.

3. Schlüsselerzeugung und Zertifikatsanforderung [G] durch den Administrator der Realm. Der Administrator kommuniziert mit dem IPSec-Peer und übergibt dem Peer Informationen, damit dieser ein privaten und öffentlichen Schlüssel erzeugen und ein Zertifikat bei dem PKI-System beantragen kann.

4. Enrollment [E]. In diesem Schritt fordert der IPSec-Peer ein Zertifikat vom PKI-System an und übergibt gleichzeitig seinen erzeugten öffentlichen Schlüssel.

5. Antwort auf die Enrollment-Anfrage [E]. Jetzt reagiert das PKI-System auf den Schritt (4.), indem ein neues Zertifikat ausgestellt wird, andernfalls wird ein Fehler erzeugt und es kommt dann zwangsläufig zum Abbruch der gesamten Anfrage. In diesem Fall muss dann wieder mit Schritt (1.) begonnen werden.

6. Bestätigung des Enrollment [E]. Dies ist die positive Variante des Schritt (5.). Es findet eine Bestätigung statt, indem der IPSec-Peer dem PKI-System gegenüber den Erhalt des neuen Zertifikates bestätigt.

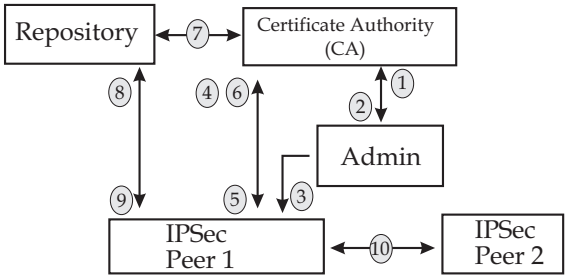


Abb. 7.33: Interaktion zwischen einem IPSec-Peer und einem PKI-System

7. Schritt zur Veröffentlichung der PKC. Das soeben neu erzeugte Zertifikat des IPSec-Peer 1 wird in das Repository überführt und der Öffentlichkeit (Internet) meist in Form eines allgemeinen Verzeichnisses zur Verfügung gestellt.

8. Erhaltung/Betrieb [M]. Im Wirkbetrieb nehmen die IPSec-Peers in regelmäßigen Intervallen Kontakt mit dem PKI-System auf, um Support-Anfragen von anderen IPSec-Peers z.B. Überprüfung von Zertifikaten und Pfadüberprüfungen sowie Revokationen, zu prüfen (CRL).

9. Antwortverhalten im Wirkbetrieb [M]. Das PKI-System antwortet auf die Anfrage (8.) mittels dem gewünschten Zertifikat bzw. mit einer CRL, falls das Zertifikat nicht mehr gültig ist.

10. Letzter Schritt IKE/IPSec-Kommunikation [I]. Damit sind alle notwendigen Schritte ausgeführt, um mit einem unbekannten IPSec-Peer ein vertrauliche VPN-Verbindung mittels Zertifikaten einzugehen.

In dem Ablauf wird deutlich, dass zwei unbekannte Firmen z.B. im Fall eines Extranet mit diesem zweistufigen Verfahren miteineinander ein IPSec-VPN etablieren können. Die Authentifizierung der Peers verläuft über den VPN-Administrator. Doch dieser kann das IPSec-VPN nicht komplett beherrschen, da die eigentlichen Zertifikate vom PKI-System ausgestellt werden und die zugrunde gelegten Schlüssel von beiden Peers selbst erzeugt werden. Damit werden sich zum einen die Public-Key-Infrastrukturen (PKI) weiter etablieren und in naher Zukunft selbstverständlich in der elektronischen Kommunikation werden. Ebenso wird die aufgezeigte Entwicklung die B2B-Kommunikation, weg von Preshared Keys, hin zu Zertifikaten gemäß X.509 v3 führen.

7.4.17 Secure VPN im Wireless LAN (WLAN)

Die Kommunikationstechnologie *Wireless Lokal Area Network* (WLAN), also die über Funkwellen übertragenen Nachrichten im Sinne des OSI-Modells (vgl. Abschn. 2.2.1), ist mittlerweile eine weitverbreitete Technologie. Ihre Vorteile aber auch die Nachteile, gerade im Sinne der Informationsabsicherung, sind hinlänglich bekannt.

Im Kern ist die WLAN-Technologie bzw. Nachrichtenübertragung auf der OSI-Schicht 2, also auf der Data-Link Layer angesiedelt. WLAN ist in dem IEEE 802.11-Standard spezifiziert. Aber auch die zugrunde liegende Bitübertragungsschicht folgt anderen Verfahren als die, die im Ethernet eingesetzt werden. Ethernet ist z.B. ebenso auf der Data-Link Layer durch den IEEE 802.3-Standard spezifiziert. Dies hat einen Autor dazu veranlasst, von einem drahtlosen Ethernet zu sprechen [Nett 2001]. Das Buch von [Nett 2001] lehnt sich an den Standard an und erklärt tiefgehende technische Zusammenhänge. Auch wird die physikalische Ebene nicht ausgespart und die unterschiedlichen Funktechniken wie z.B. FHSS und DSSS werden exakt beschrieben.

Doch gibt es eine Reihe von Unterschieden zwischen den beiden o.g. Standards, also [IEEE 802.3] und [IEEE 802.11]. So werden die möglich auftretenden Kollisionen in beiden Standards unterschiedlich behandelt. Im Fall des Ethernet wird

von Kollisionserkennung (*Collision Detection*) gesprochen und Techniken zur Behandlung von Kollisionen definiert. Beim WLAN wird von Kollisionsvermeidung (*Collision Avoidance*) gesprochen und Techniken zur Vermeidung spezifiziert.

Die WLAN-Technologie kommt sowohl im privaten Umfeld als auch im betrieblichen Umfeld zum Einsatz. Die WLAN-Technologie hat sich innerhalb kürzester Zeit zum Massenprodukt entwickelt. Doch es gibt auch Schattenseiten dieser Technologie, wenn die Vertraulichkeit der Datenübertragung auf der Funkstrecke betrachtet wird. Das im Standard [IEEE 802.11] vorgesehene Verschlüsselungsprotokoll (WEP), das mittels einem statischen Shared-Key-Schlüsselaustausch arbeitet, hat in der Fachwelt heftige Kritik hervorgerufen, da es einige kryptographische Schwächen aufweist [Goldberg 2001]. Zur Absicherung der Funkstrecke sind verschiedene Entwicklungen seit Bekanntwerden der kryptographischen Schwäche zu verzeichnen. Eine Entwicklungsrichtung versucht die Übertragungssicherheit (Vertraulichkeit) durch bessere Schlüsselverfahren zu erhöhen. Es wird sowohl das Schlüsselaustausch-Verfahren, als auch das Verschlüsselungsprotokoll durch andere, z.B. AES, ersetzt. Die andere Entwicklungsrichtung verfolgt – ausgehend von der Überlegung, das das OSI-Modell jeder Schicht eine bestimmte Aufgabe zugedacht hat, eine andere Richtung. Diese Richtung verfolgt konsequent den IEEE 802.11-Standard. Denn die eigentliche Aufgabe der Layer-2 liegt in den fehlersichernden Übertragungsmechanismen, also der Fehlererkennung und -korrektur. Somit hatte das IEEE-Konsortium auch nur eine mit dem Ethernet[17] vergleichbare Vertraulichkeit (*Wireless Equivalent Privacy*, WEP) angestrebt. Im OSI-Modell sind zur Absicherung einer IP-Übertragung eigene Mechanismen vorgesehen. Das Standardverfahren zur Absicherung von IP ist eben IPSec. Damit besteht – wie auch etliche Hersteller umgesetzt haben – die im Sinne des OSI-Modells vorgesehene Möglichkeit, die Verbindung zwischen Funkstation (Access Point) und dem IEEE 802.11-Client mittels VPN abzusichern.

Diese Art der Absicherung bietet gerade für größere Unternehmen einen weiteren nicht zu unterschätzenden Vorteil. Denn wird ein VPN in Verbindung mit einem zentralen Zugriffsserver wie z.B. RADIUS hinsichtlich der Authentifizierung gekoppelt, kann eine zentrale Verwaltung der Zugriffs erfolgen (vgl. Abschn. 5.4.5). Somit muss nicht jeder AP getrennt behandelt werden. Für eine größere Anzahl von APs stieße dieses Verfahren schnell an seine Grenzen. Als Beispiel kann die moderne Lagerverwaltung von Stückgütern (z.B. Autoteile) herangezogen werden, deren Bestand durch Barcode-Informationen mittels entsprechenden Lesegeräten direkt ins angeschlossene SAP-System übertragen wird. Bei Zentrallagern wird schnell eine Fläche erreicht, die eine erhebliche Anzahl von Access Points nach sich zieht.

Vor diesem Hintergrund wird eine Verbindung zwischen Access Point und IEEE 802.11-Client mittels EAP/TLS in Verbindung mit einem RADIUS-Server disku-

[17] So sind auch die Ethernet Frames auf der Layer-2 nicht sonderlich abgesichert. Ein unbefugter Dritter, der Zugriff auf einen Ethernet Port hat, kann sich häufig – bedingt durch das weitverbreitete DHCP – relativ einfach eine Verbindung in einem fremden Netz erschleichen.

tiert. Der 802.1X-Standard, der bereits in Verbindung mit dem SSL/TLS-Protokoll – auch unter dem Namen L2Sec bekannt gewurde – ist bereits in dem Abschnitt 7.2.4 beschrieben worden. EAP/TLS ist zur defacto IEEE 802.11i-Authentisierungsmethode avanciert. Mit IEEE 802.11i wird ein so genanntes *Robust Security Network* (RSN) beschrieben. Vorausgeschickt werden muss, bevor der nachfolgende Betriebsablauf beschrieben wird, dass der 802.1X-Standard drei Rollen definiert. Es werden der *Supplicant* (z.B. WLAN-Funkkarte), der *Authenticator* (z.B. Access Point) und der *Authenticator Server* (z.B. RADIUS) unterschieden. Der Authenticator greift weiterhin auf ein Dual-Port-Konzept zurück. Das Dual-Port-Konzept basiert auf einen unkontrollierten und einen kontrollierten Port.

Der Betriebsablauf für die Einrichtung einer gesicherten Verbindung mittels IEEE 802.11i verläuft grob in drei Phasen (Discovery, Authentication, Key Management) und insgesamt in 7 Schritten. Die Abb. 7.34 illustriert die 7 Schritte, die nachfolgend aufgeführt sind.

1. Der IEEE 802.11i-Client meldet sich über den *Uncontrolled Port* beim Access Point (AP).

2. Der AP schickt Sicherheitseigenschaften an den Supplicant. Dabei blockiert der AP gleichzeitig alle potentielle Anfragen des Clients über den *Controlled Port* (z.B. IP-Requests) hinweg, bis dieser sich am Netzwerk (Server) final angemeldet hat.

3. Der IEEE 802.11-Client meldet sich über seine normale Netzwerkanmeldung (*Network Login*) mit Nutzerkennung und Passwort beim RADIUS-Server an, wobei der Access Point diese Anfrage weiterleitet.

4. Der RADIUS-Server authentifiziert den User. Hierzu wird ein SHA-1-Hash-Paket (*Message Digest*) mit einem zu verschlüsselnden Text (*Challenge Text*) über den Access Point an den Client übertragen (*EAP Request*). Ab jetzt wird das TLS-Protokoll zusätzlich eingesetzt.

5. Der Client sendet seine Antwort (EAP-Response, TLS Client Hello (random_1)) über den Access Point an den Radius-Server. In dem er einen zu verschlüsselnden Text über den Access Point (AP) an den RADIUS-Server sendet (Access Request/EAP-Response TLS Client Hello).

6. Der RADIUS-Server sendet seine Antwort (Access Challenge/EAP-Request) über den Access Point an den Client. RADIUS-Server und Client berechnen den Master Key (PMK), der für die Verschlüsselung eingesetzt wird. Dieser wird unter Einbeziehung des User-Passworts und der Challenge Requests sowie Responses von Client und Server berechnet.

7. Der AP verschlüsselt seinen Broadcast Key mit dem Master Key (PMK) und sendet ihn an den Client. RADIUS-Server und Client haben sich nun wechselseitig authentifiziert und verfügen ebenso wie der Access Point über einen Nutzer- und sitzungsspezifischen Schlüssel.

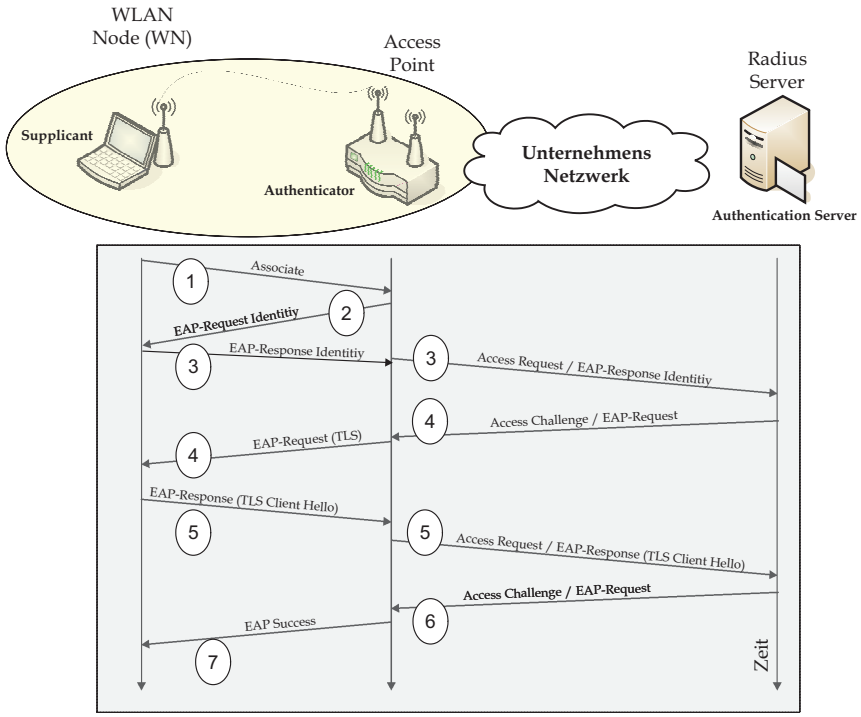


Abb. 7.34: Absicherung einer WLAN-Verbindung mittels EAP/TLS

Über die Möglichkeit von EAP-TLS und einem RADIUS-Server hinaus können umfassende und bereits bestehende Sicherheitskonzepte auf den höheren Protokollebenen (z.B. IPsec) eingesetzt werden. Bei IPSec wird dann auf Zertifikate zurückgegriffen. Dennoch können Wireless-LANs auf der beschriebenen Grundlage der SSL/TLS-VPN zuverlässig abgesichert werden – zumindest was die heutigen Angriffstechniken betrifft.

7.4.18 Das Simple Key Management for Internet Protocol (SKIP)

Mit SKIP existiert ein weiteres Schlüsselverteilungsschema. Es stellt ein vereinfachtes Verfahren dar und wurde bisher von der IETF nicht spezifiziert. Dennoch setzen es Unternehmen vereinzelt ein, da es im Gegensatz zu IKEv1, das Session-orientiert ist, einen packetorientierten Schlüsselaustausch im *In-Band*-Verfahren vornimmt. Somit werden im gleichen Kanal mit den zu sichernden IP-Paketen Schlüsselwechsel vorgenommen.

7.4.19 Layer-2- und Layer-3-Vergleich

Ein tabellarischer Vergleich wesentlicher Unterschiede und Gemeinsamkeiten soll die Betrachtungen zwischen dem Layer-2-Tunneling und dem Layer-3-Tunneling abschließen. Die Tabelle 7.6 listet die Punkte auf.

Tabelle 7.6: Im Vergleich VPN-Techniken der Layer-2 und Layer-3

Eigenschaften	PPTP	L2TP	IPSec	L2Sec
Nutzer-Authentifizierung	Ja	Ja	Nein	Ja
Unterstützung von NAT	Ja	Ja	Nein	Ja
Multiprotokollfähigkeit	Ja	Ja	Nein	Ja
Dynamische Zuweisung von Tunnel-IP-Adressen	Ja	Ja	N/A	Ja
Verschlüsselung	begrenzt	Nein	Ja	Ja
Public Key Infrastruktur	Nein	Nein	Ja	Ja
Überprüfung der Authentizität von Paketen	Nein	Nein	Ja	Ja
Überprüfung von Multicasts	Ja	Ja	Nein	Ja

7.5 Layer-4-Techniken

Zu den wesentlichen Layer-4-Techniken gehören das SSLv3.0- und das TLSv1.0-Protokoll.

7.5.1 Secure Socket Layer (SSL) und Transport Layer-Sicherheit (TLS)

Mit zunehmender Beliebtheit des Internet hat sich eine andere Art, ein VPN einzurichten, durchgesetzt: Die zwischen Browser und Server bestehende HTTP-Verbindung wird kryptographisch abgesichert, um ein Belauschen *(Spoofing)* bzw. Verfälschen von Informationen zu unterbinden und außerdem sicherzustellen, dass nur autorisierte Kommunikationspartner miteinander Daten austauschen. Die für die Anwendungsschicht aufgebaute sichere Client-/Server-Verbindung wird häufig auch als SSL-VPN bezeichnet. Vielfach wird die Diskussion zwischen SSL-VPN versus IPSec-VPN geführt. In dem Abschnitt 7.5.2 werden zu dieser oftmals vehement geführten Diskussion einige Argumente angeführt. Ein nahe liegender Vorschlag, das HTTP-Protokoll abzusichern, ist mit dem *Secure Hypertext Protocol* (S-HTTP) im [RFC 2660] beschrieben worden. Es handelt sich um eine anwendungsspezifische Lösung, die hier nicht weiter verfolgt werden soll. Einen anderen Weg ist die Firma Netscape Communications Corporation gegangen. 1994 entwickelt Netscape, die auch den gleichnamigen Browser herstellt, das *Secure Socket Layer*-Protokoll (SSL). In der Praxis sind die zwei Versionen SSLv2.0 und

SSLv3.0 im Umlauf. Das Ziel, das damals von Netscape verfolgt wurde, galt der Absicherung der Transportschicht, die bis dahin Daten ausschließlich im Klartext über das Netz schickte. Mit SSL war mit der Netscape Technologie eine verbindungsorientierte Ende-zu-Ende-Kommunikationssicherheit (Vertraulichkeit) zwischen einer Browser-Anwendung (HTTP) und einem Webserver möglich. SSLv3.0 ist zwar als Internet Draft bei der IETF eingereicht worden – zum RFC kam es nie – doch bereits im Mai 1997 hatte das Draft seine Gültigkeit verloren, als es den Status *expired* erlangte. Dennoch hat SSL, und zwar gerade die Version SSLv3.0, eine recht große Bedeutung erlangt. Mittlerweile hat die IETF dies erkannt und die grundlegenden Ideen aufgegriffen.

Eine Weiterentwicklung durch die Arbeitsgruppe *(TLS Working Group)* der IETF, die auf der Version SSLv3.0 aufbaute, führte im Jahre 1999 zu einem allgemeinen Standard [RFC 2246]. Dabei kann die erste Version des Transport Layer-Sicherungsprotokoll (TLS) als eine inhaltlich geringfügige Ergänzung zur SSLv3.0 angesehen werden. Insofern ist die TLSv1.0 eigentlich die Version SSLv3.1. Inzwischen liegt ein Überarbeitungsvorschlag in Form des TLSv1.1 der IETF-Arbeitsgruppe vor. Die Anfälligkeit des Protokolls gegenüber Attacken gegen den IV wurde behoben.

Für die Protokolle höherer Schichten ist die Verwendung von SSL/TLS vollkommen transparent, d.h. sie sind komplett unabhängig von SSL/TLS. Doch können vorhandene Applikationen nicht automatisch die SSL/TLS-API anwenden. Es müssen Modifikationen in der Applikation bzw. im Programm (Quelltext) vorgenommen werden. Als Ergebnis einer Implementierung werden der Anwendungsschicht spezielle Funktionen zur sicheren Nutzung der Transportschicht bereitgestellt.

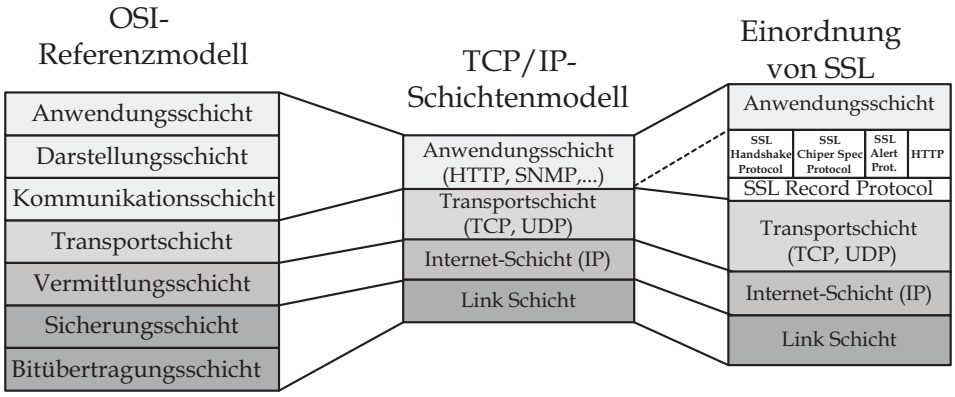


Abb. 7.35: Einordnung der SSL-Architektur im ISO/OSI-Referenzmodell

Neben der kryptographischen Absicherung einer Verbindung zwischen Cli-

ent und Server wird als Ziel die Interoperabilität[18] und offene Weiterentwicklung in Form eines Framework[19] verfolgt. Die SSL-Architektur (Abb. 7.35) sieht vor, dass das SSL-Record-Protokoll eine Grundlagenfunktion wie Vertraulichkeit und Integrität für verschiedene höhere Schichten bereithält, speziell für das Hypertext-Transfer-Protokoll (HTTP). Ergänzend zum SSL-Record-Protokoll werden das Handshake-Protokoll, das Change-Cipher-Spec-Protokoll und das Alert-Protokoll[20] in die SSL-Architektur integriert. Diese drei spezifischen Protokolle sind für das Management eines SSL-Austauschs verantwortlich und oberhalb des SSL-Record-Protokolls angesiedelt. Die zwei grundlegende Konzepte, die SSL-Connection und die SSL-Session, beherrschen eine SSL-Verbindung:

SSL-Connection: Eine Connection ist im Sinne des ISO/OSI-Referenzmodells eine Transportverbindung, die geeignete Dienste bereitstellt. Für eine SSL-Verbindung ist dies eine transparente Punkt-zu-Punkt-Verbindung. Dabei bestimmen mehrere Parameter eine Verbindung. Hierzu gehören die Connection-Kennung, eine Bytes-Sequence, die vom Server und vom Client ausgewählt wird, außerdem geheime Schlüssel (MAC-Secrets), die Server- und Client-seitig für Integritätsüberprüfungen eingesetzt werden, sowie symmetrische Schlüssel, die Server- und Client-seitig (*server write key, client write key*) zur Ver- und Entschlüsselung auf der jeweiligen Gegenseite eingesetzt werden. Weiterhin gehören dazu der Initialisierungsvektor (IV) bei Benutzung einer Blockverschlüsselung im CBC-Modus sowie eine Message-Sequence-Number, denn innerhalb einer SSL-Connection können mehrere Nachrichten (*messages*) die Seiten wechseln. Jede SSL-Verbindung ist an eine SSL-Session gekoppelt.

SSL-Session: Eine Session ist eine Verbindung zwischen einem Client-Browser und einem WWW-Server, die durch das Handshake-Protokoll ausgehandelt wird. Eine Session legt unter anderem die kryptographischen Parameter fest, die für mehrere SSL-Connections gültig sind. Damit wird ein aufwändiges Aushandeln von neuen Sicherheitsparametern bei einem wiederholten Verbindungsaufbau vermieden. Eine Session ist durch sechs Parameter gekennzeichnet: Eine eindeutige Identifikationsnummer (Session Identifier), die aus einer willkürlichen Byte-Sequence vom Server aus erzeugt wird, einem X.509 v3-Zertifikat, das allerdings ungenutzt bleiben kann; ein Algorithmus zur Datenkompression (*compression method*), bevor diese verschlüsselt werden, eine Schlüsselspezifikation (cipher spec.) wie z.B. DES oder NULL Integritätsalgorithmen wie MDS oder SHA-1 ein Session-Schlüssel (Master Secret) für die

[18] Hiermit soll sichergestellt werden, dass Applikationen voneinander unabhängig entwickelt werden können und dennoch einen gesicherten Datenaustausch vollziehen können. Dies wird erreicht, indem kryptographische Parameter ausgetauscht werden, ohne das zuvor der Quellcode der Applikation gegenseitig bekannt sein muss.

[19] Als Framework kann TLS immer an den aktuellen Stand der Technik, z.B. der kryptographischen Protokolle, angepasst werden.

[20] Das Alert-Protokoll hat verschiedene Aufgaben. Zum einen liefert es bei Verbindungsabbrüchen oder -komplikationen in Form von festen Kennungen (*warning, fatal, error*) Informationen. Zum anderen wird ein *close-alert* verschickt, um eine *Truncation Attack* wirkungsvoll zu unterbinden.

Client-Server-Verbindung; ein Flag, der zeigt, ob diese Session für die Initiierung einer neuen SSL-Connection genutzt werden kann oder nicht.

SSL-Record-Protokoll

Bei einem Verbindungsaufbau, der vom Client zum Server initiiert wird, werden die Daten von der Anwendungsschicht gekapselt (*Encapsulation*). Die Daten werden nicht direkt dem Betriebssystem zur Übertragung übergeben, sondern zunächst von der SSL-Schicht bearbeitet. Gemäß dem SSL-Record-Protokoll (Abb. 7.36) werden die Anwendungsdaten, die zum Server übertragen werden sollen, in Blöcke geeigneter Größe fragmentiert, bei Bedarf komprimiert und mit einem Hash-Wert (MAC) versehen. Als MAC kann MD5 oder SHA-1 eingesetzt werden. Anschließend wird eine symmetrische Verschlüsselung nach den Verschlüsselungsalgorithmen der Tab. 7.7 vorgenommen. Einer dieser Algorithmen wird einvernehmlich mit der Gegenseite durch das SSL-Handshake-Protokoll ausgewählt. Damit wird die Integrität für die aufzubauende Verbindung mittels Hash-Wert und die Vertraulichkeit durch Verschlüsselung gewährleistet (Abb. 7.37).

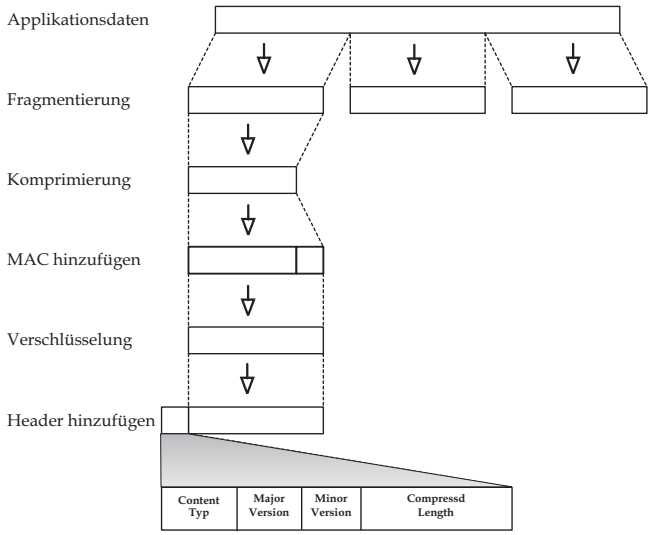


Abb. 7.36: Vorgehensweise des SSL-Record-Protokoll

Es kann eine blockorientierte *Block-Cipher* oder eine kontinuierliche *Stream Cipher* eingesetzt werden. Tab. 7.7 listet die verfügbaren Algorithmen und ihre Schlüssellängen auf.

Der Algorithmus Fortezza wird häufig für Smart-Card-Verschlüsselungen eingesetzt. Bei den stromorientierten Verfahren wird die komprimierte Nachricht und der MAC verschlüsselt. Bei den blockorientierten Verfahren wird je nach Bedarf ein Padding eingesetzt, um eine konstante Byte-Länge zu erzeugen. Als letzter

Tabelle 7.7: Block- und Strom-Chiffren, die beim SSL/TLS-Record-Protokoll verwendet werden können

Block-Chiffre		*Strom-Chiffre*	
Algorithmus	**Schlüssel (Bit)**	**Algorithmus**	**Schlüssel (Bit)**
IDEA	128	RC4-40	40
RC2-40	40	RC4-128	128
DES-40	40		
DES	56		
3DES	168		
Fortezza	80		
AES (TLS)	128		
AES (TLS)	256		

Schritt wird ein SSL-Record-Protokollkopf vorangestellt, wie Abb. 7.36 im unteren Abschnitt zeigt. Abschließend werden die modifizierten Daten dem TCP-Segment zur Weiterleitung übergeben. Der gleiche Vorgang läuft umgekehrt auf der Gegenseite ab, wenn das TCP-Segment Daten empfangen hat. Damit liefert das SSL-Record-Protokoll die beiden für eine SSL-Connection wichtigen Eigenschaften:

Vertraulichkeit: Durch das Handshake-Protokoll wird ein gemeinsamer Sitzungsschlüssel ausgehandelt, mit dem anschließend der dazugehörige Verschlüsselungsmechanismus für die Chiffrierung der Nutzlast (SSL-Payload) eingesetzt, wird.

Integrität: Mit dem Handshake-Protokoll wird ein gemeinsamer Sitzungsschlüssel ausgetauscht, um die Nachricht mit einem Message Authentication Code (MAC) zu versehen.

Das Handshake-Protokoll ist, verglichen mit den übrigen SSL-Protokollen, das Protokoll mit der größten Komplexität. Mit ihm wird eine gegenseitige Authentifizierung sowie Vertraulichkeit und Integrität der zu übertragenden Daten erreicht. Vor der Datenübertragung muss das Handshake-Protokoll vollständig erfolgreich durchgeführt worden sein.

SSL-Handshake-Protokoll

Beim Handshake-Protokoll werden eine Reihe von Nachrichten zwischen Client und Server verschickt. Es können bis zur vier Phasen durchlaufen werden. Oftmals endet jedoch das Handshake nach drei Phasen, und zwar, wenn vom Client keine *change_cipher_spec*-Nachricht in der dritten Phase zurückgeschickt wird. Jede Nachricht beinhaltet ein Typenfeld *(message type)* von 1-Byte, ein Feld, mit der Länge *(length)* der Nachricht (3-Byte) und schließlich ein Inhaltsfeld *(content)* ($\geq$ 1-Byte), in dem Parameter des Typenfeldes weitergereicht werden.

Tab. 7.8 zeigt die unterschiedlichen Message-Type und die dazugehörigen Parameter, die beim Handshake-Protokoll ausgetauscht werden (Abb. 7.37). Um eine

Tabelle 7.8: Unterschiedliche Nachrichtentypen die im SSL/TLS-Handshake-Protokoll während der Phasen zwischen Client und Server ausgetauscht werden

Nachrichtentyp	Parameter
hello_request	null
client_hello	client_version, random, session_id, cipher_suite, compression_method
server_hello	server_version, random, session_id, cipher_suite, compression_method
certificate	RSA, DHE_DSS, DHE_RSA, DH_DSS, DH_RSA, certificate_list
server_key_exchange	DHE_DSS, DHE_RSA, DH_anon
certificate_request	type, authorities
server_done	null
certificate_verify	signature
client_key_exchange	parameters, signature
finished	hash value

logische Verbindung *(SSL-Connection)* aufzubauen, übernimmt das Handshake-Protokoll den initialen Datenaustausch zwischen einem Client und einem Server. Diese Initiierung wird durch vier Phasen erreicht (Abb. 7.37). Die in der Abbildung grau unterlegten Nachrichten in den Identifikationsphasen *(Phase-2, Phase-3)* sind optional. Nachfolgend werden die vier Phasen beschrieben.

Phase-1 / Aufbau / Client Hello Message

In dieser Phase wird die erste Kontaktaufnahme mit dem Server initiiert, um eine Verbindung herzustellen. Damit wird ein IP-Paket, welches als Payload TCP[21] vom Client zum Server gesendet. Zu Beginn werden in einer *client_hello message* die Parameter von Tab. 7.8 zum Server geschickt. Dabei wird mit dem Parameter *(Version)* die höchste SSL-Version, die vom Client verstanden wird, weitergereicht. Um gerade in der sensiblen Anfangsphase des Verbindungsaufbaus ein Wiedereinspielen *(Replay Attack)* zu unterbinden, wird eine Zufallszahl *(random)* mitgeschickt.

Mit dem Parameter *Session Identification* wird eine numerische Identifizierung der Session erreicht. Dabei induziert der Wert (Session-ID$=0$), dass vom Client eine neue Verbindung gewünscht wird. Wird dagegen ein Wert (Session-ID$\neq 0$) als Parameterwert übertragen, wünscht der Client eine Aktualisierung der Parameter bei einer existierenden Verbindung oder eine neue Verbindung innerhalb der Session.

Die kryptographischen Methoden, die vom Client angeboten werden können, werden im Parameter (*cihper suite*) in absteigender Reihenfolge der Bevorzugung weitergereicht. Dabei enthält jede kryptographische Methode der Liste jeweils einen eigenen Schlüsselaustausch-Mechanismus und eine kryptographische Spezifizierung (cipher spec.), auf die später eingegangen wird. Beim Schlüsselaus-

[21] Als Protokoll-Kennung im IP-Header des IP-Pakets ist hierfür die hexadezimale Kennung (0x06) eingetragen. TCP nutzt für den Verbindungsaufbau einen Port größer 1024 (z.B. 1309) auf dem Client-System. Zielport ist jedoch immer 443. Ebenfalls wird die *cipher suite* mit übertragen.

tausch-Mechanismus handelt es sich um eine konventionelle Austauschmethode und um ein Integritätsverfahren (MAC). Bei letzterem sind derzeit nur MD5 mit einer Hash-Größe von 0 und 16 Bytes sowie SHA-1 mit einer Größe von 20 Bytes zulässig. Als Austauschverfahren, die sicherstellen müssen, dass eine Verbindung mit dem gewünschten Server und nicht mit einem eventuell dazwischengeschalteten Server zu Stande kommt, werden die folgenden Verfahren zugelassen:

RSA: Eine als sehr sicher geltende Methode ist das Public-Key-Verfahren, das den Einsatz des asymmetrischen RSA-Schlüsselverfahrens erfordert. Hier wird der geheime Schlüssel mit dem öffentlichen Schlüssel des jeweiligen Kommunikationspartners (Client, Server) verschlüsselt.

Fixed Diffie-Hellman: Eine nicht ganz so sichere Methode ist der Fixed Diffie-Hellman-Schlüsselaustausch, wenn im Serverzertifikat die globalen Diffie-Hellman-Parameter (g, p) von der Certificate Authority (CA) signiert werden. Der Client schickt seine globalen Diffie-Hellman-Parameter entweder in einem Zertifikat, wenn eine Client-Authentifizierung erforderlich ist, oder in der Schlüsselaustausch-Nachricht *(Key Exchange Message)*.

Ephemeral Diffie-Hellman: Diese Technik beinhaltet die Erzeugung von ephemeren, also temporären Einmal-Schlüsseln. Die globalen Diffie-Hellman-Parameter (g, p) werden vom Sender mit seinem privaten RSA- bzw. DSS-Schlüssel signiert. Der Empfänger kann an Hand des öffentlichen Schlüssels des Senders die Echtheit der Parameter (g, p) überprüfen. Der öffentliche Schlüssel wird durch ein Zertifikat abgesichert, mit dem gleichzeitig eine Authentifizierung durchgeführt wird. Dies ist von den möglichen Diffie-Hellman-Verfahren das sicherste.

Anonymous Diffie-Hellman: Hierunter wird das reine Diffie-Hellman-Verfahren verstanden. Die globalen Diffie-Hellman-Parameter (g, p) werden ohne eine Authentifizierung über das Netz geschickt. Der Eingriff eines unbefugten Dritten *(Man-in-the-middle-Attack)* bleibt unerkannt (Abb. 4.10).

Daher ist es empfehlenswert, als Austauschverfahren entweder das RSA-Public-Key- oder das Ephemeral Diffie-Hellman-Verfahren einzusetzen, wenn die Vertraulichkeit und die Integrität beim SSL-Verbindungsaufbau im Vordergrund steht, wie zum Beispiel beim Aufbau einer Homebanking-Verbindung. Allerdings gehören diese beiden Verfahren zu den aufwändigsten, da eine Public-Key-Infrastruktur (PKI) existieren muss und Zertifikate erstellt, verteilt und verwaltet werden müssen.

Mit dem 1 Byte großen Change Cipher Spec-Protokoll, dem einfachsten unter den drei spezifischen SSL-Protokollen, wird eine Kennung innerhalb der *cipher suite* übertragen, welche den zur Verfügung stehenden Verschlüsselungsmethoden (Tab. 7.7) in der *client_hello*-Nachricht angeboten werden. Ebenso wird in dem Protokoll die Art der Verschlüsselung (Block oder Stream), der MAC-Algorithmus (MD5 oder SHA-1), die Hash-Größe, die Größe des Initialisierungsvektors (IV) bei Verwendung des CBC-Modus, ein Flag *(IsExportable)*, das die Werte 0 oder 1

annehmen kann, sowie eine Byte-Sequenz *(Key Material)*, die zur Erzeugung der *Write Keys* verwendet wird, festgelegt. Damit ist die Aufbauphase abgeschlossen und der Client wartet, bis der Server eine entsprechende Antwort schickt. Sollte in der Zwischenzeit ein *Time-out* eintreten, wird die *client_hello*-Nachricht nochmals angeboten bzw. auf dem Bildschirm des Client erscheint eine entsprechende Nachricht.

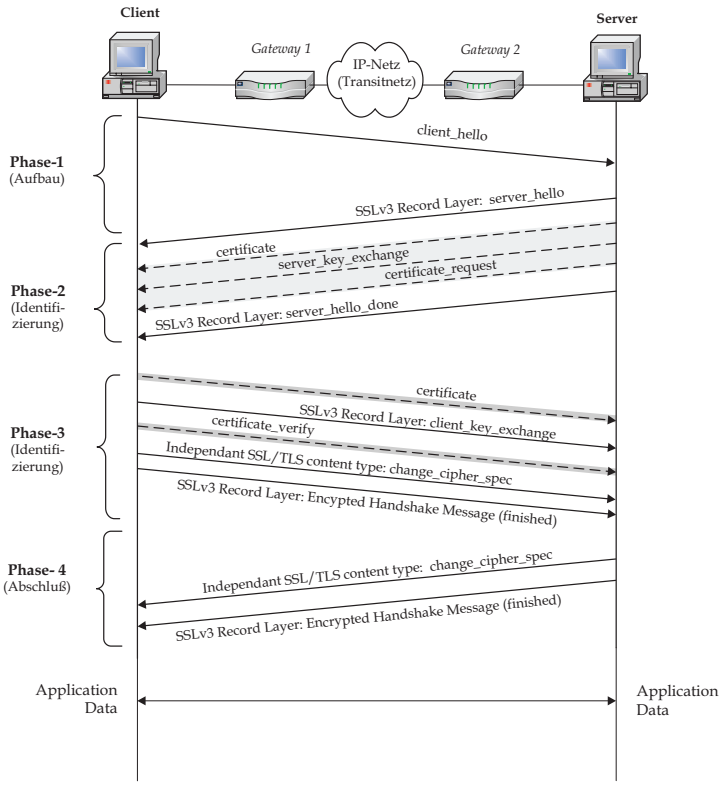


Abb. 7.37: Arbeitsweise des SSL/TLS-Handshake-Protokoll zwischen Client und Server; die grau unterlegten Nachrichten sind optional

Phase-2 / Server-Identifizierung

Der Server sendet nach Erhalt einer *client_hello*-Nachricht seine *server_hello*-Nachricht an den Client zurück. Falls das bevorzugte Austauschverfahren eine Absicherung erfordert, wird ebenfalls die *cipher suite* zurückgeschickt. Die *server_certificate*-Nachricht beinhaltet ein oder mehrere Zertifikate. Sie ist wenn, für alle Austauschverfahren – außer beim Anonymous Diffie-Hellman-Verfahren (DH_anon) – zwingend. Zur Verdeutlichung sind die optionalen Nachrichten in Abb. 7.37 grau unterlegt.

Als nächstes wird, falls erforderlich, die *server_key_exchange*-Nachricht mitgeschickt. Diese Nachricht wird nicht benötigt, wenn entweder der Server Fixed Diffie-Hellman-Parameter oder ein RSA-Schlüsselaustausch verwendet wird. Erforderlich wird die Nachricht beim Anonymous Diffie-Hellman-Verfahren, beim Ephemeral Diffie-Hellman-Verfahren und beim RSA-Schlüsselaustausch, bei dem der Server die RSA-Schlüssel lediglich zur Signierung nutzt. Hier kann der Client nicht einfach die geheimen Sitzungsschlüssel verschicken, die mit den öffentlichen Schlüsseln des Servers verschlüsselt sind, sondern der Server muss ein temporäres Schlüsselpaar (private/public) in der *server_key_exchange*-Nachricht versenden. Diese enthält die beiden temporären RSA-Parameter (*Exponent und Modulus*), versehen mit einer Signatur.

Die *certificate_request*-Nachricht wird von einem *non-anonymous* Server mit den beiden Parametern *certificate_typ* und *certificate_authorities* optional eingesetzt. Für den *certificate_typ* stehen die folgenden *Public-Key*-Algorithmen zur Verfügung:

- RSA, nur als Signatur-Komponente,
- DSS, nur als Signatur-Komponente,
- RSA, für das Fixed Diffie-Hellman-Verfahren, indem die Signatur nur für die Authentifizierung genutzt wird,
- DSS, für das Fixed Diffie-Hellman-Verfahren, indem hierfür nur die Authentifizierung eingesetzt wird,
- RSA, für das Ephemeral Diffie-Hellman-Verfahren,
- DSS, für das Ephemeral Diffie-Hellman-Verfahren.

Der zweite Parameter *certificate_authorities* wird verwendet, um die unterschiedlichen Namen der akzeptierten *certificate_authorities* zu übermitteln. Die letzte *server_done*-Nachricht der Phase-2, die parameterlos ist, ist wieder zwingend und beendet die Phase-2 Server-seitig. Anschließend wartet der Server auf eine Antwort vom Client.

Phase-3 / Client-Identifizierung

Sobald der Client die *server_done*-Nachricht erhält, verifiziert er die Zertifikate und es findet eine Überprüfung der Parameter statt, die mit der *server_hello*-Nachricht mitgeschickt wurden. Treten keine Probleme auf, werden vom Client eine oder mehrere Nachrichten zum Server zurückgeschickt. Falls der Server eine Zertifikatsforderung gestellt hat, sendet der Client eine *certificate*-Nachricht zurück. Kann dem Server kein geeignetes Zertifikat zurückgeschickt werden, folgt vom Client eine *no_certifcate_alert*-Meldung. Regulär (zwingend) wird die *client_key_exchange*-Nachricht zurückgesandt. Der Inhalt hängt entscheidend vom Austauschverfahren ab:

RSA: Der Client erzeugt einen 48-Byte großen Zwischenschlüssel *(Pre-Master-Secret)*, der entweder mit dem Serverzertifikat oder dem temporären RSA-Schlüssel von der *server_key_exchange*-Nachricht verschlüsselt und verschickt wird. Der eigentliche Schlüssel *(Master Secret)* wird von beiden Kommunikationspartnern separat gebildet.

Ephemeral Diffie-Hellman bzw. Anonymous Diffie-Hellman: Hier werden die globalen Diffie-Hellman-Parameter (g, p) geschickt.

Fixed Diffie-Hellman: Die vom Client verschickten, globalen Parameter sind bereits in der *certificate*-Nachricht versenden worden, so dass der Inhalt der Nachricht null ist.

Abschließend kann in dieser Phase optional (grau unterlegt) in Abb. 7.37 die *certificate_verify*-Nachricht zur expliziten Überprüfung des Client-Zertifikats mit zurückgeschickt werden – allerdings nur, wenn das Client-Zertifikat eine Signatur erstellen kann. Außer bei Fixed Diffie-Hellman-Parametern ist dies bei allen Zertifikaten möglich. Die *certificate_verify*-Nachricht erzeugt einen Hash-Wert, dessen Bildung auf eine vorausgegangene Nachricht *(message authentication code)* im SSL-Record-Protokoll (Abb. 7.36) unter Verwendung von MD5 oder SHA-1 zurückgeht. Falls der Client als privaten Schlüssel DSS einsetzt, wird zur Hashwert-Bildung SHA-1 genommen. Bei Verwendung von RSA Schlüsseln wird eine Hashwert-Bildung von MD5 und SHA-1 durchgeführt, um sich Klarheit über den Besitz der privaten Schlüssel des Clients zu verschaffen. Denn auch bei einem Missbrauch des Client-Zertifikats könnte ein unbefugter Dritter diese Nachricht nicht senden. In den überwiegenden Fällen wird hier das Handshake beendet werden, wenn nicht eine optionale *change_cipher_spec*-Nachricht mitgeschickt wird, weil vom Server übermittelte Parameter nicht verarbeitet werden können.

Phase-4 / Außerordentlicher Abschluss (finished)

Diese Phase schließt den sicheren Verbindungsaufbau außerordentlich ab, so dass anschließend die eigentlichen Applikationsdaten an den Server verschickt werden können (vgl. Abb. 7.37 grau unterlegt). Der Client sendet hierzu die *change_cipher_spec*-Nachricht und kopiert kryptographische Spezifikationen in die vereinbarte *Cipher_Spec*. Dabei gehört diese Nachricht nicht zum eigentlichen Handshake-Protokoll, sondern wurde durch das *Change Cipher*-Protokoll in einer früheren Phase entgegengenommen. Nachdem beide Parteien auf dem gleichen Informationsstand angekommen sind, wird die *finished*-Nachricht mit den aktuellen Algorithmen, Schlüsseln und Geheimnissen geschickt. Dabei findet eine finale Überprüfung des Schlüsselaustausches und des erfolgreichen Authentifizierungsprozesses statt. Als Antwort sendet der Server die gleiche Überprüfungsnachricht zum Client.

Unterschiede zwischen SSLv3.0 und TLSv1.1

Wie zuvor ausgeführt, ist der Unterschied zwischen SSLv3.0 und TLSv1.1 marginal. Ob bei einem SSL-Verbindungsaufbau tatsächlich SSLv3.0 oder TLSv1.1 vorliegt, ist dem Versionsfeld des SSL-Record-Protokoll-Header zu entnehmen. Falls

TLSv1.1 vorliegt, ist im *Major-Version-Field* eine 3 und im *Minor-Version-Field* eine 2 eingetragen, bei SSL liegt der gleiche *Major-Version-Field*-Eintrag vor, nur der *Minor-Version-Field*-Eintrag ist 0.

Der wesentliche Unterschied liegt in dem verwendeten MAC-Verfahren und in der Hashwert-Bildung. TLSv1.0 nutzt den HMAC-Algorithmus streng nach [RFC 2104], inklusive der Padding-Bildung – anders SSLv3.0. Es nutzt zwar [RFC 2104], jedoch ist die Padding-Bildung unterschiedlich, denn die Padding-Bytes werden bei SSLv3.0 an den Schlüssel angehängt und es wird keine XOR-Verknüpfung eingesetzt. Folglich ist bei SSLv3.0 die Gesamtgröße der zu übertragenden Daten ein Vielfaches der chiffrierten Blocklänge. Dagegen kann bei TLSv1.0/TLSv1.1 durch Padding ein Vielfaches der chiffrierten Blocklänge (bis maximal 255 Bytes) eingenommen werden. Ist zum Beispiel ein Klartext – komprimiert oder nicht – plus MAC und Padding-Länge 79 Byte lang, kann die Padding-Länge 1, 9, 17, bis 249 Byte lang sein. Diese Variabilität erschwert eine Kryptoanalyse erheblich.

Weiterhin unterscheiden sich die beiden Verfahren im *SSL-Alert-Code*. Bei TLSv1.0/TLSv1.1 werden die gleichen Kennungen wie bei SSLv3.0 benutzt, jedoch wird der *no_certificate_alert* nicht unterstützt. Im Gegenzug hält TLSv1.0/TLS1.1 andere und detailliertere Kennungen (insgesamt 255) parat. Allerdings bietet TLS bei den Client *Certificate Types* weder Ephemerale Diffie-Hellman noch Fortezza an. Ebenso gibt es in der Behandlung der *certificate-verify*- und *finished*-Nachrichten geringe Unterschiede. Gleich sind bei beiden Versionen die Berechnung des *Pre-Master-Secrets*, unterschiedlich jedoch die Ermittlung des *Master-Secrets*.

7.5.2 Vergleich zwischen IPSec und SSL/TLS

Der aktuelle Stand von IPSec basiert auf einer Vielzahl von RFCs. Bedauerlicherweise wird derzeit eine Kompatibilität in Verbindung mit einer ausreichenden Verschlüsselung nicht durchgängig gewährleistet. Ungenaue Definitionen lassen den Herstellern zuviel Freiraum für eigene Interpretationen, die letztendlich zu unterschiedlichen Implementierungen führen. Allerdings ist mit dem jüngst erschienen AES-Protokoll eine Änderung eingetreten. Es ist damit zu rechnen, dass die nächste Generation der IPSec-Geräte (Router, VPN-Gateways, WLAN-Access-Points) im Wesentlichen auf AES setzen.

Um im praktischen Einsatz kompatibel zu sein, reduziert sich oftmals bei IPSec ein mögliches hohes Sicherheitsniveau auf ein geringeres Niveau, wenn unternehmens- und herstellerübergreifend kommuniziert werden soll. Denn der kleinste gemeinsame Nenner DES gilt seit geraumer Zeit als nicht mehr sicher. IPSec ist ursprünglich für einen LAN-to-LAN-Betrieb konzipiert. Ein Anschluss von entfernten Endgeräten mit dynamischen IP-Adressen ans Unternehmensnetz wurde anfänglich nicht berücksichtigt.

Eklatant wird die Unzulänglichkeit von IPSec, wenn beide Kommunikationspartner über Netze kommunizieren, die z.B. das Network-Address-Translation-

Verfahren (IP-NAT) einsetzen. Durch IP-NAT wird der IP-Header verändert, wodurch Probleme mit dem Authentication Header Protocol (AH) entstehen.

Andererseits bietet IPSec eine mittlerweile ausgereifte Protokollfamilie, die eine starke Authentifizierung und hinreichende Verschlüsselungsverfahren unterstützt [RFC 2401 bis RFC 2412 und RFC 2451]. Ebenso ist durch IKEv1 – den zertifikatsbasierten Schlüsselaustausch und -management – eine ideale Ergänzung gelungen. Da IKEv1 auf der Applikationsebene der OSI-Schicht und SSL/TLS auf der Transportebene (Abb. 6.3) eingesetzt wird, könnte der Gedanke aufkommen, dass die gleiche Funktionalität mit SSL/TLS erreicht werden kann. Um diesen Idee weiter zu verfolgen, werden nachfolgend beide Techniken verglichen.

- **Gemeinsamkeiten von IPSec und SSL/TLS:**
  - IPSec (mittels IKEv1) und SSL/TLS bieten eine Client- und Server-Authentifizierung.
  - IPSec und SSL/Tls gewährleisten eine Datenintegrität und -authentifizierung sowie Vertraulichkeit, wenn auch auf unterschiedlichen OSI-Ebenen.
  - IPSec und SSL/TLS können starke kryptographische Techniken zur Verschlüsselung und zur Integrität (Hash-Wert-Bildung) einsetzen. Weiterhin ist eine zertifikatsbasierte Authentifizierung (IPSec/IKEv1) möglich.
  - IPSec und SSL/TLS bieten eine Schlüsselerzeugung und einen Schlüsselwechsel, ohne Schlüssel über das Netz übertragen zu müssen.
- **Unterschiede zwischen IPSec und SSL/TLS:**
  - SSL/TLS ist als API zwischen der Applikations- und der Transportschicht im OSI-Schichtenmodell angesiedelt.
  - SSL/TLS bietet eine Applikation-zu-Applikation-Sicherheit (zwischen Webbrowser und Webserver), IPSec dagegen eine End-zu-Ende-Sicherheit.
  - SSL/TLS schützt den IP-Protokollkopf (Header) nicht. Somit kann ein *Spoofing* und *Session Hijacking* nicht verhindert werden. IPSec hingegen bietet Mechanismen, um den IP-Header zu schützen.
  - SSL/TLS kann, im Gegensatz zu IPSec, den UDP-Verkehr nicht absichern.
  - SSL/TLS arbeitet mittels einer Ende-zu-Ende-Verschlüsselung und nutzt kein Tunnelverfahren. Dies kann zu Problemen führen, wenn das Datagramm z.B. auf Viren hin untersucht werden soll. IPSec bietet mit dem Transportverfahren die Möglichkeit, eine Virenprüfung durchzuführen. Wenn IPSec im Tunnelverfahren eingesetzt wird, entstehen die gleichen Probleme wie bei SSL/TLS.
  - SSL/TLS kann ein NAT und SOCKS überbrücken, um die internen Adressstrukturen zu verbergen. Somit wird ein Konflikt mit privaten IP-Adressen umgangen. IPSec kann im Transportmodus (Ende-zu-Ende) keine NAT-Unterstützung bieten, jedoch kann mit dem Tunnelmodus das

gleiche Ziel erreicht werden, sogar mit einer höheren Sicherheit im Vergleich zu NAT, da ein IPSec-Tunnel üblicherweise verschlüsselt ist.

- Um SSL/TLS auf Applikationsebene zu nutzen, ist eine Modifizierung im Programm (Quelltext) notwendig. Dies kann zu Problemen führen, wenn der Quelltext nicht vorliegt oder keine Zeit zum Austausch zur Verfügung steht. IPSec dagegen ist für die Applikationsebene transparent, Programmänderungen sind nicht notwendig.

SSL/TLS ist sehr gut geeignet, wenn eine einzelne Applikation abgesichert werden soll und diese in einer SSL/TLS angepassten Version vorliegt. Dies kann der Fall sein, wenn eine Applikation im *3-Tier-Client-Server*-Konzept realisiert worden ist und Web-Application-Gateways an der Netzgrenze installiert wurden. Hierzu zählen etliche Homebanking-Lösungen, auch Internet-Bestellshops sind häufig mit einer SSL/TLS-Lösung ausgestattet. Wenn mehrere Applikationen abgesichert werden sollen, ist es einfacher, nicht jede Applikation abzusichern, sondern eine Absicherung auf Netzebene mit IPSec durchzuführen.

Bei einer Individualentwicklung der Applikation bietet IPSec eine gute Lösung, da IPSec sehr flexibel und in mancherlei Hinsicht anpassbar ist (Verschlüsselungsverfahren, Kombinationen von Authentifizierung und Übertragungsmodus (Tunnel/Transport) etc.). Letztendlich ist die Wahl der Absicherung vom Geschäftsmodell abhängig. Sollte der Applikationsserver eine öffentliche und schlecht abgrenzbare Zielgruppe ansprechen, ist eine HTTP-basierte Technologie, abgestützt auf SSL/TLS, die bessere Wahl. Ist jedoch ein begrenzter Teilnehmerkreis mit schon vorhandenen unterschiedlichen Applikationen oder abgesicherten Einzel-Netzwerken zu untersttzen, ist ein IPSec-VPN oder ein auch auf Layer-2-Tunneltechniken basiertes VPN die bessere Technologie. Ein prominentes Beispiel ist das Branchennetz der Automobilindustrie ENX (Abb. 1.4).

7.6 Layer-5-Techniken

7.6.1 SOCKS v5

SOCKS v5 ist das von der IETF mit dem [RFC 1928] eingeführte Standardprotokoll zum sicheren Passieren einer Firewall und es gehört zu den IP-basierten Weiterleitungsdiensten. Verfahren zum Passieren einer Firewall werden als Gateways bezeichnet. Es existiert das *Application Level Gateway* und das *Circuit Level Gateway*. Ein Circuit Level Gateway stellt z.B. bei einer Ende-zu-Ende-TCP-Verbindung, die eine Firewall passieren soll, zwei TCP-Verbindungen her. Die eine (innere) TCP-Verbindung reicht von der Firewall ins Firmennetz bis zu dem Server, zu dem die TCP-Verbindung aufgebaut werden soll; die andere TCP-Verbindung reicht von der Firewall bis zum entfernt gelegenen TCP-Nutzer – üblicherweise in einem Rechnersystem außerhalb des Firmennetzes. Innerhalb der Firewall zwischen beiden TCP-Verbindungen können je nach Einstellung verschiedene Prüfungen der

eintreffenden oder der verschickten TCP-Pakete vorgenommen werden. Als ein Beispiel für ein Circuit Level Gateway kann eine SOCKS-Implementierung nach [Koblas 1992] erfolgen. Dabei benötigt SOCKS v5 als Client-/Server-Anwendung die folgenden Komponenten:

- einen SOCKS-Server, der auf dem Firewall-System installiert und aktiviert ist,
- die SOCKS-Client-Library, die auf dem internen Computer hinter der Firewall installiert ist,
- spezielle *(socksified)* Versionen der Standardprogramme wie z.B. von Telnet und FTP. Dabei erfordert die Implementierung des SOCKS-Protokolls eine Re-Compilierung und Verlinkung des Quell-Programmcodes der TCP-basierten Client-Anwendungen, um die speziell gekapselten Routinen der SOCKS-Library ansprechen zu können.

Beim TCP-Verbindungsaufbau eines TCP-Clients wird eine Verbindung zum SOCKS-Server von außen über den TCP-Port 1080 zur Firewall aufgebaut. War der Aufbau erfolgreich, werden noch Authentifizierungsverfahren durchlaufen. Anschließend wird eine Verbindung vom SOCKS-Server zum Client geschaltet.

In Kombination mit der Secure Socket Layer (SSL) bildet die SOCKS-Technologie die Grundlage für den Aufbau hochsicherer VPN, die mit jeder Firewall kompatibel sind. SOCKS v5 arbeitet auf Schicht 5 des ISO/OSI-Referenzmodells. Aus diesem Grund bietet es weit bessere Kontrollmöglichkeiten als Protokolle, die auf tieferen Schichten arbeiten, da mehr Informationen über die laufenden Anwendungen zur Verfügung stehen. SOCKS v5 richtet zwischen einem Client und einem Anwendungsserver einen temporären Kanal *(Virtual Circuit)* auf einer *Session-by-Session*-Basis ein. Es unterstützt eine starke Zugriffskontrolle und Nutzer-Authentifizierung, ohne dass eine Anwendung neu konfiguriert werden muss.

SOCKS v5 identifiziert einzelne Benutzer und leitet den gesamten Datenverkehr über eine Firewall. So ist es möglich, die Zugriffsrechte innerhalb des VPN für jeden Benutzer individuell zu konfigurieren, ohne neue Anwendungen extra anpassen zu müssen. Durch die Ansiedlung in Schicht 5 des ISO/OSI-Basisreferenzmodells sind SOCKS v5 und SSL in der Lage, mit VPN-Protokollen niedrigerer Schichten, wie z.B. IPv4, IPSec, PPTP und L2TP zusammenzuarbeiten. Als nachteilig beim Einsatz von SOCKS v5 erweist sich die geringe Durchsatzgeschwindigkeit. Alle Daten, die die Firewall passieren, müssen über den SOCKS-Server geleitet werden; gleiches gilt für Programme auf den Endgeräten, die innerhalb des VPN einen Verbindungsaufbau durch die Firewall ermöglichen.

7.7 Übungen

1. Welche Schutzeigenschaften bietet IPSec einem IP-Datagramm?

2. Welches sind die Aufgaben von IKE und ISAKMP und worin liegen ihre Unterschiede?
3. Warum ist IPSec respektive eine SA an eine IP-Adresse gebunden?
4. Welches sind die Eigenschaften und die Unterschiede zwischen IKEv1 und ISAKMP bei einem IPSec-VPN?
5. Wie wird eine EAP-Authentifizierung bei IKEv2 durchgeführt und wie erweitert sich das IKE_ATUH-Protokoll in der Abb. 7.27?
6. Was ist der Unterschied zwichen einer Domain und einer Realm?
7. Erläutern Sie den Begriff Seamless Session im Zusammenhang mit IKEv2 .
8. Welche Probleme gibt es bei IKE im Zusammenhang mit einem Remote-Access-Verfahren noch, außer NAT-Traversal?
9. Welche Aufgabe hat das Cipher spec-Protokoll im Rahmen des SSL-Handshake bei einem SSL-VPN?
10. Welche Rolle spielt das SSL-Alert-Protokoll bei einem SSL-VPN und wie wirkt es sich auf eine bestehende SSL-Verbindung aus?
11. Wann kommt es bei dem regulären Drei-Wege-SSL/TLS-Handshake zu einem (außerordentlichen) vierten Nachrichtenaustausch?

8 Trusted VPN

Weitverkehrsnetze (WAN) können eine Ausdehnung von 1.000 km oder 10.000 km haben und bieten damit eine Grundstruktur für die VPN-Technologie zur (vertraulichen) Distanzüberbrückung zwischen Firmennetzen *(LAN-to-LAN-Kopplung)*. Eine für Firmen/Anwender ganz entscheidende Frage der Übertragungsraten hat sich in den letzten Jahren äußerst positiv entwickelt. Waren Anfang der 90er Jahre noch Übertragungsgeschwindigkeiten von 64 kbit/s Stand der Technik, sind mit ISDN 2 Mbit/s und über E3-Verbindungen sogar 34 Mbit/s möglich. Durch die Nutzung von ATM können dem Anwender heute bereits Datenraten von 155 Mbit/s oder auch 622 Mbit/s zur Verfügung gestellt werden.

Als WAN-Techniken sind die Datenpaketvermittlungsnetze nach X.25 und ISDN sowie die Technologien FPS, SDH (Synchronous Digital Hierarchy) und ATM zu nennen. Im Vordergrund steht hier die FPS-Technologie und ihre Anwendung bei der Frame-Relay-Technologie sowie ATM, die für die virtuellen Netze eine große Rolle spielen (vgl. Kap. 9).

Erwähnenswert ist der heute noch grundsätzliche Unterschied zwischen der LAN- und der WAN-Welt, der zumindest bei den Ende-zu-Ende-VPN mit berücksichtigt werden muss. Der Unterschied dieser beiden Welten wird durch das OSI-Referenzmodell (Abb. 2.2) deutlich. Während in der LAN-Technologie die Ziel- und Nutzinformationen in einer Dateneinheit transportiert werden, werden sie in vermittelten Netzen völlig getrennt geführt. Daher müssen bei verbindungslosen Netzen die zu übertragenden Ziel- und Nutzinformationen bis einschließlich Layer-3 interpretiert werden. Oft reicht dieses für eine Weiterleitung nicht aus, da die Layer-3 keine Ende-zu-Ende-Sichtweise in verbindungslosen Netzen erlaubt. Somit muss fast immer die Layer-4 mit berücksichtigt werden, in der diese Endsystemverbindungen existieren. Hier hat sich einheitlich die TCP/IP-Protokollfamilie durchgesetzt. Dabei gehört IP zur Layer-3 und TCP zur Layer-4. In verbindungsorientierten Netzen wird dagegen, wie in den nachfolgenden Abschnitten weiter ausgeführt, *nur* die Signalisierung bis einschließlich Layer-3 interpretiert, während die reinen Nutzdaten nur innerhalb Layer-1 weitergeleitet werden. Damit findet eine strikte Unterscheidung zwischen Signalisierungsweg und Nutzweg statt.

Bei einem Trusted VPN setzt der Kunde sein ganzes Vertrauen auf die Zuverlässigkeit seines Providers. Kein anderer außer der Provider selbst kann einen Pfad innerhalb eines VPN einrichten oder wieder aufheben. Dabei hat niemand außer dem Provider Zugriff auf die Daten im VPN und kann diese ändern, anpassen oder löschen. Ein Trusted VPN ist allerdings mehr als nur ein virtueller Pfad durch ein Netz. Denn Kunde und Provider arbeiten eng zusammen. Beide kennen gegenseitig ihre Erwartungen und Ansprüche. Typischerweise wird ein Routing

und eine Adressierung im Vorfeld zur Einrichtung eines VPN vorgenommen. Obgleich sich mehrere Kunden die virtuellen Pfade in einem Trusted VPN teilen, ist jedoch jedem Kunden ein spezieller virtueller Pfad zugeordnet.

8.1 VPN und Multiprotocol Label Switching

Der MPLS-Standard beschreibt die derzeit jüngste Entwicklung in der kontinuierlichen Evolution der Multi-Layer-Switching-Technologie. Im Kern wird eine Verknüpfung des Label-Swapping-Paradigmas mit der traditionellen Routing-Technologie vorgenommen. Denn nur ein hybrides Netzwerk ist in der Lage, beide Technologien zu vereinigen.

Damit wurde ein langwieriges Problem gelöst, das sich mit folgender Frage umreissen liess: „How to make IP and ATM interoperate? “Die IETF und das ATM-Forum hatten sich diese nicht einfache Frage zur Aufgabe gemacht und im Laufe der Zeit mehrere Standards, wie z.B. IP over ATM [RFC 1577, RFC-2225] oder auch MPOA *(Multiprotcol over ATM)*, entwickelt. Doch erst mit MPLS ist die Antwort durch die Kombination der Vorteile der Layer-2 *(Data-Link Layer)* mit denen der Layer-3 *(Network Layer)* zufriedenstellend gelungen.

Historisch gesehen reicht die MPLS-Entwicklung bis in die Mitte der 90er Jahre zurück. Es wurde ein effizienterer Weiterleitungsmechanismus gesucht, nachdem sich die herkömmlichen Router in den immer schneller werdenden Datennetzen zu klassischen Engpässen entwickelten. Ausgehend von der Überlegung, IP-Router durch IP-Switches zu ersetzen, wurden mehrere ähnliche Lösungsvarianten entworfen. Die bekanntesten sind das *IP-Swichting* von Ipsilon, der *Cell-Switching-Router*-Ansatz von Toshiba, das *Tag Switching* von Cisco und der *IP-Navigator* von Lucent/Ascend. Alle genannten Entwicklungen haben eines gemeinsam: sie benutzen ein sogenanntes *Label Swapping* oder auch *Label Switching* zur Weiterleitung der Daten.

In den nächsten zwei Abschnitten werden die beiden für MPLS elementaren Transportmechanismen, die Routing- und die Switching-Technologie, als Basistechnologien eingehender diskutiert.

MPLS und Routing-Eigenschaften

IP-Pakete enthalten einen Protokollkopf mit speziellen Informationen, mit denen es möglich ist, Pakete durch IP-Netze zu leiten. Dies sind in der Regel die Quell- und die Zieladresse *(source address, destination address)*. Damit basiert diese Technologie auf dem traditionellen Datagramm-Routing-Mechanismus. Der Weiterleitungsmechanismus wird durch das *Hop-by-Hop*-Verfahren bestimmt. In jedem Router wird neu entschieden, in welche Richtung das Paket als nächstes geschickt wird *(next hop)*. So gelangt das IP-Paket von der Quell- zur Zieladresse. Die Datagramm-Routing-Technologie, die in IP-Netzen genutzt wird, basiert auf dem Ziel-Routing-Paradigma. Damit wird ein Paket *individuell* durch ein Netz geleitet und

folgt keinem voreingestellten bzw. vordefinierten Weg. Kennzeichnend für dies Verfahren ist der *verbindungslose* Zustand [Comer 1995].

Router tauschen Informationen gesteuert durch Tabelleneinträge mit ihren in direkter Verbindung stehenden Nachbarn aus. Handelt es sich um Router innerhalb desselben Autonomen Systems (AS), wird ein *Interior Gateway Protocol* (IGP)[1] genutzt. Handelt es sich dagegen um einen Router, der im benachbarten Autonomen System platziert ist, kommt ein *Exterior Gateway Protocol* (EGP)[2] zum Einsatz.

Ein Beispiel: Ein Router (A) unterhält mit drei angrenzenden Routern (B, C, D) eine Verbindung über eine Indextabelle (Abb. 8.1). Router (C) hat zwei direkte Nachbar-Router (A, D), so dass Router C mindestens zwei Tabelleneinträge benötigt.

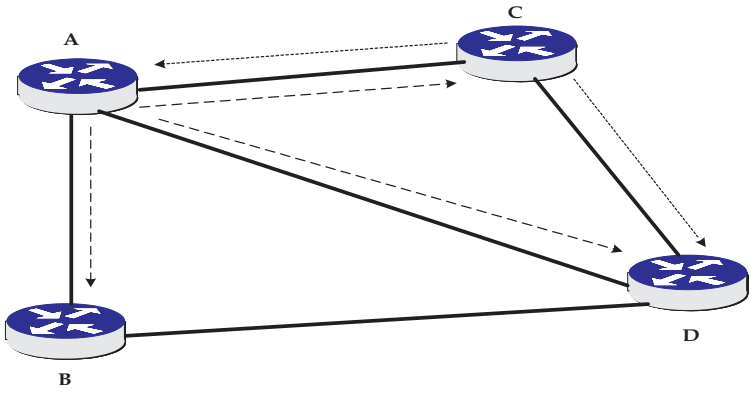


Abb. 8.1: Informationsaustausch zwischen Routern mittels OSPF

Um für eintreffende Pakte z.B. beim Router (A) geeignete Nachbarn *(next hop)* für den Weg parat zu haben, kursiert im Netzwerk ein Protokoll, das über die aktuelle Netztopologie informiert. Das Inter-Domain-Routing-Protokoll *Open Shortest Path First* (OPSPF) ermöglicht Routern, ihre Tabelleneinträge zur Weiterleitung über angrenzende Router stets aktuell zu halten. Dabei wird allerdings nur der IP-Präfix statt der ganzen IP-Adresse gespeichert. Dennoch ist der Weiterleitungs-

[1] Das Interior Gateway Protocol ist ein Routing-Protokoll innerhalb einer Routing-Domain/-Area. Typische IGP sind OSPF (Open Shortest Path First), IS-IS (Intermediate System to Intermediate System) und RIP (Routing Information Protocol). Diese Protokolle sorgen dafür, dass sich die Router in einer Domain/Area untereinander kennen und automatisch Routing-Informationen miteinander austauschen. Zusätzlich besitzen sie einen Routing-Discovery-Algorithmus, um sich gegenseitig zu finden und kennen somit die ganze Netztopologie.

[2] Im Gegensatz zu den IGP verbindet ein Exterior Gateway Protocol mehrere Routing-Domains miteinander. Ein typischer Vertreter ist das Border-Gateway-Protokoll (BGP), das allerdings ausschließlich Informationen weiterleitet, ohne einen Routing-Discovery-Algorithmus zu besitzen. Die Beziehungen zum Nachbarrouter werden manuell erstellt.

mechanismus auf der Layer-3 für die Router ein zeitraubender Prozess[3], der auch in geschickter Kombination von Hard- und Softwareausstattung der Router nicht wesentlich verbessert werden konnte. Zu diesen Erkenntnissen gelangten Netzbetreiber und Firmen mit eigenem Backbone schnell. Die hohen Kosten für High-Speed-Router und die mangelnde Zuverlässigkeit der Performance-Bestimmung, die ein stark vermaschtes Netz nach sich zieht, wenn es nach den traditionellen Routing-Konzepten aufgebaut ist, ließen sie nach neuen Möglichkeiten suchen, die in der Switching-Technologie gefunden wurden.

8.1.1 MPLS und Switching-Eigenschaften

Die Switching-Technologie ist im wesentlichen durch die ATM- und Frame-Relay-Technologie aufgekommen. Beide Technologien nutzen dabei einen völlig anderen Weiterleitungsmechanismus, der stark mit dem Label-Swapping-Algorithmus verknüpft ist. Der Algorithmus ist derart einfach, dass er in Hardware vollzogen werden kann, und somit ein wesentlich besseres Preis-Leistungs-Verhältnis gegenüber traditionellem IP-Routing erreicht.

ATM (Abschn. 8.4), und Frame Relay (Abschn. 8.3), sind verbindungsorientiert, so dass zwischen zwei Endpunkten eine relativ starre Verbindung aufgebaut wird, auf der anschließend ein Datenaustausch erfolgt. Eine Verkehrssteuerung über vordefinierte Wege erleichtert ein Netzwerkmanagement wesentlich und deshalb wird der Kernbereich *(core)* von großen umfangreichen Netzen inzwischen vornehmlich mit einer Switching-Technologie ausgestattet.

Der Eingangsbereich wird jedoch weiterhin vom Routing-Verfahren dominiert (Abb. 8.2). Um dennoch eine Verbindung zwischen entfernt gelegenen Routern z.B. (A) und (D) zu erreichen, entstand mit der Zeit eine IP-basierte Overlay-Technologie, welche auf die Kernnetze (ATM, Frame Relay) aufgesetzt wurde. Diese Overlay-Strategie erweitert damit die Vorteile des Switching-Bereiches auf das gesamte Netzwerk. Werden Verbindungsstrecken zwischen entfernt gelegenen Routern nach dieser Strategie aufgebaut, erfolgt eine Verbindung im Kernbereich über Switches, die zwar eine starre Verbindung nach sich ziehen, jedoch wesentlich einfacher in der Wartung und Betreuung sind.

8.1.2 MPLS und das $n(n-1)/2$ Problem

Die Umsetzung einer Overlay-Strategie gemäß obiger Beschreibung zieht einige erhebliche Nachteile für das Gesamtnetzwerk nach sich. Falls ein IP-Netzwerk als Overlay auf den Switching-Komponenten aufgesetzt wird, wie z.B. bei einem ATM-Netzwerk, scheinen alle Router untereinander direkt verbunden zu

[3] Für CPU-basierte Routersysteme bedeutet ein IP-Forwarding eine Verzögerung von ca. 700-800 μs. Beim Durchlaufen mehrerer Router addieren sich die Verzögerungszeiten (Latenz) entsprechend. Erst die neu aufkommenden ASIC-basierten Routersysteme entschärfen dieses Problem etwas, da die IP-Paketanalyse Hardware-basiert abläuft und nur noch ca. 6-7 μs benötigt.

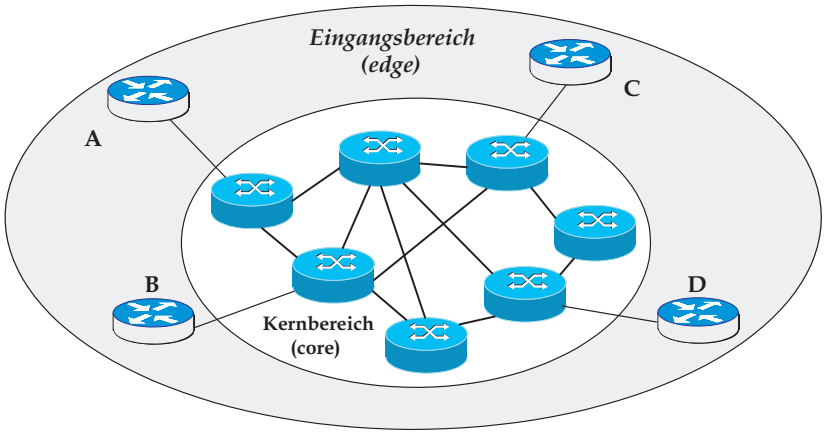


Abb. 8.2: Kern- und Eingangsbereich mit unterschiedlichen Weiterleitungsmechanismen

sein. Damit fordert ein Overlay-Modell, dass jeder Router seine angrenzenden Router über die Tabelleneinträge kennt. Folglich müssen *alle* Verbindungen zu den Nachbarroutern mittels Virtual Circuits (VC) realisiert werden (Abschn. 8.4). Abb. 8.3 zeigt einen Zustand der Vermaschung mit vier Routern gemäß einem Overlay-Modell. Hier benötigen die vier Router schon sechs VC. Wird nur ein

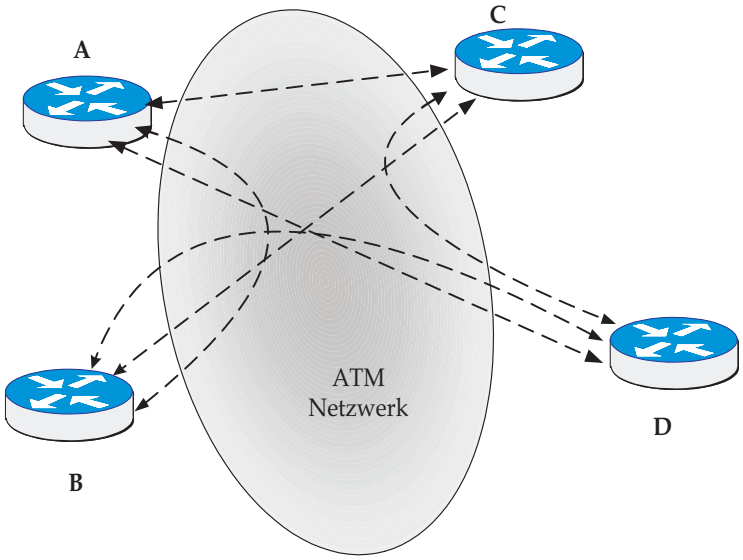


Abb. 8.3: Vermaschung von vier Routern mittels Virtual Circuits

einziger Router hinzugefügt, werden für diese fünf Router schon zehn VC erforderlich. Somit wächst die Vermaschung eines ATM-Netzwerks überproportional im Verhältnis zur Zunahme der Router. Genau genommen wächst die Anzahl der VC im Netzwerk, wenn n Router hinzugefügt werden, in dem Verhältnis von

$$VC = n(n-1)/2 \tag{8.1}$$

Allgemein wird dieses Phänomen das n^2-Problem genannt, das bei einer Vielzahl von Abhängigkeiten auftritt, wie z.B. in der Kryptographie, wenn verschiedene symmetrische Schlüssel zwischen unterschiedlichen beteiligten Partnern ausgetauscht werden.

Für ein Netzwerk zieht eine quadratische Zunahme von VC neben den erheblichen Problemen des Netzwerkmanagements eine erhebliche Skalierungseinschränkung nach sich.

8.1.3 MPLS als Königsweg für Quality of Service in VPN

MPLS ist eine Technologie, mit der sich komplexe vermaschte Virtual Circuits, wie in Abb. 8.3 dargestellt, für einzelne VPN umgehen lassen. Tausende von Multi-Service-VPN können auf einer schon vorhandenen Technik äußerst flexibel aufgebaut werden, ohne die Transportverfahren ATM oder Frame Relay nutzen zu müssen. Im Bedarfsfall können diese jedoch auch mit MPLS zusammen eingesetzt werden. Damit trägt diese Technologie erheblich zur Leistungssteigerung von Weitverkehrsnetzen bei und erweist sich als ideales Mittel, sowohl um den stark anwachsenden IP-Verkehr zu bewältigen, als auch Dienstgüten in IP-Netzen bereitzustellen. Die technische Basis von MPLS beruht auf einem Label-basierten Weiterleitungsmechanismus, mit dem das herkömmliche zeitaufwändige Weiterreichen der Datenpakete im Hop-by-Hop-Routing vermieden wird. Die Router kontrollieren anhand einer Label-Switching-Tabelle nur noch das Label und nicht mehr das Gesamtpaket.

Die eingesetzten Labels entsprechen speziellen Protokollköpfen (Header), die sowohl Routing- als auch Service-Attribute beinhalten. Die Zuordnung eines Datenpaketes zu einem Datenstrom *(Stream)* wird bei MPLS nur *einmal* durchgeführt, und zwar bei Eintritt am *ingress device* in das MPLS-Netz. Wird ein Datenpaket zum nächsten Knoten gesendet, wird ein Label mit bestimmten Wegeinformationen mitgeschickt. Dadurch entfällt beim nächsten Knoten die aufwendige Analyse der Layer-3-Information[4]. Das Label wird als Tabellenindex genutzt, in dem werden der nächste Knoten *(core LSR)* sowie ein neues Label erstellt. Das alte Label wird ersetzt und das Datenpaket zum nächsten Knoten geschickt. Am Ende

[4] In traditionellen verbindungslosen IP-Netzwerken wird in jedem Netzknoten eine Layer-3-Bearbeitung vorgenommen, um den nächsten Hop in der für die Zieladresse geeigneten Richtung vorzunehmen. Dies erfordert einen Vergleich der im Protokollkopf befindlichen Zieladresse mit der im Router gespeicherten Routing-Tabelle und führt zu einer intensiven CPU-Belastung des Routers. Bei jedem auf dem Weg liegenden Router wird dieser Vorgang wiederholt.

des MPLS-Netzes *(egress LSR)* werden die eingehenden Labels aus den Datenpaketen herausgefiltert und das Paket zur Weiterleitung ausgeliefert. Durch die

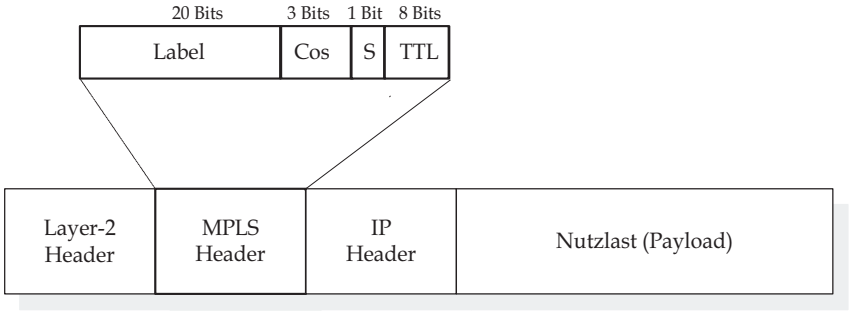


Abb. 8.4: Der 32-Bit MPLS-Protokollkopf

Definition des gleichen Weges für alle Pakete eines Datenstroms liegt bei MPLS, ähnlich wie bei ATM, eine verbindungsorientierte Übertragung vor. Damit existiert die wesentliche Voraussetzung für ein effektives Verkehrsmanagement und eine definierte Dienstgüte.

Das MPLS-Label, früher von der Firma Cisco als *Tag Switching* bezeichnet, ist wie in Abb. 8.4 als Zwischen-Header implementiert. Dieser befindet sich 32 Bit umfassend zwischen dem Layer-2-Header (Ethernet, Frame Relay, FDDI, ATM-Zellen) und dem Layer-3-Header (IP, IPX, AppleTalk). Dabei bezeichnet das 20-Bit-Label-Feld den aktuellen Wert des MPLS-Labels. Das sich anschließende CoS-Feld kann zur Festlegung des Warteschlangenverhaltens und einer notwendigen Paketentsorgung in einer Überlastsituation genutzt werden. Das 1 Bit lange S-Feld *(Stack-Field)* dient zur hierarchischen Kennzeichnung des Label-Stacks, da in einem Paket eines MPLS-Netzes mehr als ein Label enthalten sein kann. Ein Label-Stack arbeitet nach dem *Last-in-First-out*-Modell. Das abschließende TTL-Feld *(Time-To-Live-Field)* wird, wie in herkömmlichen IP-Netzen, zur Beschränkung der Paketlebenszeit eingesetzt.

Die IETF hat im [RFC 3036] ein Protokoll zur Beantragung von Tags und deren Änderungen unter dem Namen *Label Distribution Protocol* (LDP) spezifiziert. Einen gesamten Überblick über die MPLS-Architektur liefert [RFC 3031]. Dabei charakterisiert der Satz *„Route at the edge, switch in the core"* am besten das grundlegende Verfahren. Die Definition eines Label Switched Path (LSP) in einem MPLS-Netz setzt die Bestimmung des Weges und die des verwendeten Labels fest (Abb. 8.5).

Streng genommen liefert MPLS allein noch keine QoS-Eigenschaften. Erst in Verbindung mit IP-Switch-Geräten der nächsten Generation und modernem Traffic Engineering sowie der MPLS-explicit-Routing-Möglichkeit (CR-LDP, RSVP-TE) entsteht die richtige Mischung, mit der sich QoS-Eigenschaften garantieren lassen. Aufgrund der einschneidenden Verbesserungen für Backbone-Router haben

viele Netzwerkbetreiber bereits MPLS und MPLS-VPN im Einsatz. Denn MPLS verschiebt den Skalierungsaufwand von den Kernroutern in den Randbereich, so dass diese im Kernbereich nur noch die Labels betrachten müssen.

Neben dem extra für MPLS spezifizierten Traffic Engineering Protocol, dem Label Distributed Protocol (LDP) mit dem zusätzlichen Constraint Based Routed Label Distribution Protocol (CR-LDP), wird das erweiterte Ressource Reservation Protocol (RSVP-TE) für die Reservierung von Netzwerkressourcen in MPLS-Netzen eingesetzt.

Über die Vor- und Nachteile beider Protokolle werden derzeit noch Diskussionen geführt. So bevorzugen einige Hersteller RSVP-TE, andere hingegen das CR-LDP.

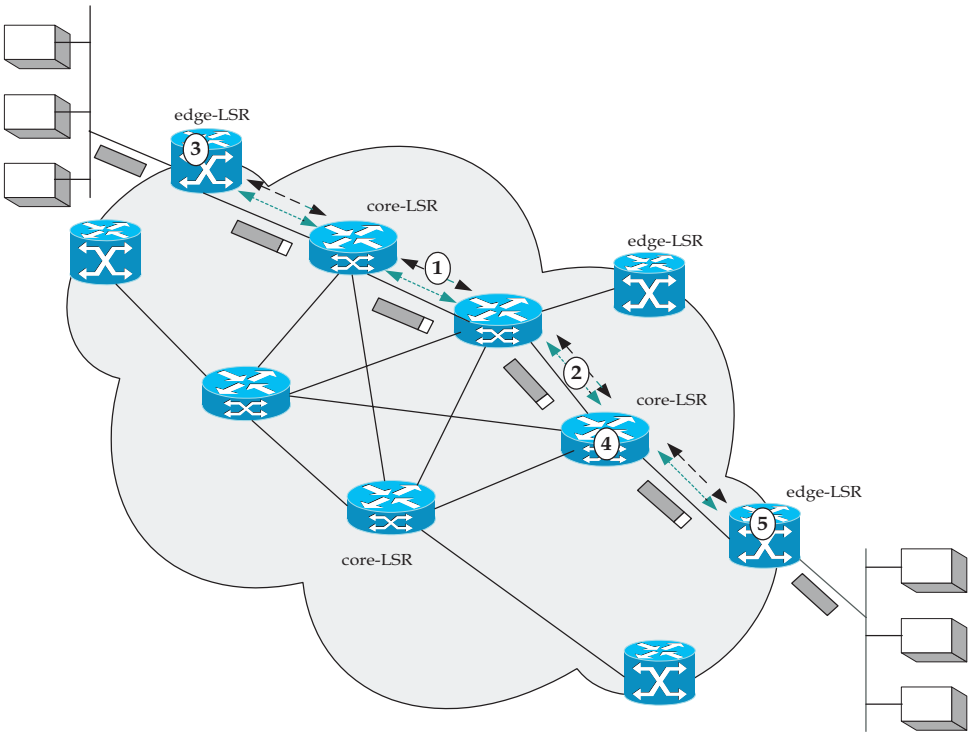


Abb. 8.5: Im MPLS-Netz werden die Pakete anhand der Labels weitergeleitet

Unter Traffic Engineering versteht man die Fähigkeit, in Abhängigkeit von den verfügbaren Ressourcen, geeignete Wege durch das Netz zu suchen. Bereits bestehende Verbindungen lassen sich bei Bedarf dynamisch auf andere physikalische Strecken verlegen (Re-Routing) und höher priorisierte Datenströme können bestehende Verbindungen verdrängen. Dieser Mechanismus macht MPLS zu einer Technik, die anwachsende IP-Ströme schnell durch große Netze leiten kann und das Netz dabei gleichmäßig auslastet. Traffic-Engineering-Parameter können

in einem MPLS-Netz mit den Protokollen IBGP-TE, ISIS, OSPF-TE verschickt werden.

Abb. 8.5 zeigt, wie in einem MPLS-Netz – oft auch als MPLS-Domain bezeichnet – mit einem ankommenden Datenstrom verfahren wird. Dabei ist im Vorfeld, wie in umfangreichen Netzen üblich, eine Einteilung nach Dienstklassen erfolgt, da die Zusicherung einer Ende-zu-Ende-Dienstqualität nicht für jeden einzelnen Datenstrom zu realisieren ist. Datenströme mit vergleichbaren Übertragungsanforderungen werden in geeigneten Klassen zusammengefasst *(aggregation)*. Sie werden als *Forward Equivalence Classes* (FEC) bezeichnet. Die Zusammenfassung von Datenströmen *(Stream Merging)* stellt einen unschätzbaren Vorteil hinsichtlich einer Netzskalierbarkeit dar und ist eine herausragende Eigenschaft von MPLS, die allerdings nur richtig zur Entfaltung kommen kann, wenn die darunterliegende Transportplattform dies zulässt (Abschn. 8.3.1 und 8.4.4).

Nachfolgend wird, in Anlehnung an Abb. 8.5, in vier Schritten beschrieben, wie eine Paketweiterleitung in einem MPLS-Netz vollzogen wird.

Schritt 1: Das MPLS-Netzwerk erzeugt automatische Einträge in den Routing-Tabellen der MPLS-fähigen Router bzw. in den IP+ATM-Switches mittels einem der gängigen Interior Gateway Protocols. Der Label Switched Path (LSP) nutzt die Routing-Topologie der Tabellen, um Labels zwischen benachbarten Routern (devices) in der MPLS-Domain zu erzeugen. Dieser Vorgang generiert LSP bzw. vorgezeichnete Wege zwischen den vorhandenen Endpunkten. Anders als bei den von ATM eingesetzten Permanent Virtual Circuits (PVC), die eine manuelle Zuweisung der VPIs/VCIs erfordern, werden die Labels automatisch zugewiesen.

Schritt 2: Erreicht ein Paket einen der Eckrouter (edge LSR), wird in diesem die Layer-3-Service-Qualität ermittelt, wie z.B. bestimmte Anforderungen an QoS oder an die Bandbreiten. Basierend auf den Routing- und Policy-Vorgaben wird ein bestimmtes Label vom Eckrouter ausgewählt und ergänzend dem Paket-Header angehängt (in Abb. 8.5 skizziert als dem eigentlichen Paket vorangestellte weiße Rechtecke).

Schritt 3: Die LSR im Kernnetz (core-LSR) der MPLS-Domain lesen die Labels. In jedem Pakt tauschen sie jeweils das vorhandene Label mit einem neuen aus dem Tabellenindex aus und leiten das Paket zum nächsten LSR im Kernnetz weiter. Dieser Vorgang wird wiederholt, bis der Ausgangsrouter erreicht wird.

Schritt 4: Der Ausgangsrouter entfernt die Labels, die nur in der MPLS-Domain eine Gültigkeit besitzen, liest die eigentliche Kopfinformation des Pakets und leitet das ursprüngliche Paket an die Zieladresse weiter.

Um eine Vorstellung von einem MPLS-Label zu gewinnen, kann man das MPLS-Label mit einer vorausberechneten Switching-Tabelle vergleichen, die zusätzliche Layer-3 Informationen beinhaltet. Weiterhin enthalten die Labels spezielle Bedeutungen, je nachdem, welche unterschiedliche Zieladresse bzw. Type of Service vom Eckrouter mitgegeben wird. Gerade diese Flexibilität zählt zu den größten

Vorteilen, die MPLS für einen IP-Geschäftsverkehr zu bieten hat. Abb. 8.6 stellt diese Vorteile graphisch dar.

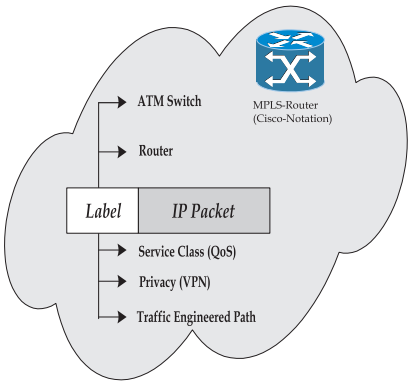


Abb. 8.6: MPLS Netzwerkvorteile durch Flexibilität

Diese Flexibilität äußert sich zum einen darin, dass jeder Switch automatisch jedes IP-Paket mit dem gewünschten Service verarbeitet. Zum anderen sind die Tabellen in einer MPLS-Domain im Vorfeld berechnet, so dass kein Paket zur Wegbestimmung neu analysiert werden muss. Daher stellt sich für ein IP-Paket eine MPLS-Domain lediglich als ein einziger Hop dar.

Durch das beschriebene Szenario wird es nicht nur möglich, unterschiedliche Verkehrsanforderungen (Traffic Types) wie Best Effort und Mission Critical Traffic unterschiedlich zu bedienen. Es wird außerdem eine hohe Skalierbarkeit erreicht, indem bei MPLS unterschiedliche Regelwerke *(Policy Mechanisms)* zur Label-Kennzeichnung eingesetzt werden. Dabei spielt der ursprüngliche IP-Header für eine Weiterleitung in einer MPLS-Domain keine Rolle mehr, da dieser vollständig entkoppelt ist. Die Leistungsfähigkeit einer MPLS-Domain hängt jedoch wesentlich von der Verkehrssteuerung (Traffic Engineering) ab. Nachfolgend soll dieser Punkt daher näher betrachtet werden. Weiterhin haben die beiden meistverwendeten Traffic-Engineering-Protokolle RSVP-TE und CR-LDP jeweils besondere Stärken, auf die Hersteller Wert legen.

8.1.4 Gemeinsamkeiten und Unterschiede von RSVP-TE und CR-LDP

Derzeit werden zwei unterschiedliche Entwicklungen einer Verkehrssteuerung in MPLS-Netzwerken von der *MPLS-Working Group* der IETF verfolgt. Die eine ist das RSVP bzw. das RSVP-TE, die andere Constrained-Based LDP, kurz CR-LDP. Diese charakterisieren vornehmlich die Signalisierung in der Verkehrssteuerung innerhalb einer MPLS-Domain. Um einen LSP (Label Switched Path) in

einem MPLS-Netz aufzubauen, kann zum einen ein kontrollierter *(Hop-by-Hop)*-Mechanismus mit dem Label Distribution Protocol (LDP) und zum anderen ein explizites Routing des LSP bzw. ER-LSP errichtet werden.

Beide Ansätze, RSVP-TE und CR-LDP, verfolgen den zuletzt genannten Weg des ER-LSP. Damit kann für einen einzurichtenden LSP die optimale Route mit vorbestimmten CoS und QoS festgelegt werden. Weiterhin besteht eine Justierung mit der lockeren ER-LSP *(loose ER-LSP)*, bei der eine Gruppe von mehr oder weniger bestimmten Zwischenknoten am Weg *(path)* beteiligt ist und folglich mehrere Freiheitsgrade gegeben sind. Damit wird ein Autonomes System (AS) definiert, das gewisse *abstrakte* Zwischenknoten beinhaltet. Im Gegensatz dazu existiert eine strikte ER-LSP-Möglichkeit *(strict ER-LSP)*, die nur einen Freiheitsgrad aufweist, indem die Zwischenknoten in einer dafür erstellten Liste, unter Ausnutzung der aktuellen Adressen, genutzt werden.

Wird ein Traffic Engineering mit ESVP-TE in einer MPLS-Domain mittels RSVP-TE realisiert, geschieht dies gemäß [RFC 2205] in enger Anlehnung an das RSVP-Protokoll. Abb. 8.7 veranschaulicht die Wegefindung nach diesem Protokoll.

Jedoch ist es nicht erforderlich, dass bei Verwendung von RSVP-TE das Protokoll RSVP vollständig an jedem Eckrouter (LER) oder Zwischenrouter (LSR) implementiert sein muss. Es muss lediglich in den LERs und LSRs die Möglichkeit bestehen, das MPLS-explizit-Routing verwenden zu können. RSVP-TE ist ein *soft-state*-Protokoll und nutzt ein verlustbehaftetes UDP[5]- bzw. IP-Datagramm, um den Signalisierungsvorgang zur Einrichtung eines LSP umzusetzen.

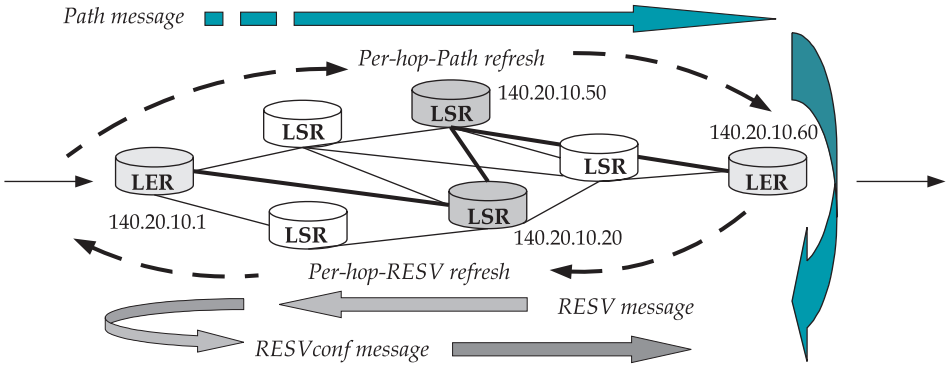


Abb. 8.7: Beispiel für eine lose (lockere) explizit Wegstreckenfindung (LSP) mittels RSVP-TE

[5] Im Gegensatz zu TCP ist UDP genau wie IP ein verbindungsloses Protokoll. Es werden keine Garantien übernommen ob die in Form von Datagrammen übertragenen Informationen auch tatsächlich beim Empfänger angekommen sind. Gegenüber IP hat UDP zwei Zusätze: die Auswahlmöglichkeit bestimmter Programme durch Portnummern und eine optimale Fehlererkennung in den Nutzdaten durch Prüfsummenbildung.

In Abb. 8.7 wurde BGP-4 genutzt, um einen geeigneten Egress-LER (Eckrouter) zu finden, damit der eintreffende Datenverkehr zu einem weiteren Autonomen System (AS) geroutet werden kann. Der Ingress-LER (140.20.10.1) schickt *(Downstream)* eine spezielle Wegenachricht *(path-message)* über eine Reihe von Zwischenknoten (LSR) an den nächsten Egress-LER. Jeder Zwischenknoten erhält die spezielle Wegenachricht und speichert diese Information für nachfolgende Sendungen. Damit wird eine lockere Wegstrecke *(path-state)* erzeugt. Anschließend schickt *(Upstream)* der Egress-LER (140.20.1.60) eine Nachricht *(RESV-message)*, um Ressourcen entlang dieser Wegstrecke bei den zu passierenden LSR für Qualitätseigenschaften (QoS) zu reservieren. Erreicht diese Nachricht den Ingress-LER (140.20.10.1), wird sofort eine Bestätigungsnachricht *(RESVconf-message)* zur gelungenen Einrichtung eines LSP an den Egress-LER (140.20.10.60) verschickt.

Von Zeit zu Zeit werden – solange die Verbindung unterhalten wird – Bestätigungsnachrichten *(refresh-messages)* ausgetauscht, um zu prüfen, ob der eingerichtete Zustand noch Bestand hat oder ob Störungen oder Änderungen den LSP modifiziert haben. Dabei wird bei allen Nachrichten auf das verbindungslose UDP- bzw. IP gesetzt, das sich nachteilig auswirken kann. Dieser Verbindungszustand wird als *soft state* bezeichnet und besitzt eine selbstreinigende Eigenschaft, falls Auffrischungsnachrichten aus irgendwelchen Gründen nicht ausgetauscht werden oder im Netz verloren gehen. Nach geraumer, einstellbarer Zeit wird die Verbindung automatisch abgebaut, indem die allokierten Labels zurückgesetzt werden und die Bandbreite freigegeben wird.

Die RSVP-TE-Protokoll-Eigenschaften bieten dennoch robuste und interessante Möglichkeiten, um effektive Verkehrssteuerungsmechanismen in einer MPLS-Domain einzurichten:

- QoS- und Traffic-Parameter werden für das Traffic-Management als reguläre Daten wahrgenommen.
- Falls ein Fehler beim Aufbau eines LSP auftritt bzw. ein existierender verloren geht, wird eine Fehlererkennung mittels Fehlernachrichten, die vom zeitlichen Sendezyklus der *refresh message* abhängen, eingeleitet.
- Eine Fehlerbehebung erfolgt nach dem Wiederherstellungsprinzip; erst in einem zweiten Schritt wird ein LSP neu aufgebaut.
- Eine Schleifenbildungserkennung ist nur bei einer losen expliziten Wegefindung erforderlich.
- Eine Multiprotokoll-Unterstützung ist bei RSVP-TE möglich.
- Das Netzwerkmanagement wird durch eindeutige Identifizierung eines jeden LSP erleichtert und erlaubt die diskrete Behandlung einzelner LSP.
- Eine eingerichtete Wegstrecke kann für Dritte mittels bestimmter Objekte *(record route objects)* von außen verfolgt werden.
- Eine Wegeabbrucheigenschaft ist ebenfalls vorhanden, um einen plötzlich auftretenden höher priorisierten Verkehr den Vorzug zu geben.

Bei einem Traffic Engineering mittels CR-LDP, als Ergänzung zum Label Distribution Protocol, das Bestandteil von MPLS ist, wird kein weiteres Protokoll benötigt. Das CR-LDP unterscheidet sich damit zum RSVP-TE-Ansatz. Denn lediglich die existierenden Strukturen werden durch Erweiterungen für eine Verkehrssteuerung eingerichtet.

Ebenso wie RSVP-TE unterstützt CR-LDP eine strikte und eine lockere Wegstreckenfindung (LSP). Statt GBP-4 oder ähnlicher Protokolle wird das UDP-Protokoll genutzt, um entfernte MPLS Ausstiegspunkte *(peers)* zu finden. Das verbindungsorientierte TCP-Protokoll wird dagegen zu Kontroll- und Managementzwecken ebenso wie zu Label-Anforderungen und zum Label-Mapping genutzt.

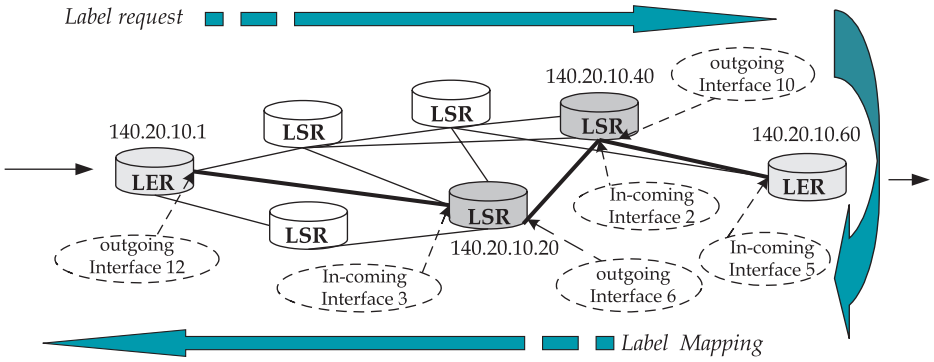


Abb. 8.8: Beispiel für eine strikte explizite Wegefindung (LSP) mittels CR-LDP

Abb. 8.8 zeigt eine explizite strikte Wegstreckenfindung mittels CR-LDP zwischen einem Ingress- und einem Egress-LER im Netzwerk eines Providers. Die genutzten Interfaces sind gestrichelt skizziert. Die eingerichtete Wegstrecke zwischen Ingress- und Egress-LER ist auf zwei bestimmte LSR in der MPLS-Domain beschränkt. Die Label-Anforderung ist *Downstream* vom Ingress- zum Egress-LER (140.20.10.60) in einem *Hop-by-Hop*-Verfahren entlang der LSR erfolgt. Anschließend ist in ähnlicher Weise in *Upstream*-Richtung ein Label-Mapping zurück zum Ingress-LER durchgeführt worden. Wie in Abb. 8.8 deutlich erkennbar, kann somit eine explizite Wegstrecke zwischen den beiden LER und den vorgesehenen LSR sowie den damit verbundenen LSR-IP-Adressen eingerichtet werden. Dieser Verbindungszustand wird als *hard state* bezeichnet. Das bedeutet, dass *nur* während der Initialisierungsphase Label-Informationen ausgetauscht werden müssen. Gerade diese Eigenschaft als spezielle Verkehrssteuerung ist ideal für eine Sprachübertragung (Voice-over-IP, VoIP) oder auch für VPN, weil Einfluss auf die Bandbreite bzw. auf die Verkehrspriorisierung genommen werden kann.

Zusammenfassend können die folgenden Eigenschaften von CR-LDP beschrieben werden:

- Einflüsse durch QoS- und Traffic-Parameter erfolgen durch Regeln, ausgelegt für Eckrouter und *Per-Hop-Behavior*, die sich auf Datenraten, Bandbreitenanforderungen und Wichtungen beziehen.
- Ein Wege(vor)recht wird durch eine Priorisierungsmöglichkeit gegenüber weiteren LSP eingeräumt.
- Eine Wegstreckenoptimierung ermöglicht eine Änderungen der Verkehrsbeziehungen der LSR untereinander und beinhaltet die Option einer Wegefixierung *(route-pinning)*.
- Eine Fehlererkennung und -weiterleitung erfolgt durch das TCP-Protokoll.
- Eine Fehlerbehebung wird an jedem Gerät, das ein LSP unterstützt, durch ein Policy-Mapping zur automatischen Fehlerbeseitigung erreicht.
- Eine Schleifenbildungserkennung ist nur bei einer losen expliziten Wegefindung erforderlich. LDP unterstützt eine derartige Erkennung.
- Es wird ein Multiprotokoll-Service unterstützt.
- Ein Netzwerkmanagement wird durch eine eindeutige Identifizierung eines jeden LSP erleichtert und erlaubt die diskrete Behandlung einzelner LSP.

Wenn beispielsweise das Netzwerkmanagement bestimmt, dass ein LSP nicht länger benötigt wird, werden Nachrichten an alle Router *(peers)* geschickt, die für den LSP allokierten Ressourcen wieder freizugeben. Dieser Re-Allokierungsprozess ist infrequent, erfordert lediglich eine geringe Bandbreite und verbraucht wenig CPU-Ressourcen.

Tabelle 8.1: Ähnlichkeiten zwischen CR-LDP und RSVP-TE

Merkmal	**CR-LDP**	**RSVP-TE**	**Bemerkung**
Initialisierung	Label Request Message	Path Message enthält ein Label Request Objekt	
Setup Durchführung	Mapping Message	RESV Message	
Definition des Differentiated Services	DIFF-SERV-PSC TLV	DIFFSERV-PSC Objekt	Beide enthalten die DiffServ Code Point (DSCP) Information und binden diese in die Setup Message ein (siehe Zeile 1).
Unterstützung für n:m LSPs	Nein	Nein	von der IETF definiert
Wegemöglichkeit	Mitgeführt in der Explizit Route List TLV	Mitgeführt im Explizit Route Objekt	Spezieller Weg wird zum Aufbau des Switch Path genutzt

Tab. 8.1 stellt Ähnlichkeiten beider Verfahren gegenüber. Ein Vergleich zwischen den beiden MPLS-Traffic-Engineering-Möglichkeiten zeigt eine Reihe von Unterschieden, die beachtenswert sind.

Falls ein LDP initialisiert wird, übernimmt eine TCP/IP-Session einen verbindlichen Austausch der Kontrollinformationen. Jeder beteiligte Router (peer) überträgt eine Reihe von Labels, um den LSP aufzubauen. Falls keine Labels zur Verfügung stehen, wird die Session erfolglos abgebrochen.

Bei RSVP gibt es keine Label-Aushandlung. Hier übernimmt das Netzwerkmanagement die Konfiguration. Handelt es sich allerdings um ein sehr großes Netzwerk, das eine große Anzahl von unterschiedlichen Interfaces betreut, ist eine Label-Verteilung gemäß CR-LDP die bessere Lösung.

CR-LDP führt beispielsweise gleich bei der Initialisierung des Weges eines LSP die Kennzeichnungsmöglichkeit einer expliziten Wegführung mittels TLV innerhalb der *Label Request Message* mit. Ähnliche Eigenschaften werden bei RSVP-TE mit dem *explicit route object* transportiert. Beide Verfahren unterstützen das Konzept der lockeren (losen) Verbindung. Dies sind Verbindungen durch ein Netzwerk, bei dem eine bestimmte Anzahl von Zwischenknoten als Transitknoten hinzugezogen werden können – aber nicht alle zwingend hinzugezogen werden müssen. Ebenso unterstützen beide Verfahren den erfolgreichen oder misslungenen Verbindungsaufbau eines LSP bis zurück zum Ingress Router. Weiterhin lassen beide ein *route-pinning* zu. Dabei wird bei CR-LDP ein Pinning nur während der Anfangsphase vorgenommen, bei RSVP-TE kann dies dagegen zu jeder Zeit im Rahmen der *path-message* geschehen. Vorteilhaft bei RSVP-TE ist, dass bei dem *Record Route object* die Liste der Zwischenknoten, die beim LSP-Aufbau involviert sind, für Analysezwecke zum Startrouter übermittelt werden kann. Diese Eigenschaft erleichtert es einem Netzwerkadministrator erheblich, Auskünfte über den aktuellen Netzstatus zu erlangen. Diese oder eine vergleichbare Eigenschaft hat CR-LDP nicht zu bieten und ist somit komplexer in der Fehler- und Statusbehandlung.

MPLS stellt derzeit den letzten Entwicklungsstand in der Evolution des Zusammenwachsens der Switching-Technologie auf Layer-2 *(Data-Link Layer)* mit der Routing-Technologie auf Layer-3 *(Network Layer)* dar. Dabei wird beim Standardisierungsprozess primär das Ziel verfolgt, eine flexible, skalierbare und mit verbesserter Performance versehene Netzinfrastruktur für Netzbetreiber zu schaffen. Obwohl MPLS ausgelegt ist, einen umfangreichen Bereich an Transportmechanismen bis hin zu optischen Netzen zu unterstützen, erfolgten die ersten Implementierungen zunächst bei den von Netzbetreibern vornehmlich eingesetzten Systemen wie ATM und Frame Relay.

8.1.5 IP-MPLS und Multiprotocol Lambda Switching ($MP\lambda S$)

Die jüngste Entwicklung entfernt sich weiter von der ATM-Technologie als Schicht-2-Transportebene und geht eindeutig in Richtung optischer Netze, wie Abb. 8.16 nahelegt. Der Grund liegt in den zunehmenden Anforderungen der Applikationen an Flexibilität und Performance, mit der die ATM-Technologie nicht schritthalten kann. Gerade die Zunahme der Netzwerkkomplexität erfordert Transportstrukturen, die im wesentlichen durch die zwei Faktoren Kosten-

Tabelle 8.2: Unterschiede zwischen CR-LDP und RSVP-TE

Merkmal	**CR-LDP**	**RSVP-TE**	**Bemerkung**
Entwicklungsstand	relativ neu	Im Prinzip alt, Ergänzungen hinzugefügt, Unterstützung von Altsystemen	RSVP Objekte modifiziert für eine MPLS-Umgebung
Signalisierungstransport	UDP zur Wegfindung, TCP während der Session	IP oder UDP	Kein Algorithmus zur Fehlererkennung bei RSVP; TCP-Fehler können katastrophale Auswirkungen auf den LSP und CR-LDP haben
Verbindungszustand	*Hard-State*	*Soft-State*	Ein *Soft-State* ist nicht skalierbar, RSVP unterstützt Refresh Aggregation
Verfügbarkeit	Fehler erzeugen ein proaktiven Signalisierungsvorgang.	Abhängig vom *Soft-State*-Zeittakt können Fehler erkannt werden	Kein Algorithmus zur Fehlererkennung bei RSVP
Management	LSR, LDP, TE, MIBs	RSVP modifiziert und LSR MIBs	
Erweiterbarkeit	Hersteller-spezifisch, undurchsichtige und experimentelle TVLs	Experimentelle Objekte	Funktional sehr ähnlich
Skalierbarkeit	Hard-State-Verbindungen reduzieren den Signalisierungsaufwand.	Erfordert eine Refresh Reduktion, Aggregation zur Minimierung des Soft-State-Aufwands	
Interoperabilität	Gute Unterstützung, für ATM, Frame Relay und Ethernet	Tunnel durch ATM-Netzwerke müssen manuell konfiguriert werden	

Leistung-Relation und Skalierbarkeit bestimmt werden. Gleichzeitig müssen die geforderten Transportstrukturen eine nach oben erweiterbare Performance ermöglichen. Einige dieser Anforderungen (z.B. Skalierung mittels *Stream Merging*) werden von MPLS in idealer Weise erfüllt. Andere wiederum können mit optischen Netzen, den Optical Transport Network (OTN), zukunftsträchtig erfüllt werden.

Als Ergebnis vieler Überlegungen und Diskussionen begann man MPLS-Funktionalitäten in *optical cross-connect* (OXC) Geräten zu implementieren, die derzeit unter den Namen $MP\lambda S$ zusammengefasst werden. Dabei deutet das λ auf eine Übertragung mittels optischen Netzen hin.

Aus diesen Überlegungen sind eine Menge vielversprechender Ansätze ent-

wickelt worden, die im einzelnen weiterverfolgt werden. Einige dieser Ansätze sind:

- Die Kombination (MPLS/OTN) kann durchaus eine Hebelwirkung erzielen, um eine Methodologie für Echtzeitübertragungen in optischen Kanälen zu entwickeln. Sie trägt somit dazu bei, dass derzeitige Entwicklungen auf diesem Gebiet vorangetrieben werden.
- Ebenso ermöglicht die Zusammenführung von MPLS und OTN beiden Technologien ein einfacheres Netzwerkmanagement.
- Ein weiterer Zugewinn kann in einer gemeinsamen Architektur darin liegen, dass ein *Label Switched Path* (LSP) über unterschiedliche Geräte, wie z.B. Router und OXC-Geräte, geführt wird.
- Eventuell besteht sogar die Möglichkeit für IP-Router, die *Dense Wave Division Multiplexing* (DWDM) Technologie einzubringen.

MPLS und optische Netze ergänzen sich hervorragend in einer Reihe von sehr ähnlichen Techniken und bilden wohl *die* Transportstrukturen der Zukunft im Netzwerkbereich. Im Einzelnen sind dies:

- In der MPLS-Technologie beschreibt ein LSP eine Punkt-zu-Punkt-Übertragung anhand der Labelstruktur. Bei $MP\lambda S$ wird in ähnlicher Weise ein optischer Kanal zwischen zwei Endpunkten beschrieben.
- In einem MPLS-Netzwerk wird mittels einer LSR eine Beziehung der beiden Tupel <*input port, input label*> und <*output port, output label*> eindeutig hergestellt. Vergleichbar geschieht eine Tupelbildung bei $MP\lambda S$ durch <*input port, input optical channel*> und <*output port , output optical channel*>. Sind diese einmal eingerichtet, können sie von den Datenpakten selbstständig nicht verlassen werden und bilden eine wichtige Grundlage für die VPN-Technologie, denn damit ist die Privatsphäre in ihren Grundzügen eingerichtet.
- In einem MPLS-Netzwerk sind die LSR für die Nachrichtenverteilung, die Wegefindung und den notwendigen Informationsaustausch bei Wartungsaktivitäten zuständig. Die gleichen Aufgaben nimmt ein OXC-Gerät in einem OTN wahr.
- In einem MPLS-Netzwerk übernimmt ein LSR die Aufgabe, einen LSP einzurichten, zu warten und die bestehenden Richtlinien *(Policys)* für die Verkehrssteuerung *(Traffic Engineering)* anzuwenden. Die gleiche Funktionalität ist in den OXC-Geräten abgebildet.
- Wie in einem MPLS-Netzwerk ein LSP ist in einem OTN ein optischer Kanal unidirektional ausgerichtet.

In einer $MP\lambda S$-Umgebung kann eine Glasfaser *(Fiber)* durchaus mit einer Gruppe von Links verglichen werden, bei der jeder Link wiederum als eine Gruppe von Kanälen verstanden werden kann. Ein IP-Routing-Protokoll (Inter Domain

Protocol) kann, allerdings mit Erweiterungen, so Informationen über die optische Netzwerktopologie, verfügbare Bandbreite und andere passende Zustandsinformationen verteilen. Diese Informationen können dann, z.B. mit den MPLS-Protokollen (RSVP-TE, CR-LSP), benutzt werden, um eine explizite Route für optische Kanäle einzurichten.

Dennoch – obwohl viele Gemeinsamkeiten ideal zusammenpassen – gibt es einige Unterschiede zwischen einem MPLS-Netzwerk und einem OTN, die zu beachten sind:

- In einem MPLS-Netzwerk werden Weiterleitungsinformationen als Teil des Labels in jedem Datenpaket mit transportiert. Im Gegensatz dazu sind Switching-Informationen in der Wellenlänge oder im optischen Kanal inbegriffen.
- In einem optischen Netzwerk (OTN) existiert kein vergleichbares Konzept zu einer Label-Zusammenführung *(merging)*. Ein OXC-Gerät ist nicht in der Lage, unterschiedliche Wellenlängen zu einer gemeinsamen Wellenlänge zu überführen.
- Ein OXC-Gerät ist nicht in der Lage, für Labels einen push- oder pop-Mechanismus zu unterstützen, da das Analogon zum Label die Wellenlänge selber ist. Hierfür gibt es derzeit auf weiter Sicht keine Technologien für ein optisches Netzwerk.

Entscheidend für die zukünftige Entwicklung der Transportplattformen ist jedoch, wie sich der Geschäftsverkehr weiter in Richtung Internet, Intranet und Extranet entwickeln wird. Aus gegenwärtiger Sicht ist die Entwicklung *IP/MPLS-over-OTN* vorgezeichnet.

8.2 Fast-Packet-Switching (FPS)

Die schnelle Paketvermittlung ist ein grundlegendes Verkehrskonzept in der modernen Hochgeschwindigkeitskommunikation. In den 60er Jahren wurde bei der herkömmlichen klassischen Paketvermittlung eine virtuelle Verbindung nicht nur in den Endsystemen eingerichtet. Auch in allen Zwischenstationen (Netzknoten) wurde bis zur Layer-3 eine Verarbeitung vorgenommen. Dort wurde das nächste Teilstück umständlich zwischen Quelle und Ziel berechnet.

Im Gegensatz dazu wird in den FPS-Netzen eine Weitervermittlung auf Layer-2 vorgenommen. Dies ist möglich, weil die Layer-2 in drei Ebenen nämlich in *Fast-Packet-Relay*, *Fast-Packet-Adaption* und *Data-Link-Control-Sublayer* unterteilt wurde. Die FPR-Sublayer ist weiterhin in der Lage, eine Ende-zu-Ende-Verbindung in den Zwischensystemen ohne aufwändiges Routing herzustellen. Gleichzeitig entfällt noch eine Fehler- und Flusskontrolle, im Sinne einer herkömmlichen Paketvermittlung.

Die Fast-Packet-Switching-Technologie kann in zwei unterschiedliche Betriebsverfahren unterteilt werden. Zum einen ist dies das Frame-Relay-Verfahren mit Datenpaketen, die bei der Übertragung unterschiedliche Längen einnehmen können, auch als *Packet Switching* bekannt. Zum anderen handelt es sich um das ATM-Verfahren mit Datenpaketen, die bei der Übertragung immer eine konstante Länge besitzen; diese werden auch als Cell-Relay bezeichnet. Nachfolgend werden diese beiden Betriebsverfahren näher diskutiert. Im Vordergrund steht dabei allerdings nur eine der beiden möglichen Dienstarten, die in einem paketvermittelten Netzwerk einsetzbar sind. Die eine wird als Datagrammdienst bezeichnet, bei dem jedes Paket eine für sich geschlossene Einheit bildet, die allein übertragen wird. Die andere Dienstart wird als virtuelle Verbindung *(Virtual Circuit)* bezeichnet und bildet einen logischen Weg zwischen zwei Teilnehmern. Dabei übernimmt das Netz vollständig die Kontrolle über die Einhaltung aller wichtigen Parameter wie z.B. die Wiederherstellung verlorengegangener Daten, die Eliminierung von Duplikaten, die Flusssteuerung zur Vermeidung von Überlastsituationen sowie die Erkennung und Korrektur von Übertragungsfehlern.

8.3 Frame Relay

Viele Unternehmen stehen heute vor einem Dilemma: Einerseits fordert ein immer heftigerer Wettbewerb immer höhere Investitionen in die Informationstechnik, andererseits muss immer härter kalkuliert werden. Vor allem die Kosten für die Weitverkehrsverbindungen zu den Niederlassungen, Zulieferern und Kunden stellen einen großen Kostenblock dar – zumal vielerorts bereits das Bandbreitenende der X.25-Verbindung (64 kbit/s) erreicht oder zumindest abzusehen ist. In dieser Situation hat sich Frame Relay als eine Verbindungsalternative angeboten, mit der Unternehmen in den Vorteil höherer Bandbreitendimensionen kommen und nicht wie bei ATM eine hohe Gebühr für den Fernanschluss zahlen müssen.

Frame Relay ist streng genommen ein Beispiel für VPN der ersten Generation (vgl. Seite 6), denn es bringt alle geforderten Eigenschaften dieser Definition mit, wie nachfolgend ausgeführt wird. Bei Frame-Relay-Netzen handelt es sich um vermaschte Konstruktionen, in denen Pakete über Frame-Handler (FH) vermittelt werden. Je nach Netzgröße sind diese teilvermascht oder hierarchisch mit Backbone- und Anschlussnetz aufgebaut. In den Backbone-Netzen erfolgt der Datentransport über die FH-Knoten. Das Zugangsnetz ist Linienförmig an den Backbone angeschlossen. Die Zugangsnetze bilden den Anschluss über herkömmliche Fernmeldenetze zum Endteilnehmer sowie zu anderen Netzwerkarchitekturen mittels FRAD[6].

Frame Relay hat gegenüber X.25-Verbindungen nicht nur den Geschwindigkeitsvorteil – so kann maximal 2 Mbit/s, also das 30-fache der konventionellen X.25-

[6] Unter einem Frame Relay Access Device wird eine Einheit verstanden, die Datenpakete verschiedener Netzwerkarchitekturen bzw. deren Protokolle, wie IPX, SNA, DECnet, IP, UDP usw., umwandelt, damit diese über eine Frame-Relay-Verbindung verschickt werden können.

Verbindungen übertragen werden –, sondern Frame Relay kommt auch mit erheblich weniger Steuerdaten aus. Der Steuerdatenanteil konnte durch die ausschließliche Nutzung von digitalen Strecken stark reduziert werden. Denn digitale Strecken weisen wesentlich geringere Fehlerrisiken und -raten auf als analoge Verbindungen. Weiterhin werden Kontroll- und Protokoll-Restaurierungsmechanismen weitgehend in die Endgeräte verschoben. Dies führt zu einem hohen Netto-Durchsatz und einem geringen technischen Aufwand in den Vermittlungsknoten. Ebenso ist für den hohen Netto-Durchsatz förderlich, dass Datenpakete mit einer maximalen Länge von 4 kbit/s möglich sind und somit der Steuerdatenanteil pro Paket besonders klein ausfällt. Darüber hinaus spricht für Frame Relay, dass eine sanfte Migration von X.25 – ohne Investition in zusätzliche Hardware – zur Frame-Relay-Übertragung vollzogen werden kann. Ein Software-Upgrade auf den Kopplungssystemen, wie z.B. Multiplexer, Brücken oder Router, zu beiden Seiten der Frame- Relay-Verbindung genügt gewöhnlich, um auf die durchsatzstarke Kommunikationsschiene zu wechseln. Eine weiterhin überzeugende Eigenschaft ist, dass sowohl eine permanente Grundlast an Bandbreitenbedarf als auch sporadische Hochlasten *(Burst)* keinerlei Probleme bereiten.

Kennzeichnend für Frame Relay ist die Fast-Packet-Switching-Technologie, die einen verbindungsorientierten Datenübertragungsdienst darstellt. Diese Technologie liefert die Möglichkeit, gewählte virtuelle Verbindungen, (Switched Virtual Connections, SVC) sowie festgeschaltete Verbindungen, (Permanent Virtual Connections, PVC) einzurichten. Diese virtuellen Verbindungen werden durch statistisches Multiplexen[7] eingerichtet, bei dem nur bestimmte Wege durch das Netz festgelegt sind. iesen virtuellen Verbindungen ist jedoch keine Bandbrei-

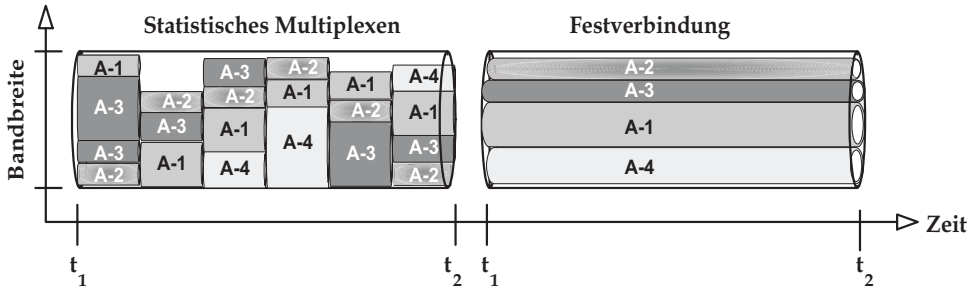


Abb. 8.9: Bandbreitenausnutzung über ein Zeitintervall bei einer Festverbindung und einer Frame-Relay-Verbindung

te explizit zugeordnet, solange nicht Daten (echte Informationen) übertragen werden. Die erforderliche Bandbreite wird bei einer Übertragung innerhalb des

[7] Im Gegensatz zum statistischen Multiplexen wird beim traditionellen Zeitmultiplexen bei einer Leitungsvermittlung jedem Pfad (Leitung) durch das Netz eine feste Bandbreite zugeordnet. Diese Zuweisung ist statisch und gilt für die Dauer der Verbindung. Bei einer Sprachverbindung wird z.B. die volle Bandbreite genutzt, auch um Stille zu übertragen (wenn zugehört wird oder wenn Sprechpausen eintreten).

Netzes dynamisch, Paket für Paket, zugewiesen. Gleichzeitig werden damit Zugangskosten reduziert, denn innerhalb einer einzigen physikalischen Verbindung können mehrfach logische Verbindungen aufgebaut werden. Abb. 8.9 zeigt den prinzipiellen Vergleich einer Bandbreitenauslastung innerhalb der Zeit $t_1 \cdots t_2$ zwischen einer Festverbindung und einer Frame-Relay-Verbindung. Während bei der Festverbindung die Auslastung durch die Verbindungen $A_1 \cdots A_4$ festliegt, kann bei einer Frame-Relay-Verbindung durch statistisches Multiplexen wesentlich flexibler auf unterschiedliche Bandbreitenanforderungen reagiert werden.

Daten bzw. Informationen werden bei Frame Relay in nicht nummerierten Informationsrahmen (Frames) übertragen. Diese Rahmen haben weder eine Sendefolgenummer noch eine Empfangsfolgenummer. Die Frame-Größe ist dabei variabel und kann bis auf den maximalen Wert von 2100 Bytes eingestellt werden. Um dem Verlust von Frames entgegenzuwirken, wird bei einer eintretenden Überlastsituation ein entsprechendes Signalisierungsverfahren zur Regelung eingesetzt. Liegt eine geringe Überlastung vor, dann signalisieren die FECN-Bits *(Forward Explizit Congestion Notification)* und die BECN-Bits *(Backward Explizit Congestion Notification)* in und entgegen der Übertragungsrichtung an die angeschlossenen Endeinrichtungen, dass eine Überlastung droht und die Sendelast verringert werden sollte. Durch diese Flusskontrolle wird eine ernsthafte Überlastung im Netz, die zum Informationsverlust führen könnte, vermieden. Abb. 8.10 zeigt einen entscheidenden Vorteil der Frame Relay-Technologie.

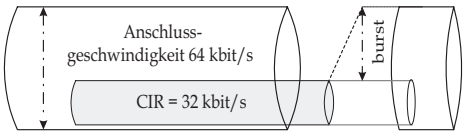


Abb. 8.10: Frame-Relay-Eigenschaft durch Mehrfachausnutzung der Anschlussleitung

Der Datendurchsatz einer Frame-Relay-Verbindung wird durch mehrere Parameter bestimmt. Zum einen ist dies die CIR *(Committed Information Rate)*, die die Übertragungsgeschwindigkeit in einem Frame-Relay-Netz unter normalen Betriebsbedingungen garantiert (Abb. 8.10), zum anderen ist es die Datenmenge, die in einem Zeitintervall (TC) mindestens übertragen wird. Diese Größe, die mit Bc (*Committed Burst Size*) bezeichnet wird, wird oft auch als vereinbarte Datenmenge verstanden, die verlustfrei über das Netz transportiert werden muss.

Diejenige Datenmenge, die zusätzlich zur minimalen Datenmenge (Bc) in einem festen Zeitintervall (TC) übertragen werden kann, wird mit Be (*Excess Burst Size*) tituliert. Damit ist die maximal zu übertragende Datenmenge durch Bc + Be zu bestimmen. Begrenzt ist die maximal – explizit also die Be – zu übertragende Datenmenge durch die Anschlussgeschwindigkeit (Access Rate) des kleineren der beteiligten Ports der beiden Endeinrichtungen. Die bestimmende Relation lautet $0 \leq Be \leq (AR - CIR) \cdot TC$.

Jetzt kann unmittelbar die Übertragungsgeschwindigkeit CIR durch den Zusam-

menhang

$$CIR = \frac{Bc}{TC} \tag{8.2}$$

bestimmt werden. Bei Einstellung der CIR und somit der garantierten Datenmenge BC z.B. für TC=1s ist darauf zu achten, dass Bc nicht kleiner als die Länge der Nutzdaten-Frames ist – z.B. die maximale Fenstergröße des Netzwerkprotokolls. Durch Gegenüberstellung einer Ethernet-Verbindung soll folgendes Rechenbeispiel diesen Zusammenhang verdeutlichen. Es wird nur überschlagsmäßig gerechnet.

$$\begin{aligned} Beispiel: \quad & AR = 64kbit/s \\ & CIR = 8kbit/s = 8000bit/s \\ & Bc = 8Kbit = 8000bit \mathrel{\hat{=}} 1000Byte \\ & Be = (64-8)kbit \mathrel{\hat{=}} 7000Byte \\ & ein Ethernet Frame hat dagegen eine\, MTU = 1500Byte \end{aligned} \tag{8.3}$$

Bei Ethernet ist die Rahmengröße (MTU)[8] zwischen 64 Byte und höchstens 1518 Byte festgesetzt. Im vorliegenden Beispiel bedeutet dies, dass die Nutzdatengröße von 1500 Byte $\gg$ Bc ist. Mit diesem ungünstigen Verhältnis von Overhead zu Nutzdaten würde theoretisch keine einzige Daten-Frame innerhalb der CIR übertragen werden können.

Das Frame-Relay-Format ist in enger Anlehnung an das HDLC-Protokoll[9] entstanden, das ebenfalls in den X.25-Netzen verwendet wird. Die grundsätzlichen Definitionen des Adress- und Steuerfeldes entsprechen den allgemeinen Definitionen von HDLC-Protokollen. Beide Felder sind jedoch gegenüber dem HDLC-LAPB[10] erweitert, sie sind jeweils zwei Oktetts lang.

Der Aufbau eines Frames[11] ist in Abb. 8.11 dargestellt. Ein Frame-Relay-Paket (Header und Trailer) wird durch ein Flag-Byte (1 Byte) mit bestimmten Mustern

---

[8] Eine Maximum Transfer Unit (MTU) ist die größtmögliche Dateneinheit bzw. Frame-Länge, die über ein vorhandenes physikalisches Übertragungsmedium bzw. über einen LAN- oder WAN-Pfad gesendet werden kann. Wenn größere Frame-Längen auftreten, werden sie entweder entsprechend der verwendeten Protokollregeln fragmentiert oder verworfen.

[9] Beim High Level Data Link Control, kurz HDLC-Protokoll, handelt es sich um einen strukturierten Satz von Standards, der die Mittel bestimmt, mit denen ungleiche Geräte über Datennetze miteinander kommunizieren können. Das HDLC-Protokoll ist ein bitorientiertes und damit codeunabhängiges, von der ITU-T standardisiertes Sicherungsprotokoll für Punkt-zu-Punkt-Verbindungen und Mehrpunktverbindungen. Nach DIN 66 221 besteht ein HDLC-Rahmen aus der Blockbegrenzung (Flag), dem Adressfeld, dem Steuerfeld, dem Datenfeld, der Rahmenprüffolge (FCS) und einer abschließenden Blockbegrenzung (Flag).

[10] Frame Relay arbeitet mit einem speziellen Schicht-2-Protokoll, das in der ITU-T-Empfehlung [Q.922 1988] beschrieben ist. Diese Empfehlung wird sowohl bei Datex-P als auch bei ISDN verwendet.

[11] Bei einem Frame werden Pakete durch Anfügen eines Link-Headers und eines Link-Trailers zu Rahmen (Frames) verwandelt. Ein Frame liefert dem Netzwerk wichtige Informationen über eine mögliche Trennung von aufeinanderfolgenden Paketen sowie die bitweise Prüfung der Integrität auf Layer-2 mit dem HDLC-Protokoll.

begrenzt. Dem *Trailer Flag* wurde eine 2 Byte umfassende Rahmenprüffolge (*Frame Checking Sequence*) vorangestellt. Die Nutzdaten schließen sich unmittelbar dem Header an und können günstige und weniger günstige Längen, wie im obigen Beispiel berechnet, einnehmen.

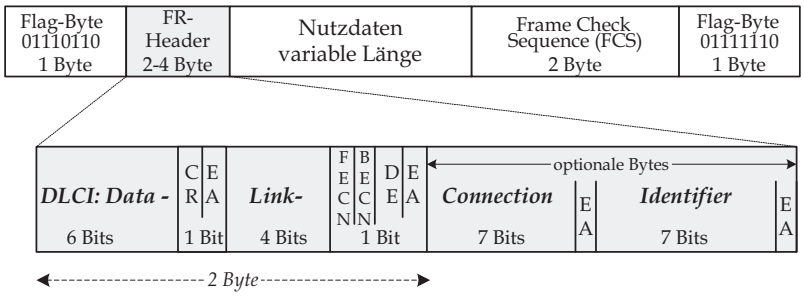


Abb. 8.11: Aufbau eines Frame-Relay- Frame-Format in Anlehnung an HDLC

Der Frame-Header kann zwischen 2-4 Byte groß werden und enthält optionale Bytes. Ein mögliches Header-Ende wird nach jedem Byte durch das EA-Bit mit EA-Bit=1 angezeigt. Bei EA-Bit=0 folgt eine weitere optionale Sequenz, die dann wieder mit einem EA-Bit abschließt. Für Nutzeranwendungen ist das CR-Bit vorbehalten. Das wichtigste Element im Adressfeld ist der *Data Link Connection Identifier* (DLCI), der verschiedene virtuelle Verbindungen an einem Anschluss unterscheidet. Mittels des *DLCI* sowie mit den Verbindungstabellen in den Vermittlungsstellen werden die Blöcke durch das Netz transportiert. Unterschiedliche *DLCI* können gleichen oder verschiedenen Zielen zugeordnet werden. Ergänzend zu den Möglichkeiten der Flusskontrolle mit dem *FECBN* und *BECN* ist das *Discard Eligible*-Bit (DE-Bit) zu verstehen. Das DE-Bit=1 zeigt an, welche Pakete im Fall einer einsetzenden Überlastsituation bevorzugt entfernt werden sollen. Oder welche Pakete (DE-Bit=0) unbedingt in einer solchen Situation weitergeleitet werden müssen.

Man rechnet bei Frame Relay mit ca. 5 Byte Overhead zu den Nutzdaten (Payload) hinzu (Abb. 8.11). Damit ist das prozentuale Verhältnis Overhead/Nutzdaten im Vergleich zu X.25 und ATM auch bei unterschiedlicher Nutzlast sehr günstig (Tab. 8.3). Abschließend kann festgehalten werden, dass Frame Relay in der Lage ist, Ansätze eines Quality of Service (QoS) zu liefern. Damit ist es dem Best-Effort-Delivery-Service, wie es z.B. beim IP in Verbindung mit dem UDP-Protokoll für Anwenderprogramme bereit gestellt wird, überlegen. Interessant ist der L2F-Tunneltechnik-Einsatz (Abschnitt 7.2.1) im Zusammenspiel mit Frame Relay. L2F löst einerseits das Adressierungsproblem aus Sicht der Internet Service Provider (ISP) und stellt eine auf Layer-2 gesicherte Kommunikation dar, andererseits liegt eine elegante und flexible Plattform zur LAN-zu-LAN-Kopplung vor.

Tabelle 8.3: Prozentualer Vergleich zwischen Overhead und Nutzdaten für verschiedene Paketvermittlungen

Nutzdaten	Overhead		
	X.25	ATM	Frame Relay
8 Byte	87,5%	562,5%	62,5%
512 Byte	5,5%	13,9 %	1 %
1500 Byte	5,6%	13,1 %	0,3%

8.3.1 MPLS über Frame Relay

Obwohl die Frame-Relay-Technologie hinsichtlich einer QoS-Anforderung viele gute Ansätze bietet, wird Frame Relay nicht die Transportplattform der Zukunft für die VPN-Technologie sein. Allen Anzeichen nach wird sich die IP/MPLS-Technologie (Abschn. 8.1) im Bereich der Trusted VPN durchsetzen. Zwar bietet Frame Relay mit den Switched Virtual Connections (SVC) und den Permanent Virtual Connections (PVCs) eine interessante Grundlage für die VPN-Technologie, dennoch mangelt es an der Skalierbarkeit, die die IP/MPLS-Technologie mit der Stream-Merging-Möglichkeit bietet.

8.4 Asynchroner Transfer Modus (ATM)

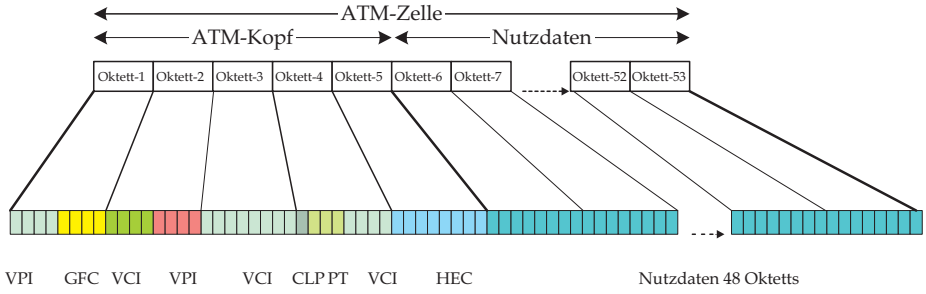
Auf die ATM-Technologie wurde zu Beginn der 90er Jahre große Hoffnung gesetzt. 1994 wurde sie in Deutschland in einem Pilotversuch breitflächig erprobt. Zu den Erprobungsstandorten gehörten Berlin, Hamburg und Köln, an denen ATM-Vermittlungsstellen mit abgesetzten ATM-Einrichtungen installiert wurden. Auch auf internationaler Ebene wurde der Einsatz von ATM ab dem Jahr 1994 eingeführt. In der damals einsetzenden Euphorie über die Leistungsfähigkeit von ATM wurde geplant, ATM bis ins LAN und darüber hinaus direkt zu den Endgeräten einzurichten. Mittlerweile hat sich die Euphorie weitgehend gelegt und ATM wird derzeit im Wesentlichen im Backbone-Bereich eingesetzt. Im LAN ist die Gigabit-Ethernet-Technologie auf dem Vormarsch.

Die ATM-Technologie ist sehr komplex, liefert jedoch weitreichende Möglichkeiten, die zu Beginn der 90er Jahre als sensationell erachtet wurden. Im Folgenden soll der Blick soll auf den Leistungsumfang und auf Aspekte der virtuellen Netztechnologie gerichtet werden. Dabei können zwei grundsätzliche VPN-Lösungen unterschieden werden:

- Zum einen gibt es den Breitband-VPN-Service, der – falls die ganze Infrastruktur auf ATM-Technologie basiert – bis zum Endgerät reicht.

- Zum anderen wird ATM als Trägertechnologie eingesetzt. Hier ist ATM mit anderen Layer-2-Protokollen gleichgestellt, wie z.B. Ethernet. Dann wird auf Protokolle höherer Schichten zurück gegriffen und ein VPN z.B. mittels IP-over-ATM eingerichtet und mit IPSec abgesichert.

Der Asynchrone Transfer Modus ist ein paketorientiertes Verfahren, das auf Schicht 2 des OSI-Referenzmodell (Abb. 2.2) arbeitet. ATM kann auf unterschiedlichen physikalischen Medien eingesetzt werden, die dann Übertragungsraten von 2 Mbit/s über 34 Mbit/s und 155 Mbit/s bis hin zu 622 Mbit/s besitzen können. Der Vermittlungsansatz in ATM besteht darin, alle nicht unbedingt notwendigen Funktionen aus dem Teil des Netzes, in dem die Vermittlungsfunktion stattfindet, zu entfernen und in periphere Einheiten (Endsysteme, Steuer- und Überwachungssysteme) zu verlagern. Damit kann die Vermittlungsfunktion vollständig in Hardware implementiert werden. Vermittelt wird auf Basis von kurzen Paketen jeweils gleicher Länge, Zellen genannt, die neben einem Zellkopf Nutzinformationen übertragen. Der Zellkopf (Header) und die Nutzinformationen bestehen jeweils aus einer festen Anzahl ganzzahliger Oktetts. Der Header besteht aus 5 Oktetts, das Nutzfeld aus 48 Oktetts. Die Gesamtlänge der Zelle besteht somit aus 53 Oktetts und ist konstant. Größe und Aufbau einer Zelle sind immer gleich, egal welcher Dienst auf ATM aufsetzt und welche Daten benötigt werden. Abb. 8.12 zeigt den ATM-Kopf und die Nutzdaten. In der Bildbeschreibung der Oktetts sind die zur Verfügung stehenden Kopfelemente detaillierter ausgeführt.



CLP = Cell Loss Priority (Prioritätsfeld bei eventuellem Zellverlust)
GFC = Generic Flow Control (Datenflusskontrolle)
HEC = Header Error Control (Zellkopf-Prüfsummen-Kontrolle)
PT = Payload Type (Nutzdatenidentifikationsfeld)
VCI = Virtual Channel Identifier (Adressierung eines virtuellen Kanals)
VPI = Virtual Path Identifier (Adressierung eines virtuellen Pfades im System)

Abb. 8.12: ATM-Zelle mit insgesamt 53 umfassenden Oktetts

Weiterhin lassen sich beim Header zwei geringfügig unterschiedliche Strukturen ausmachen, die sich nur im ersten Oktett unterscheiden. Zum einen ist dies der

UNI-Header (User Network Interface), zum anderen der *NNI-Header* (Network Network Interface). NNI-Header werden innerhalb einer ATM-Plattform eingesetzt, dagegen kommen am Rande dieser Plattform UNI-Header zum Einsatz.

Der Zellkopf identifiziert Zellen, die zu demselben virtuellen Kanal gehören. Blöcke bzw. Zellen werden in Zeitfenstern asynchron übertragen. Asynchron, weil die Bitrate, die von den Quellen benötigt wird, unabhängig von der insgesamt zur Verfügung stehenden Bitrate ist. Somit werden Zellen von unterschiedlichen Verbindungen aus zeitlich verschachtelt übertragen. Ein anderes Verfahren, das eine Bandbreitenausnutzung nach statistischen Größen vornimmt, ist bereits in Abschn. 8.3 vorgestellt und in Abb. 8.9 illustriert worden.

Durch die übliche Hardwareimplementation kann eine geforderte Rate der vermittelten Zellen (ca. 360.000 Zellen/s bei einem Kanal mit einer Übertragungsrate von 155 Mbit/s) erreicht werden. ATM verwendet die Technik der vereinfachten, verbindungsbezogenen Paketvermittlung und nutzt die asynchronen Zeitmultiplextechnik (*Time Division Multiplexing*) aus, um mehrere Kanäle in einen Pfad zu bündeln, während die ATM-Switches die Aufgabe haben, die Pfade auf den jeweiligen Zielport zu schalten. Andere Beispiele für paketvermittelnde Systeme sind X.25 und IP.

Bei der verbindungsorientierten Technik benötigt eine Ende-zu-Ende-Übertragung von Information einen vorausgehenden Verbindungsaufbau (Signalisierung). Dabei fällt den Headern die wichtige Aufgabe zu, eine Zellenkennzeichnung für diejenigen Zellen vorzunehmen, die innerhalb des asynchronen Zeitmultiplex zur selben Verbindung gehören. Die Kennzeichnung der Zellen erfolgt durch spezielle Kennzeichnungsfelder im Header (Abb. 8.12).

Eine virtuelle Verbindung ist durch Pfade und Kanäle definiert. Dabei bildet die kleinste logische Einheit der Virtuelle Kanal (*Virtual Channel*, VC). Die nächste Abstraktionsstufe ist der Virtuelle Pfad (*Virtual Path*, VP), der aus einem Bündel von mehreren Übertragungskanälen (VC) besteht, die innerhalb eines physikalischen Verbindungsabschnittes das gleiche Ziel haben. Eine Analogie ist im Domainkonzept bei IP zu finden, in dem ein Unternehmen ein Klasse-C-Netz zugewiesen bekommt und anschließend über die in diesem Netz befindlichen IP-Adressen selbstständig verfügen kann.

VC und VP werden im Header durch die Adressinformationen VCI und VPI eindeutig festgelegt. Die Festlegung ist gleichbedeutend mit der Zuweisung eines Identifier, d.h. einem eindeutigen VPI/VCI-Paar wie z.B. VCI=57 und VPI=2. ATM-Netzknoten können sowohl nach Pfaden als auch nach Kanälen vermitteln (vgl. Abb. 8.13). Dabei gibt der Pfad den Weg zum nächsten Netzknoten (VP-Switch) an. Die Unterscheidung zwischen VPI und VCI wird in den Netzknoten ausgewertet, die zusammen als *Virtual Path Connection Identifier* (VPCI) bezeichnet werden. Das VPCI beinhaltet auf Teilnehmerseite im ersten Abschnitt in Abb. 8.13 VPI=2 und auf der Vermittlungsstelle VPI=7. Ausgehend von einer VPI- und einer VCI-Kennzeichnung kann eine *Virtual Path Connection* (VPC) und *Virtual Channel Connection* (VCC) eingerichtet werden. Eine VPC ist gekennzeichnet durch den jeweiligen VPI, der innerhalb einer VPC durch den ATM-Cross-

Connect (VP-Switch) verändert werden kann. Damit bestimmt ein VPC nur eine Teilstrecke. Abb. 8.13 zeigt ein Beispiel für eine Richtung einer virtuellen Kanal- und zweier virtueller Pfad-Verbindungen. Die gesamte durchgängige VCC (über den *Cross-Connect* hinweg) entspricht einer Ende-zu-Ende-Verbindung.

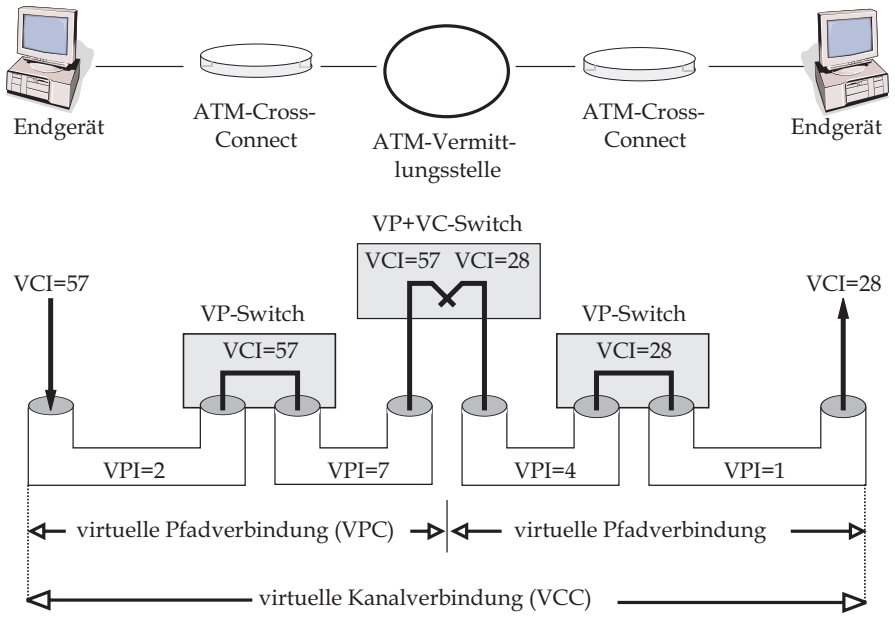


Abb. 8.13: Darstellung einer virtuellen Verbindung

Die Verbindung von Instanzen oberhalb der ATM-Schicht wird als Virtual Channel Connection (VCC) definiert. In ihr kann ein VCI-Wert durch z.B. ATM-Vermittlungsstellen verändert werden (VCI=57 $\Rightarrow$ VCI=28). Die VCC stellt die Ende-zu-Ende-Verbindung zwischen den beiden Endsystemen her, die VPC die jeweiligen Teilstrecken zwischen den Teilnehmern und den Vermittlungsstellen. Die Vermittlung im ATM basiert auf Multiplex- und Switch-Funktionen. Dabei haben Multiplexer die Aufgabe, mehrere Kanäle in einem Pfad zu bündeln, während Switches die Pfade auf den jeweiligen Zielport schalten.

VPI und VCI kennzeichnen alle Zellen, die zu einer Verbindung gehören. Somit wird für die Dauer jeder Nutz- und Signalisierungsverbindung ein VPI (8-Bit) und ein VCI (16-Bit) je Richtung vergeben. Für jede Nutzverbindung ist je Richtung ein VPI plus VCI notwendig und zusätzlich bedarf es noch eines VPI plus VCI je Richtung für die Signalisierung dieser Nutzverbindung. Dabei sind die VCI-Kennungen 0 bis 31 für bestimmte Funktionen reserviert bzw. für zukünftige Festlegungen freigehalten. Beispiele für bereits reservierte Kennungen sind:

- Leerzellen werden immer dann von Schicht 1 übertragen werden, wenn Quellen keine ATM-Zellen produzieren und kein kontinuierlicher Zellenstrom vor-

handen ist. Leerzellen sind durch VPI=0 und VCI=0 sowie PT=0 und CLP=1 festgelegt.

- Nicht zugewiesene Zellen (*unassigned cells*) sind Zellen der ATM-Schicht (VPI=0, VCI=0, PT=X, Abb. 8.12), die keiner Verbindung zugeordnet sind.
- Schicht-1-Steuerinformationen, die nicht an die ATM-Schicht weitergeleitet werden. Gekennzeichnet sind diese Zellen durch VPI=0 und VCI=XX mit ($XX \neq 0$ und $XX \neq 1$).
- Meta-Signalisierungen die zum Auf- und Abbau von Signalisierungsverbindungen dienen. Diese werden ebenfalls aus virtuellen Verbindungen hergestellt. Hierfür wird VPI=Y mit ($Y \neq 0$) und VCI=1 gesetzt.
- Signalisierungsverbindungen die alternativ zur Meta-Signalisierung eingesetzt werden können. Es wird dann VPI=Y mit ($Y \neq 0$) und VCI=5 gesetzt.
- Wartungs- und Überwachungsnachrichten (*operation and maintenance*), die als OAM-Nachrichten bezeichnet werden. qy1

Abb. 8.13 zeigt einen VP-Cross-Connector und eine VP+VC-Vermittlungsstelle. Doch es gibt außer diesen noch weitere Arten von ATM-Netzknoten, die danach unterschieden werden, ob virtuelle Pfad- oder virtuelle Kanalabschnitte abgeschlossen werden und ob die Steuerung über Signalisierungsroutinen oder Einrichtungen des Netzwerkmanagements erfolgt, wie hier aufgelistet:

VP-Cross-Connector: verbindet VP-Abschnitte und übersetzt VPI-Kennungen (keine VCI-Kennung); eine Steuerung erfolgt über die Netzwerk-Managementfunktionen

VC-Cross-Connector: verbindet VC-Abschnitte, terminiert virtuelle Pfadverbindungen und übersetzt VCI-Kennungen; eine Steuerung erfolgt über die Netzwerk-Managementfunktionen

VP-VC-Cross-Connector: wirkt sowohl als VP- als auch als VC-Cross-Connector; eine Steuerung erfolgt über die Netzwerk-Managementfunktionen.

VP-Vermittlungsstelle: verbindet VP-Abschnitte untereinander und übersetzt VPI-Kennungen (keine VCI-Kennungen); eine Steuerung erfolgt mittels Signalisierungsfunktionen.

VC-Vermittlungsstelle: verbindet VC-Abschnitte untereinander, terminiert virtuelle Pfadverbindungen und übersetzt VCI-Kennungen; eine Steuerung erfolgt mittels Signalisierungsfunktionen

VP+VC-Vermittlungsstelle: arbeitet als Zwitter und bietet die Funktion einer VP- als auch einer VC-Vermittlungsstelle; eine Steuerung erfolgt mittels Signalisierungsfunktionen

Für eine virtuelle Kanalverbindung wird für die Dauer der Verbindung eine vereinbarte Dienstgüte während der Kanalaufbauphase mitgeteilt, die auch für die gesamte Verbindungsdauer bestehen bleibt. Eine Änderung der Dienstgüte bedarf eines erneuten Verbindungsaufbaus mit neu zugewiesenen Dienstgüten. Allerdings muss beachtet werden, dass beim Aufbau einer virtuellen Verbindung zunächst ein geeigneter virtueller Pfad ausgesucht wird und anschließend ein Teil der Bandbreite dieses Pfades als virtueller Kanal mit gewünschter Dienstgüte belegt wird. Der virtuelle Pfad wird somit zur virtuellen Hochgeschwindigkeitsstandleitung, innerhalb derer mittels virtueller Kanäle private Subnetze eingerichtet werden können.

Ein ATM-Netz besteht aus einer Sammlung von ATM-Switches und Leitungen zwischen den Endgeräten und den Switches sowie zwischen den Switches. Dabei übernehmen die ATM-Switches die Funktionen von Schaltstellen und Kreuzungspunkten. Die hinter den ATM-Schaltelementen befindliche Logik geht auf die Grundidee der einfachen Weichen im Eisenbahnbau zurück. Mit einer genügend großen Anzahl von Weichen kann ein Rangierbahnhof realisiert werden. Die gleiche Erkenntnis setzte sich vor mehr als 20 Jahren bei der Erforschung von schnellen Strukturen für die Vermittlung von Nachrichten zwischen Prozessoren im Multiprozessor- oder Feldrechnersystemen durch. So werden auch bei ATM-Netzen üblicherweise Schalteinheiten mit zwei Eingängen und zwei Ausgängen gebaut. Die einzige Fähigkeit der Schaltelemente besteht darin, die Ein- und Ausgänge linear zu verbinden oder zu kreuzen. Werden diese Schaltelemente geschickt zusammengesetzt, können beliebig große Netze gebaut werden. In Analogie zur Eisenbahnweiche benötigt ein Schaltelement interessanterweise nur die zwei Zustände: (0) für *geradeaus* und (1) für *überkreuz*. Damit kann ein Paket, welches durch das Netz geführt werden soll, mit einer Reihe von Nullen und Einsen auskommen, wenn die Zellen dazu veranlasst werden, diese Informationen Bit für Bit auszuwerten (*self routing*). Forschungen in diesem Bereich laufen unter dem Stichwort Multi Stage Exchange Networks oder, wenn mehrere Wege zwischen Quelle und Ziel eingerichtet werden sollen, unter dem Begriff *Multi Path Multi Stage Exchange Networks*.

8.4.1 Dienstgüten und -klassen in ATM-Netzen

Dienstgüten, wie sie in Abschn. 2.3.3 vorgestellt wurden, finden in der ATM-Technologie weitreichende Beachtung. Dienstgüten können eine feste oder eine variable Bitrate besitzen. Sie können einen kontinuierlichen Bitstrom genauso bieten wie einem Burst-Betrieb genügen. Weiterhin können sie einen festen Zeitbezug zwischen Sender und Empfänger herstellen oder hierarchisch unabhängig sein. Ebenso kann zwischen Nutzdaten und Signalisierungsinformationen unterschieden werden. Verantwortlich ist hierfür die Adaptionsschicht, die die verschiedenen Anforderungen der Datenübertragung in vier Klassen (A) bis (D) abbildet. Tab. 8.4 zeigt die vier Dienstklassen gemäß [I.362]. Für Dienste der Klasse (A) besteht eine feste Zeitrelation zwischen Sender und Empfänger, die nur eine

minimale Verzögerung (Latenz) zwischen Aussenden und Empfangen der Zellen zulassen. Außerdem wird eine konstante Bitrate der Dienste sowie eine Verbindungsorientierung geliefert. Eine typische Anwendung wird durch die Emulation (*Circuit Emulation*) einer synchronen Durchschaltevermittlung – wie bei der Sprachübertragung erforderlich – erzeugt. Im Gegensatz zu den Diensten der

Tabelle 8.4: Diensteinteilung in vier unterschiedliche Klassen nach [I.362]

	Klasse A	**Klasse B**	**Klasse C**	**Klasse D**
Zeitbezug	zeitkontinuierlich		nicht zeitkontinuierlich	
Bitrate	konstant (CBR)	variabel (VBR)		
Verbindungsart	verbindungsorientiert (CO)			verbindungslos (CL)
Beispiele	Circuit Emulation	Video	Datenübermittlung	Datenübermittlung

Klasse (A) ist die Bitrate der Klasse (B) variabel, jedoch auch zeitkontinuierlich. Eine ideale Anwendung für einen derartigen Dienst wäre die Übertragung einer komprimierten Video-Datei oder die Übertragung von komprimierter Sprache.

Die Klasse (C) bietet keine Zeitrelation zwischen Sender und Empfänger. Auftretende Verzögerungen zwischen Zellversand und Zellempfang fallen nicht störend ins Gewicht. Die Bitrate ist variabel und verbindungsorientiert, wie auch die der Klasse (B). Als ein geeignetes nicht isochrones Übertragungsbeispiel kann der Frame-Relay-Dienst angesehen werden. Dienste der Klasse (D) und Klasse (C) verbinden die nicht zeitkontinuierliche Nachrichtenübertragung und unterscheiden sich im verbindungslosen Austausch (Klasse D) von übertragenen Nachrichten. Es werden nur einzelne Datenpakete ohne Zusammenhalt durch eine virtuelle Verbindung übertragen. Damit stellt dieser Dienst den typischen IP-basierten Dienst im Internet dar.

Aufsetzend auf den vier Grundklassen (Tab. 8.4) hat das ATM-Forum fünf Dienstgüteklassen bzw. Verkehrsarten formuliert [AF56-96]. Sie sind in Tab. 8.5 mit ihren Eigenschaften und Parametern aufgelistet. Dabei ist die Bezeichnung der Dienstgüteklassen ebenso wie ihre Anwendung auf die oben spezifizierten Dienstklassen weitgehend selbsterklärend. Die erste Spalte zeigt die Dienstgüteklassen, die mit den Dienstklassen in der zweiten Spalte der Tab. 8.4 im Einklang stehen.

Die Dienstgüteparameter in der letzten Spalte von Tab. 8.5 definieren bzw. grenzen die Dienste ein. Für alle Dienste muss eine Spitzenlast, die *Peak Cell Rate* (PCR), die zu keinem Zeitpunkt überschritten werden darf, angegeben werden. Als Untergrenze sichert die *Minimum Cell Rate* (MCR), die nur im Dienst (ABR) vertreten ist, einem Sender ein garantiertes Minimum an Übermittlungskapazität zu. Die anhaltende bzw. *Sustainable Cell Rate* (SCR) ist eine Zellenrate, die für den Dienst (VBR) von erheblicher Bedeutung ist. Sie stellt einen Medianwert dar, um den die Dienstgüte zeitlich schwankt. Kurzfristige Überschreitungen nach oben werden durch die *Maximum Burst Size* (MBS) begrenzt. Für isochrone Dienste (CBR, rt-VBR) werden die Freiheitsgrade durch die *Maximum Cell Transfer Delay*

Tabelle 8.5: Einteilung der Dienstklassen gemäß ATM-Forum

Dienstgüte-klasse	**Verkehrs-charakteristik**	**Dienstgüte Garantien**	**Dienstgüte-parameter**
CBR (Constant Bit Rate)	Isochroner Verkehr Klasse A	Konstante Zellenrate; begrenzte Verzögerungen; begrenzte Fehlerrate	PCR (Peak Cell Rate), maxCTD (Maximum Cell Transfer Delay), CDVT (Cell Delay Variation Tolerance), CLR (Cell Loss Ratio)
rt-VBR (Real-Time Variable Bit Rate)	Realzeit-bedingungen; variable Zellenrate Klasse B	Am Mittelwert orientierte Zellenrate; begrenzte Verzögerungen; begrenzte Fehlerrate	PCR, SCR (Sustainable Cell Rate), MBS (Maximum Burst Size), maxCTD, CDVT, CLR
nrt-VBR (Non-Real-Time Variable Bit Rate)	Keine Realzeitbedingungen; variable Zellenrate Klasse C und D	Am Mittelwert orientierte Zellenrate; begrenzte Verzögerungen; begrenzte Fehlerrate	PCR, SCR, MBS, CLR
ABR (Available Bit Rate)	Keine Realzeit-bedingungen; Mindestzellenrate; Mitbenutzung freier Kapazitäten Klasse C und D	Mindest- Zellenrate; fairer Anteil an unreservierter Kapazität; begrenzte Fehlerrate	PCR, MCR (Minimum Cell Rate), CLR
UBR (Unspecified Bit Rate)	Sporadische Nutzung von Kapazitätslücken	Keinerlei Zusicherung	PCR

(maxCTD) beschränkt, indem die Latenz, die Verzögerungen der Zellen bei deren Übermittlung zwischen den Kommunikationspartnern, nicht überschritten werden darf. Ebenso ist eine *Cell Delay Variation Tolerance* (CDVT) definiert, die die maximal zulässige Verzögerung zwischen Fertigstellung und Übertragung einer Zelle vorgibt. Ergänzend ist als die möglicherweise auftretende Verlustrate die *Cell Loss Ratio* (CLR) definiert, die das Verlustverhältnis zwischen Zellenverlust und Gesamtzellenübertragung einer Verbindung beschreibt.

8.4.2 Verkehrs- und Überlaststeuerung

Wurde bisher die ATM-Netztechnologie vorwiegend aus der Sichtweise eines Teilnehmers betrachtet, soll in diesem Abschnitt auf die Verkehrs- und Überlaststeuerung *(Traffic and Congestion Control)* eingegangen werden. Hier tritt eine Überlastsituation dann ein, wenn die für die bereits bestehenden Verbindungen vereinbarten Dienstgüte-Parameter (QoS-Parameter) nicht mehr eingehalten werden können. Aufgabe der Verkehrssteuerung *(Traffic Control)* ist es, mit geeigneten

Maßnahmen einer Überlastsituation entgegenzuwirken.

Eine Verkehrssteuerung setzt eine gleichzeitige Verkehrsüberwachung voraus, um frühzeitig zu erkennen, ob das Netz in einen kritischen Zustand hineinläuft. Somit ist ein Überwachungsmechanismus, verbunden mit Korrekturmaßnahmen, erforderlich. Die Menge dieser Maßnahmen wird als *Usage Parameter Control* (UPC) oder auch als *Policing* bezeichnet. Der Kern dieser Maßnahmen besteht darin, jede einzelne ATM-Zelle, die von einem Teilnehmer ins Netz geschickt wird, dahingehend zu prüfen, ob sie mit den ausgehandelten Verkehrsparametern konform ist oder nicht. Wird z.B. eine CBR-Anwendung angenommen, ist die Spitzen-Zellrate (PCR) der einzige zu vereinbarende und folglich zu überwachende Verkehrsparameter. Der Abstand zwischen zwei ATM-Zellen, die von der Quelle erzeugt werden, darf damit den Wert 1/PCR nicht unterschreiten. Da jedoch bereits auf einer physikalischen Anschlussleitung mehrere virtuelle Verbindungen bestehen, kann es aufgrund unterschiedlicher Wartezeiten auf dieser Leitung zu unterschiedlichen Laufzeiten der ATM-Zelle kommen.

Es hat sich gezeigt, dass eine Überwachung der Messung einzelner Zellabstände nicht ausreicht. Es muss ein flexibleres Verfahren eingesetzt werden, welches die Verbindung über einen größeren Zeitraum beobachtet und nicht bereits bei einem einmaligen Unterschreiten des Zellabstandes Korrekturmaßnahmen einleitet. Hier hat sich das *Leaky-Bucket*-Verfahren (Abschn. 2.3.3) durchgesetzt, welches auf dem *Generic Cell Rate Algorithm* (GCRA) beruht. Bei diesem Verfahren wird eine kurzzeitige Häufung von Zellankünften *(Burst-Toleranz)* zugelassen, falls sich diese durch entsprechend größere Abstände im weiteren Verlauf wieder ausgleicht. Abb. 8.14 zeigt den Algorithmus als Ablaufplan. Die Ankunftszeit $t(k)$ einer ATM-Zelle (k) wird mit einer theoretischen Ankunftszeit (TAT) verglichen. Der Anfangswert ist dabei $TAT = 0$. Kommt die Zelle (k) später an $(t(k) \geq TAT)$, ist die Zelle konform und als aktuelle Ankunftszeit um $I = 1/PCR$ inkrementiert. Kommt die Zelle dagegen zu früh an $(t(k) \leq TAT)$, wird geprüft, ob das Limit der Häufung $(TAT - L)$ bereits erreicht ist. Wenn dies nicht zutrifft, ist die Zelle ebenfalls konform und die neue TAT ergibt sich dann durch die Inkrementierung der alten TAT um 1/PCR. Andernfalls handelt es sich um eine nicht konforme Zelle, die die Verkehrsparameter verletzt hat. Als Reaktion kann jetzt eine Reduzierung der Prioritätsangabe im Zellkopf erfolgen oder gar die Zelle ganz vernichtet werden.

Als Modellvorstellung kann ein undichter Eimer betrachtet werden, der mit der Zeit 1/PCR Wasser verliert. Das Wasser tropft aus dem Eimer, der einer Zelle entspricht. Solange auf dem Transportband (Übertragungssystem) die ATM-Zellen einen Abstand von 1/PCR einhalten, wird der Eimer nur bis zu einer bestimmten Marke (*limit*) gefüllt. Kommen die Zellen in dichterer Folge, füllt sich der Eimer und läuft im Extremfall über, was zu einem Zellverlust führen würde.

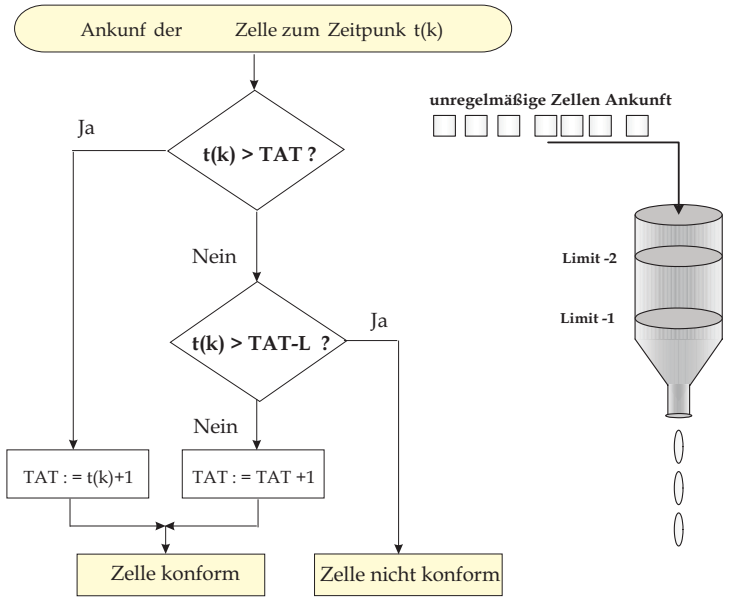


Abb. 8.14: Grundidee des Leaky-Bucket-Verfahrens

8.4.3 ATM-Referenzmodell

Das ATM-Referenzmodell ist in Anlehnung an das Schichtenmodell des OSI-Referenzmodells (Abb. 2.2) von der ITU-T entwickelt worden. Allerdings unterscheidet sich das Schichtenmodell für die Kommunikation in offenen Systemen vom ATM-Referenzmodell in einigen wesentlichen Punkten. Es ist nicht so linear aufgebaut, da die dienstintegrierende Kommunikation wesentlich mehr Komponenten besitzt als die reine Datenkommunikation gemäß OSI-Modell.

In beiden Modellen gleich bzw. ähnlich definiert, hängt die Bitübertragungsschicht – auch als physikalische Schicht (PL) bezeichnet – direkt vom Übertragungsmedium ab. Dieses kann z.B. aus Glasfaser oder aus einem Koaxialkabel bestehen. Diese Schicht führt die Umsetzung auf die Leitungsebene sowie die Synchronisation durch. In den ITU-T-Empfehlungen werden zusätzlich zu den aufeinander aufbauenden Schichten drei Kommunikationsebenen (*planes*) eingerichtet:

- Die Nutzerebene (*user plane*) stellt einer Anwendung den Transport von Nutzdaten zur Verfügung
- Die Steuerebene nimmt den Auf- bzw. Abbau und die Unterhaltung von Nutzer- bzw. Anwenderverbindungen vor und
- Die Managementebene teilt sich auf in zwei Unterebenen, unfd zwar in

das Schichtenmanagement (Layer Management) und das Ebenenmanagement (*plane management*). Dabei versieht das Schichtenmanagement die Koordination der einzelnen Schichten; das Ebenenmanagement übernimmt überwachende und koordinierende Aufgaben im Netz (Abb. 8.15).

Herausragende spezifische Schichten im Referenzmodell sind die ATM-Schicht *(ATM-Layer,* ATL) und die ATM-Anpassungsschicht *(ATM Adaption Layer,* AAL). Im direkten Vergleich mit dem OSI-Referenzmodell (siehe auch Abb. 2.2) sind diese beiden Schichten zwischen Schicht 1 und 3 (Abb. 8.15) angesiedelt.

Die ATM-Schicht sorgt für den Zellentransport inklusive der Vermittlung von ATM-Zellen in den Netzelementen für alle Dienste. Sie stellt alle Funktionen bereit, die sich im Zellkopf wiederfinden:

- Bearbeitung und Identifizierung der virtuellen Kanäle (VC) und der virtuellen Kanalbündel (VP)
- Sicherung der Zellkopfinformationen
- Zellenkennzeichnung für spezielle Verwendungen
- Überwachung der maximalen Übertragungsrate
- Multiplexen von Zellen

Weiterhin wird in der ATM-Schicht dem Nutzfeld der Zelle der Zellkopf hinzugefügt (vgl. Abb. 8.12). Abb. 8.15zeigt das vollständige ATM-Referenzmodell gemäß CCITT I.321. Die ATM-Adaptionsschicht (AAL), die direkt oberhalb auf

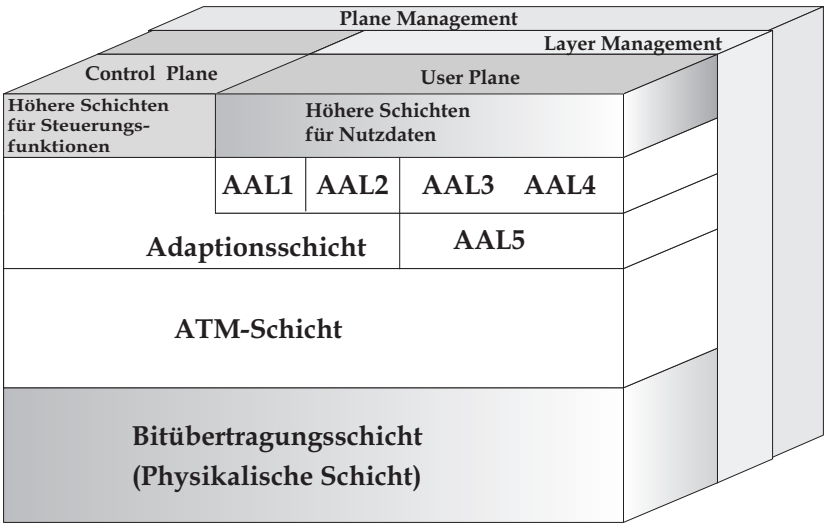


Abb. 8.15: ATM-Referenzmodell, Dienste und Übertragungstechniken nach CCITT I.321

die ATM-Schicht aufsetzt, stellt ein Bindeglied zwischen den zu übertragenden Nutzdaten und der zellorientierten Übertragung durch die ATM-Schicht dar. Die Dienste können unterschiedliche Dienstgüten haben (Tab. 8.5). Die Aufgabe der Adaptionsschicht besteht darin, diese verschiedenen Forderungen jeweils auf die ATM-Zellen abzubilden und die Nutzdaten aus den empfangenen Zellen wieder den höheren Schichten bereitzustellen.

Die unterschiedlichen AAL-Typen Abb. (8.15) haben folgende Anwendungsgebiete:

AAL-Typ 1: für zeitkontinuierliche Dienste mit konstanter Bitrate

AAL-Typ 2: für zeitkontinuierliche Dienste mit variabler Bitrate

AAL-Typ 3/4: für eine gesicherte verbindungsorientierte bzw. verbindungslose Datenübermittlung

AAL-Typ 5: für eine einfache und schnelle Datenübermittlung

Dabei kann – grob betrachtet – die AAL, wiederum in zwei Teilschichten untergliedert werden: zum einen in die *Segmentation and Reassembly Sublayer* (SAR), deren Aufgabe darin besteht, eine Aufteilung auf der Sendeseite sowie eine Zusammenfassung auf der Empfangsseite der Nutzdaten in der Länge einer ATM-Zelle vorzunehmen; zum anderen in die *Convergence Sublayer* (CS), die eine dienstabhängige Aufgabe inne hat, z.B. Einkapselung der Nutzdaten oder Sicherung der übertragenen Nutzdaten durch eigene Protokollelemente.

Tab. 8.6 fasst die Funktionen der einzelnen Schichten des ATM-Protokoll-Referenzmodells zusammen. Die Physikalische Schicht (PL) ist direkt vom Übertra-

Tabelle 8.6: Funktionen der Schichten des ATM-Protokoll-Referenzmodells, gemäß I.321

<table>
<tr><th>Funktionen höherer Schichten</th><th colspan="2">Höhere Schichten</th></tr>
<tr><td>Konvergenz</td><td>CS</td><td rowspan="2">AAL</td></tr>
<tr><td>Segmentieren und wieder zusammensetzen</td><td>SAR</td></tr>
<tr><td>Generische Flusskontrolle
Erzeugen / Extrahieren des Headers
Übersetzen der VPI- / VCI-Werte
Zellen-Multiplex und -Demultiplex</td><td colspan="2">ATM</td></tr>
<tr><td>Entkopplung der Zellrate
Erzeugen und Verifizieren der HEC-Sequenz
Erkennen von Zellanfang und -ende
Anpassen an den Übertragungsrahmen
Erzeugen / Erkennen des Übertragungsrahmens</td><td>TC</td><td rowspan="2">PL</td></tr>
<tr><td>Bit-Timing / Synchronisation
Physikalisches Medium</td><td>PM</td></tr>
</table>

gungsmedium abhängig und ebenfalls in zwei Subschichten unterteilt, die *Transmission Convergence Layer* (TC) und die *Physical Medium Layer* (PM). Die TC übt da-

bei eine Transformation der zu sendenden ATM-Zellen auf das jeweilige Übertragungssystem aus, denn die ATM-Technologie ist unabhängig vom Übertragungssystem. Die mediumabhängigen Funktionen zur Bitübertragung, wie z.B. Signalform und Leitungskodierung, sind ebenfalls in der Physikalischen Schicht (PL) und dort in die Teilschicht (PM) eingegliedert (Tab. 8.6).

In den Netzknoten eines ATM-Übertragungsnetzes werden lediglich Funktionen der Physikalischen Schicht (PL) und der ATM-Schicht (ATL) ausgeführt. Die ATM-Anpassungsschicht (AAL) ist in den Endgeräten am Domainrand vorhanden, da innerhalb eines ATM-Netzes Informationen der verwendeten Dienste nur in ATM-Zellen übertragen werden. Weitere Informationen zur ATM-Technologie sind z.B. bei [Kauffels 1994] oder [Siegmund 1999] zu finden. Mehr theoretische Ansätze verfolgt [Hasslinger 1999].

Ein anderer Aspekt, der zunehmend mit der VPN-Technologie in Verbindung gebracht wird, ist die Privatsphäre bzw. die Vertraulichkeit bei der Datenübertragung. Dieser Aspekt wird in der ATM-Technologie lediglich durch eine *Closed User Group* (CUG) gewährleistet. Dabei werden die zu übertragenden Daten, wenn sie nicht auf höheren Ebenen verschlüsselt werden, transparent übers Netz geschickt. Andere Möglichkeiten eine Vertraulichkeit z.B. mittels Verschlüsselung auf ATM-Stufe wurde lange Zeit überhaupt nicht verfolgt. Bis zur Drucklegung des Buches sind keine Standards oder gemeinsame Absichtserklärungen von Herstellern bekannt. Es gibt allerdings vielversprechende Untersuchungen und Projekte, wie eine Verschlüsselung implementiert werden könnte. Prinzipiell sind zwei Möglichkeiten denkbar:

- Bei der Verschlüsselung auf *Cellstream*-Ebene wird der ganze Zellstrom, der das ATM-Netzwerk-Interface verlässt, einer Verschlüsselung unterzogen. Hierbei kann noch unterschieden werden, ob ausschließlich a) die Nutzlast oder b) die Nutzlast und der Zellkopf verschlüsselt werden sollen. Allerdings ist eine Kodierung des Zellkopfes wenig sinnvoll, da dieser dann in allen auf dem Wege passierenden ATM-Switches wieder dekodiert werden muss, um die VP- und VC-Informationen auswerten zu können. Ein weiterer Nachteil dieser Methode ist, dass alle Zellen mit dem gleichen Schlüssel kodiert werden, auch wenn sie aus unterschiedlichen Quellen stammen.
- Sinnvoller ist dagegen eine Verschlüsselung der virtuellen Kanäle (VC), die durch die Ende-zu-Ende-Verbindung den Einsatz eigener Schlüssel für jedes VP/VC-Paar ermöglichen.

Diesen beiden Möglichkeiten stehen heute noch einige Probleme gegenüber. So stellen die Übertragungsraten von 2 GBit/s aufwärts erhebliche Anforderungen an die Elektronik. Kommen dann noch zeitintensive Verschlüsselungsalgorithmen hinzu, reicht die zur Verfügung stehende Rechenkapazität nicht aus. Wird dagegen eine zellenweise Verschlüsselung eingesetzt, entstehen Blöcke von 384 Bit, die aufgrund ihrer geringen Größe ungeeignet sind für z.B. asymmetrische Verfahren wie RSA. Im Idealfall findet eine Verschlüsselung in den Endgeräten statt – die für die ATM-Switches transparent sind –, indem nur die Nutzlast verschlüsselt wird.

Als jüngste Entwicklung kann verzeichnet werden, dass an einer Neudefinition der AAL gearbeitet wird, die – parallel zu den bestehenden AAL 1-5 – einen verschlüsselten Service zur Verfügung stellt.

Zum Abschluss des Kapitels über Trusted VPN sollen Möglichkeiten und Grenzen der ATM-Verbindungen aufgezeigt werden. Obwohl immer mehr MPLS-Router auf dem Markt gebracht werden, die eine elegante VPN-Einrichtung zulassen, nutzen viele Anbieter (NSP) und Netzbetreiber großer Firmen aus Kostengründen die vorhandene ATM-Technologie als Unterbau für die MPLS-Technologie.

8.4.4 MPLS über ATM-Verbindungen

Der Name MPLS (*Multiprotocol Label Switching*) könnte nahe legen, dass mehrere Protokolle unterstützt werden, jedoch ist bisher nur daran gedacht worden, IPv4 in ATM und Frame Relay zu integrieren.

Im Prinzip kommt eine Frame-basierte Umgebung einem Stream- Merging-Verfahren – also Eigenschaften, die MPLS hat – entgegen, bei dem beispielsweise mehrere Upstream-Labels in einem einzigen Downstream-Label zusammengefasst werden können. Bei MPLS müssen in so einem Fall keine Änderungen in einer existierenden Label-Swapping-Struktur vorgenommen werden, jedoch stellt dies Anforderung die ATM-Technologie vor einige ernsthafte Probleme. D.h. für Firmen die die ATM-Technologie als Unterbau für die MPLS-Technologie nutzen, sind deutliche Grenzen gesetzt.

Stream-Merging-Verfahren sind in der ATM-Technologie sehr komplex und unhandlich gehalten. Dies liegt im Wesentlichen an den früher entwickelten Designanforderungen. In der ATM-Technologie werden Datenpakete in einer AAL5-PDU gekapselt und als ATM-Zellen verschickt. Diese Zellen haben bestimmte spezifische VPI/VCI-Werte. Alle Zellen innerhalb einer VPI/VCI werden in einer Sequenz verschickt. Weiterhin sind alle ATM-Switches entlang eines Übertragungsweges dazu angehalten, die anfänglich eingerichtete Zellordnung einzuhalten und ggf. wieder korrekt in der Sequenz herzustellen.

Damit taucht für die MPLS-Technologie, die eine Stärke in den Stream- Merging-Verfahren aufweist und somit eine gute Netzskalierbarkeit zulässt, ein erheblicher Konflikt auf, wenn MPLS in einer ATM-Umgebung eingesetzt werden soll.

In diesem Szenario müssten mehrere eintreffende VC in einem einzigen weitergeführten VC einen ATM-Switch verlassen. Sofort gibt es Probleme, die ursprünglichen PDU zu rekonstruieren, da die ATM-Zell-Köpfe keinerlei Informationen über die ursprüngliche Ordnung enthalten.

Es haben sich jedoch zwei Hilfskonstruktionen herauskristallisiert, die eine Zell-Zusammenführung unterstützen und dem Stream-Merging-Problem begegnen:

VC-Zusammenführung: Es werden mehrere an einem Switch angekoppelte VC in einem Knoten zusammengeführt. Anschließend verlassen die gesamten Informationen dann in einem einzigen VC wieder den Switch. Ein MPLS-Knoten

vollzieht diese Zusammenführung; dabei werden die Zellen von einer AAL5 getrennt von Zellen der nachfolgenden AAL5 behandelt. Dazu sendet der beteiligte ATM-Switch verzögert Zellen aus, die zu den nachfolgenden Frames gehören, solange Zellen, die zum gerade passierenden Frame gehören, übertragen werden. Erst wenn der Indikator für das Frame-Ende erreicht ist, wird das nächste Frame übertragen. Allerdings ist dieser Speicher- *(buffering)* und Weiterleitungsmechanismus *(store-and-forward)* nicht typischerweise in den heutigen ATM-Switches verfügbar.

VP-Zusammenführung: Ebenso wird in einem Switch ermöglicht, Informationen aus mehreren angekoppelten VP in einem einzigen *Virtual Path* zusammenzuführen. Dabei unterscheiden die VCI innerhalb der VP-Zusammenführung Frames von verschiedenen Quellen. Diese Art der Zusammenführung hat den Vorteil, dass eine größere Anzahl von schon vorhandenen, im Betrieb befindlichen ATM-Switches eingesetzt und vorhandene Netzstrukturen ausgenutzt werden können. Ein weiterer Vorteil der VP-Zusammenführung liegt in der nicht benötigten Verzögerung bzw. Zwischenspeicherung von Frames, wie sie in der VC-Zusammenführung notwendig ist. Allerdings besteht ein Hauptnachteil darin, dass eine VCI-Koordinierung bei jedem VP durchgeführt werden muss.

Abschließend ist zu erwähnen, dass die MPLS-Architektur sowohl die VP- als auch die VC-Zusammenführung unterstützt. Allerdings muss dann ein ATM-Switch, wenn er in einer MPLS-Domain eingebunden werden soll, zusätzlich in der Lage sein, von den Nachbar-ATM-Switchen zu erfahren, ob diese ebenfalls eine VP/VC-Zusammenführung unterstützen, und wenn ja welche. Langfristig ge-

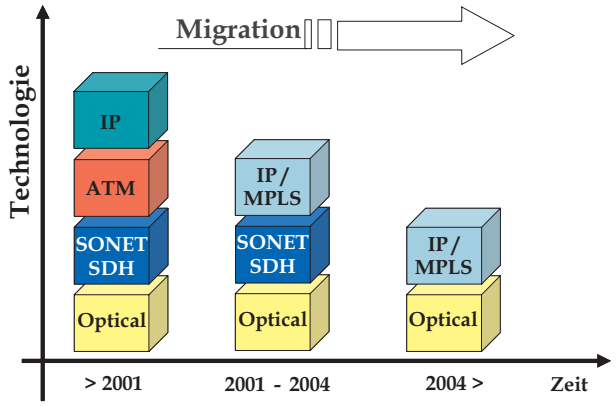


Abb. 8.16: Mutmaßliche Entwicklung von IP-MPLS und anderen Übertragungsmedien

sehen ist damit die ATM-Technologie nur als Übergang für andere Transportplattformen, wie z.B. optische Netze, anzusehen. Abb. 8.16 gibt einen Eindruck, wie

die zeitliche Entwicklung für die Transportplattformen unterhalb von IP/MPLS aussieht.

8.5 Übungen

1. In welcher Dienstgütenklasse und in welcher Verkehrscharakteristik ist bei ATM i.d.R. eine E-Mail angesiedelt?
2. In welcher Dienstgütenklasse und in welcher Verkehrscharakteristik ist bei ATM eine E-Mail platziert, die mit *high priority* versandt wurde?
3. In welcher Dienstgütenklasse und in welcher Verkehrscharakteristik soll ein Video-Stream eingebracht werden, damit die Laufzeitverzögerungen so gering wie möglich sind?
4. Welchen Unterschied gibt es in der Dienstgüte zwischen Internet und Frame Relay?
5. Was wird bei der MPLS-Technologie benötigt, um QoS umsetzen zu können?
6. Warum wird in einer MPLS-Domain kein DiffServ bzw. IntServ benötigt?
7. Welche Anforderungen sind hinsichtlich der Vertraulichkeit bei Voice-over-IP (VoIP) zu stellen?
8. Welche(s) Protokoll(e) wird/werden für VoIP eingesetzt?
9. Worin besteht der Unterschied zwischen CoS und Qos?
10. Wie werden die Verfahren *Priorisierung* und *Reservierung* in IP-Netzen umgesetzt?
11. Worin bestehen die Unterschiede von RSVP-TE und CR-LDP?
12. Worin unterscheidet sich die Burst-Toleranz zwischen Frame Relay und ATM?
13. Wie ist die Verkehrscharakteristik der ATM-Zelle (k), die mit einer theoretischen Ankunftszeit ($t(k) \geq TAT$) am Ziel ankommt, einzustufen?

9 Hybrid VPN

Virtuelle Private Netze sind ein geeignetes Medium, um Datenströme innerhalb eines Unternehmens und zu externen Partnern auf einer Plattform zu vereinheitlichen. Aufwand und Verwaltung der Netze erfordern jedoch Fachwissen und ständige Betreuung, der nicht zu unterschätzen ist. Somit kann es gerade für kleine und mittelständische Unternehmen (KMU) durchaus sinnvoll sein, das notwendige Wissen und die Betreuung bei einem Netz-Service-Provider (NSP) einzukaufen. Aber auch große Firmen, die sich ausschließlich auf ihr Kerngeschäft konzentrieren, sind Auftraggeber für VPN-Provider. Allerdings gerät ein Unternehmen bei einer VPN-Fremdrealisierung bei der Übertragung firmeninterner Daten in die Abhängigkeit Dritter. Aufschlussreich sind somit Informationen, wie leistungsstark das Backbone eines Providers ausgelegt ist, und ob und in welcher Form z.B. eine Überbuchung (*over-subscription*) stattfindet. Ebenso ist die Frage wichtig, ob Sicherungsmaßnahmen hinsichtlich der Vertraulichkeit automatisch oder erst auf Anforderung eingerichtet werden.

Ob oder ggf. in welchem Umfang eine Abhängigkeit erwünscht bzw. akzeptabel ist, kann letztendlich nur nach einer sorgfältigen Betrachtung und Abwägung aller Aspekte beantwortet werden. Für eine solche Entscheidung ist es hilfreich, das Kerngeschäft eines VPN-Anbieters zu kennen und zu verstehen. Welche Leistungen werden wie angeboten, wie sieht eine spätere Betreuung im Störfall aus, wann, in welcher Zeit und wie werden Störfälle behoben – um nur einige Fragen aufzugreifen.

Die Leistungen und die Anforderungen, aber auch die Perspektive einer solchen Dienstleistung aus Sicht eines NSP sollen Gegenstand des vorliegenden Kapitels sein. Abschn. 9.1 geht auf typische Strukturen und Netzverflechtungen eines Providers ein. Interessant erscheint die Frage der Definition des Übergabepunktes zwischen Netzbetreiber und einem Unternehmen. Inzwischen liegen hierzu Referenzmodelle vor, denen sich die Abschnitte 9.1.4 und 9.1.5 widmen. Dabei diskutiert Abschn. 9.1.5 ein VPN, dass ausschließlich in dem Verantwortungsbereich eines Providers fällt. Abschn. 9.1.4 beschreibt das Referenzmodell eines VPN, das vornehmlich in den Händen des eigenen Unternehmens liegt.

Ein weiterer Anhaltspunkt für eine Entscheidung ist die Netzwerk-Performance sowie das Netzwerkmanagement des Providers (Abschn. 9.2). Die hierzu zählenden, zu vereinbarenden Liefer- und Leistungsbedingungen, also die *Service Level Agreement* (SLA), die mit dem Kunden des Netzbetreibers auszuhandeln sind, werden in Abschn. 9.2.3 betrachtet.

Für einen Netzbetreiber stellt sich die Herausforderung nach der Realisierung von Leistungsklassen bzw. Serviceklassen, den *Class of Services* (CoS) und deren messbarer Qualität von Dienstgüten, den *Quality of Services* (QoS) (vergl. Abschn.

2.3.3), die einem Kunden zu unterschiedlichen Konditionen zur Verfügung gestellt werden. Weiterhin ist deren technische Umsetzung mittels *Virtual Circuits* (VC) oder mit einem *Multiprotocol Label Switching* (MPLS) von Interesse (vergl. Abschn. 8.1). Zur Orientierung wird im Abschn. 9.3 eine VPN-Klassifizierung nach sinnvollen Größenordnungen in vier Leistungsklassen vorgenommen. Abschließend wird in diesem Kapitel eine Methodik zur Beurteilung verschiedener Provider mit Musterwerten vorgestellt (Abschn. 9.3.1).

9.1 Provider-Netze und Netzstrukturen

Motor der VPN-Technologie und damit auch des IP-Protokolls ist die sprunghafte Verbreitung der Intranetze, die das Tagesgeschäft der Unternehmen rasant änderten. Gleichzeitig führte dies zu einer Anforderungsänderung für die darunter liegenden Netze. Gerade die einfache Möglichkeit, mit Webbrowsern, die firmeninterne Kommunikation bzw. Informationsdarstellung für das Tagesgeschäft zu nutzen, fand schnelle Verbreitung. Standardisierte Nutzerschnittstellen, die einfach zu entwickeln sind (HTML-Dokumente), und die Weiterverwendung der Altsysteme (*legacy systems*), die oftmals auf Stammdaten zugreifen, die auf Großrechner lagern, sowie die Möglichkeit, Client-Server-Applikationen einzubinden, haben enormen Anklang in der Wirtschaft gefunden. Mehr und mehr wurden Geschäftsprozesse ins Intranet verlagert, Kosten eingespart und ein erheblicher Produktivitätsgewinn erzielt.

Das neue Jahrhundert eröffnet völlig neue Wege und Vorstellungswelten, wie kommuniziert werden kann. Die Veränderung ist derartig einschneidend, dass von zwei verschiedenen Welten gesprochen werden kann. Mussten sich noch früher Service-Provider damit zufrieden geben, ihren Kunden *nur* Transportdienstleistungen, z.B. Mietleitungen (*leased lines*) bzw. Frame-Relay-Verbindungen anzubieten, haben in der *neuen* Welt Service-Provider und Geschäftspartner (Kunden) eine wesentlich engere Beziehung miteinander geknüpft. VPN werden gemeinsam mit dem Kunden nach seinen Bedürfnissen eingerichtet und abgesichert. Der Service-Provider wird vertrauensvoller Teilhaber und Experte seiner Kunden in Bezug auf ihre Internet-Geschäftsentwicklungen sowie deren Extranet-Geschäftsverbindungen.

Dabei spielt das IP eine immer wichtigere Rolle, so dass sich für die VPN-Technologie verstärkt der Begriff *IP-VPN* verwendet wird. IP ist zum Standardprotokoll der elektronischen Kommunikation geworden und verdrängt andere Netzprotokolle. Auch beim Standort-übergreifenden Datenverkehr einer Firma beginnt sich IP durchzusetzen. Derartig eingerichtete VPN laufen über ein gesichertes, nicht-öffentliches Backbone eines NSP, der diesen Netzservice als Kommunikationstechnik anbietet. Hierzu zählen Firmen wie z.B. Arcor, BT Ignite, Cable & Wireless, KPN International, Telekom und Worldcom. Die eingesetzte Technologie schließt häufig ein Trusted VPN mittels ATM oder Frame Relay ein, über die dann das IP geführt wird (Abschn. 8).

Optionen wie unterschiedliche Priorisierung von Daten oder Hochverfügbarkeitsanforderungen sind damit prinzipiell erfüllbar. Weiterhin verbreitet sich die Verwendung von IP-Switching und Multiprotocol Label Switching (MPLS). Dabei steigert MPLS neben einer größeren Flexibilität und Skalierbarkeit den Paketdurchsatz und somit die Leistungsfähigkeit der WAN-Strecken erheblich, denn das zeitaufwändige Weiterleiten und Lesen der Routing-Einträge von Router zu Router wird drastisch gesenkt.

Bevor auf die Leistungen der Netz- bzw. Serviceanbieter im Einzelnen eingegangen wird, ist es sinnvoll, sich mit dem Geschäftsmodell eines Netzbetreibers auseinanderzusetzen, um später eindeutige eigene Anforderungen an die Betreiber und deren Dienstleistungen formulieren zu können.

9.1.1 Struktur der globalen Netze

Ausgehend von einem globalen Hochgeschwindigkeits-Backbone, das ein weltumspannendes Kernnetz darstellt, an dem z.B. MCI und AT&T beteiligt sind, entstehen hierarchische Untergruppierungen. Firmen, die auf der obersten Ebene Netze unterhalten, zählen zur ersten Kategorie, die auch als *Tier-1-Carrier* bezeichnet werden. Firmen mit Hauptnetzzugängen – den so genannten *Network Access Points* (NAP) – zur obersten Ebene bilden die zweite Kategorie, die auch als nationale Ebene bezeichnet wird. Gekennzeichnet sind diese durch Firmen, die extensiv eigene Netze aufbauen und verwalten. Diese voneinander unabhängigen Firmen pflegen einen eigenen Hauptnetzzugang. Hierzu zählen Firmen wie z.B. Worldcom, France Telecom, Deutsche Telekom und Sprint.

Abb. 9.1 skizziert die Hierarchiestufen unterschiedlicher Netzanbieter an einigen Beispielen. Die weißen Rechtecke deuten auf die jeweils unterschiedlichen Anbieter einer Kategorie hin. Die regionale Ebene erstreckt sich unterhalb der zweiten Kategorie. Diese sind üblicherweise auf die Ausdehnung in einem Bundesland oder auch nur auf Teile davon beschränkt. Ableger der großen Energieversorger sind typische Vertreter dieser Kategorie. Die letzte Kategorie bilden die lokalen Netzanbieter (ISP), die oftmals neben Diensten im Datenbereich auch Sprachservice anbieten und im Umfeld einer Großstadt angesiedelt sind und deren Angebote sich häufig auch nur auf diese Großstadt oder das nahe liegende Ballungszentrum begrenzen. Natürlich ist diese Einteilung etwas idealisiert, denn so klar wie in Abb. 9.1 die Abgrenzungen der Kategorien skizziert wurden, sind diese längst nicht.

Es gibt Anbieter, die sich über mehrere Ebenen erstrecken. So ist z.B. die T-Online International GmbH eine derjenigen Anbieter, die überregional flächendeckend – nicht nur als Internet Service Provider, sondern auch mit ihrem VPN-Produkt Secure VPN – ganz unterschiedliche Dienste für Kunden bereithält. Weiterhin drängen ausgelagerte IT-Abteilungen, die sich zu eigenen GmbHs entwickelt und den Weg zum IT-Dienstleister erfolgreich beschritten haben, auf den Drittmarkt und bieten ebenfalls Mehrwertdienste an. Die ehemaligen Kostentreiber der Kon-

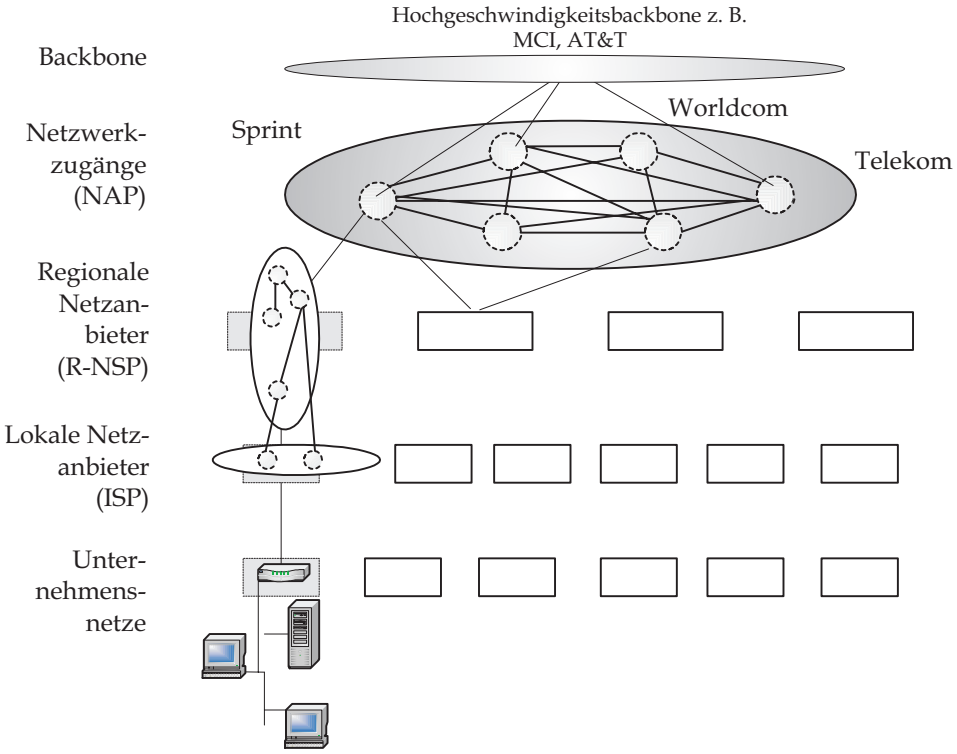


Abb. 9.1: Hierarchie vom globalen Backbone zum Unternehmensnetz

zerne werden so meistens zu profitablen Wirtschaftsunternehmen. Dieser sich gerade abzeichnende Trend wird zunehmend sichtbar.

Die auf dem freien Markt positionierten IT-Dienstleister unterhalten oftmals einen direkten Zugang zu den Hauptnetzen (NAP). Sie kaufen wie die herkömmlichen Carrier Bandbreiten im großen Umfang preiswert ein, „veredeln“ diese mit eigenen Produkten (häufig IP-Produkte) und bieten dann ihrer Muttergesellschaft, aber auch dem Drittmarkt, durchaus konkurrenzfähige Produkte an. Das klassische Geschäftsmodell der Netz-Provider, das sich hinter der Hierarchie der Ebenen (Abb. 9.1) verbirgt, wenn Bandbreiten portioniert in die nächste untere Ebene veräußert werden, löst sich also zunehmend auf.

Einer dieser Mehrwertdienste sind IP-VPN, die im Leistungsportfolio der Netzanbieter eine immer größere Rolle spielen. Gleichzeitig verschwindet die Übersichtlichkeit zwischen den Angeboten der Betreiber und den tatsächlichen Leistungen der Anbieter. Somit sollte genau überlegt und analysiert werden, welches Angebot in welcher Kombination für die eigenen Geschäftsvorfälle am geeignetsten ist.

Das Netz eines Netzwerkanbieters oder auch eines Internet Service Providers

(ISP) stellt sich bei einer genaueren Betrachtung ähnlich wie in Abb. 9.2 skizziert dar. Kennzeichnend für ein Provider-Netz ist, dass ein eigenes Backbone redundant ausgelegt ist – oftmals basierend auf einer Frame-Relay-Technologie. Das Geschäftsmodell eines Providers sieht typischerweise vor, den Kunden des Anbieters eine geschaltete Verbindung zwischen zwei Firmenstandorten (Lokationen), hier z.B. München und Darmstadt, zur Verfügung zu stellen. Mittels Router wird eine Verbindung von der Filiale zum PoP aufgebaut und dort in den Frame-Relay-Switch (FR-Switch) weiter in das Backbone des Providers geführt. Auf der Ausgangsseite erfolgt der Ausstieg ebenfalls über einen Switch nebst Router bis zum Standort der Zentrale.

Eine der wichtigen Fragen zur Entscheidung für oder gegen ein vom Serviceanbieter verwaltetes VPN ist, in wessen Verantwortung die Betreuung des letzten Routers auf der Kommunikationsstrecke liegt. Allgemeiner formuliert: Es muss die Frage des Übergabepunktes sorgfältig abgewogen werden. In diesem Zusammenhang müssen darüber hinaus Fragen zu den Vertraulichkeitsanforderungen der beauftragenden Firma geklärt werden. Zur Entscheidungsfindung sind am Ende des Kapitels in der Tab. 9.2 Kernfragen aufgelistet, die Anhaltspunkte liefern. Weitere Ausführungen sind in Kap. 10 zu finden. Neben der Netzinfrastruktur eines Providers ist auch die Granularität des VPN-Angebots ein Entscheidungskriterium. Denn es existieren in dem mittlerweile wachsenden und unübersichtlichen VPN-Markt – wenn man den Aussagen der Firmen Infonetics und Datamonitor Glauben darf – mehr als die drei herkömmlichen Varianten eines VPN. Dabei werden die klassischen Kategorien in die drei Alternativen eingeordnet: Eigenrealisierung *(Inhouse)*, Mischrealisierung *(Hybrid)* und Fremdrealisierung *(Outsourcing)*.

Aus den ursprünglichen klassischen Varianten haben sich inzwischen insgesamt sechs Stufen gebildet, die eher ein Kontinuum darstellen als streng abgestufte Varianten. Abb. 9.3 zeigt den kontinuierlichen Übergang, beginnend links mit einer Eigenrealisierung, die eine hohe Eigenverantwortung des VPN-betreibenden Unternehmens nach sich zieht, bis hin zu einer nahezu völligen Fremdrealisierung des VPN durch einen Netzanbieter. Einhergehend damit übernimmt der Netzanbieter folglich die komplette Verantwortung für Aufbau, Betrieb und Wartung des VPN. In dem Maße, wie eine Fremdrealisierung zunimmt, wie in Abb. 9.3 auf der unteren Achse von links nach rechts stufenmäßig grau unterlegt, nehmen die Freiheitsgrade und damit die Verantwortung der beauftragenden Firma ab. Dabei erstreckt sich die Darstellung des kontinuierlichen Übergangs über alle drei VPN-Kategorien: Intranet-VPN, Extranet-VPN und Remote-Access-VPN. Dies bedeutet bei einem eigenrealisierten VPN, dass der NSP nur den Internetzugang mit einer entsprechenden Bandbreite anbietet. Auf der anderen Seite des Kontinuums vertraut das Unternehmen dem Netzanbieter gänzlich (hat entsprechende Serviceverträge (SLA) vereinbart) und überlässt dem NSP-Betrieb und Verwaltung des VPN (rechte Seite in Abb. 9.3).

Das Unternehmen beschränkt sich auf die Konfiguration und Verwaltung des eigenen Sicherheitsservers, der als Übergabepunkt des VPN zum firmeneigenen LAN dient, sowie auf die Überprüfung der Serviceverträge. Die Abhängigkeit

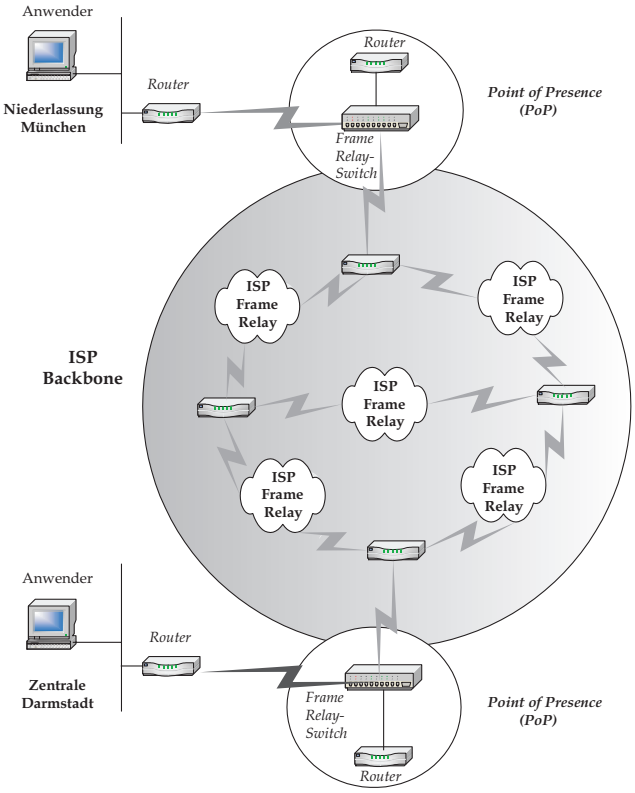


Abb. 9.2: Typisches Backbone eines Internet Service Providers (ISP)

zum Netzanbieter ist entsprechend hoch und es existiert ein besonderes Vertrauensverhältnis, das dieser Lösung zugrunde liegt. Insofern muss ein Schritt in diese Richtung sorgfältig überlegt werden. Denn wird nach Jahren an ein *Insourcing* gedacht, also wieder die Eigenrealisierung favorisiert, muss mühsam das entsprechende Know-how und Wissen erneut aufgebaut werden.

Jedoch auch Netzanbieter (NSP) sind sehr unterschiedlich ausgestattet. So gibt es heutzutage ein weites Spektrum von IP-VPN-Architekturen und Lösungen, wenn die unterschiedlichen Angebote der Anbieter verglichen werden. Dies reicht oft von einer Möglichkeit der Altlasteneinbindung bis hin zu innovativen technischen Lösungen der nächsten Generation, die etliche Millionen Euro an Investitionen nach sich ziehen. Auf der anderen Seite des Spektrums befinden sich Startup-Anbieter, die eine geringe Infrastruktur aufweisen und somit ein IP-VPN von Grund auf neu entwickeln und anbieten können.

Eine weitere Variante bilden die Anbieter, die sich von ihren Konkurrenten durch spezielle Angebote abzusetzen versuchen, indem sie z.B. über ATM, TDM oder IP Netzwerke zur Verfügung stellen. Meistens bieten sie ihren Kunden darüber

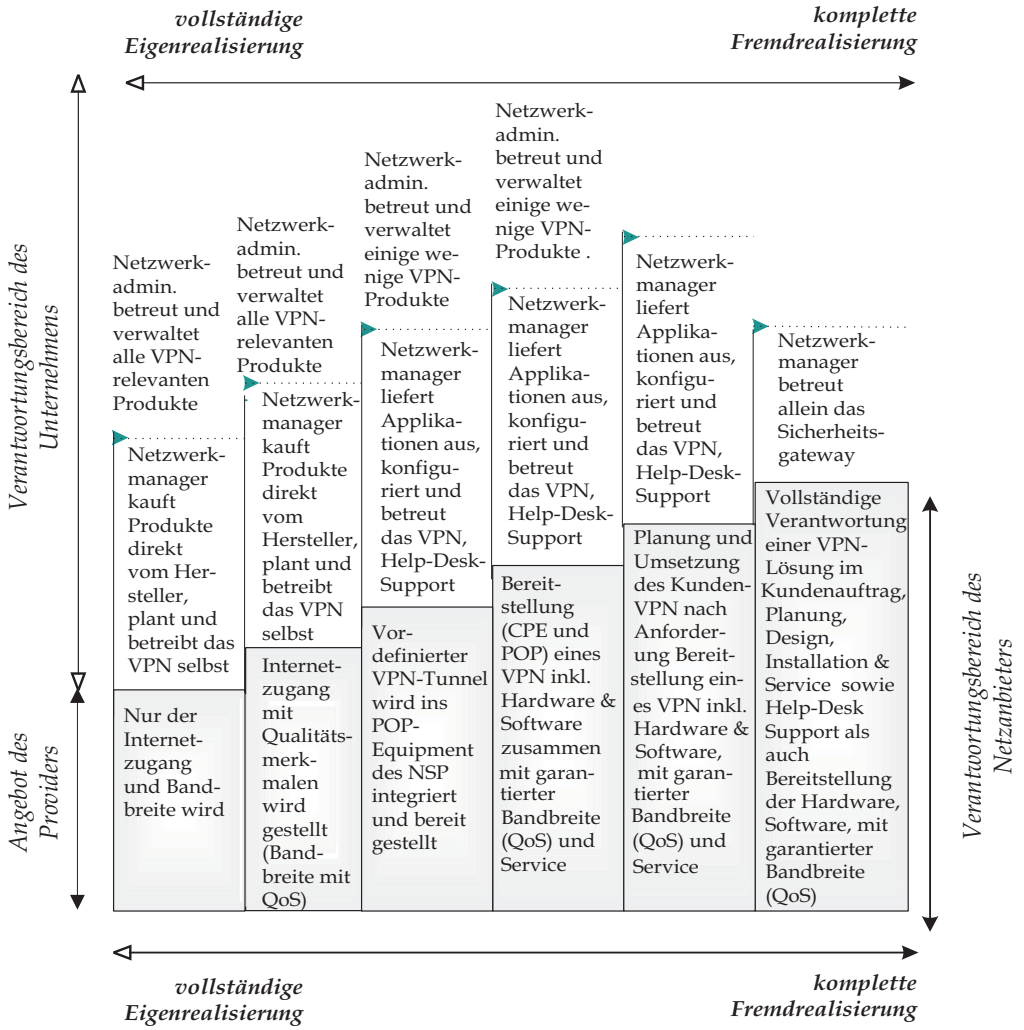


Abb. 9.3: Kontinuierlicher Übergang von einer VPN-Eigenrealisierung bis zur Fremdrealisierung durch einen NSP

hinaus eine große Palette von Produkten und Softwarelösungen an. Abb.9.4 zeigt unterschiedliche IP-VPN-Architekturen, die in die Gruppe Einwahl *(Dial-In)* und in die Gruppe der zugewiesenen VPN eingeordnet worden sind.

Nähere Ausführungen der unterschiedlichen Architekturen sind in den folgenden Abschnitten zu finden.

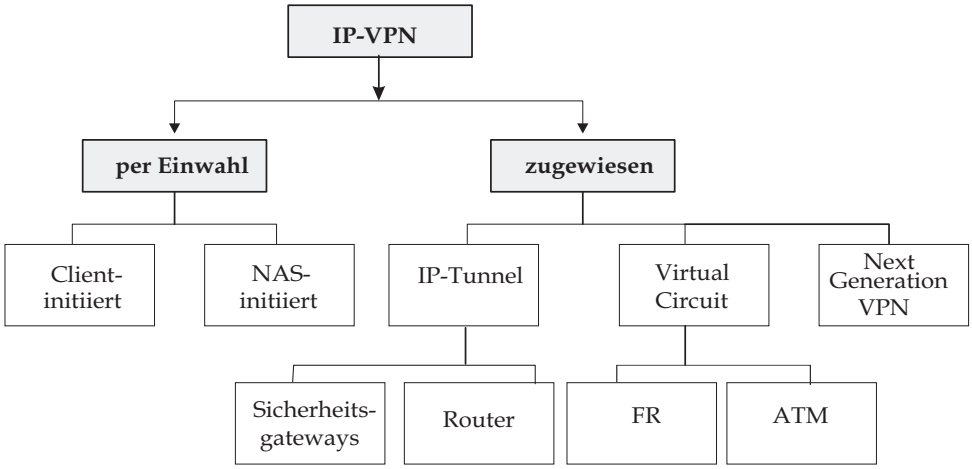


Abb. 9.4: Überblick verschiedener IP-VPN-Architekturen

9.1.2 IP-VPN über Wählverbindungen

Alle mittels Wählverbindungen aufgebauten IP-VPN haben gemeinsame Charakteristika:

- Ein Serviceanbieter (ISP) stellt Einwahlmöglichkeiten bereit, die von seinen Kunden über Zugangsnummern kostengünstig im Ortsnetz erreicht werden.
- Es stehen meist für alle Kunden des ISP aus Kostengründen die gleichen Einwahlmöglichkeiten bereit, die sie sich teilen.
- Es werden Tunnel über öffentliche IP-Netzwerk oder über IP-Netzwerke des Providers geschaltet.
- Kunden können Sicherheitsvorschriften zur Authentifizierung und zur allgemeinen Kontrolle über spezielle Datenbanken einrichten. Als eine weitere Variante kann dieser Dienst allerdings auch vom ISP ausgeführt werden.

Es gibt in dieser Gruppe wie Abb. 9.4 zeigt, zwei unterschiedliche Aufbaumechanismen.

Initiierung durch den Anwender *(Client-initiated)*

In diesem Fall wählt sich ein Anwender per Wählverbindung in den Zugangsserver aktiv ein und fordert einen verschlüsselten Tunnel zwischen seinem Computer und dem Firmennetzwerk bzw. dem Intranet an. Häufig geschieht dies mit einer IPSec ausgestatteten Software, die mit einem Sicherheitsgateway, z.B. einer Firewall, kommuniziert. Befindet sich auf der Anwenderseite ein Router, reduziert dies den Datendurchsatz. Das hat den Vorteil, dass dieser einfacher aus der

Ferne gewartet werden kann, falls der Router dafür ausgelegt ist. Außerdem muss im Endgerät keine IPSec-Installation vorgenommen werden. Für eine Ende-zu-Ende-Absicherung ist allerdings ein IPSec-fähige Anwendung notwendig.

Fremdinitiierte Verbindung zum Anwender (NAS-initiated)

Hier wird eine Verbindung vom Service-Provider, ausgehend vom Network Access Server (NAS), zum Gateway eines Telearbeiters bzw. zum Firmengateway aufgebaut. Dabei kommen Layer-2-Protokolle wie L2F oder auch L2TP zum Einsatz, um den Tunnel aufzubauen. Eine Authentifizierung muss bei dieser Konstruktion zweimal durchgeführt werden. Einmal findet eine Basisidentifikation meist mittels (PPP, PAP oder CHAP) bei der Einwahl am Zugang (PoP) statt, die ihn als Berechtigten für diesen Dienst ausweist. Damit wird eine Tunnelverbindung zum Serviceanbieter aufgebaut. Eine zweite Authentifizierung findet an der Netzwerkgrenze zum Firmennetz statt und wird häufig mit TACACS+, RADIUS oder Kerberos durchgeführt. Für weitere Absicherungen kann entweder auf der Applikationsebene oder auf der Verbindungsebene mit Verschlüsselungsmechanismen gearbeitet werden. Für den Service-Provider bietet dieser Ansatz eine interessante Geschäftsperspektive. Die Vorteile sind:

- Es wird keine extra Software auf der Endnutzerseite notwendig, die aufwändig gewartet werden muss.
- Solange der Service-Provider den Tunnel initiiert, können bestimmte Serviceklassen (*Premium, Gold, Silver*), wie z.B. reservierte Modemports, bestimmte Modemverfügbarkeiten sowie eine Priorisierung im Datentransport angeboten werden.
- Über den NAS-Zugang kann sowohl der Zugang zum Internet als auch zum VPN realisiert werden.
- Ebenso kann ein bestimmter Datenverkehr zu einem bestimmten Endpunkt über einen Tunnel vom NAS aus gesteuert werden. Es werden somit größere Freiheitsgrade bei der Skalierung und Wartung erreicht.

9.1.3 VPN über fremde Netze

IP-Tunnel

IP-Tunnel werden häufig durch Firewall-Systeme mit ausgestatteten Zusatzmodulen über das Internet geschaltet. Hierzu zählen, um nur zwei zu nennen, die Firewall der Firma Cisco (PIX) oder auch die der Firma Checkpoint (Firewall-1). Außerdem können auch Router diese Funktionen übernehmen, falls sie dafür ausgelegt sind.

Bei den Sicherheitseinrichtungen hat sich IPSec durchgesetzt. Auch bei den Routerverbindungen kann IPSec oder GRE (Generic Routing Encapsulation) eingesetzt werden, je nachdem wie viel Wert auf QoS oder Vertraulichkeit gelegt

wird. Dabei ist IPSec mittlerweile zum Quasistandard geworden (Abschn. 7.4). IPSec wird von vielen Anbietern sowohl für Hardware- als auch für Softwarekomponenten genutzt. Allerdings muss bei einem Mix von verschiedenen Herstellerlösungen auf die Kompatibilität geachtet werden.

Ein Service-Provider hat durch den Einsatz von IPSec den Vorteil, dass die vorhandene Infrastruktur nicht aufwändig geändert werden muss, wie z.B. bei MPLS, und dann somit ein VPN zeitnah eingerichtet werden kann. Zum anderen verfügen die heutigen Sicherheitsgateways (Firewall-Systeme) meist über eine hardwarebasierte Verschlüsselung, die für einen ausreichenden Datendurchsatz sorgt. Durch den Einsatz des neuen Verschlüsselungsstandards AES kann der Datendurchsatz nochmals deutlich gesteigert werden.

Eine weitere Größe ist die Bereitstellung von Dienstgüten wie z.B. Quality of Services (QoS) in einem VPN. Es bietet dem Kunden die Möglichkeit, nach seinen Bedürfnissen eine für ihn passende Klasse zu wählen. Die Angebotspalette reicht dabei häufig von einem Standardangebot bis zu einem Premium-Service. Damit wird für den Service-Provider ein Mix von Serviceklassen sowie QoS auf Anwendungsebene erreicht. Abschließend kann noch die einfache IPSec-Anwendung genannt werden, die in den neueren Betriebssystemen beim Aufbau einer Wählverbindung als Bestandteil mitgeliefert wird und ebenfalls keinen Änderungsbedarf für die Infrastruktur des Service-Providers nach sich zieht.

Aber auch bei der in die Jahre gekommen Generic Routing Encapsulation-Technologie (GRE), die als Standardlösung für ein Provider verwaltetes IP-VPN angesehen wird, gibt es signifikante Vorteile aus dem Blickwinkel eines Providers. So ist z.B. eine wesentlich feinere Abstimmung bei Dienstgüten (QoS) möglich, da der Protokollkopf, im Gegensatz zu IPSec, ausgewertet werden kann.

Weiterhin ist für die GRE-Technologie kennzeichnend, dass eine Ende-zu-Ende-Dienstgüte gewährleistet werden kann, da diese Lösung auf jeweils einen Provider beschränkt ist. Diese Begrenzung macht eine Verschlüsselung hinfällig, da der GRE-Tunnel die Privatsphäre schützt. Allerdings bleibt es dem Kunden überlassen, z.B. auf Applikationsebene eine Verschlüsselung einzurichten, etwa mit SSL bei einer Webanwendung. Alternativ kann die gesamte Verbindung verschlüsselt werden. Dies führt jedoch zu einer negativen Auswirkung bei der Performance und Granularität der Dienstgüten.

Virtual Circuits (VC)

Eine interessante Lösung bietet sich für Provider, indem permanente virtuelle Verbindungen (PVC) geschaltet werden, die eine Punkt-zu-Punkt-Verbindung über Frame Relay oder auch ATM ermöglichen. Dabei kommen Router zum Einsatz, die die Layer-3 verwalten. Zusammengefasst wird diese Lösung oft als Managed Router Service angeboten. Reine Carrier bzw. Telekommunikationsanbieter nutzen diese Methode häufig, um einen IP-VPN-Service über bestehende Frame- oder Zellinfrastrukturen anzubieten (siehe Abschn. 8). Anders als bei den Lösungen, die in irgendeiner Weise ein IP-VPN mittels Tunnel über ein

öffentliches IP-Netzwerk routen, wird hier ein IP-Service über ein Frame-/Zellnetzwerk geroutet. Die Privatsphäre wird mittels Tunnel durch PVC erreicht; eine zusätzliche Verschlüsselung ist meist optional.

Die wesentlichen Vorteile dieser Lösung sind:

- Der Managed Router Service ist ein kostengünstiger und schneller Weg, IP-Services einzurichten, wenn die Infrastruktur auf einem Frame- bzw. Zellnetzwerk basiert.
- Die Möglichkeit eines Quality of Service (QoS) kann bei Frame Relay durch die Committed Information Rate (CIR) beeinflusst werden.
- Durch die VC sind Möglichkeiten einer Skalierung vorhanden.
- Es besteht nicht unbedingt die Notwendigkeit, aufwändige und Performance-reduzierende Verschlüsselungsmechanismen einzusetzen.

VPN der nächsten Generation *(ng-VPN)*

Aus den vorangegangenen Betrachtungen wird deutlich, dass überwiegend auf herkömmliche Technologie gesetzt wird; nur langsam setzt sich MPLS durch. In dem Maße jedoch, wie der VPN-Markt weiter wächst, werden neue Anforderungen an eine VPN-Lösung gestellt, die wesentlich einfacher in der Handhabung und skalierbar sein muss. Eine VPN-Lösung der nächsten Generation muss:

- hoch skalierbar sein, um
  - tausende von Sites pro VPN einzurichten und
  - tausende von VPN selber zu initiieren,
  - ein einfaches Management der VPN-Teilnehmer zu ermöglichen, um ein schnelles Wachstum nicht zu behindern,
  - eine Any-to-Any-Verbindung für ausgedehnte Intranets und Extranets für diverse Geschäftsvorfälle zu erreichen;
- Unterstützung für anspruchsvolle IP-Intranet-Applikationen bieten, wie
  - die Verwaltung von dynamischen Bandbreiten und
  - einen bedarfsgerechten applikationsspezifischen Datentransport, z.B. bei Sprache (Voice-over-IP);
- neue Services und Serviceklassen bereitstellen, wie
  - Multicast-Technologien für Multimedia-Anwendungen,
  - zeitkritischen und übertragungskritischen Datenverkehr wie Video und Sprache.

Um diesen Anforderungen zu genügen, schlug Cisco Inc. eine Technik vor, die von der IETF aufgegriffen wurde und inzwischen zu einem Paradigmen-Wechsel führte. Denn bei den herkömmlichen VPN-Technologien handelt es sich immer um Zusatzeigenschaften. Dabei wird eine *Overlay*-Technik eingesetzt, um ein Punkt-zu-Punkt-Netz über das eigentliche Netzwerk zu legen. Grenzen, die bei der Overlay-Technik auftreten, zeichnen sich bei weltumspannenden Entwicklungen ab, die durch die Komplexität an die Grenzen eines Managements stoßen. Es wird die Änderung gefordert, dass die VPN-Eigenschaft zu den Grundeigenschaften eines Netzes gehört und zudem noch hoch skalierbar sein muss. Als maßgebliches Kennzeichen der neuen Klasse von VPN bzw. VPN der nächsten Generation werden VPN-Eigenschaften Bestandteil des Netzes selber sein. Cisco nennt diese Art der Netze *Internet Scale VPN* (ISV), die wie das Internet selbst verbindungslos arbeiten.

Jedoch ist es bei allen Varianten erforderlich, klare Grenzen zwischen den Verantwortungs- und Zuständigkeitsbereichen des Netzbetreibers und der beauftragenden Firma zu unterscheiden. Dabei sind verschiedenste Konstellationen denkbar, in der z.B. das Übergabeequipment (*Customer Edge*) Eigentum der beauftragenden Firma – kurz CE[1]– ist und in firmeneigenen Räumlichkeiten untergebracht ist. Verwaltung und Betreuung jedoch erfolgt durch einen Netzbetreiber, der dann freien Zugang zu den Geräten benötigt. Das gesamte VPN-Equipment kann auch Eigentum des Netzbetreibers (*Provider Edge*) sein und in seinen Räumlichkeiten stehen. Nur am Übergabepunkt des Netzbetreibers – kurz PE[2] – werden Dienstleistungen vom Kunden eingekauft. Daraus ergibt sich die Frage des exakten Übergabepunktes und damit der Verantwortlichkeiten.

Seit geraumer Zeit existiert ein Vorschlag der IETF, in dem zu der Schnittstelle zwischen Provider und Kunden Referenzmodelle vorgeschlagen werden. Auf diese wird in den nachfolgenden Abschnitten eingegangen.

9.1.4 Referenzmodell für ein verwaltetes CE-basiertes VPN

Referenzmodelle postulieren i.d.R. Vorlagen und Strukturen, nach denen eine Orientierung für weiterführenden Entwicklungen möglich ist. In dem vorliegenden Fall des verwalteten CE-basierten[3] VPN beschreibt das Referenzmodell eine Schnittstelle – die beispielsweise aus der Sicht des Providers – den Gefahren- und Verantwortungsübergang vom Netz des Netz-Providers zum Kunden aufgreift. So trivial diese Schnittstellendefinition zunächst erscheinen mag, so gewinnt diese häufig bei Störfällen und bei Leistungsschwankungen des VPN-Tunnels des

[1] Z.B. können die Cisco-Router der Serien 47xx, 45xx, 3810, 36xx, 26xx, 25xx, 17xx, 16xx und 14xx mit dem IOS-Betriebssystem Version 11.1 als Customer-Edge-Geräte eingesetzt werden.

[2] Z.B. können die Cisco-Router der Serien 75xx, 72xx, 71xx, 47xx, 45xx und 36xx, Cisco DSL 6400 Cisco uBR7246 Universal Broadband Router und MGX 8850 hierzu eingesetzt werden.

[3] Die Abkürzung CE-basiertes VPN besagt, das dass VPN-Gateway (Equipment) des Kundennetzes (Customer) selbst verwaltet wird.

Service-Providers erheblich an Bedeutung. Der Abschn. 9.2.3 geht auf diesen Punkt ein.

Grundsätzlich kann eine Netzkopplung für ein VPN sowohl auf Layer-2 als auch auf Layer-3 geschaltet werden, je nachdem welche Art des VPN eingesetzt wird und wie weit der Einfluss der Kopplung reichen soll. In einem CE-basierten VPN endet der Tunnel direkt an der CE, also im Equipment des Kunden (Abb. 9.5). Übergabepunkt kann dann z.B. das äußere Schnittstellen-Interface sein, aber auch das firmenseitige (innere) Interface. Dies hängt von den technischen Möglichkeiten und dem Vertrag zwischen den Parteien ab.

Bei einem Layer-2-VPN-Service erhält der Kunde des Netzbetreibers auf der Data-Link-Schicht Unterstützung. IP-Pakete registrieren die Kopplung nicht und die PE[4] reicht die Datenpakete des Kunden aufgrund von Informationen im Data-Link-Layer-Header weiter, wie z.B. DLCI bei einer Frame Relay-Verbindung oder mittels *tags* bei einem VLAN nach IEEE 802.1q. Somit sieht die CE eine PE als ein Layer-2-Gerät *(device)*, wie eben einen FR-Switch oder ein Ethernet VLAN-Switch an. Als nahe liegendes Beispiel kann ein CE-basierter, vom Provider verwaltetes *Frame Relay Access Device* (FRAD) dienen.

Bei einem Layer-3-VPN-Service erhält der Kunde IP-Pakete auf Layer-3 vom Netzbetreiber. Die CE und die PE kennen gemeinsam sowohl die Data-Link Layer als auch die IP-Layer. Die PE reicht die Datenpakete aufgrund der Informationen im IP-Protokollkopf weiter, wie z.B. eine IPv4 oder IPv6-Zieladresse. Damit sieht die CE die PE des Netzbetreibers als IPv4 bzw. als IPv6-Router.

Abb. 9.5 skizziert das Referenzmodell für ein vom Netzbetreiber verwaltetes CE-basiertes VPN. Dargestellt wird der Access-Bereich zweier Kunden (A, B) sowie das Netz eines Service-Providers über das jeweils eine private logische Verbindung zur Filiale des Kunden eingerichtet worden ist (Strecke A $\longleftrightarrow$ A). Das Service-Provider-Netz beinhaltet ein IP-Netzwerk und CE-Managementfunktionen, die über spezielle Konsolen verwaltet werden. Dabei können auf der Kundenseite und auf der Provider-Seite proprietäre Netzwerk-Management-Systeme, SNMP-basierte oder auf LDAP-abgestützte Systeme, eingesetzt werden. Jedoch benötigen die in Abb. 9.5 eingezeichneten PE-Router keine VPN-spezifischen Funktionalitäten.

Der PE-Router dient als Zugangselement auch für andere VPN-Kunden. Der Tunnel reicht – eingerichtet für den Kunden (A) – von Site zu Site bzw. von CE-Eingangsgerät bis CE-Eingangsgerät. Es kann sich z.B. um ein IPSec-VPN handeln, bei dem der Kunde die Verschlüsselungsparameter in seiner Hoheit hat. Damit hat der Kunde die Gewissheit, das Vertraulichkeitsniveau selber bestimmen zu können. Der Provider übernimmt bei diesem VPN im Wesentlichen die Verfügbarkeit.

[4] Unter dem Begriff PE wird der Netzrand (Edge) des Providers verstanden.

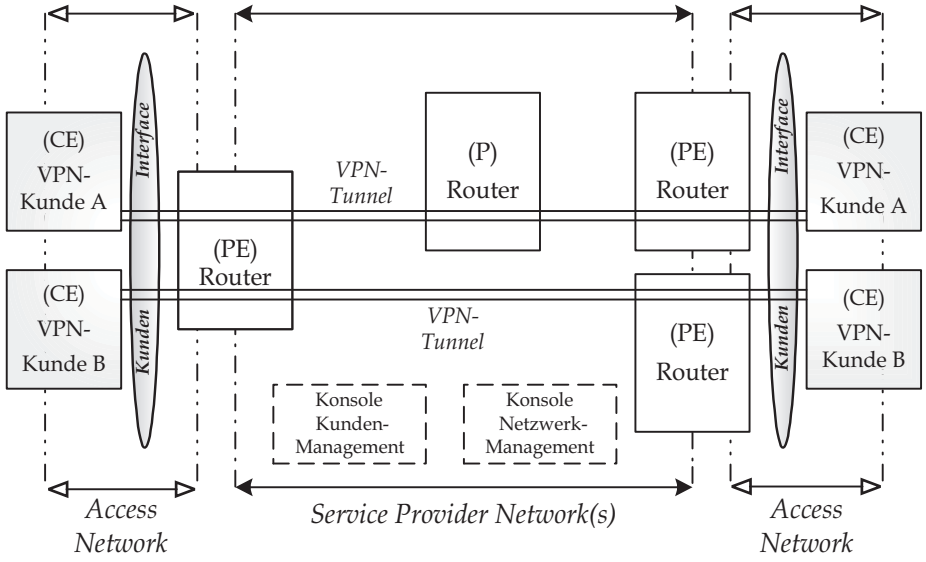


Abb. 9.5: Referenzmodell für ein vom Netzbetreiber verwaltetes CE-basiertes VPN

9.1.5 Referenzmodell für ein NB-basiertes VPN

In einem Netzwerk-basierten VPN (NB-VPN) endet der Tunnel am Netzrand (*Provider Edge*) des vom Netzbetreiber verwalteten Servicenetzes (Abb. 9.6). Die entsprechenden PE-Router können in einem PoP stehen. Falls sie nicht im PoP stehen, befinden sie sich in den Räumlichkeiten des Kunden und werden vom Provider gepflegt und gewartet. Der vertrauliche Zugang zum Netz (VPN) obliegt dem Kunden.

Die ITU-T hat ebenfalls eine dem Sinn der IETF entsprechende Definition für ein Netzwerk-basiertes VPN in einem Draft zur Diskussion gestellt [Y.1311.1 2000]. Auch dies folgt der Bedingung, dass ein NB-VPN von der Zugriffsnetztechnologie unabhängig sein muss.

Für ein Netzwerk-basiertes Layer-2-VPN steht z.B. ein MPLS kontrollierendes Backbone eines Netzanbieters (Abschn. 8) zur Verfügung. Für ein Layer-3-Netzwerk-basiertes VPN kann ein BGP/MPLS nach [RFC 2547] oder auch ein virtuelles Routernetz gemäß [RFC 2917bis] als Beispiel dienen. Protokolle, die für einen IP-Tunnel zur Verfügung stehen, haben unterschiedliche Mechanismen. Die drei wesentlichen sind MPLS, GRE, IPSec und wurden im Kap. 8 bzw. Kap. 7 bereits vorgestellt.

Abb. 9.6 zeigt das Referenzmodell nach dem PPVPN Internet Draft-Vorschlag der IETF eines Netzwerk-basiertes VPN mit gleichzeitiger Beziehung unterschiedlicher Objekte (Entitys), die an einem VPN beteiligt sind. Auf der Kundenseite (CE) wird eine Verbindung (*Access Connection*) zum PE-Router aufgebaut. Eine Access

Connection stellt eine isolierte Layer-2-Verbindung dar, die auf einer physikalischen Leitung aufsetzt. Es wird eine logische Verbindung (*logical circuit*) mittels Frame Relay (FR) oder ATM nebst einem IP-Tunnel mit IPSec oder L2TP eingerichtet. Die CE kann dabei aus einem Router, einem Host oder auch aus einem Switch bestehen, der die Kundenseite abgrenzt. Ein PE-Router des Providers beinhaltet eine VPN Forward Instance (VFI), die aus einer logischen Einheit besteht. Sie ist mit der kundenseitigen Access Connection verbunden.

Weiterhin wird in Abb. 9.6 deutlich, dass an einem PE-Router über eine logische VFI unterschiedliche Kunden angebunden sein können. Ein P-Router, also ein Router, der im Provider-Netzwerk steht, verbindet hier symbolisch die PE-Router. Dieser hat jedoch für das VPN keinerlei Bedeutung und keine direkte Verbindung zur CE des Kunden. Der eingezeichnete Zugriffsbereich (Access Net-

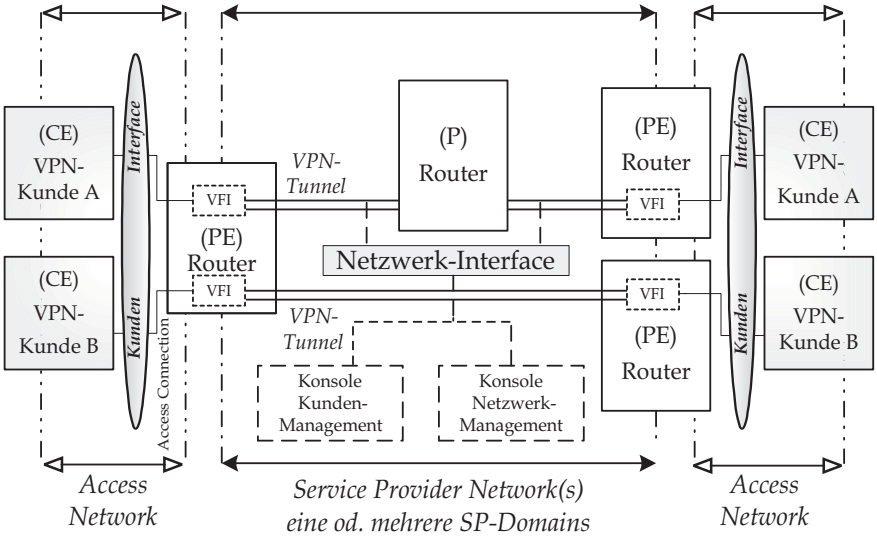


Abb. 9.6: Referenzmodell für ein vom Provider betriebenes NB-basiertes VPN

work) zwischen dem CE-Router/Switch und dem PE-Router kann bestehen aus einem Zeitmultiplexing-Netzwerk (TDM Network), einem L2-Netzwerk z.B. mittels FR, ATM, Ethernet oder aus einem IP-Netzwerk, dessen Zugriff getunnelt ist, wie z.B. mit L2TP nach [RFC 2661].

Ein VPN-Tunnel ist eine logische Verbindung *(logical link)* zwischen zwei Objekten (Entitys), die durch Verkapselung der Pakete und Header bei der Übertragung zwischen diesen Entitys aufgebaut wird (siehe auch Abschn. 7.1). Wird MPLS für den Tunnelmechanismus eingesetzt, geschieht dies durch den Label-Switch-Path (LSP) und durch ein Multiplexing der Zwei-Ebenen-Labels. Der genestete Tunnel wird durch das unterste Label bewirkt, das Multiplexing durch das obere Label erreicht. Diese Label-Aufteilung führt zu einem hohen Paketdurchsatz, da der

Weiterleitungsprozess nur das untere Label benötigt. Wird MPLS in einem ATM-Netzwerk implementiert, wird von dem CPCS (User-to-User)-Feld in dem AAL5-Trailer oder von dem VPN-ID-Feld in dem VPN-Encapsulation-Header gemäß [RFC 2684] Nutzen gezogen.

Falls Generic Routing Encapsulation (GRE) als Tunnelmechanismus eingesetzt und das Schlüsselfeld unterstützt wird, wird mittels des Schlüsselfeldes ein genesteter VPN-Tunnel eingerichtet. Wird kein Schlüsselfeld unterstützt, wird nur eine logische Verbindung aufgebaut. Ebenso kann ein GRE-Tunnel über einen MPLS-Netzwerk geleitet werden.

Bei einem Einsatz von IPSec als Tunnelmechanismus, werden diese durch das SPI-Feld identifiziert. Ebenso wie bei GRE kann ein IPSec-Tunnel über ein MPLS-Netzwerk geführt werden.

9.2 Netzwerk-Performance und Management

Eine weitere wichtige Einschätzungsgröße eines Netzwerk-Providers (NSP) ist die Verfügbarkeit oder auch Netzwerk-Performance und die Art und Weise, wie das Netzwerk betrieben und verwaltet wird. Darüber hinaus ist es interessant, wie ein NSP seine Bandbreite unterteilt und wie viel Bandbreite der Netzwerk-Provider anderen Kunden zugesprochen hat.

Wird beispielsweise eine 10-Mbps-Verbindung vertraglich zugesichert, ist es von Vorteil zu wissen, wie diese aggregiert ist. Resultieren also die 10-MBit/s aus einer E3-(34-Mbit/s)- oder aus einer 5xE1-(2,048 MBit/s)-Verbindung? Im Störfall sind dies entscheidende Fragen für eine Fehlerbehebung und lassen Rückschlüsse über zeitliche Dauer der Behebung indirekt ableiten.

Das Netzwerkverhalten ist auch bei auftretenden Spitzenlasten *(Burst)* gegenüber einer mittleren AuSLAtung zu betrachten. Die vom Provider geführten Statistiken geben hier wichtige Informationen Es ist somit empfehlenswert – und zwar unabhängig von den mit dem Provider ausgehandelten Liefer- und Leistungsbedingungen (SLA) – diese auf Einhaltung zu überprüfen. Dies erfordert firmenseitig ebenfalls geeignete Kontrollmessgeräte.

Ein Netzwerk-Management-System (NMS) hat etliche Komponenten; jedoch lassen sich diese im Wesentlichen auf vier reduzieren, wenn die Überprüfung der ausgehandelten Liefer- und Leistungsbedingungen im Vordergrund steht:

1. An den Übergabepunkten *(Schnittstelle)* zwischen Kunden und Provider müssen Kontrollmessungen *(Monitoring)* vorgenommen werden (Abb. 9.6).
2. Eine Datenbank zur Filterung des Performanceverhaltens des VPN muss eingerichtet werden.
3. Applikationen zur Datenanalyse und zur Erzeugung von Reports *(Berichtswesen)* müssen installiert und genutzt werden.

4. Webbasierte HTML-Versionen zur Reporterzeugung für eine Echtzeitüberprüfung *(Lastverhalten)* sollten vorhanden sein.

Abb. 9.7 skizziert die wesentlichen Komponenten zur Überprüfung eines Netzwerkdatenverkehrs.

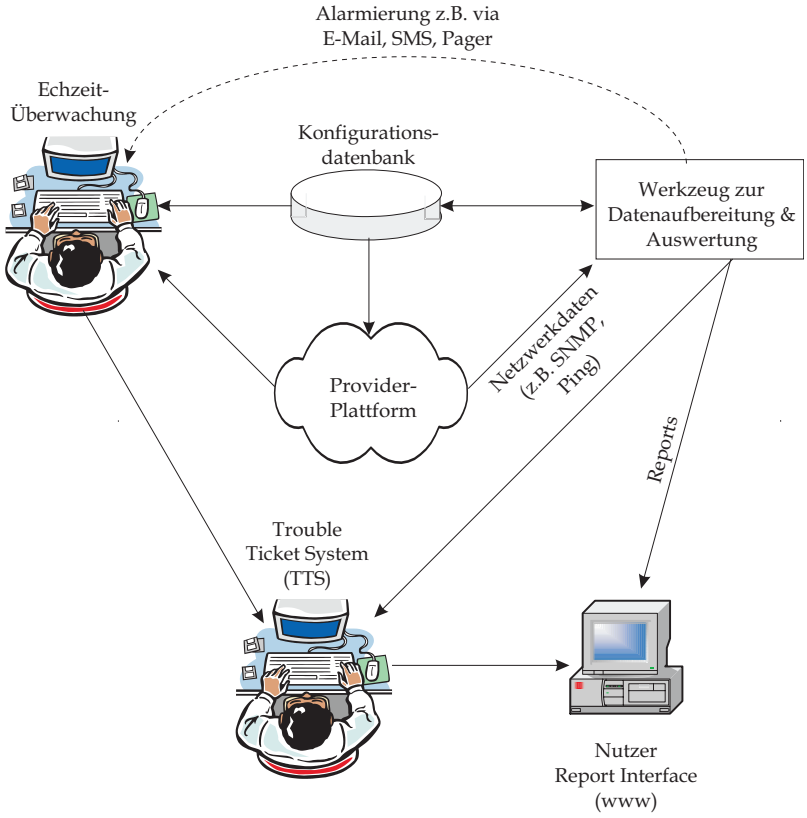


Abb. 9.7: Komponenten eines Netzwerk-Management-Systems (NMS) nebst Überwachungseinheit für den Endnutzer

Provider-seitig wird üblicherweise eine Echtzeitüberprüfung der Netzwerkplattform durchgeführt. Dabei werden die Konfigurationsdaten der Plattform aus einer Datenbank zu den Daten, die von der Plattform gemeldet werden, hinzugezogen. Korrespondierend hierzu wird ein Analysewerkzeug zur Datenaufbereitung der Daten eingesetzt, die vom Netzwerk via *Simple Network Management Protocol* (SNMP) kommen.

Bei Störfällen oder Engpässen wird automatisch ein Nachricht zur Überwachungsstation geschickt. Die Störfallnachricht (*Trouble Ticket*) wird in ein spezielles Störfallbearbeitungsprogramm (*Trouble Ticket System*, TTS) eingetragen. Mit dem

TTS wird der Störfall katalogisiert, werden Statusänderungen, Fehlerbehebungsansätze oder Herstellerrückfragen etc. eingetragen. Nach erfolgreicher Fehlerbeseitigung wird das Ticket geschlossen.

Der Endnutzer wird ständig über den Status des Vorgangs informiert. Außerdem bekommt er Informationen vom Analysewerkzeug, die in Form von Berichten (Reports) über eine Webschnittstelle zur Verfügung gestellt werden. Neben der reinen Informationsübermittlung ist dabei natürlich für den Endnutzer auch die Informationsdarstellung und -auflösung von evidenter Bedeutung. Leider gibt es noch keinen Standard für die Reportformate und -inhalte. So bleibt es dem Verhandlungsgeschick des Kunden überlassen, welche Daten in welchem Verdichtungsgrad er zur Verfügung stellt.

Für die kundenseitige Überprüfung der SLA sollten einige Randbedingungen bei der Implementierung der Kontrollmessgeräte beachtet werden. Zunächst muss mit dem Provider vereinbart werden, an welchen sinnvollen Punkten die Messungen durchgeführt werden sollen. Hierfür stehen zwei Möglichkeiten offen. Entweder wird eine End-to-End-Messung oder eine Messung innerhalb der Provider-Plattform durchgeführt. Weiterhin hat der *Local Loop*, auch als letzte Meile bekannt, einen erheblichen Einfluss auf die Netzwerk-Performance und damit auf die Messungen. Allerdings spielt dies bei einer Switch-to-Switch-Überprüfung keine Rolle. Abb. 9.8 zeigt die möglichen Messgebiete zur Überprüfung der Serviceparameter, die in den Liefer- und Leistungsbedingungen festgeschrieben sind.

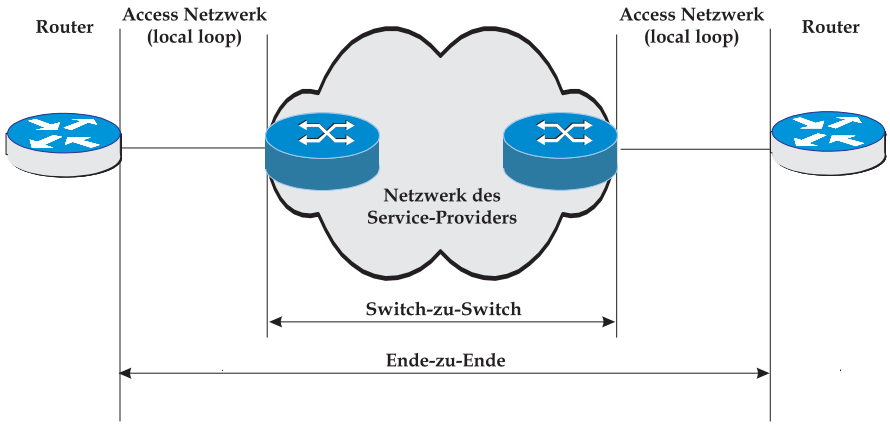


Abb. 9.8: Mögliche Messpunkte zur Überprüfung der gelieferten Servicequalität

Für die Performance-Messung und für die Fehlerbehebung muss eine Ende-zu-Ende-Messung durchgeführt werden. Eine weitere Beachtung sollte dem Messsystem und Messparametern selbst gelten. Um objektive Messungen durchführen zu können, sollte ausschließlich ein Netzwerk-Messsystem benutzt werden, das unabhängig von der Switch- und Router-Architektur des Providers misst. Auch

hier ist die Darstellung der Messungen und die Datenaufbereitung von enormer Bedeutung für den Kunden. Bedauerlicherweise existierten bisher kaum geeignete standardisierte Metriken für die relevanten Messungen und Messparameter, die für große Netze oder Plattformen der ISP notwendig sind. Hierzu hat die IETF die Arbeitsgruppe *Internet Provider Performance Metrics* (IPPM) eingesetzt, die sich seit 1997 dieses Problems annimmt. Etliche Vorschläge und einige Standards sind seitdem verabschiedet worden. Allerdings soll hier nicht weiter darauf eingegangen werden.

Viele Service-Provider bieten einen Dienst, der garantiert, dass Messungen an den lokalen Geräten des Kunden am sogenannten Customer Premise Equipment (CPE) durchgeführt werden. Hier sollten an den Fremdgeräten parallel eigene Geräte angeschlossen werden, die unabhängig Messungen durchführen.

9.2.1 ITIL als Defacto-Standard für IT-Service-Management

Die Lieferung einer gleichbleibenden Qualität ist einer der wichtigsten, aber auch einer größten Herausforderungen bei der Serviceerbringung. Daher gehen viele Service-Provider dazu über, ihre Aktivitäten und Tätigkeiten, die im Zusammenhang mit ihren Kunden stehen, Qualitätsnormen und Qualitätsmessungen zu unterwerfen.

Dieser Schritt ist durchaus angebracht, wenn mit der Nichteinhaltung von zugesicherten Serviceparametern wie z.B. in Abschn. 9.2.3 beschrieben Vertragsstrafen zu erwarten sind. Der gesamte Liefer- und Leistungsservice wird von dem Service-Provider einer prozessgerichteten und serviceorientierten Methode unterworfen.

Hier hat sich die aus mehreren Büchern bestehende *IT Infrastructure Library* (ITIL) als Standardwerk im IT-Service-Management etabliert. ITIL zielt auf die Qualitätssicherung eines Services ab und lehnt sich für die Qualitätssteuerung an den Qualitätskreis von Deming an. ITIL ist von der Idee her eng verknüpft mit der ISO 9000:2000 Norm, die einem Unternehmen ein Qualitätssystem bietet, sowie den Total-Quality-Richtlinien wie EFQM.

Der Qualitätskreis beschreibt in der Interpretation eine selbstlernende Organisation, die in Zyklen die vier Schritte *plan-do-check-act* (PDCA) absolviert. Dabei bedeuten die vier Schritte:

plan: Was muss wann getan werden, wer macht das, wie und womit?

do: Die geplanten Aktivität werden durchgeführt.

check: Es wird ermittelt, ob die Aktivitäten den Erwartungen entsprechen.

act: Aus den Erkenntnissen, die in der Messphase gewonnen wurden, werden Rückschlüsse gezogen, um die (neuen) Pläne anzugleichen.

Es gibt in der neueren Leseart nach ITIL zwei Bände – von ehemals zehn Bänden –, die die beiden Prozessgruppen *Service Support* und *Service Delivery* beschreiben. Adressiert werden fünf Hauptbereiche, die wiederum mittels Schnittstellen mit den vier übrigen Bereichen – z.T. in Überschneidung – verbunden sind. Diese fünf Bereiche sind:

- Geschäftliche Perspektiven (*Business Perspective*)
- Planung und Lieferung von IT-Services (*Service Delivery*)
- Unterstützung und Betrieb der IT-Services (*Service Support*)
- Management der Infrastruktur (*ICT Infrastructure Management*)
- Management der Anwendungen (*Application Management*)

Dabei bilden Service Support und Service Delivery die beiden übergeordneten Prozessgruppen, zusammengefasst im Begriff IT-Service-Management [Bon 2002]. Die Abb. 9.9 zeigt das Gesamtmodell in Form eines integrierten Prozessablaufs am Beispiel eines Service-Providers, der seinen Kunden ein VPN anbietet. Auf der rechten Bildhälfte (vertikal) sind schematisch die Zulieferer des Service-Providers dargestellt. Diese werden mit einem *Underpining Contract* an den Service-Provider gebunden.

Der Anwender – also der VPN-Nutzer – befindet sich dazu auf der gegenüberliegenden Seite und hat den *Service Desk* und das Störfall-Management (*Incident Management*) des Providers als Ansprechpartner. Störungen des VPN werden über diese Schnittstelle weitergegeben. Die operationellen Prozesse schließen sich hinter der Kundenschnittstelle an. Auf dieser Ebene werden alle Aktivitäten ausgeführt, die zur Erbringung der IT-Services für den Kunden notwending sind. Die unterschiedlichen Einheiten – meist eigene Abteilungen, die die Prozesse bearbeiten – stehen sich mit eigenen Liefer- und Leistungsbedingungen (*Operation Level Agreements*, OLA) gegenüber.

Dem Supportservice obliegen die folgenden Aufgaben:

Der Service Desk bildet den ersten Ansprechpartner der IT-Organisation für den Anwender.

Das Incident Management versucht Störungen so schnell alle möglich wieder zu beheben. Dabei wird zwischen Störungen und Problemen unterschieden.

Das Problem Management kümmert sich um die Ursachen von Störungen und beschäftigt sich mit strukturellen Schwierigkeiten.

Das Configuration Management kontrolliert die sich verändernde IT-Infrastruktur (Statusüberwachung).

Das Change Management sorgt für eine kontrollierte und durchdachte Durchführung von Änderungen innerhalb der IT-Infrastruktur.

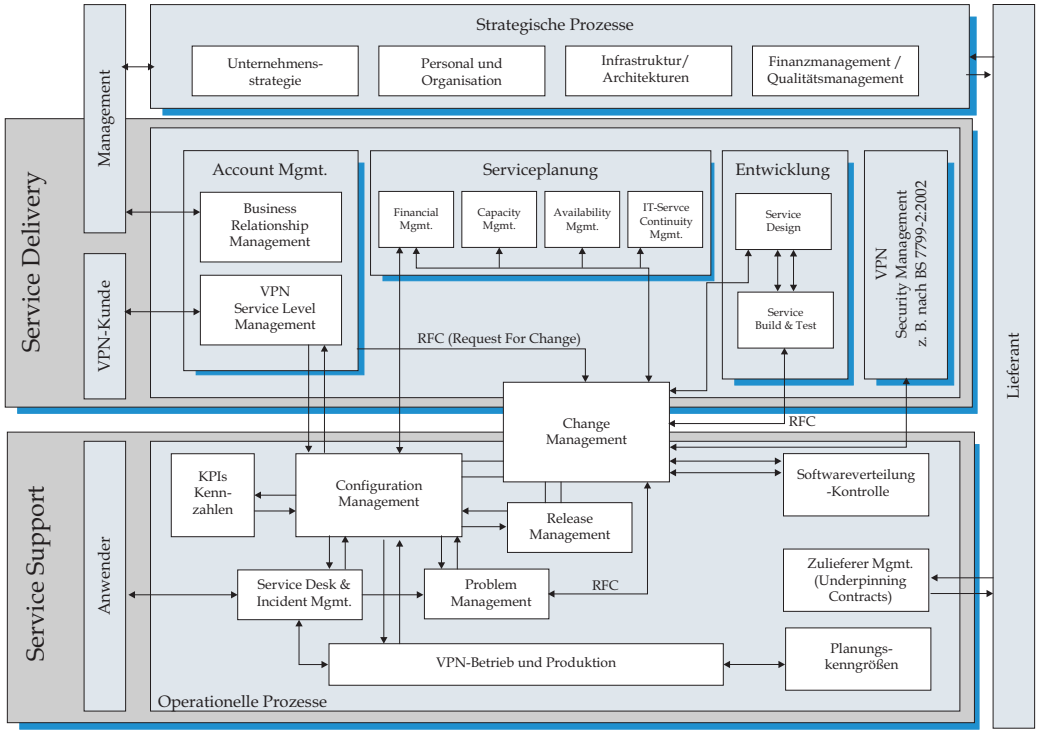


Abb. 9.9: Aufbau eines Integrated Process Workflow (IPW) nach ITIL

Das Release Management vollführt das erfolgreiche Rollout von Releases einschließlich Integration, Testen und Aufbewahren.

Im Bereich des Service Delivery fällt die Schnittstelle zum VPN-Kunden auf der Ebene der Geschäftsbeziehungen. Der Provider hält hierfür eine Abteilung bereit, die sich mit der Kundenbeziehung und speziell mit den Liefer- und Leistungsbedingungen *(Service Level Management)* mit dem Kunden auseinandersetzt. In dieser Beziehung werden die SLA vereinbart und die Pönalen festgelegt.

Dem Service Delivery obliegen die folgenden Aufgaben:

Das Service Level Management besteht darin, mit dem Kunden Vereinbarungen zu treffen und diese zu verwirklichen.

Das Finance Management für IT-Services sorgt für die betriebswirtschaftlichen Belange des IT-Service und kalkuliert Kosten und Nutzen.

Das Capacity Management hierdurch werden die IT-Ressourcen geplant und optimiert eingesetzt.

Das Availability Management gewährleistet die mit dem Auftraggeber (kunden) vereinbarte Verfügbarkeit von IT-Services.

Das Continuity Management für IT-Services legt die Vorbereitung und Planung von Kontinuitätsmaßnahmen der Geschäftsvorfälle im Katastrophenfall fest.

Eine Sonderrolle nimmt das Security Management ein, das noch nicht zentraler Bestandteil von ITIL ist, jedoch ideal durch Best- Practice-Werke wie z.B. durch BS 7799-2:2002 ergänzt werden kann. Das im BS 7799-2:2002 geforderte prozessorientierte Information Security Management System (ISMS) folgt ebenso dem PDCA Modell. Mit dieser prozessorientierten Herangehensweise erfährt die zu erbringende Dienstleistung einen weiteren Schritt in Richtung Industrialisierung der Informationstechnologie.

9.2.2 Sicherheitsaspekte

Neben den Servicevereinbarungen, die im nächsten Abschnitt behandelt werden, ist es wichtig zu wissen, welche Sicherheitsvorkehrungen für die zu übertragenden Daten vom Provider angeboten und realisiert werden. Denn in der ursprünglichen VPN-Definition, speziell für die IP-VPN, sind Datensicherheitsaspekte wie Vertraulichkeit und Integrität nicht enthalten (vgl. VPN-Definition auf Seite 6). Ein IP-VPN initiiert eine logische Verbindung in Form eines Tunnels zwischen zwei entfernten Kundenlokationen in der Weise, dass beidseitig die im privaten LAN eingesetzten IP-Adressen ohne Probleme weiter genutzt werden können. Das dazwischenliegende Netzwerk wird von den beiden Lokationen nicht wahrgenommen (Abschn. 7.1). Im Prinzip können damit IP-Pakete im Provider-Netzwerk ausgelesen werden. Dies gilt sowohl für die Router-Architektur im Internet als auch für WAN-Strecken, die mittels ATM ausgerüstet sind.

Hier spielt die Sicherheitsphilosophie des Unternehmens eine entscheidende Rolle (siehe Abschn. 3.2.6). Wird Wert auf eine Privatsphäre der zu übertragenden Daten gelegt, so ist es unabdingbar, dass zusätzlich zum Tunnel und zu den QoS-Anforderungen auch eine geeignete Verschlüsselung und Integritätsprüfung durchgeführt wird. Da allerdings eine Verschlüsselung generell Performance-intensiv ist, wird auf der Provider-Seite häufig angeführt, dass sich jeder Kunde in einer geschlossenen Nutzergruppe (CuG) befindet. Gerade bei MPLS-VPN wird dieses Argument benutzt. In diesem Fall kann und muss der Kunde entscheiden, welche Bedeutung die Vertraulichkeit und die Integrität der Daten haben. Weitere Ausführungen hierzu sind in Kap. 10 zu finden.

9.2.3 Servicevereinbarungen (SLA)

Lässt man das eigene VPN von einem Provider aufbauen und betreiben, ist es unabdingbar, geeignete Liefer- und Leistungsbedingungen – so genannte Service-

vereinbarungen oder auch Service Level Agreements (SLA) – auszuhandeln. Dieser relativ neue Typ von Leistungsvereinbarungen in der Telekommunikation fixiert die Erwartungen durch schriftliche Verträge, die an das fremdverwaltete VPN gestellt werden.

Ursprünglich wurden SLA für Sprachnetze und etwas später für Frame-Relay-Netze vereinbart. Das Ziel einer SLA ist klar umrissen – soll sie doch helfen, Konfliktfälle zwischen Anbietern und Unternehmen zu vermeiden. Es beschreibt die beidseitig ausgehandelten Erwartungen an die Serviceleistungen, die vom Provider (Netzanbieter) bereitgestellt werden.

Neben den drei wesentlichen Punkten Verfügbarkeit, effektiver Datendurchsatz und Übertragungsverzögerungen gilt es die folgenden Punkte zu beachten, zu denen sich der Anbieter klar äußern sollte:

- Port-Verfügbarkeit in Prozentangaben,
- Performance-Garantien,
- mittlere Zeit der Fehlerbehebung und nicht nur Antrittszeit,
- konkretisierte Wartungsfenster, in denen kein Betrieb stattfindet,
- Aussagen über Bandbreitenauslastung und Priorisierungsmöglichkeiten,
- Service-Hotline bzw. User Help Desk (UHD),
- Aussagen über Paketverlustrate (von/bis),
- Aussagen über Paketverzögerungen (von/bis),
- Aussagen über Sicherheitsmechanismen, insbesondere Verschlüsselungsmethoden und Schlüsselwechsel und gegebenenfalls Firewall-Systeme,
- Aussagen über Authentifizierungsverfahren,
- Aussagen über das Berichtswesen allgemein und für z.B. QoS-Monitoring,
- Aussagen über Nutzungserfassung und Zahlungsmodalitäten (Accounting und Billing),
- Aussagen zur finanziellen Motivationsunterstützung zur Einhaltung der SLA (Penalties),
- Notfallverfahren und Eskalationsmechanismen und
- Aussagen zu Bedingungen für eine vorzeitige Vertragsbeendigung.

Allerdings sind die getroffenen Vereinbarungen in den Liefer- und Leistungsbedingungen die eine Seite der Medaille, ihre Überprüfung die andere. Dabei gehört die Netzwerkverfügbarkeit noch zu den einfacheren nachprüfbaren Größen, in denen die tatsächliche Verfügbarkeit bzw. Wirkungsgrad η in Prozent gemäß Gl. 9.1 berechnet wird.

$$\frac{(24\,Std. \times Tage\,im\,Monat \times Anzahl\,der\,Sites) - Ausfallzeit}{(24\,Std. \times Tage\,im\,Monat \times Anzahl\,der\,Sites)} = \eta[\%] \qquad (9.1)$$

Insbesondere gilt dies für die Netzverfügbarkeit eines Netzwerk-basierten VPN. Hier sollte exakt die Definition des Netzanbieters beachtet werden, ob z.B. die Wartungsfenster enthalten sind oder wie es im Fall von höherer Gewalt aussieht. Bei einer Verschlüsselung ist es wesentlich schwieriger nachzuprüfen, ob z.B. nur mit DES, mit 3DES oder gar mit AES verschlüsselt wird. Bei einem CE-basierten VPN kommen die Einzelverfügbarkeiten der Komponenten hinzu, die als eine Serienschaltung zu betrachten ist, falls die Gesamtverfügbarkeit berechnet werden soll.

Viele Service-Provider sind heutzutage willens und in der Lage, Service Level Agreements zu vereinbaren, machen sie jedoch oftmals davon abhängig, wie viele Sites verbunden werden sollen. Netzanbieter, die in erster Linie Frame Relay anbieten, vereinbaren SLA in der Regel erst ab einer Anzahl von 10 Sites. Allerdings gibt es keine standardisierten SLA, so dass der Kunde bei den Verhandlungen auf sich selbst gestellt ist. Ebenso ist es hilfreich, sich die unterschiedlichen Größenkategorien vor Augen zu halten, die sich jüngst herauskristallisiert haben. Eine Betrachtung hierzu wird im nächsten Abschnitt durchgeführt.

9.3 VPN-Klassifizierungen

Werden die heute zur Verfügung stehenden VPN-Technologien und die Möglichkeiten der Skalierung und Komponentenfelxibilität betrachtet, können erhebliche Größenunterschiede zwischen einzelnen VPN-Realisierungen desselben Typs entstehen. Diese Unterschiede liegen jedoch nicht unbedingt im Typ (Intranet-VPN, Extranet-VPN, Remote-Access-VPN) begründet, sondern hängen stark von der Komplexität, dem Einsatzbereich, der Größe, der Anzahl der gelieferten Dienste sowie von den geforderten Technologien und Produkten und nicht zuletzt von der Firmengröße ab. Um diese zum Teil gegenseitigen Abhängigkeiten und Verzahnungen zu strukturieren, wird in einer tabellarischen Gegenüberstellung eine Klassifizierung nach fünf Stufen vorgenommen.

Doch zunächst seien die Kategorien näher erläutert:

Kat-0: VPN dieser untersten Kategorie sind geeignet für kleine Firmen mit einer einzigen Site und einer sehr begrenzten Anzahl von Fernzugriffsmöglichkeiten. Es ist die einfachste Art, ein VPN zu betreiben, und gleichzeitig eine kostengünstige Variante bei der Implementierung. Es wird häufig das PPTP-Verfahren mit einem zusätzlichen Paketfilter zur Absicherung des Intranets eingesetzt. All dies kann in der minimalen Konfiguration mit Windows NT oder Linux realisiert werden. Bei einem etwas größeren Sicherheitsbedarf kann eine extra VPN-Software auf einem Server installiert werden. Ein Kat-0 VPN ist ausgerichtet, auf die Firmen-E-Mails zuzugreifen und auf interne Datenbanken zu gelangen. Ein Datenzugriff ist für etwa 50 Nutzer ausgelegt, die über Wählzugänge ins Intranet gelangen. Ein Internetzugriff wird über xDSL oder 64-KBit realisiert. Diese unterste Kategorie eines VPN ist relativ unkompliziert kostengünstig im Unterhalt und gleichzeitig die einfachste Art, einen

Fernzugriff auf das Firmen-LAN zu realisieren. Nachteilig allerdings ist die Site-to-Site-Inflexibilität und die wohl längste mittlere Reparaturdauer (Mean-Time-To-Repair, MTTR) bei einem Ausfall der VPN-Software.

Kat-1: VPN dieser Kategorie – wohl die geeignetste für kleine und mittelständische Unternehmen – sind über mehrere Standorte verteilt und haben häufig schon eine 2-MBit-Internetanbindung im oberen Spektrum und ungefähr 250 Fernanwender. Meist wird eine Grundsicherheit erreicht, indem IPSec mittels DES-Verschlüsselung eingesetzt und zusätzlich eine Passwort-Authentifizierung für den Zugriff auf die Firmen-E-Mails, Daten und internen Datenbanken durchgeführt wird. Diese Kat-1-VPN werden zumeist mit einem hardwarebasierten VPN-Gateway realisiert, dessen Fernzugriff über eine spezielle IPSec-abgesicherte Client-Software erfolgt. Ein Vorteil dieser Lösung liegt klar in dem vergleichsweise einfachen Design und der Installation, geringen Kosten bei einem Site-to-Site-Zugriff sowie dem Fernzugriff bei größerer Datensicherheit ohne Performanzverlusten. Extranets werden mit IPSec-Implementierungen erzielt.

Kat-2: VPN dieser Kategorie sind ideal für eine mittlere Firmengröße von etwa 500 Fernnutzern (Remote User) mit einem Umfang von ca. 10 firmeneigenen Sites. Typischerweise sind dies Ingenieurfirmen, Werbe- oder Marketingagenturen, die anspruchsvolle Anforderungen haben. Niederlassungen haben eigene 128 Kbit- oder 2-MBit-Anbindung. Die Zentrale liegt dann im Bereich von ca. 2-MBit- bis hin zu mehreren 2-MBit-Anbindungen. Eine Verschlüsselung wird meist mit 3DES und einer starken Zwei-Wege-Authentifizierung, wie z.B. einer Token-Lösung, realisiert. Eine Skalierbarkeit wird durch den Einsatz von RADIUS-Servern erreicht, die die Fernnutzerverwaltung wie Namen, Passwort und Policys regeln. Diese KAT-2-VPN können koexistieren mit Firewall-Lösungen und einer IP-Adressumsetzung (NAT), um private IP-Adressen zu nutzen. Damit fällt eine extra Adressumsetzung bei Einwahl in das Firmen-LAN weg. Die Vorteile dieser Lösung liegen im relativ hohen Sicherheitsniveau und den geringen Kosten sowie bei gleichzeitiger Site-to-Site- und Fernzugriffsanbindung (Remote Access). Nachteilig ist allerdings die mangelnde Unterstützung bei Extranet-Einrichtungen und Echtzeitanwendungen.

Kat-3: VPN dieser Kategorie unterstützen mittelgroße bis sehr große Firmen mit tausenden von Fernzugriffen und Hunderten von Sites inklusive der Geschäftspartner und Kunden. Statusbericht, Änderungsverhalten und ECommerce-Transaktionen werden allen Nutzern geschickt bzw. von ihnen entgegengenommen. Typische Vertreter dieser Größe sind Anbieter aus dem Medizinsektor, große Versicherungskonzerne, Produktionsbetriebe oder Zulieferfirmen. Anbindungsgrößen der Niederlassungen bewegen sich bei Leitungsgrößen im Bereich von gesplitteten 1,5 Mbit/s bis hin zu mehreren 1,5 Mbit/s-Leitungen. Zentralen dieser Größenordnung werden entsprechend mit bis zu 34 Mbit/s oder weniger von einem Netzbetreiber versorgt. Fernzugriffe werden für jegliche Technologie, von xDSL über Kabelmodems bis

hin zu analogen Wählverbindungen, angeboten. Firmen dieser Kategorie nutzen den Service eines oder mehrer Netzanbieter und haben QoS mit Liefer- und Leistungsvereinbarungen (SLA) für zeitkritische Anwendungen, die zwischen den Firmenstandorten zur Anwendung kommen, ausgehandelt. Interoperabilitätszertifizierte IPSec-Geräte werden zur Anbindung von Extranets eingesetzt, um Fremdfirmen mit anderer Ausstattung anzubinden. Bei der Nutzer-Authentifizierung wird auf eine starke Zwei-Wege-Authentifizierung zurückgegriffen, wie z.B. Secure-ID-Tokens oder Smart Cards, wenn sich Mitarbeiter von extern ins Firmennetz einwählen. Das verursachergerechte Berichts- und Abrechnungswesen ist eine Selbstverständlichkeit. Eine skalierbare Administration erfolgt über Directory-Services und ist regelbasiert. Ebenso werden digitale Zertifikate zur Authentifizierung eingesetzt. korrespondierend hierzu ist entweder ein firmeneigenes Zertifikatsmanagement (CA) bzw. ein fremdverwalteter Zertifikatsdienst oder eigene Möglichkeiten einer Public-Key-Infrastruktur-Verwaltung vorhanden. Diese Art der VPN benötigen entsprechend geschultes Personal, das in ausreichender Anzahl vorhanden ist und eine ständige Betreuung durchführt. Zusätzlich sind ausgeklügelte Sicherheitsrichtlinien für Mitarbeiter und Partnerzugriffe vorhanden, die ständig angepasst und erweitert werden.

Kat-4: Diese VPN bieten ein größtmögliches Sicherheitsniveau, Flexibilität und eine hinreichende Skalierbarkeit. Es werden sichere transnationale Verbindungen unterhalten für Firmen mit entsprechender Größe, die ca. 10 000 Nutzer bedienen und im Bereich von tausend Sites liegen. Weiterhin sind diese Firmen mit einer Reihe von Partnerunternehmen verbunden und erreichen einen hohen Grad an Fremdrealisierung. Hierzu zählen z.B. Wirtschaftsministerien und große Finanzdienstleister. Niederlassungen sind breitbandig angeschlossen; die Zentrale liegt in ihrer Anbindung im Größenbereich von 34 MBit/s. Das ganze Spektrum von Möglichkeiten wird im Fernzugriffsbereich unterstützt, angefangen von xDSL bis hin zu Modempools. Oftmals wird dabei auf das Netz eines Service-Providers zurückgegriffen, der Echtzeit QoS und SLA in Verbindung mit Bandbreiten-Management und moderner Sprachdatenintegration wie Voice-over-IP (VoIP) und IP-Video-Konferenzen, anbietet. Diese VPN-Kategorie macht intensiven Gebrauch von Directory-Services wie z.B. LDAP sowie einer PKI-Technologie, um eine Rollenzuordnung mit begleitender, sicherer Nutzer-Authentifizierung und -verifizierung zu erreichen. Diese VPN unterstützen anspruchsvolle Extranet-Beziehungen, bei denen mehrere Partner und unabhängige parallele PKI-Systeme eingerichtet sind. Verständlicherweise sind diese Systeme relativ komplex und kostenintensiv in der Unterhaltung und erfordern ein ständige Betreuung.

Tab. **??** zeigt die Kategorien im direkten Vergleich nach unterschiedlichen Gesichtspunkten. Die letzte Spalte enthält eine Bewertung (für/wider) aus der Anwenderperspektive. Nach heutigen Erkenntnissen und Aussagen von Analysten liegt eine wesentliche Zielgruppe für VPN aus Sicht der Service-Provider bei einer Firmengröße von 100 bis 999 Mitarbeitern. Diese Firmen befinden sich häufig in

einem enormen Wachstumszwang und einer anstehenden Internationalisierung sowie der damit verbundenen Notwendigkeit, auf Unternehmensdaten international zuzugreifen. Bei diesen Firmen ist die IT-Infrastruktur meist nicht in dem Maße mitgewachsen wie die geschäftliche Expansion. Nach obiger Definition sind dies die *Kat-2* Firmen.

Befinden sich Firmen oberhalb von 1000-Mitarbeitern *(Kat-3)*, so gehören sie ebenfalls zu dieser Zielgruppe. Sie haben meist ihre Marktposition gefunden und versuchen nun, ihre Kosten zu minimieren und ihre Effizienz zu steigern. Damit reift oft der Gedanke heran, die steigenden IT-Kosten aufzufangen und die zunehmende Komplexität und Abhängigkeit hinsichtlich einer notwendigen WAN-Infrastruktur in fremde Hände *(Outsourcing)* zu legen. Mit anderen Worten: Je größer eine Firma ist, um so eher wird eine VPN-Fremdrealisierung ins Kalkül gezogen.

Für kleine Firmen allerdings kann eine VPN-Fremdrealisierung ebenfalls zum kritischen Erfolgskriterium werden, wenn sie in einer Zulieferkette größerer Unternehmen eingebunden sind, wie beispielsweise die Zulieferer der Automobilindustrie in das Branchennetz ENX (siehe Abb. 1.4).

Tabelle 9.1: Vergleich der Größenkategorien

VPN Kat	typische Nutzer	typische Anforderungen	Skalierbarkeit u. Bandbreite	Technologie u. Produkte	für/wider
Kat-0	Kleine Firmen mit Telearbeitern	E-Mail Interne Datenbanken Allg. Datenzugriff	eine Site bis zu 50 Telearbeiter Internetzugriff über DSL oder 1,5 Mbit/s-Wählverbindungen für Fernzugriffe	PPTP Windows NT/2000 Software VPN-Lösung auf einer PC-Standardplattform Paketfilterung	+ Einfach und geringe Kosten + Gute VPN-Einstiegsmöglichkeit − Keine Site-to-Site-Verbindung − Inflexibel, da Pkt.-zu-Pkt. − Längste MTTR (bei Serverausfall)
Kat-1	Kleine bis mittlere Firmen mit mehreren Lokationen	E-Mail Interne Datenbanken Allg. Datenzugriff	von 2 bis 10 Sites bis zu 250 Telearbeiter Internet-Zugriff bis zu 1,5 Mbit/s-Wählverbindungen für Fernzugriffe	IPSec (DES, IKE) Passwort- u. Nutzer-Authentifizierung Hardware VPN-Gateway (bis zu 1,5 Mbit/s Bandbreite und 250 Sessions) Extra Client-Software für Fernzugriffe Einfache Firewall oder Paketfilterung	+ Einfach zu konzipieren und zu installieren + Preisgünstig + Site-to-Site u. Fernzugriff vorhanden + Hardware VPN-Gateway bringt Sicherheit mit kaum Performanceverlust − Keine Extranet-Unterstützung, wenn IPSec nicht kompatibel
Kat-2	Mittlere Firmen mit besonderen Ansprüchen	E-Mail Interne Datenbanken Allg. Datenzugriff Produkt-Design z.B. CAD/WebCAD Übergreifende Projektplanungen	Bis zu 10 Sites Bis zu 500 Telearbeiter Internetzugriff mit 1,5 Mbit/s Bandbreite und mehr bei der Zentrale Internet-Zugriff bis zu 1,5 Mbit/s in der Niederlassung Wählverbindungen für Fernzugriffe	IPSec (DES,IKE) NAT Starke Nutzer-Authentifizierung (z.B. Secure-ID Token) Firewall-Systeme in der Zentrale RADIUS-Server Hardware VPN-Gateways mit Geschw. Leistungsstufen (von 1,5 Mbit/s bis n $\times$ 1,5 Mbit/s) mit 500 Sessions Extra Client-Software für Fernzugriffe	+ Hohes Sicherheitsniveau + Moderate Kosten + Site-to-Site u. Fernzugriff vorhanden − Zusätzlicher Wartungs- und Pflegeaufwand für Firewall und RADIUS etc. − Kein Extranet (fehlende Kompatibilität) − Keine Echtzeitanwendungen

Tabelle 9.1: Vergleich der Größenkategorien (Fortsetzung)

VPN Kat	typische Nutzer	typische Anforderungen	Skalierbarkeit u. Bandbreite	Technologie u. Produkte	für/wider
Kat-3	Mittlere Firmen bis große Firmen mit eigenen Geschäfts-partnern u. eigenen Kunden-stamm, wie z.B. Versi-cherungen und Pharma-firmen	E-Mail Interne Datenbanken Allg. Datenzugriff Design-Informationen Anschluss an Zulieferungsketten E-Commerce-An-wendungen	ca. 100 Sites ca. 1000 Telearbeiter von 1,5 Mbit/s bis n× Mbit/s zur Anbindung einer Filiale von E1 bis E3 Bandbreite für die Zentrale QoS/SLA für Site-to-Site-Verbindungen Wählverbindungen, ISDN, xDSL oder Modembänke für Fernzugriffe vorhanden	Zertifizierte Kompatibilität für IPSec (3DES,IKE) NAT Starke Nutzerauthentifizierung (Smart Cards, Token) Firewall-Systeme in der Zentrale und in großen Filialen Einsatz von LDAP Einsatz einer eigenen PKI Hardware-VPN-Gateways mit Ge-schw. Leistungsstufen (von T1 bis n × T1 oder auch E1 für 5000 Sessions und mehr) Automatismus für Policy-ver-schickende Client-Software für Telearbeiter	+Unterstützung von Extranets +Unterstützung von zeitkritischen E-Commerce Transaktionen −Allg. Sicherheitspolicy sowie Si-cherheitsarchitektur und Sicher-heitsrichtlinen notwendig −Vertieftes Wissen zur Planung und Umsetzung des VPN erforderlich −Ständige intensive Wartung und Pflege des VPN notwendig
Kat-4	Große multinatio-nale Firmen mit extrem vielen Geschäfts-partnern bzw. Zu-lieferkette mit einem hohen Grad an Fremd-realisierung	E-Mail Interne Datenbanken Allg. Datenzugriff Anschluss an Zu-lieferungsketten E-Commerce-An-wendungen Sprachanwendungen Video-/ Konferenz-systeme	ca. 1000 Sites ca. 10.000 Telearbeiter von 1,5 Mbit/s bis n× Mbit/s zur Anbindung einer Filiale von E1 bis E3 Bandbreite für die Zentrale QoS/SLA für Site-to-Site-Verbindungen Wählverbindungen, ISDN, xDSL oder Modembänke für Fernzugriffe vorhanden	Zertifizierte Kompatibilität für IPSec (3DES,IKE) NAT Starke Nutzer-Authentifizierung (Smart Cards, Token) Firewall-Systeme in der Zentrale und in großen Filialen Einsatz von LDAP Einsatz einer eigenen PKI Hardware-VPN-Gateways mit Ge-schw. Leistungsstufen (von T1 bis n × T1 oder auch E1 für 5000 Sessions und mehr) Bandbreiten-Management Mehrere VPN-Service-Stufen Echtzeit QoS & SLAs Automatismus für Policy-ver-schickende Client-Software für Telearbeiter	+Unterstützung von Extranets +Hohes Sicherheitsniveau +Unterstützung von Echtzeit-App. u. Video +Unterstützung von E-Commerce-Anwendungen +Skalierbare Administration +Beziehungen zu mehreren Geschäftspartnern −Sehr komplex und kostenintensiv −Profundes Wissen von Netzwerktechnik u. Sicherheitsmechanismen erforderlich −Ständige intensive Wartung und Pflege des VPN notwendig

Unabhängig von der Firmengröße ist es sinnvoll, einen Vergleich zwischen den unterschiedlichen Netzanbietern durchzuführen. Ein Vorschlag der Gartner Group wird im nächsten Abschnitt diskutiert.

9.3.1 Vergleichsverfahren und Anforderungen

Einem Vorschlag der Gartner Group von 1998 folgend (Tab. 9.2) lassen sich 16 aussagekräftige Vergleichskriterien formulieren, um die Leistungen verschiedener Netzanbieter zu charakterisieren, die für eine Entscheidungsfindung heranzuziehen sind. Allerdings sind nicht alle 16 Vergleichskriterien gleich. Dem wird mit einer Gewichtung von 1-5 Rechnung getragen. Dabei ist der Wert 1 von geringerer Wichtung als der Wert 5. Die Tab. 9.2 ist als Anregung zu verstehen; eigene Kriterien können hinzugefügt werden.

Tabelle 9.2: Gewichtete Kriterien zur Beurteilung unterschiedlicher VPN-Anbieter

Kriterium	**Wichtung**	**Anbieter A**	**Anbieter B**	**Anbieter C**
Präsenz allg.	5			
Präsenz (Personen)	3			
PoP-Präsenz	4			
Zahlungsmodi	2 oder 5			
VPN-Plattform	3			
Management-Tools	5			
Zugriffsarten	3			
Servicevarianten	3			
Nummernplan	3			
TK-Kopplung	1 oder 5			
Pre-Sales-Service	3			
Post-Sales-Service	3			
Referenz-Sites	2 oder 5			
QoS-Garantien	5			
Penalties	4			
Preis	4			
Gesamtpunktzahl				

Gemäß Tab. 9.2 kann die Zahlungsflexibilität mit dem Wichtungswert 2 oder 5 bewertet werden, je nachdem ob besondere Zahlungsmodalitäten erforderlich sind. Ist dieser Punkt unwichtig, sollte der Wert 2 eingesetzt werden. Eine ähnliche Differenzierung kann bei der TK-Kopplung bzw. TK-Anlagenkopplung vorgenommen werden. Sollte die eigene TK-Anlage mit in das VPN eingeschlossen werden müssen, ist dies eine wichtige Forderung, der entsprechend ein Wichtungswert von 5 zugeordnet werden sollte. Trifft diese Anforderung nicht zu, sollte der Wert wesentlich geringer gesetzt werden.

9.4 Übungen

1. Was ist unter einem genesteten VPN-Tunnel zu verstehen?
2. Welche Aufgaben hinsichtlich der Vertraulichkeit der Daten im Tunnel obliegen dem Kunden, wenn er ein CE-basiertes VPN bei einem Provider vertraglich abgeschlossen hat?
3. Worin liegen die Unterschiede zwischen dem CE-basiertem und einem NB-basiertem VPN-Referenzmodell?
4. In der Abb. 9.3 wird ein kontinuierlicher Übergang von Eigenrealisierung zur Fremdrealisierung gezeigt. Wo ist auf dem Kontinuum ein CE-basiertes VPN einzuordnen?
5. In der Abb. 9.3 wird ein kontinuierlicher Übergang von Eigenrealisierung zur Fremdrealisierung gezeigt. Wo ist auf dem Kontinuum ein NB-basiertes VPN einzuordnen?
6. Erläutern Sie die Struktur der globalen Netze.
7. Worin liegen die Unterschiede zwischen einem NSP (Network Service Provider) und einem ISP (Internet Service Provider)?
8. Welches sind die vier Kernkomponenten eines Netzwerk-Management-Systems?
9. Was sind Service Level Agreements (SLA)?
10. Was wird durch ITIL (IT-Infrastructure Library) beim Netzwerk-Management-System (NMS) und bei den Service Level-Agreements (SLA) abgedeckt?
11. Welche Aufgabe hat ein ISMS in einer nach ITIL ausgerichteten Systemarchitektur?
12. Worin liegen die Unterschiede zwischen SLA und OLA?

10 Einsatz von VPN

In diesem Kapitel werden zunächst Betrachtungen über die Entwicklung des VPN-Marktes, prognostiziert von verschiedenen Wirtschaftsanalysten, vorgestellt und diskutiert. Ausgehend von diesen Marktbetrachtungen werden Überlegungen hinsichtlich einer Eigen- bzw. Fremdrealisierung, bezogen auf die drei VPN-Typen Access-VPN, Intranet-VPN und Extranet-VPN, angestellt. Der Schwerpunkt dieses Kapitels 10 behandelt die wesentlichen Planungsaspekte. Diese nicht triviale Aufgabe wird in vier Phasen – von der Analyse bis zum Betrieb – vorgenommen.

10.1 VPN-Marktbetrachtungen

Aus der Sicht eines Service-Providers lohnt sich die Investition in die VPN-Technologie, denn alle bedeutenden Wirtschaftsanalysten bestätigen dieser Technologie ein enormes Wachstum. Der Grund: Das Kosten-Nutzen-Verhältnis der VPN-Technologie stellt neben der Flexibilität und Skalierbarkeit die herkömmlichen Kommunikationstechnologien wie Mietleitungen, ATM oder die Frame-Relay-Technologie sowie Modembänke für den Fernzugriff betriebswirtschaftlich weit in den Schatten.

Die VPN-Technologie ist die technologische Antwort auf das schnelllebige Informationszeitalter des 21. Jahrhunderts. Die Zielgruppe für die Service-Provider besteht nicht nur aus großen und und global tätigen großen Unternehmen (Konzernen), sondern auch kleinere und mittelständische Firmen werden sich dieser Technologie annehmen müssen. Für Unternehmen stellt sich nicht mehr die Frage, ob ein VPN für die eigene Firma relevant ist oder nicht, sondern nur noch die Frage, wie und mit wem ein VPN umgesetzt werden soll. Ein breites Kundenspektrum steht einer enormen Geschäftsfeldentwicklung gegenüber. Diese Überlegung deckt sich mit der Marktstudie von Frost & Sullivan aus dem Jahre 2003, in der der Mittelstand als die potenzielle Zielgruppe für IP-VPN-Dienste genannt wird [Frost & Sullivan 2003].

Die VPN-Technologie unterliegt, wie alle am Markt angebotenen Produkte, einem wirtschaftlichen Lebenszyklus. Wird der Produktlebenszyklus des VPN-Marktnäher betrachtet, kommen interessante Aspekte zum Vorschein, wie die Erhebungen von Infonetics oder Forester zeigen. Der Zyklus gibt, angelehnt an die Gauß-Verteilung, den natürlichen Ablauf vom Markteintritt bis zur Degeneration wieder.

Dem Zyklus entsprechend wird das Produkt zeitlich von unterschiedlichen Gruppen wahrgenommen und akzeptiert. Bei dieser Aufteilung in fünf Kategorien, stellt die erste die innovative Kategorie *(Innovators)* dar. Diese Gruppe ist

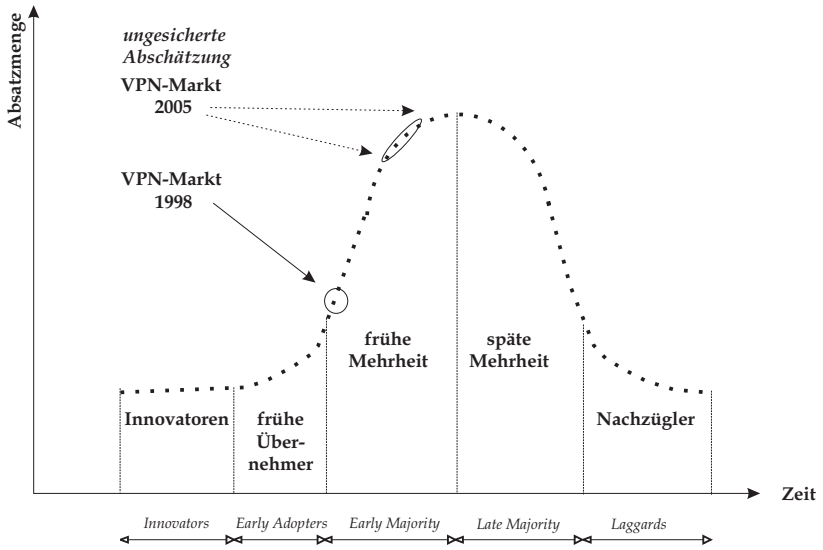


Abb. 10.1: Produktakzeptanzzyklus unterteilt in fünf Kategorien

frühzeitig bereit, ein neues Produkt am Markt – oftmals trotz „Kinderkrankheiten" – zu kaufen. Abb. 10.1 zeigt die Absatzmenge bezogen auf die fünf Kategorien, die auf der Zeitachse eingezeichnet sind. Weiterhin ist eine Einschätzung der VPN-Marktsituation für das Jahr 1998 eingezeichnet. Im Jahr 2005 entspricht die Marktsituation etwa den Marktprognosen der Analysten aus den vergangenen Jahren. Verlässliches Zahlenmaterial liegt allerdings nicht vor, denoch kann gemutmaßt werden, das die VPN-Technologie im Mainstream angelangt und in der Nähe des Zenits zu platzieren ist. Die zweite Gruppe zeigt die frühen Käufer *(Early Adopters)*, die dem eigentlichen Trend am Markt voraus sind und als Trendsetter gelten. Als nächste Gruppe erscheint die frühe Mehrheit *(Early Majority)*, die ein Produkt kauft, das sich am Markt zu etablieren beginnt. Spätestens jetzt sollte ein Produktwechsel für einen potenziellen Käufer ins Auge gefasst werden. Nach Marktaussagen, z.B. der Analysten von TeleChoice, befindet sich der VPN-Markt gegenwärtig in dieser Phase des Produktlebenszyklus. Somit hat die VPN-Technologie Marktreife erreicht. Ähnliche Aussagen liefern auch andere Analysten wie z.B. die der Yankee Group oder die der Infonetics Research. Allerdings beziehen sich die Erhebungen auf den amerikanischen Markt, verlässliche Zahlen für Europa scheint es nicht zu geben.

In der nächsten Phase ist der Zenit des Produktabsatzes überschritten, auch wenn sich jetzt die zweite große Gruppe, die späte Mehrheit *(Late Majority)*, dem Produkt zuwendet. Als fünfte und letzte, tritt die als Zögerer bezeichnete Gruppe in Erscheinung und bildet die Phase der Nachzügler *(Laggards)*. Weitere Erklärungen und Hintergrundinformationen zur Theorie des Produktlebenszyklus sind bei

[Becker 1998] zu finden.

Neben den obigen Betrachtungen, die eine allgemeine Aussage über den VPN-Markt liefern, ist es ebenso interessant, sich die Entwicklung der unterschiedlichen VPN-Varianten detallierter zu betrachten. Nach Untersuchungen und Experteneinschätzungen der Meta Group aus dem Jahr 2001 lässt sich wie in der Abb. 10.2 dargestellt eindeutig entnehmen, dass ein Trend zu Gunsten der Dial-Up-VPN zu verzeichnen ist [Meta Group 2001]. In der Untersuchung wurden 205 Unternehmen in Deutschland befragt. Weniger als ein Viertel der befragten Unternehmen haben bereits ein VPN im Einsatz. Großunternehmen sind meistens in der Realisierung ein Schritt weiter gegenüber kleinen und mittelständischen Unternehmen (KMU). Somit liegt gerade für dieses Marktsegment ein enormes Wachstumspotenzial vor.

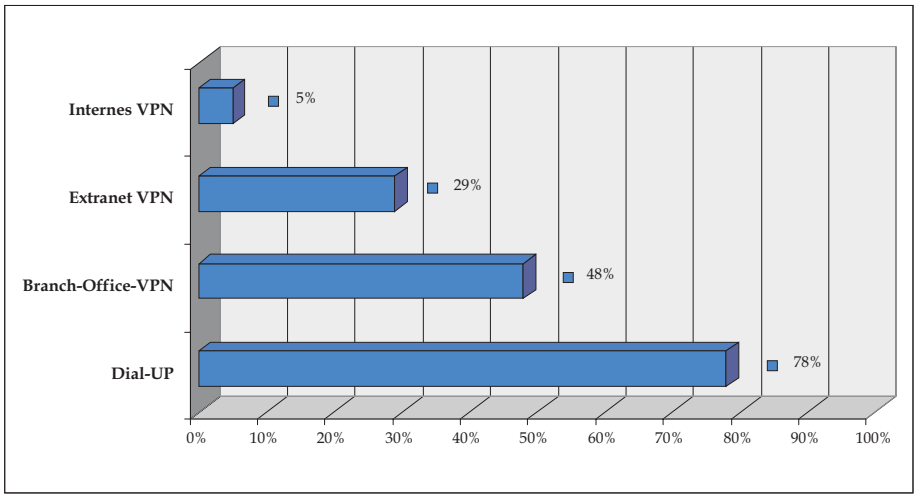


Abb. 10.2: Trends und Marktentwicklung in Deutschland (Stichprobenumfang 205 Unternehmen, Mehrfachnennungen möglich, Quelle: Meta Group, 2001)

Aufgrund der von den Firmen verfolgten Ziele, die in der Studie herausgearbeitet wurden, ist der Aspekt der Flexibilität der Infrastruktur von entscheidender Bedeutung bei der Konzeption eines VPN. Denn 78% der Unternehmen gaben an, ihren Mitarbeitern den Zugriff auf das Firmennetzwerk zu ermöglichen. Gerade auch kleinere Niederlassungen richten den VPN-Zugriff über eine Wählverbindung ein, um die kostenintensiveren Standleitungen zu vermeiden. Es kann vermutet werden, dass für die Außenstellen des Unternehmens der Zugriff auf die Ressourcen in der Firma durch ein VPN erst ökonomisch gestaltet werden kann.

Die in der Abb. 10.2 aufgezeigten Trends korrelieren mit den Angaben, die in der Abb. 10.3 zu sehen sind. Interessant ist der Trend in Richtung Mobilität, der sich noch weiterhin verstärken wird. Der Trend belegt, dass Unternehmen eine unkomplizierte Anbindung von Außenmitarbeitern, Niederlassungen, Kunden und

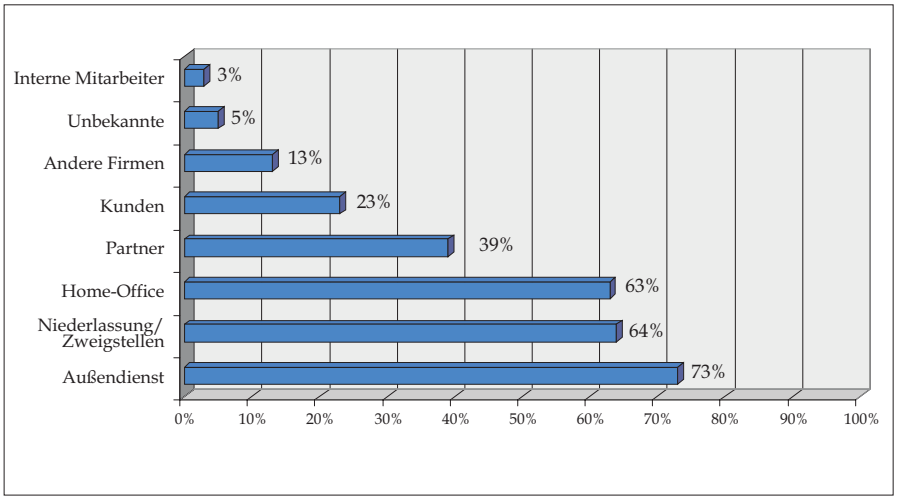


Abb. 10.3: Verteilung der VPN Zugriffsarten (Stichprobenumfang 201 Unternehmen, Mehrfachnennungen möglich, Quelle: Meta Group, 2001)

Partner mit dem Einsatz von Virtual Private Networks, verfolgen. Ebenso spielen Kosteneinsparungen, Ausfallsicherheit bei schwankendem Ressourcenbedarf eine erhebliche Rolle. KMUs werden in die Lage versetzt, bedingt durch den herrschenden Kostendruck, gleichwertige Dienstleistungen wie Großunternehmen anbieten zu können, obwohl sie nicht über den Ressourcenbedarf verfügen.

Grundsätzlich wird die moderne Kommunikation dem sich abzeichnenden Trend folgen und zunehmend bestimmt werden durch mehr Dynamik, größere Zugriffsmöglichkeiten – begleitet von eine gesteigerten Individualisierung als je zuvor. Hierzu gehört auch, dass die Unternehmen ihre Geschäftsbeziehungen vermehrt in einer virtuellen Welt mit vertrauenswürdigen Verbindungen zu Anbietern, Partnern, Mitarbeitern und Kunden abwickeln.

Analysten der Firma TeleChoice [TeleChoice 2001] haben die sich verändernde Geschäftswelt durch acht Kennzeichen charakterisiert. Demnach wird die Geschäftswelt zukünftig bestimmt durch:

1. Globalisierung und zunehmender Wettbewerb
2. Dezentralisierung mit gleichzeitiger Zunahme von mobilen Mitarbeitern und einer Erhöhung des Telekommunikationsaufkommens
3. Weitere Verbreitung des IP in den Netzwerken
4. Zunahme der webbasierten internen Prozesse mit begleitender Kosteneinsparung der administrativen Bürotätigkeiten
5. Integration der Zulieferkette aus Kosten- und Strategiegründen

6. Konzentration auf das Kerngeschäft mit einer erhöhten Bereitschaft zum Outsourcing
7. Perfektere Infrastruktur zu geringeren Kosten,
8. Zunehmender Bedarf an hoch vertraulichen, flexiblen und hoch sicheren Netzwerken

Allerdings stellt sich weiterhin die Frage, inwieweit eine Eigenrealisierung in welcher Abstufung notwendig und vernünftig ist, oder ob auf eine völlige Fremdrealisierung zurückgegriffen werden soll, wie das Kontinuum in Abb. 9.3 nahelegt.

Mittlerweile existieren Referenzmodelle, mit denen die Schnittstellen eindeutig und austauschbar definiert sind, falls ein Anbieterwechsel vorzunehmen ist. In den Abschnitten 9.1.4 und 9.1.5 sind die beiden gängigen Referenzmodelle bereits behandelt worden, jedoch ohne Abwägung der Vor- und Nachteile einzelner Lösungen vorzunehmen. Dies soll an dieser Stelle nachgeholt werden. Doch kann es kein pauschales Votum zugunsten eines Referenzmodells geben. Zu verschieden sind die unterschiedlichen Gegebenheiten und Anforderungen, die eine Lösung bestimmen. Somit wird wohl langfristig eine Koexistenz zu verzeichnen sein.

Nur eine Geschäftsbeziehung, von denen beide Unternehmen sich einen Gewinn erhoffen, ist Erfolg versprechend. Entschließt sich ein Provider, ein CPE-basiertes gemanagtes IP-VPN in seine Produktpalette (Portfolio) aufzunehmen, profitiert ein Kunde bei einem kompletten Outsourcing von den wegfallenden Installations- und Wartungsarbeiten und -kosten, die bei einem großen, zum Beispiel länderübergreifenden, IP-Netzwerk in erheblicher Höhe anfallen würden. Nebenbei fallen auch alle anderen größeren und kleineren Netzprobleme nicht mehr beim Kunden, sondern beim Provider an.

Generell gilt für IP-VPN-Produktanbieter, dass sie einen großen Einfluss auf die Marktentwicklung ausüben. So vertreten beispielsweise die meisten Anbieter, dass CPE-basierte Lösungen weitaus sicherer sind als Netz-basierte Lösungen. Diese Meinung ist heftig umstritten und wird kontrovers diskutiert, indem unter anderem angeführt wird, dass gerade die letzte Meile zur Kunden-Site eine der sichersten Komponenten im ganzen Netzwerk ist. Tab. 10.1 liefert in komprimierter Form sowohl für Kunden als auch für Service-Provider die Vorteile einer CPE-basierten Lösung. Auch liegt ein Schlüsselargument in den geringen Investitionskosten einer CPE-basierten IP-VPN-Lösung. Außerdem kann eine Wartung wesentlich schneller und kostengünstiger durchgeführt werden als bei einer Netzbasierten IP-VPN-Lösung.

Obwohl für beide Seiten eine vorteilhafte Lösung in der CPE-basierten IP-VPN-Architektur liegt, gibt es auch einige Nachteile, die nicht zu unterschätzen sind. Diese sollten, solange die Wirtschaft zu dieser IP-VPN-Lösung tendiert, ebenfalls Beachtung finden. Einer der wesentlichen Nachteile sind die gemeinsam anfallenden Kosten, die sich in der CPE-Schnittstelle ergeben. Außerdem müssen Performance-Probleme immer von beiden Seiten gelöst werden. Tab. 10.2 gibt

Tabelle 10.1: Vorteile einer CPE-basierten IP-VPN-Lösung für Kunden und Service-Provider

Kundenvorteile	**Service-Provider-Vorteile**
■ Kontrolle, Kontrolle, Kontrolle ■ Kontrolle über Sicherheitseinrichtungen, Credentials, Systeme und direkter Zugriff auf das Access-Netzwerk. – Volle Ende-zu-Ende-Verschlüsselung (inkl. der lokalen Zugriffe) – Direkter Einfluss auf das Equipment zur Aggregation und zur Verschlüsselung – Ende-zu-Ende-Zugriff kann entweder beim Kunden oder beim Serviceprovider gewartet werden ■ Wartung erfolgt unabhängig vom ISP bzw. Carrier ■ Kontrolle, welches Equipment eingekauft wird; es kann das am Markt beste Equipment eingekauft werden. ■ Die Lösung kann wesentlich feiner, auf die Netzbedürfnisse einer Site-to-Site, abgestimmt werden	■ Geringe Investitionen erforderlich ■ Deutlich bessere Absicherung der letzten Meile durch eine Ende-zu-Ende-Verschlüsselung ■ Möglichkeit der Einflussnahme für bestimmte Kunden, die eine übergeordnete Kontrolle einfordern (z.T. besitzen große Firmen ein ausgeklügeltes CPE-VPN und Firewall-Überwachungssystem und ziehen eine eigene Wartung vor) ■ Keine große Umstellung für die Kunden erforderlich, die ihre Frame Relay- oder ATM-Netze ebenfalls nicht selbst betreut haben. ■ Eine ideale Möglichkeit, andere gemanagte Dienste, wie Router, Ethernet oder Switches, anzubieten

die wesentlichen Punkte in Kurzform wieder. Schließlich kann sich auf Kunden- und auf Provider-Seite eine negative Atmosphäre breit machen, wenn Störfälle entstehen, die sich auf die Performance auswirken, und deutlich wird, dass die CPE nicht auf dem üblichen Niveau einer Carrier-Anforderung bezüglich der Verfügbarkeit und Vertraulichkeit ausgelegt wurde.

Da die CPE-basierten IP-VPN im Wesentlichen zur ersten VPN-Generation (traditionelle VPN-Technologie, wie Frame Relay und ATM) gehören, bestehen etliche Altlasten, die zu zwei wesentlichen Anforderungen im Markt geführt haben:

- Erstens erwarten die Endnutzer, dass ein Service-Provider das VPN für ihn betreut und Wartungsaufgaben übernimmt. Allerdings sind nicht alle Kunden bereit, alle Funktionalitäten eines VPN in allen Konsequenzen aus der Hand zu geben. So haben meist größere Firmen mit umfangreichen Geschäftsbeziehungen den größten Vorteil von diesem Modell. Das typische Serviceangebot deckt jedoch die meisten Anforderungen des Marktes ab.
- Zweitens sind die Kunden unerbittlich in ihren Forderungen bei der Absicherung des IP-VPN, die besser oder zumindest gleich gut sein muss wie die traditionelle Absicherung bei einer Frame Relay oder ATM-Netzverbindung. Insbesondere erwarten Kunden, dass Sicherheitsvorkehrungen eingerichtet wer-

Tabelle 10.2: Nachteile einer CPE-basierten IP-VPN-Lösung für Kunden und Service-Provider

Kundennachteile	**Service-Provider-Nachteile**
■ Erfordert umfangreiche Installationszeit ■ Keine mit Carriern vergleichbare Vertraulichkeit und Verfügbarkeit ■ Als Kunde müssen alle Zeitvorgaben des Providers bei gemeinsam anfallenden Wartungsarbeiten und Problemen hingenommen werden ■ Begrenzte Skalierbarkeit: Eingeschränkte Möglichkeiten, um zusätzliche Services oder Funktionalitäten nachträglich ins Equipment einzusetzen ■ Es ist üblicherweise ein Einzelanbieter für das gesamte Equipment vorgegeben	■ Lange Installationszeit = Umsatzeinbußen ■ Eventuell hohe Installationskosten, falls ein kompletter Austausch aller Sites innerhalb des VPN, des Fernzugriffs sowie bei schwierigen Sites erforderlich wird. ■ Hohe Management- und Wartungskosten bei einem Upgrade; bestimmte Wartungsprobleme ziehen einen kompletten Austausch der Kunden-Sites nach sich ■ Geringere Performance-Leistung gegenüber einer reinen Carrier-Leistung ■ Der Kunde muss bei nahezu allen Installations- und Wartungsproblemen mit einbezogen werden ■ Begrenzte Skalierbarkeit: Schwierig, den Kunden erweiterte Services und Funktionalitäten zu verkaufen ■ Eingeschränkte Management-Möglichkeit, eingeschränkte Fernwartbarkeit und Überwachungsmöglichkeit, solange Plattformen unterschiedlicher Hersteller betreut werden

den. Hierzu zählen Firewall-Systeme, Verschlüsselungsmöglichkeiten, Tunnelbereitstellung und digitale Zertifikate zur Authentifizierung sowie zukünftig auch PKI-Lösungen.

Zukunft der IP-VPN

Während ein durchgängiger Service und vielfältige Sicherungsmöglichkeiten zu den heutigen Grundanforderungen der IP-VPN gehören, entwickeln sich kontinuierlich neue Anforderungen für zukünftige VPN-Lösungen, die im Kern teilweise schon vorhanden sind. Hierzu gehören erstens Applikationen, die das IP-VPN passieren und die über die Grenzen der herkömmlichen E-Mail-Kommunikation und des Internetzugriffs hinausgehen. Die zukünftigen Geschäftsvorfälle erfordern, dass auch Geschäftspartner mittels komfortabler und sicherer Verbindungen (*Streamlines*) in die geschäftliche Kommunikation über Extranets eingebunden werden. Als Ergebnis muss eine Firma eine einfache Möglichkeit bieten, schnell, verbindlich und zuverlässig auch Stream-orientierte Verbindungen zu allen Kommunikationspartnern, die intern und extern am Geschäftserfolg teilhaben, einzurichten.

Zweitens verlangen die Kunden mehr und mehr nach Kontrollmöglichkeiten über

das installierte IP-VPN, speziell erwarten sie mehr Einblick und Management-Möglichkeiten über das Netz. Solche Einblicke ermöglichen den Kunden, sich intensiv mit dem Netzwerk auseinander zu setzen; sie können proaktiv mit dem Provider das Netz managen und kontrollieren. So fühlen sich Kunden bei Netzproblemen nicht nur betroffen, sondern sie können zusammen mit dem Provider gemeinsam nach einer Lösung suchen, um die Ausfall- und Endstörzeiten zu minimieren.

Derartige Möglichkeiten werden durch moderne webbasierte Kontroll- und Management-Systeme mit so genannten *Customer Network Management*-Systemen (CNMS) bereitgestellt. Eine der erwarteten minimalen Anforderungen an derartige Systeme besteht darin, dass der Kunde die QoS-Parameter einfach überprüfen, Endnutzer-Privilegien bestimmen und Zugriffe der Endnutzer reglementieren kann. Die grundlegende Idee eines CNMS ist, dass der Kunde die volle Verantwortung aus den Händen geben kann, um das Netzwerk komplett betreuen zu lassen, jedoch die volle Kontrolle über alle Schlüsselparameter behält.

Damit ändern sich die Anforderungen an zukünftige IP-VPN, die sich in folgenden Trendaussagen widerspiegeln:

- IP-VPN gehören inzwischen fast zum Massenmarkt (Mainstream), werden jedoch als Erweiterung für neue Firmen-Services eingestuft.
- Netzwerkbasierte IP-VPN-Lösungen werden in zunehmendem Maße die CPE-basierten IP-VPN ablösen, um den Erwartungen des Massenmarktes gerecht zu werden.
- Vordringlichstes Problem der IP-VPN ist es, die IuK-Sicherheit mit allen Facetten abzudecken.
- Sowohl Hardware- als auch Software-basierte Sicherheitslösungen werden eingesetzt werden.
- Es wird eine Kombination zwischen CPE- und Netzwerk-basierten VPN-Variationen geben.
- Es wird breitbandige Zugriffsmöglichkeiten für VPN, wie xDSL, Kabel, Spitzenlast stabiles Ethernet etc., geben.
- Neue QoS-Standard-Mechanismen für VPN, wie Diffserv, MPLS, Traffic Shaping etc., werden selbstverständlich sein.
- Es wird einen zunehmenden Bedarf an Policy-basierten Services geben, der übergreifend über Applikationen, Nutzer und Gruppen agiert.
- Es wird einen zunehmenden Bedarf an Überwachung und Kontrolle für das Netz-Management kundenseitig geben, wie es z.B. CNMS-Tools bieten. Damit wird es dem Kunden ermöglicht, eine eigene Online-Überwachung für Applikationen, Nutzer und Gruppen vorzunehmen.

Tabelle 10.3 zeigt die Vorteile einer Netz-basierten Lösung sowohl für den Kunden als auch für den Provider.

Somit können Service-Provider ihren Kunden grundsätzlich zwei unterschiedliche Lösungsalternativen anbieten: Zum einen den IP-VPN-Typ der ersten Generation, der von Kunden in Eigenregie aufgebaut und überwiegend unterhalten wird, zum anderen neue moderne Netz-basierte IP-VPN-Lösungen, die ein enormes Leistungsspektrum bieten. Allerdings werden noch etliche Service-Provider und Kunden an den CPE-basierten IP-VPN-Lösungen festhalten, während andere sich an den Möglichkeiten einer Netz-basierten Lösung orientieren. Für einen Service-Provider gilt allerdings, dass er die Vorteile und Fallstricke einer jeden Lösung genau betrachten muss, falls er seine eigene IP-VPN-Infrastruktur aufbauen will. Außerdem wird es für einen Provider schwierig sein, sich mit einer CPE-basierten IP-VPN-Lösung vom linearen Kostenmodell zu lösen. Dies sieht bei einer Netz-basierten Lösung anders aus, da eine Skalierung auf Seiten des Providers wesentlich besser vorgenommen werden kann.

Tabelle 10.3: Kunden- und Service-Provider-Vorteile einer Netz-basierten IP-VPN-Lösung

Kundenvorteile	**Serviceprovider-Vorteile**
■ Geringe Gesamtkosten (weniger Personal, weniger Kapital, geringerer Ressourcen-Bedarf für das interne Netzwerk-Management) ■ Schnellere Planung, Konzeption und Implementierung ■ Einfacheres und schnelleres Hinzufügen neuer Sites ■ Kein technologisches und kein Investitionsrisiko bei einem zwingenden Technologie-Wechsel, bedingt durch ein Upgrade in dem Carrier-Netzwerk (anders als bei einer CPE-Lösung) ■ Flexiblere und einfachere Gestaltung von Funktionalitäten und Absicherungen ■ Einfachere Wartung (z.B. keine langen Wartezeiten bei Hard- und Software-Upgrades) ■ Neue Dienstleistungen können ohne eine Equipmentänderung vorgenommen werden	■ Gesamtgewinn größer und schneller als bei einer CPE-Lösung ■ Hohe skalierbare Architektur ■ Umfangreiche Anpassungen an Kundenwünsche sind nun möglich ■ Flexible und einfache Gestaltungen von Funktionalitäten und Absicherungen sind mittels eines zentralisierten Managements möglich ■ Datenabsicherung entspricht der bei Frame Relay und ATM, inkl. der letzten Meile ■ Eine logische Aggregation von tausenden von Kunden ist möglich ■ Kostengünstige, zentralisierte und flexible Einrichtung ■ Eröffnet neue Märkte für Serviceprovider ■ Günstige Markt- und Zeitvorteile ■ Beibehalten des alten Kundenstammes, während neue Dienste angeboten werden können ■ Kein kompletter Austausch von Sites ■ Dienste können schneller eingesetzt werden mit gleichzeitiger Umsatz-Generierung

Allerdings kommt mit einer zunehmenden Vernetzung und gleichzeitiger Verlagerung der kritischen Geschäftsbeziehung über virtuelle Netze der Datensicherheit – insbesondere der Vertraulichkeit und Integrität – eine besondere, vorher nicht da gewesene, Bedeutung zu. Während bei einer CPE-basierten Lösung eine

volle Ende-zu-Ende-Verschlüsselung möglich ist, die häufig mit IPSec realisiert wird, befindet sich die Datenabsicherung bei einer Netz-basierten IP-VPN-Lösung auf dem gleichen Niveau wie bei einer herkömmlichen Frame-Relay- oder auch ATM-Lösung.

Mit den zuletzt genannten Lösungen vertraut der Kunden darauf, dass der Service-Provider die Daten auf der Kommunikationsstrecke mit einem Maximum an Absicherung weiterleitet. Die speziellen Zugangsknoten oder auch *Local Loops* am Rande des Provider-Netzwerkes entsprechen im Grunde den herkömmlichen Frame-Relay-Switches. Falls ein Netz-basiertes IP-VPN über das eigene *(private)* Netz des Providers geführt wird, ist es also ebenso sicher wie die traditionellen Netzwerke.

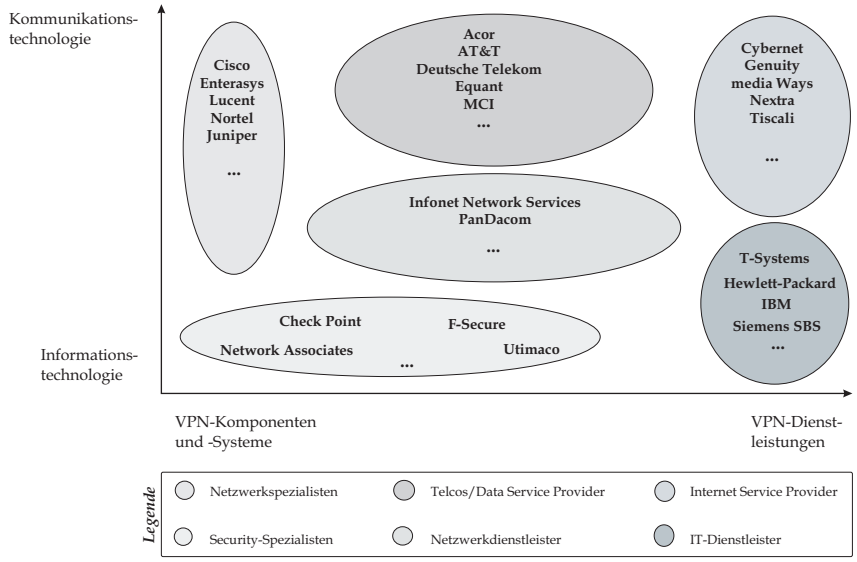


Abb. 10.4: Anbieterlandschaft bezogen auf den deutschen Markt (Quelle META Group, 2001)

In den CPE-basierten IP-VPN wird häufig IPSec zur Datenabsicherung angewendet, MPLS dagegen in den Netz-basierten IP-VPN. Interessant ist vor diesem Hintergrund, die Anbieterlandschaft im VPN-Umfeld näher zu betrachten. Diese stellt sich derzeit noch sehr heterogen dar. Auf der einen Seite gibt es die Technologielieferanten, die in verschiedenen Kerngeschäftsfeldern tätig sind. Die Abb. 10.4 illustriert die Heterogenität der VPN-Anbieter. Zu den Technologieanbietern werden die Netzwerkanbieter und Security-Spezialisten gezählt. Auf der anderen Seite positionieren sich zahlreiche VPN-Dienstleister. Zu diesen werden die Telekommunikationsunternehmen, Data Service Provider, Internet Service Provider, Netzwerkdienstleister und IT-Dienstleister subsumiert.

10.2 VPN der zweiten Generation

Hält man sich die ursprüngliche Definition eines VPN vor Augen, so galt es anfangs, in erster Linie eine logische Verbindung über eine wie auch immer geartete öffentliche Infrastruktur zu ermöglichen. Im Abschn. 1.2 sind hierzu Überlegungen vorgestellt worden. Doch mittlerweile werden zusätzliche Anforderungen gestellt, die durch die VPN der zweiten Generation erfüllt werden.

Tab. 10.4 zeigt die fünf Bedingungen, die von VPN der zweiten Generation erfüllt werden müssen. Anschließend erfolgt ein Vergleich zwischen IPSec und MPLS, um herauszuarbeiten ob dies vergleichbare Lösungen sind. Denn IPSec steht mehr oder weniger für ein CPE-basiertes VPN, MPLS für ein Netz-basiertes VPN. Werden die essentiellen Eigenschaften für VPN der zweiten Generation an den Aktivitäten der *Internet Engineering Task Force* (IETF) gespiegelt, wird deutlich, dass in zwei unterschiedlichen Arbeitsgruppen gerade die für VPN so wichtigen Themen behandelt werden. Dadurch werden Internetsicherheit, Standardisierung des Label-Switching und Quality of Services getrennt behandelt. So hat die

Tabelle 10.4: Essentielle Eigenschaften für VPN der zweiten Generation

Eigenschaften	**Beschreibung**
Skalierbarkeit	Ein VPN muss einfach skalierbar sein, angefangen von einer SOHO-Lösung bis hin zu großen Unternehmenslösungen, und es muss global erreichbar sein. Dabei ist die Möglichkeit, einem VPN kurzfristig Bandbreiten und Zugangspunkte hinzuzufügen, ein wichtiger Punkt. Denn in dem heutigen dynamischen und aggressiven Markt kann schnell ein größeres Projekt gewonnen oder verloren werden. Somit muss eine Adhoc-Reaktion wie Zuwachs oder Reduzierung eines VPN möglich sein.
Sicherheit	Für einen geschäftskritischen Datenverkehr muss gewährleistet sein, dass Sicherheitsmechanismen für die Vertraulichkeit, Paket-Authentifizierung, Nutzerauthentifizierung, Verkehrstrennung, Zugriffskontrolle und Tunnelverfahren, zur Verfügung stehen.
Dienstgüten (QoS)	Es muss eine Priorisierung für geschäftskritischen und übertragungskritischen Datenverkehr vorhanden sein. QoS-Funktionalitäten, wie Queuing, congestion avoidance, traffic shaping und Paket-Klassifizierung, müssen genauso wie ein Routing-Service durch ein optimales Routing-Protokoll gegeben sein.
Management	Es ist essentiell für ein kosteneffektives Netzmanagement, dass QoS-Parameter, Sicherheitsmaßnahmen und Billing-Informationen über ein Monitoring-System ständig erfasst werden, um z.B. neue Dienste zeitnah zu installieren oder SLAs zu kontrollieren.
Zuverlässigkeit	Es muss ein vorhersagbarer, mit extrem hoher Verfügbarkeit ausgestatteter Service vorhanden sein, den Geschäftskunden erwarten und auch einfordern.

IPSec-Arbeitsgruppe in der Fachgruppe Sicherheit (Security Area) einen Schutz für die Layer-3 mittels kryptographischer Verfahren und Sicherungsmechanismen entwickelt, die Eigenschaften wie Authentifizierung, Integrität, Zugriffskontrolle und Vertraulichkeit flexibel abdecken. Abschn. 7.4 hat IPSec bereits ausführlich behandelt.

Dagegen hat die MPLS-Arbeitsgruppe innerhalb der Fachgruppe *Routing* (Routing Area) die *Resource-Reservation* auf höherer Ebene weiterentwickelt. Außerdem werden Quality of Services (QoS) Möglichkeiten sowie eine Definition für das Host-Verhalten entworfen. Ebenso wie IPSec wurde auch MPLS ausgiebig diskutiert (vgl. Abschn. 8.1). Allerdings hat die IETF es versäumt, IPSec und MPLS in irgendeiner Weise zu harmonisieren, was zur Folge hatte, dass heutzutage zwei VPN-Architekturen parallel existieren. Die eine geht auf IPSec zurück, die andere auf die MPLS-Technologie. Service-Provider können nun ihren Kunden eine der beiden oder beide Architekturen anbieten – je nachdem, in welchem Marktsegment sie agieren. Firmen, die ein VPN auf Layer-3 einrichten und von einem Provider unabhängig sein möchten, nutzen IPSec als VPN-Architektur. Für VPN, die auf höheren Schichten angesiedelt sind, muss man ebenfalls – bis auf den regulären Internetanschluss – keine direkte Abhängigkeit zu einem Netzdienstanbieter eingehen.

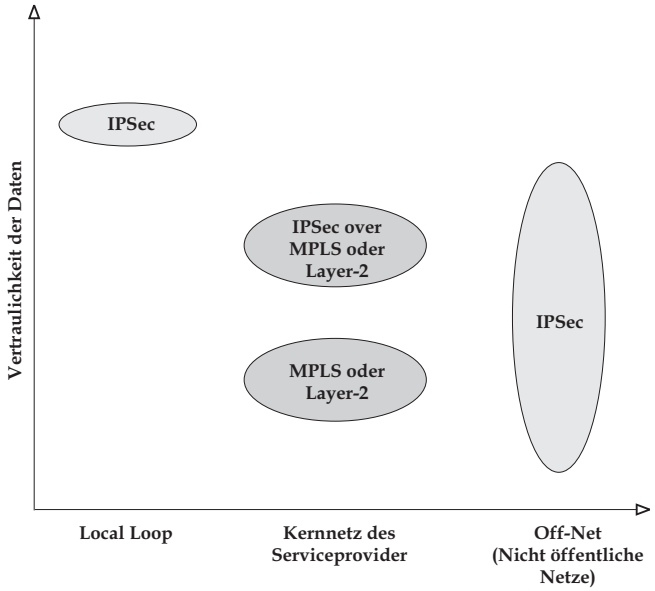


Abb. 10.5: Datenvertraulichkeit als Funktion der Einsatzgebiete von IPSec und MPLS

Zunächst ist es interessant, sich die Einsatzbereiche von IPSec und MPLS vor Augen zu führen. Abb. 10.5 gibt Aufschluss über die mögliche Datenvertraulichkeit bezogen auf typische VPN-Einsatzgebiete. Die Abb. zeigt, dass IPSec im Bereich des Local Loop und im Off-Net, also außerhalb der regulären öffentlichen Netze, genauso eingesetzt werden kann wie in Verbindung mit MPLS und einem Layer-2-Protokoll, wie z.B. L2TP. MPLS dagegen herrscht im Kernnetz des Providers vor und wird künftig die Netz-basierten IP-VPN bestimmen. Es gibt etliche Gemeinsamkeiten und Unterschiede zwischen diesen beiden Technologien. Einem Un-

ternehmen, das zwischen einer Eigenrealisierung und einer Fremdrealisierung zu entscheiden hat, gibt Tab. 10.5 genügend Anhaltspunkte für eine Entscheidung.

Tabelle 10.5: Vergleich von Kerneigenschaften zwischen IPSec und MPLS

Eigenschaften	**IPSec-VPN**	**MPLS-VPN**
Dienste-Modell	Hochgeschwindigkeits-Internetdienste, qualifizierte, geschäftlich bedeutsame IP-VPN-Services, E-Commerce und Applikations-Hosting-Services	Hochgeschwindigkeits-Internetdienste, qualifizierte, geschäftlich bedeutsame IP-VPN-Services, E-Commerce und Application-Hosting-Services
Skalierbarkeit	Umfangreicher und großer Einsatz erfordert Planung und Koordinierung der Schlüsselverteilung, Schlüsselmanagement sowie Koordination der Gegenstellen	Hochskalierbar, keine Site-to-Site-Konfiguration erforderlich; ein typisches MPLS-basiertes VPN-Netzwerk ist in der Lage, tausende von VPN-Gruppen über das gleiche Netz zu bedienen
Servicebereitstellung	Schnelle Marktverfügbarkeit; kann praktisch über jedes IP-Netzwerk installiert werden	Erfordert Netzanpassungen im Kern *(Core)* und am Rande *(Edge)*, um ein vorhandenes Netz MPLS-fähig zu machen; dies kann per Upgrade oder durch Komponentenaustausch erfolgen
Layer-Ebene	Ideal für den Local Loop, den Randbereich sowie für den nicht-öffentlichen Bereich, in denen ein hoher Bedarf des Datenschutzes vorliegt; hier kann IPSec ideal mit Sicherheitsmechanismen, der Tunnelbildung und Verschlüsselung aufwarten	Am besten geeignet für den Kernbereich eines Providernetzes, in dem QoS, Verkehrssteuerung und eine Bandbreitenausnutzung komplett kontrolliert werden können, speziell wenn SLAs als Teile des Services ausgehandelt wurden
Transparenz	Ein reines IPSec-VPN ist auf Layer-3 angesiedelt und ist komplett transparent für Applikationen	MPLS-VPN arbeiten mit IP-over-ATM oder auch reinen IP-Netzen zusammen und sind vollständig transparent für Applikationen

10.2.1 IPSec und Performance-Aspekte

Ein weiterer Entscheidungsparameter zwischen einem MPLS-VPN und einem IPSec-VPN kann aus dem Geschwindigkeitsverhalten von IPSec-AH und IPSec-ESP abgeleitet werden. Inzwischen liegen eine Reihe unterschiedlicher Betrachtungen und Messaufbauten vor. Einer der frühen praktischen Versuche zur Performance-Analyse wurden an der Universität in Helsinki vorgenommen.

1995 wurden Performance-Messungen an der Universität von Helsinki im Labor für Telecommunications Software and Multimedia (TCM) durchgeführt, deren Ergebnisse in eine Studienarbeit einflossen. Im Testaufbau zum Geschwindigkeitsverhalten von IPSec wurde der IPSec-Kontrollmechanismus unterhalb der IP-Schicht implementiert. Damit konnte unabhängig von der Layer-3 gearbeitet werden. Allerdings musste die Fragmentierung und die Checksummenbil-

Tabelle 10.7: Fortsetzung des Vergleichs der Kerneigenschaften zwischen IPSec und MPLS

Eigenschaften	**IPSec-VPN**	**MPLS-VPN**
Änderungsbedarf	Im Prinzip ist keine Veränderung am Netzwerk vorzunehmen	Weil MPLS-VPNs in direkter Verbindung mit einem Provider stehen, müssen einmalig die CPE und die PE angepasst werden, damit der Kunde Mitglied für die für ihn vordefinierte VPN-Gruppe wird
Vertraulichkeit	IPSec-VPNs bieten eine zuverlässige Datenabsicherung durch flexible Verschlüsselungsverfahren und Tunnelmechanismen auf Layer-3	MPLS separiert Verkehrsflüsse unterschiedlicher Kunden und VPN-Gruppen in ähnlicher Weise wie herkömmliche Frame Relay- und ATM-Netze
QoS und SLAs	Im Prinzip unterstützt das IPSec-Protokoll keine QoS-Mechanismen bzw. Verfügbarkeit; jedoch gibt es properitäre Herstellerlösungen, die QoS-Mechanismen bieten, indem eine *(priorisierte)* Klassenzugehörigkeit der IP-Pakete im IPSec-Tunnel erreicht wird	Eine gut konzipierte MPLS-Implementierung bietet hohe Skalierbarkeit sowie profunde QoS-Mechanismen; Verkehrssteuerungsmöglichkeiten dem Provider garantierte IP-Mehrwert-Dienste anzubieten
Session-Authentifizierung	Jede IPSec-Sitzung *(Session)* muss mittels digitaler Zertifikaten oder zuvor ausgetauschter Schlüsseln erfolgen; nicht gültige IP-Pakete im Sinne der Security-Policy werden vernichtet	Eine VPN-Zugehörigkeit wird durch den Provider vergeben und geschieht durch Zuweisung einer logischen Portnummer und Route-Descriptoren; ein nicht autorisierter Zugriff zu einer VPN-Gruppe wird durch die Gerätekonfiguration abgefangen
Client-Unterstützung	Erforderlich für Client-initiierte IPSec-VPNs, etliche Hersteller unterstützen die gängigen Betriebssysteme	Nicht erforderlich, da MPLS-VPNs zu den Netz-basierten Diensten gehört
Nutzer-Interaktion	Für Client-initiierte IPSec-VPNs muss der Nutzer eine spezielle IPSec-Client-Software bedienen	Keine Anforderungen

dung erneuert werden. Das notwendige Schlüsselmanagement erfolgte manuell. Die Messergebnisse wurden zwischen zwei SUN-Sparc-Workstations ermittelt, die eine große Datei über eine 10-MBit/s-Ethernet austauschten. Abb. 10.6 gibt einen Eindruck, wie sich das Performance-Verhalten einer Dateiübertragung ohne IPSec (erste Messung) gegenüber einer Übertragung mit IPSec verändert. Im Extremfall schrumpft die Datenübertragung von 315 KBytes/s ohne IPSec auf 18 KBytes/s zusammen. Obwohl im Testaufbau noch keine Optimierung der Geschwindigkeit getroffen wurde, ist eindrucksvoll nachzuvollziehen, wie sich eine Datenverschlüsselung auswirkt. Auch aus Abb. 10.12 wird deutlich wie unterschiedliche Verschlüsselungsverfahren einen Prozessor belasten. Zur Performance-Steigerung bieten sich Hardware-Beschleuniger an. Es ist auch hilfreich, als Verschlüsselungsverfahren AES einzusetzen, denn AES bietet gegenüber

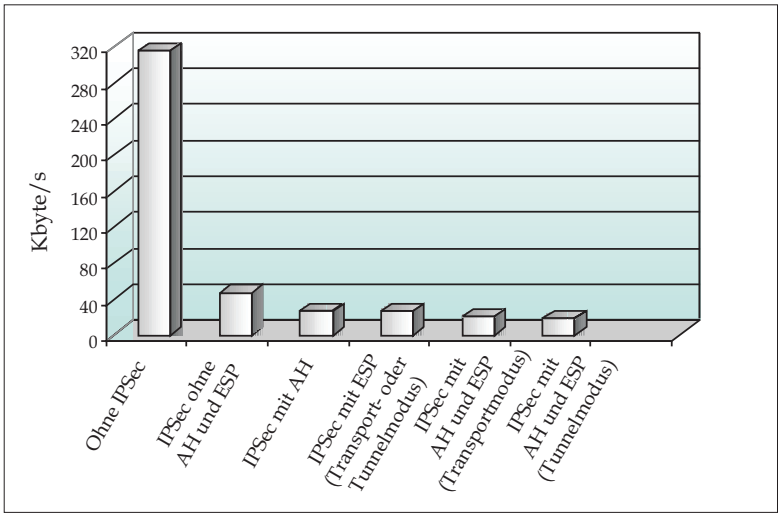


Abb. 10.6: Performance-Messungen ohne IPsec und mit IPsec; durchgeführt von der Universität Helsinki 1995

DES ein erheblich besseres Geschwindigkeitsverhalten. In Abschn. 4.2.5 ist bereits AES (RIJNDAEL) diskutiert worden. Der Algorithmus hat letztendlich durch seine bessere Performance in dem NIST-Auswahlverfahren überzeugt. Außerdem hat AES inzwischen die DES-Nachfolge bei den amerikanischen Behörden im Bereich der klassifizierten Dokumente angetreten.

[Detken und Eren 2001] haben ähnliche Untersuchungen zum Performance-Verhalten durchgeführt. So wurden nicht nur die Cisco Router 2600 und 3600 in die Messungen einbezogen, sondern auch andere Plattformen (NCP, Firewall-1) wurden im Labor der WWL Internet AG getestet. Völlig andere Durchsatzraten ergeben sich, wenn z.B. auf eine moderen Itanium Prozessor-Architektur gewechselt wird. Die Firma HP hat für die HP-UX-Plattform umfangreiche Tests durchgeführt [HP 2004].

Inzwischen haben viele Hersteller das IPSec-Protokoll in ihre Hardware integriert. Angefangen vom kleinen VPN-Concentrator und Firewall-Systemen bis hin zu multifunktionalen *Data Center Appliance*, *Enterprise Routern* und *Next Generation Security Gateways*, die IPv6 und IPSecv6 unterstützen. Durch den mehr und mehr zu verzeichnenden VPN-Trend in Richtung Dial-Up-VPN und Site-to-Site-VPN, steigt ebenso der Bedarf, mehr und mehr Clients gleichzeitig zu unterstützen. Damit fällt der IPSec-Performance eine große Bedeutung zu. Vor diesem Hintergrund ist es sinnvoll, Performance-Tests nicht isoliert zu betrachten, wie noch von der Universität Helsinki 1995 durchgeführt. Dabei spiegelt die Universität Helsinki stellvertretend für viele andere Vertreter die damalige Sicht und Beherrschung der IPSec-Technologie wieder. Szenarien, die dicht an der Realität sind, sind im Markt wesentlich wertvoller.

Ausgehend von dieser Art der Analyse, die die o.g. Trends widerspiegeln, ergeben sich für die Hersteller, Netzwerk-Administratoren und Service-Provider wesentlich bessere Erkenntnisse für den praktischen Einsatz. Nachfolgend sind drei Forderungen für praxisnahe Messungen aufgestellt:

- Performance und Skalierbarkeit können nicht durch eine einfache Herstellerspezifikation charakterisiert werden. Denn jedes Netzwerk, jede Konfiguration und jedes Nutzerprofil ist zu unterschiedlich.
- Es ist nicht mehr länger sinnvoll, IPSec-Analysen isoliert vorzunehmen. Performance, wie auch das Nutzerverhalten, müssen in einer realistischen Umgebung betrachtet werden. Dabei muss der erzeugte Datenfluss für die Messungen aus einem Mix von unterschiedlichen Applikationen und mehreren IPSec-Tunneln existieren.
- Viele Geräte erfordern ein radikales Redesign von Hard- und Software um IPSecv6 und IPv4/v6 koexistieren zu lassen und widerstandsfähig gegen IPv6 DoS-Attacken zu sein.

In Testszenarien kann z.B. untersucht werden, wie sich das Verhalten der Höchstanzahl der aufzubauenden Tunnel auf die Geräte und Verbindungen auswirkt, wie das Zeitverhalten des Aufbaus der Tunnel ist, und schließlich wie sich der Datendurchsatz *(Throughput)* bei zustandsbehafteten Verbindungen verhält.

Exemplarisch wird in Abb. 10.7 ein Messaufbau vorgeschlagen, der den Datendurchsatz bei zustandsbehafteten Verbindungen *(Statefull Traffic Throughput)* misst. Mittig in der Grafik ist das *Device Under Test, (DUT)* schematisch eingezeichnet. Das DUT sollte dabei so konfiguriert sein, dass es auf IPSec-Tunnelaufbau-Anfragen sofort reagiert, die von den Clients (links in der Abb.) kommen. Es kann mit diesem Aufbau der Applikationsdurchsatz gemessen werden. Dabei kann gleichzeitig eine Performance-Veränderung bei zunehmender Tunnelanzahl festgehalten werden. Das Geschwindigkeitsverhalten bei der Ver- und Entschlüsselung wird dann am Interface des Client und Servers ermittelt. Zu beachten ist, dass der IPSec-Tunnel nur vom Clienten bis zur DUT – im Bereich des simulierten *public network* – existiert. Anschließend wird der Klartext im simulierten *private network* zum Interface des Servers übertragen.

Für das Client-Test-Interface sollte eine IPSec-Peer-Konfiguration eingerichtet werden, die die folgenden Parameter für die IKE-Phase I prüft.

- IKE-Mode
- Authentifizierungsmethode
- Hash-Algorithmus
- Verschlüsselungsalgorithmus (Encryption)
- Diffie-Hellman-Gruppe

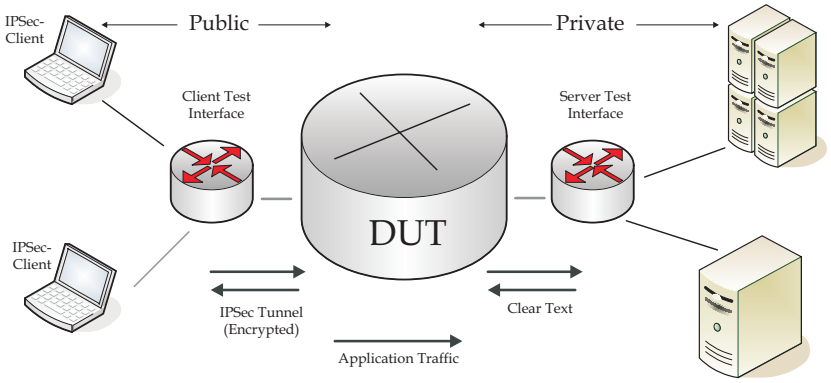


Abb. 10.7: Messaufbau zum IPSec-Durchsatz bei zustandsbehafteten Verbindungen

Für die IKE-Phase II sind die folgenden Parameter sinnvoll zu messen:

- IPSec-Protokoll
- Hash-Algorithmus
- Verschlüsselungsalgorithmus (Encryption)

Weiterhin sollte das Client-Interface so konfiguriert werden, dass es Testdaten eines Anwendungsprogramms erzeugt, die über den aufgebauten IPSec-Tunnel bis hin zum Server-Interface geführt werden. Innerhalb der DUT müssen entsprechende Access-Listen eingerichtet sein. Der IPSec-Tunnel wird in der DUT terminiert und der Klartext zum Server weitergeleitet. Als Variablen könnten die folgenden Größen eingesetzt werden:

- Anzahl der Tunnel
- Type der Anwendungsdaten
- Verschlüsselungsalgorithmus (Encryption)
- Hash-Algorithmus

Im Ergebnis werden Daten erzeugt, wie sie z.B. in der Abb. 10.8 zu entnehmen sind. Es ist deutlich zu sehen, wie der Datendurchsatz ab einer bestimmten Tunnelanzahl einbricht (links in der Abb 10.8). Weiterhin ist schematisch dargestellt, wie sich die Transferzeit zwischen einem HTTP GET und HTTP Response verhält.

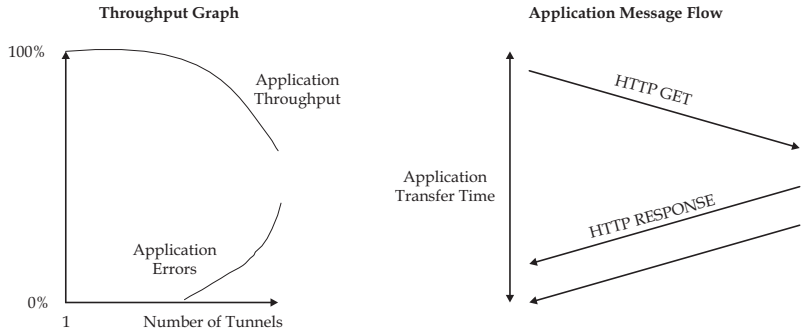


Abb. 10.8: Darstellung des Datendurchsatzes für Anwendungsdaten bezogen auf die Tunnelanzahl, Transferzeit und auftretende Applikationsfehler

10.3 Planungsaspekte

Planung und Design bzw. Konzeption eines VPN sollte mit großer Sorgfalt durchgeführt werden, denn ein VPN verbindet nicht nur zwei voneinander entfernte Unternehmensteile, sondern es kann den Netzwerkverkehr auf jeder Site beeinträchtigen und es könnten Sicherheitslücken entstanden sein. Dabei macht es für die Planung kaum einen Unterschied, ob ein VPN zur Verbindung von 2 - 3 Sites, ein Access-VPN für hunderte von Telearbeitern, ein Extranet oder gar ein Internationales VPN eingerichtet werden soll. Um bei derartig komplexen Vorhaben analytisch vorzugehen, bedarf es sowohl einer strukturierten Vorgehensweise, als auch einer entsprechenden Methodik. Es ist weiterhin vorteilhaft, ein solches komplexes Vorhaben als Projekt durchzuführen.

Dabei orientiert sich eine Planung (Vorgehensweise) an einen Phasenplan (Abschn. 10.4) mit dessen Hilfe die Durchführung eines VPN-Projektes stark erleichtert werden kann. Zusätzlich sollte noch ein Projektstrukturplan *(Methodik)* erstellt werden, der die einzelnen Arbeitsschritte und Verantwortlichkeiten sowie die Ergebnisse *(Deliverables)* der einzelnen Schritte auf einer Zeitachse, z.B. mittels Gant-Diagramm, festlegt.

Auch für den Leser, der vielleicht an einer kleineren VPN-Lösung interessiert ist, kann es hilfreich sein, zunächst umfangreiche VPN-Lösungen zu betrachten. Denn oftmals ergeben sich bei einer umfangreichen Installation enorme Probleme, die bei einer überschaubaren Lösung nicht auftreten. So kann es z.B. für kleinere Installationen eines Access-VPN ausreichen, mit vorab ausgehändigten Schlüsseln zu arbeiten. Bei einer Installation von tausend Clients, stößt dieses Verfahren jedoch an seine Grenzen. Es empfiehlt sich in diesem Fall eher, eine PKI oder Token-Cards einzusetzen.

Planungsziele

Das Ziel einer VPN-Planung und die anschließende Realisierung kann wie folgt auf zwei Punkte subsumiert werden:

Erstens muss ein Nutzen im Sinne von verbesserten Geschäftsprozessen deutlich sichtbar werden. Dies kann z.B. dadurch erreicht werden, dass verstärkt Unternehmensprozesse im Intranet abgebildet und abgewickelt werden.

Zweitens müssen nachweislich Kosteneinsparungen im IT-Budget zu verzeichnen sein. Allerdings wird eine Kosteneinsparung meistens nicht sofort erzielt, da zuerst Investitionen geleistet werden müssen. Jedoch muss der Armortisationspunkt in der Planung, speziell in der Konzeptionsphase, klar herausgearbeitet werden.

10.4 Vier-Phasen-Plan eines VPN-Projekts

Eine durchdachte Planung ist zielführend und gleichzeitig kostenschonend. Denn Fehler, die in frühen Phasen erkannt werden, sind kostenschonend, da der Aufwand zu ihrer Behebung überschaubar ist. Werden Fehler erst in der Pilotierung oder nach der Einführung *(Roll-out)* erkannt, müssen für ihre Beseitigung wesentlich mehr Kosten aufgewendet werden. Obwohl diese Erkenntnisse nicht neu und allgemein anerkannt sind, wird dennoch eher selten danach gehandelt. Dies liegt zum Teil am allgemeinen Kosten- und Zeitdruck, unter dem solche Projekte häufig durchgeführt werden. Ähnliche Verhältnisse sind in der Softwareentwicklung zu beobachten.

Ein erfolgreiches VPN-Projekt wird mittels eines Phasenplanes durchgeführt, der aus vier Einzelphasen besteht. Dabei folgt der Vierphasenplan den allgemein anerkannten Planungsgrundsätzen des *Plan-Build-Run*. In dem Vierphasenplan wird der Planungspunkt *Plan* in die beiden Phasen Analyse und Konzeption unterteilt. Hierfür gibt es gewichtige Gründe. Diese treten bei der Diskussion der Phasen deutlich zu Tage.

Abb. 10.9 zeigt diesen Phasenplan. Er beginnt bei der Analyse, geht dann über in Konzeption und Realisierung und führt schließlich zum Betrieb. Die Phasen gehen nahtlos ineinander über. Jede der vier Phasen ist in verschiedene Arbeitsschritte unterteilt. In ihnen müssen technische, organisatorische und betriebswirtschaftliche Aspekte behandelt werden. Die einzelnen Arbeitsschritte werden zunächst nur kurz vorgestellt und in den folgenden Abschnitten eingehend betrachtet. Dabei beschäftigt sich die Analysephase im Wesentlichen mit den Anforderungen und den Randbedingungen, die zu beachten sind. Denn häufig existieren Verbindungen die entweder weiter genutzt oder komplett abgelöst werden müssen. Der Berechnung des Mengengerüstes kommt eine große Bedeutung zu. Denn diese übt einen weitreichenden Einfluss auf die Performance, auf die zu bestellenden Leitungen, auf die Quality of Service, die QoS-Parameter und auf

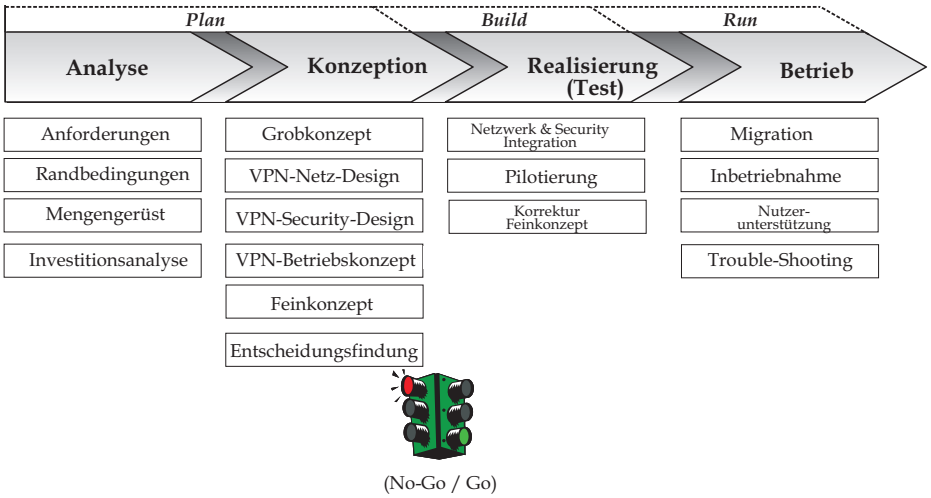


Abb. 10.9: Vier-Phasen-Plan zur Einrichtung eines VPN

die Sicherheitslösung, wie oben mit dem Punkt Pre-shared Keys oder PKI/Smart Card/Token-Card angesprochen, aus.

Weiterhin sollte in der frühen Phase eine Investitionsanalyse durchgeführt werden, damit der Kostenblock überschaubar bleibt. Neben allen diesen Punkten empfiehlt es sich, eine geeignete Dokumentation von dem Projekt anzulegen und jeden Arbeitsschritt – auch für den Fall späterer Änderungen – zu beschreiben. So kann im nachhinein verfolgt werden, weshalb bestimmte Entscheidungen getroffen wurden, oder nicht.

Die Konzeptphase baut auf die Analysephase auf. Sie besteht aus sechs Arbeitsschritten, von denen das Grob- und das Feinkonzept sowie die Entscheidungsfindung die wichtigsten sind. Je nach Arbeitsschritt erfolgen spezielle Arbeitsschritte, wie z.B. VPN-Netz-Design, VPN-Security-Design, sowie Grundzüge des VPN-Betriebskonzeptes. Der Kerngedanke zielt in der Konzeptphase auf die Berücksichtigung aller Anforderungen ab und steht damit der Analysephase gegenüber, in der danach gesucht wird, was alles zu berücksichtigen gilt. Als Ergebnis liegt ein schriftliches Feinkonzept vor, mit dem üblicherweise im letzten Arbeitsschritt, in der Entscheidungsfindung, vor einem Entscheidungsgremium diskutiert wird und die zu investierenden Mittel ausgehandelt werden. Gleichzeitig fällt die Entscheidung für ein CPE-basiertes oder ein Netz-basiertes VPN. Wird grünes Licht gegeben, kann im Phasenplan vorangeschritten werden. Wird dagegen rotes Licht gegeben, sind Nachbesserungen erforderlich, sofern nicht das gesamte Projekt gestoppt wird. In der Argumentation sollten daher die beiden Planungsziele, wie in Abschn. 10.3 formuliert, entsprechend hervorgehoben werden. Allein technische Verbesserungen, werden sie nicht mit wirtschaftlichen Vorteilen verknüpft, sind oftmals schwer durchsetzbar.

Ist die Entscheidungsfindung erfolgreich abgeschlossen *(Go)*, kann mit der vorletzten Phase, der Realisierung, begonnen werden. Entsprechend dem Investitionsplan und der Entscheidung wird ein CPE-basiertes bzw. ein Netz-basiertes VPN in einer Pilotumgebung, also vom herkömmlichen Produktionsnetz getrennt, aufgebaut. Hier werden Sicherheitsmaßnahmen auf ihre Wirksamkeit getestet, die Schlüsselverteilung durchprobiert und der Lasttest vollzogen. Oftmals wird die Pilotierung mit einigen Testpersonen durchgeführt, die dann zeitweilig mit einer Testversion arbeiten. Deren Erkenntnisse bzw. Korrekturen fließen wieder in das Feinkonzept ein.

In der letzten Phase, der Betriebsphase – oftmals auch als Wirkbetrieb bezeichnet – hat die Migration eine herausragende Stellung. Zum einen wird sie nur genau einmal durchgeführt, zum anderen ist die Durchführung mit einem ersten Akzeptanztest der Endnutzer verbunden. Je nach Umfang und Größe des VPN und Anzahl der Endnutzer kann die Migration erheblichen Aufwand verursachen. Anschließend wird gemäß dem Betriebskonzept und Betriebshandbuch der reguläre Betrieb aufgenommen. In der Einführung werden häufig oftmals Fehler gefunden, die sich aus der Anzahl der Nutzer oder durch die Größe des VPN ergeben. Diese sollten jedoch nur geringe Korrekturen erforderlich machen. Gleichzeitig sollte auch die Nutzerunterstützung (User Help Desk, UHD) bereitstehen. Ein UHD kann in der Firma selbst oder in einem Call-Center abgewickelt werden. Denn üblicherweise treten während eines Produktlebenszyklus Störfälle auf. Sie werden mittels eines Fehlerbehebungsprozesses *(Trouble-Shooting)* bereinigt. Im Sinne von ITIL entspricht ein UHD dem Service Desk und Incident Management (vgl. Abb. 9.9).

10.4.1 Analyse

Die Analysephase bildet die Basis des gesamten Projektes. Abhängigkeiten bzw. Verzahnungen, die hier nicht gefunden oder übersehen werden, können weitreichende Folgen haben.

Welcher Typ einer VPN-Variante soll geplant werden?

Wie in Kapitel 6 ausgeführt, gibt es unterschiedliche Varianten von VPN, die drei Grundtypen bilden:

- Intranet-VPN oder auch Site-to-Site,
- Extranet-VPN oder auch End-to-End,
- Remote-Access-VPN oder auch End-to-Site.

Auch Mischformen dieser drei Grundtypen können auftreten. Diese VPN-Formen werden dann häufig als Hybrid-Form bezeichnet. Dabei spielen die unterschiedlichen Hersteller-Lösungen für die Interoperabilität eine bedeutende Rolle. Allerdings sollte in der Analysephase nicht auf bestimmte Hersteller hingearbeitet

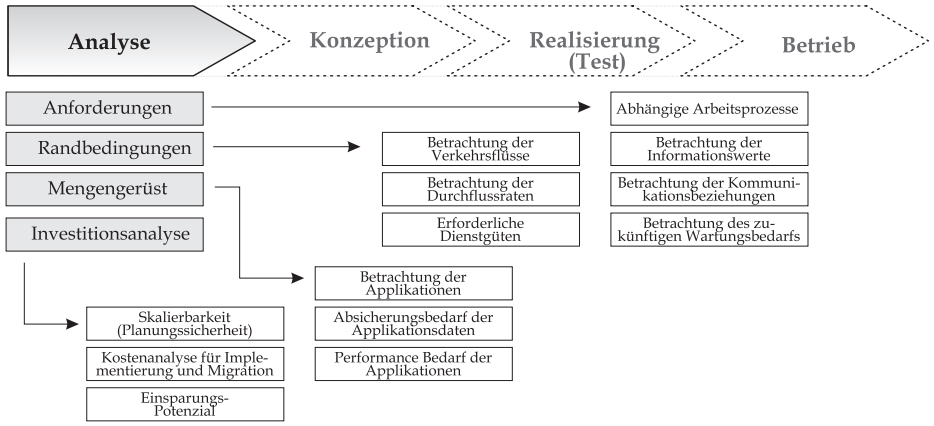


Abb. 10.10: Arbeitsschritte der Anforderungsanalyse mit Verzweigungen

werden, sondern ausschließlich die Analyse der Anforderungen im Mittelpunkt stehen. Hierzu gehören im Wesentlichen die in Abb. 10.10 skizzierten Punkte.

Zunächst geht es darum, die von dem neuen VPN betroffenen Arbeitsabläufe (Arbeitsprozesse) zu kennen. Je mehr über die Verzahnung zwischen dem zukünftigen VPN und den Abläufen in der Firma bekannt ist, um so besser können bestehende Abhängigkeiten erkannt und eingeplant werden. Hilfreich ist es, folgende Fragen zu beantworten:

- Welche Abteilung beauftragt das VPN, oder ist es eine Gesamtlösung für die Firma?
- Wer sind die zuständigen Ansprechpartner für die betroffenen Prozesse?
- Welche Gründe gibt es zur Planung des VPN (Performance, Partneranbindung, Außendienst)?
- Handelt es sich um eine Erweiterung bestehender Kapazitäten (z.B. Bandbreiten, Speicherplatz)?
- Müssen neue Dienste eingeführt werden?
- Sind alle Mitarbeiter oder nur Mitarbeiter bestimmter Abteilungen betroffen?
- Welche Aufgaben und Vorgänge erledigen diese Mitarbeiter?
- Wie soll das zukünftige VPN die Aufgaben und Vorgänge optimieren?

Welche Anwendungen sollen künftig genutzt werden?

In der Regel schreiben die Applikationen die Netzwerkinfrastrukturen vor. Um die Leistungsanforderungen an ein VPN einzugrenzen, ist es sinnvoll, sich mit den Applikationen und ihren Randbedingungen auseinander zu setzen. Ebenso

sollten zukünftige Applikationen, die über das VPN erreichbar sein sollen, mit berücksichtigt werden. Es kann mitunter sein, dass sich bestimmte Arbeitsabläufe für die Mitarbeiter drastisch ändern, so dass hier auch eine *Geschäftsprozessanalyse* (GPOA) angebracht wäre. Dies hängt jedoch stark vom Einzelfall ab und kann kaum pauschal beantwortet werden.

Im Zusammenhang mit den betroffenen Applikationen sollte in der Analyse deutlich herausgearbeitet werden:

- Auf welchem Client-Server-Model (2-Tier oder 3-Tier) die Anwendungen basieren?
- Sollten (alte) Applikationen abgelöst werden?
- Steht die Anwendungen direkt mit dem Intranet/Extranet in Beziehung und wenn ja, worin liegt der Kerngedanke einer VPN-Planung?
- Muss das Netzwerk einen Ende-zu-Ende-Service unterstützen?
- Gibt es zeitkritische bzw. Bandbreiten-intensive Anwendungen, die über das VPN geführt werden sollen (siehe auch den Punkt Mengengerüst)?
- Wie sollen in den Applikation Sicherheitsvorkehrungen, z.B. Authentifizierung und Verschlüsselung eingerichtet wurden?
- Sollen Datenabsicherung vom Netzwerk übernommen werden?

Diese aufgeführten Fragen sollen lediglich eine Anregung geben, um einige Planungspunkte aufzuzeigen. Im konkreten Fall wird schnell klar, dass noch eine Menge Fragen mehr notwendig sind, um eine vollständige Analyse durchzuführen.

Darauf aufbauend gilt es weitere Fragen zu stellen, die sich mit der Datenabsicherung (Vertraulichkeit) beschäftigen. Hilfreich ist es, sich die unterschiedlichen Auswirkungen auf die Prozessorleistung vor Augen zu halten (vgl. Abb. 10.6). Generell lassen sich vier Kategorien bilden, in die die unterschiedlichen Applikationen einzuordnen sind. Es gibt jedoch auch Vorschläge generell zwölf Kategorien zu bilden. Jedoch sollte Aufwand und Nutzen im Verhältnis stehen und die Konsequenzen von zwölf Kategorien bedacht werden. Diese sind vor dem Hintergrund der Sicherheitsrichtlinien und den unterschiedlichen Sicherheitskonzepten zu bewerten, und es hängt vom Planungsstab ab, wie fein eine Unterscheidung sein muss. Im Prinzip reichen jedoch vier Kategorien:

Level-1: Applikationen bzw. Daten dieser Applikationen benötigen keine Datenabsicherung hinsichtlich Verschlüsselung und Authentifizierung. Hierzu gehört z.B. das reguläre Surfen im Internet.

Level-2: Daten dieser Kategorie sollten gegen jegliche Veränderung auf dem Übertragungswege geschützt sein. Hierzu gehören jedoch keine sensiblen Daten. Somit reicht eine Sicherung der Integrität. Eine Verschlüsselung ist nicht nötig; Authentifizierung ist erforderlich.

Level-3: Daten dieser Kriterien sollten einer gesicherten Privatsphäre entsprechen. Eine (einfache) Authentifizierung und ein (schwaches) Verschlüsselungsverfahren reichen aus.

Level-4: Daten von Applikationen dieser Kategorie enthalten vertrauliche Informationen, die nur dem Sender und Empfänger bekannt sein sollten. Diese Daten erfordern eine starke Verschlüsselung, Authentifizierung und ein hohes Maß an Privatsphäre.

Damit sind Sicherheitsklassifikationen gebildet worden, die mit den Sicherheitsrichtlinien des Unternehmens im Einklang stehen müssen (vgl. Kapitel 3.2.6).

Abb. 10.11 zeigt, wie sich eine Datenabsicherung grob auf die anfallenden Daten in einem Unternehmen verteilt. Deutlich ist zu erkennen, dass sich die Prozessorleistung und die Datenabsicherung reziprok verhalten. Jedoch wird auch deutlich, dass die Mehrheit der anfallenden Daten keinen oder nur einen geringen Schutz erfordert. Dies kann sich allerdings je nach Geschäftsmodell eines Unternehmens drastisch ändern.

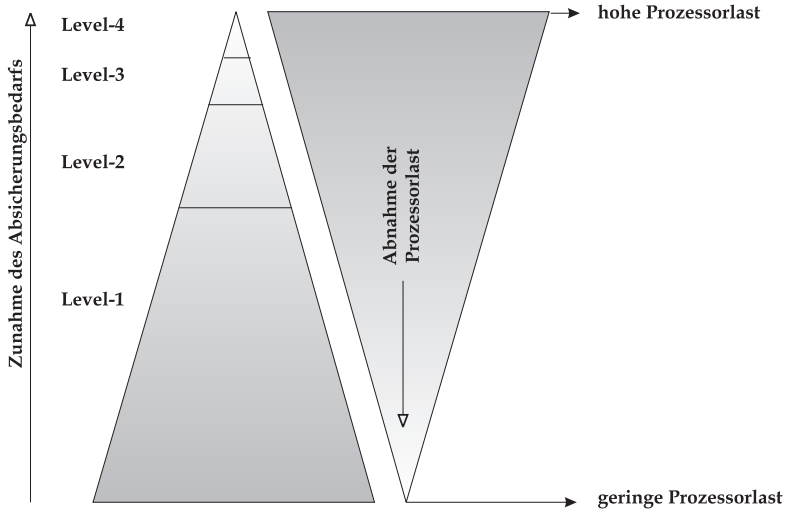


Abb. 10.11: Verteilung der Übertragungsdaten bezogen auf Sicherheits- und Prozessorleistung

Um eine Datenabsicherung genauer zu spezifizieren, ist es hilfreich zu wissen, wie sich ein Performance-Verlust gegenüber einem normalen IP-Routing auswirkt. Beachtenswert ist, dass eine Verschlüsselung einen ungünstigen Einfluss auf die Übertragungsgeschwindigkeit hat (vgl. Abb. 10.12). In dem Vergleich wird deutlich, wie stark der Performance-Einbruch bei DES und Triple DES im Gegensatz zu einem normalen IP-Routing ist. Außerdem produziert das IP-Routing auf Layer-3 einen nicht zu unterschätzenden Performance-Verlust, wie im Zusammenhang mit der Diskussion von MPLS in Abschn. 8.1 herausgearbeitet wurde.

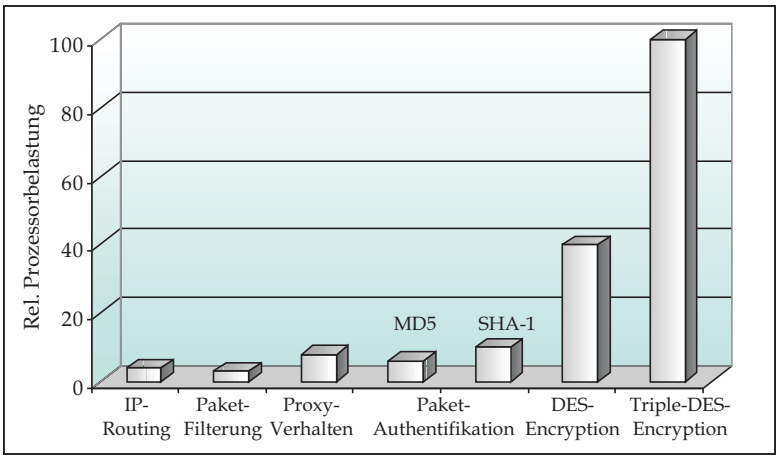


Abb. 10.12: Geschwindigkeitseinbuße durch Verschlüsselung

Insofern ist zu überlegen, ein Software-Verfahren, das mit dem deutlich schnelleren AES ausgestattet ist, einzusetzen oder auf eine Hardware-basierte Lösung zurückgreifen.

Allerdings spielt nicht nur die Verschlüsselung in der Performance eine Rolle bei der zu bestimmenden Bandbreite, sondern auch die Anzahl der Nutzer und die typischen Applikationen. Deren Bandbreitenbedarf ist ebenfalls entscheidend für die Planung. Einen Überblick über den Bandbreitenbedarf und die akzeptable Verzögerung (Latenzzeit) bei der Datenübertragung liefert Abb. 10.13. Sie zeigt die absolute Verzögerung *(latency)* für übertragungskritische Applikationen und deren typische Bandbreiten, aufgetragen auf einer unabhängigen Bandbreitenskala. So ist z.B. für eine Terminal-Session eine Latenzzeit von ca. einer Sekunde akzeptabel, bei einem Bandbreitenbedarf zwischen 1 Kbps bis ungefähr 25 Kbps. Bei einer Videokonferenz dagegen muss die Latenzzeit unterhalb von 0,2 Sekunden liegen, um von den Nutzern als noch akzeptabel empfunden zu werden.

Der Abb. ist weiterhin zu entnehmen, dass, je mehr sich die Applikationen zum Echtzeitbereich hin verschieben, diese gleichzeitig einen zunehmenden Bandbreitenbedarf produzieren. Dabei beschreibt die Latenzzeit die absolute Verzögerung. Nach der Definition wird die Zeit gemessen, die von der Datenanforderung bis zum Eintreffen der Daten verstreicht. Verzögerungen können verschiedene Ursachen haben. Sie sind in der Regel abhängig von der bereitgestellten Bandbreite, der Infrastruktur, der Routing-Technologie und der Übertragungsprotokolle. Die Übertragungsqualitäten oder auch Dienstgüten (QoS) sind bereits in Abschn. 2.3.3 diskutiert worden. Die aufgeführten Überlegungen sollten so oder so ähnlich geführten werden, wenn die Frage nach dem Grad der Datenabsicherung in dem geplanten VPN diskutiert wird. Wichtig ist die Abstimmung der Datenabsicher-

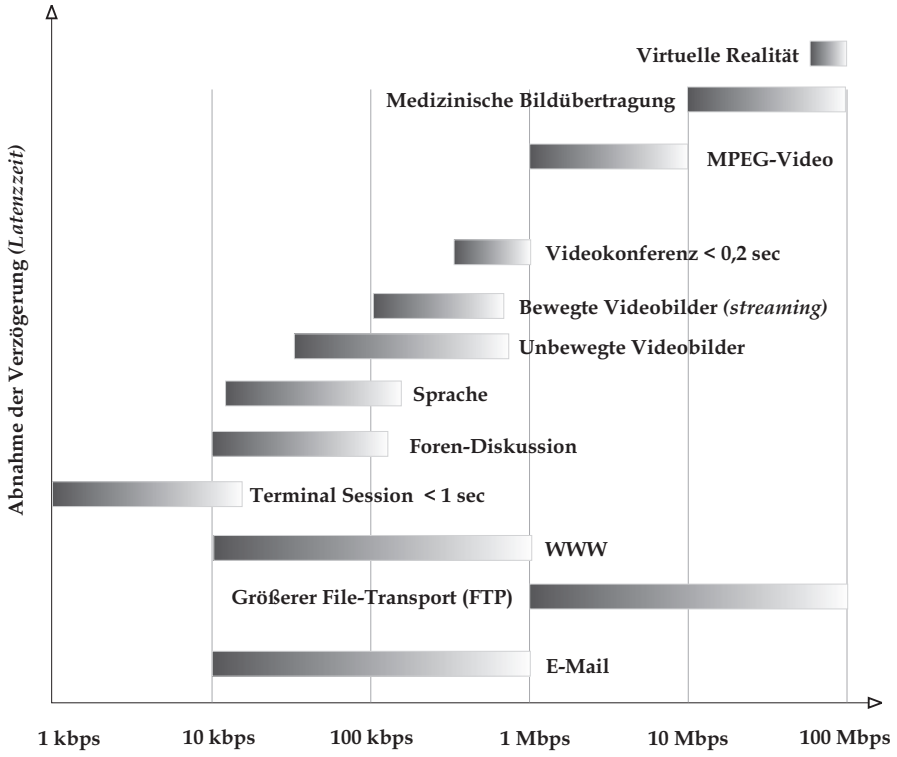


Abb. 10.13: Bandbreitenbedarf einiger Applikationen mit akzeptablen Verzögerungen

rung mit den Sicherheitsrichtlinien.

Welcher Grad von Datenabsicherung ist erforderlich?

Diese Frage führt unmittelbar zur Sicherheitspolitik für ein VPN. In Abschn. 3.2.6 sind die Grundstrukturen und der Aufbau einer Unternehmenssicherheit bereits erläutert worden. Abb. 3.13 gibt die typische hierarchische Sicherheitsregelung eines Unternehmens wieder. Zumindest die folgenden Aspekte sollten behandelt werden:

- Authentifizierung (stark, schwach)
- Schlüsselaustausch und Intervall des Schlüsselwechsels
- Ende-zu-Ende-Sicherheit – wenn ja, wie?
- Performance-Verhalten (Abb. 10.12)
- Integritätsanforderungen
- Protokollierung bei Störfällen

- Reglementierungen

Ebenso sind Erweiterungsbetrachtungen mit in die Planung einzubeziehen. Dies führt zu der Frage des Investitionsschutzes und damit zur Überlegung, wie lange die Lösung eingesetzt werden soll. In der Regel werden umfangreiche Netzplanungen für einen Zeitraum bis zu fünf Jahren ausgelegt. Für etwa diesen Zeitraum sollten in der Konzeptionsphase entsprechende Komponenten ausgesucht werden. Weiterhin sollte abgeschätzt werden, wie sich das künftigen Wachstum verhält.

Welche Ausbaustufen und welches Wachstum ist für die VPN-Topologie vorgesehen?

Die Skalierbarkeit ist ein entscheidendes Kriterium für den Investitionsschutz eines Netzwerkes. Schlüssige Argumente werden gemäß Phasenplan (Abb. 10.9) in der Konzeption und dort unter dem Arbeitsschritt Entscheidungsfindung benötigt, für die in der Analyse der Grundstein gelegt wird. Neben der Ermittlung der zukünftigen Bandbreiten bedeutet dies für ein VPN:

- Dynamisches Schlüsselmanagement (IKE) versus manuell konfigurierte Tunnel.
- Schlüsselaustausch versus Zertifikatsabfragen
- Public-Key-Infrastruktur (PKI) (ja, nein)
- Geographische Ausdehnung (national, transnational)
- Abschätzung der Implementierungs- sowie Migrationskosten
- Klärung der Schnittstellen bei einem CPE-basierten und einem Netz-basierten VPN

Nachdem ein Anforderungsprofil hinsichtlich der zu übertragenden Applikationen und ihrem Bandbreitenbedarf durchgeführt und der Einfluss durch Verschlüsselungsmaßnahmen berücksichtigt wurde, kann in einem zweiten Schritt die detaillierte Analyse der Bereitstellung Verfügbarkeit und Absicherung gemäß der Kategorien (Level-1 bis Level-4, Abb. 10.11) erfolgen. Ziel ist es, die Bedeutung und den Vertraulichkeitsbedarf der zu verarbeiteten Informationen herauszustreichen. Folglich lassen sich Anforderungen finden für:

- die Verfügbarkeit, mit der die Informationen, Dienste und Systeme bereitgestellt werden müssen,
- die Vertraulichkeit, mit der die Informationen verarbeitet und übertragen werden müssen,
- die Integrität der Informationen, mit der die Daten verarbeitet und ausgetauscht werden müssen,
- die Kommunikationsbeziehungen, die aufzubauen sind,

- die Verkehrslast, die von dem VPN zu bewältigen ist, sowie
- die Leistungskenngrößen, wie z.B. Ende-zu-Ende-Verzögerungen oder Verlustwahrscheinlichkeit für die Daten, die in dem VPN kursieren werden.

Oftmals sind den Anwendern diese technischen Hintergründe nicht transparent oder schlecht einzuschätzen. Hier kann mit einer Reihe von einfachen Fragen Klarheit geschaffen werden:

- Wie wirkt sich die Nichtverfügbarkeit von Informationen, Diensten und Systemen auf die Arbeitsprozesse der Nutzer/Mitarbeiter und auf das gesamte Unternehmen aus?
- Welche Ausfallzeiten können hingenommen, welche nicht?
- Welcher materielle oder ideelle Schäden entstünden, wenn vertrauliche Informationen zur Kenntnis unbefugter Dritter gelängen?
- Können Mitarbeiter unbeabsichtigt oder beabsichtigt in den unberechtigten Besitz vertraulicher Informationen gelangen?
- Was bedeutet das unbeabsichtigte oder beabsichtigte Verändern von Informationen innerhalb der Arbeitsabläufe für das Unternehmen? Welcher Schaden könnte entstehen?
- Welche Mitarbeiter kommunizieren mit dem neuen VPN?
- Wie viele Mitarbeiter kommunizieren gleichzeitig auf jeder Site?
- Wie sind die Kommunikationsbeziehungen ausgelegt?
- Für welche Kommunikationsbeziehungen müssen Zweitwege bereitgehalten werden?
- Welche Art von Verbindung zum Internet ist für eine Site erforderlich? Ist eine permanente Verbindung erforderlich oder reicht eine Wählverbindung?
- Falls eine permanente Internetverbindung notwendig ist, wie hoch muss die Verfügbarkeit sein?
- Falls eine Wählverbindung ausreichend ist, wie oft wird diese genutzt und wie häufig kann ein Besetztzeichen hingenommen werden?
- Welche Verkehrslast ergibt sich für die einzelnen Verkehrsbeziehungen?
- Gibt es typische Spitzenlasten zu bestimmten Zeiten (monatliches Berichtswesen)?
- Welche Verzögerungen sind pro Kommunikationsbeziehung zulässig (Abb. 10.13)?
- Können Datenverluste akzeptiert werden? Wenn ja, in welchem Umfang?
- Können Anwendungen und Kommunikationsdienste bezüglich ihrer Wichtigkeit abgestuft werden?

- Muss eine Site auch Fernnutzer unterstützen, und wenn ja, wie viele?

Die aufgelisteten Fragen erheben nicht den Anspruch auf Vollständigkeit, sondern sollen lediglich als Anregung verstanden werden. Ferner hängen die Fragen stark vom VPN-Typ ab.

Es kann mitunter einfacher sein, ein Access-VPN zu planen, als ein umfangreiches Extranet, womöglich mit mehreren Handelspartnern auf einer Plattform. Dennoch sind diese Fragen hilfreich in der Analyse. Hierzu ist die Durchführung eines Workshop vorteilhaft, gerade wenn die Netz- und Planungsabteilung der Firma keinen direkten Bezug zu den Anwendern hat. Dies lässt sich häufig in Banken oder großen Versicherungen beobachten. Auch wenn externe Berater hinzugezogen werden, ist dieser Workshop sinnvoll.

Zu keinem Zeitpunkt der Analysephase darf vergessen werden, dass die einzusetzenden Technologien nur zur Erfüllung der Anforderungen dienen. Bei einer frühzeitigen Technologiefestlegung bzw. -orientierung – wie sie oftmals bei Technikern zu beobachten ist – besteht oftmals die Gefahr, dass wesentliche Punkte nicht beachtet werden. Oder, dass bei einer frühzeitigen Technologiefestlegung auf einen Hersteller im Nachgang erst erkannt wird, welche Funktionalitäten benötigt, jedoch vom Hersteller erst in der übernächsten Produktserie geliefert werden kann. Hier schützt eine sorgfältige Analyse vor späteren unbequemen Fragen bei der Entscheidungsfindung.

Zuletzt ist noch die Frage der „Altlasten“ zu klären. Häufig existieren Kommunikationseinrichtungen, Zugangsserver etc., die noch nicht abgeschrieben sind und weiter verwendet werden müssen. Auch sind betriebliche Anforderungen des VPN in die bereits vorhandenen Betriebsabläufe zu integrieren. Daher sollte der zukünftige Wartungsbedarf ebenfalls ermittelt werden.

Vor der Konzeptionsphase sollten einige theoretische Überlegungen zur Bestimmung der Leistungskenngrößen eines Netzes die Analysephase abschließen. Häufig ist es schwierig, sich ein Bild allein aufgrund der eingesetzten Applikationen über die Verkehrscharakteristiken zu machen. Soll neben einer groben Abschätzung eine formale Beschreibung erfolgen, können nachfolgende Ausführungen hilfreich sein.

Verkehrskenngrößen und deren Bestimmung

Eine der schwierigsten Aufgaben bei der Planung eines VPN ist die Bestimmung des typischen Verhaltens (Charakter) des Nachrichtenverkehrs einer Anwendung. Ein Nachrichtenverkehr wird durch sein zeitliches Verhalten der einzelnen Verkehrsflüsse beschrieben. So ist beispielsweise das allgemeine Telefonverhalten in Deutschland von morgens 6:00 Uhr bis abends 20:00 Uhr durch zwei Wellenberge – ähnlich dem Buchstaben M – gekennzeichnet. Spitzenzeiten treten vormittags gegen 10:00 Uhr bis 11:00 Uhr auf und in den Nachmittagsstunden zwischen 15:00 Uhr und 16:00 Uhr, allerdings schwächer als am Vormittag.

Somit ist ein Nachrichtenverkehr von der Zeitskala abhängig, auf der Verkehrsflüsse betrachtet werden. Außerdem sind die Quellen und die Senken bei einem

VPN zu nennen. Hierzu gehören die Betriebssysteme der Endgeräte, die Anwendungsprogramme sowie die Komponenten einer Anwendung, die mit dem Netzwerk interagieren. Weiterhin sind die Kommunikationsprotokolle, z.B. entsprechend des ISO/OSI-Referenzmodell aufzuführen.

Angesichts der Vielfalt der Anwendungen, Protokolle und Protokollformate stehen in den meisten Fällen oft nur Erfahrungen und Messergebnisse von vorhandenen Netzen und IT-Systemen zur Verfügung. Bezogen auf das OSI-Referenzmodell für die Kommunikation in offenen Systemen heißt das konkret, dass nur Charakteristika der Nachrichtenverkehre auf den Transportschichten eins bis vier vorliegen. Das Verhalten der Anwender/Anwendung ist in fast keinem Falle vorhersagbar – wird einmal abgesehen von der mathematischen Beschreibung des Telefonverkehrs auf Verbindungsebene.

Kommunikationsprotokolle besitzen eine definierte Menge möglicher Zustände. Die Ereignisse, die zu Zustandsänderungen führen, sind ebenfalls festgelegt, ebenso die Aktionen *(Events)*, die innerhalb der Zustände ausgeführt werden. Ähnliche Betrachtungen werden in einer Risikoanalyse angestellt, wenn ein System von einem Wirkzustand in einen Risikozustand überwechselt [Böhmer 1998b]. Zur Systementwicklung und deren Betrachtung mittels endlicher Automaten ist das Buch von [Raasch 1992] lesenswert.

Nur in seltenen Fällen sind Zustandsänderungen zeitlich vorhersagbar. Somit verhalten sich Zustandsänderungen stochastisch. Das bedeutet, dass die Ursachen eines Ereignisses in seinem zeitlichen Auftreten und Zusammenwirken *nicht* deterministisch sind. Ein treffendes Beispiel für stochastische Zustandsänderungen ist der Fenstermechanismus *(Sliding Window)* bei TCP/IP (Abschn. 2.3.2). Das Vorrücken des Fensters (Abb. 2.8) in einem Endgerät wird unter anderem von der Leitungsauslastung des Netzwerkes bestimmt, über das die Protokolldateneinheit *(Protocol Data Unit, PDU)* von Endgerät zu Endgerät bzw. von Hop zu Hop transportiert werden. Das dynamische Verhalten eines Nachrichtenverkehrs kann in [Hasslinger 1999] ausführlicher nachvollzogen werden.

Die Idee, das dynamische Verhalten überhaupt zu modellieren, geht auf die Notwendigkeit einer Überprüfung der Leistungskenngrößen zurück. Bei einer Modellierung können Teile oder das vollständige Netz durch Simulation nachgebildet werden. Diese Art stochastische Prozesse zu beschreiben, ist gekennzeichnet durch eine zeitdiskrete, ereignisorientierte Simulation. Für Vertiefungen sei z.B. auf [Fishman 1978] verwiesen.

Zunächst sind jedoch statische Parameter für die Planung von Bedeutung, mit denen Nachrichtenverkehre bzw. Protokolle beschrieben werden können. Dabei sind neben den Maßeinheiten für die zu übermittelnden Informationen oder Daten auch die Protokolldateneinheiten zu nennen (Abschn. 2.2.1). Die typischen Maßeinheiten sind selbst erklärend: *Bit*, *Byte*, *Oktett*, *Nachricht*, *Block* und *File*. Sie werden je nach Übertragungsart in *Pakete*, *Rahmen*, *Zellen* oder *Übertragungsrahmen* verpackt. Dabei stellen die genannten Formate gleichzeitig die wichtigsten Formate der Protokolldateneinheiten dar. Die Begriffe sind für die einzelnen Schichten des zugrunde liegenden Protokoll-Referenzmodells eindeutig festgelegt.

Die Protokolldateneinheiten (PDU) der Netzwerkschicht (Layer-3) werden üblicherweise als Pakete bezeichnet. Im Falle des Internet Protokolls wird allerdings der Begriff des IP-Datagramms verwendet. Die Protokolldateneinheiten der Sicherungsschicht (Layer-2) heißen Rahmen. Im Gegensatz dazu werden die Protokolldateneinheiten des Asynchronen Transfer Modus (ATM) als Zellen bezeichnet (Abschn. 8.4). Bei der logischen Strukturierung des Bitstromes der Physikalischen Schicht (Layer-1) werden die Protokolldateneinheiten Übertragungsrahmen genannt.

Ein Informationsfluss wird üblicherweise in Anzahl der pro Zeiteinheit übertragenen Informationseinheiten bzw. Protokolldateneinheiten (PDU) angegeben. Für die genannten PDU heißt dies z.B. Pakete pro Sekunde, Rahmen pro Sekunde, Zellen pro Sekunde, Bytes pro Sekunde, Nachrichten pro Stunden etc.

Neben diesen rein übertragungsorientierten Kenngrößen lässt sich die Wechselwirkung zwischen Anwender und Netzwerk durch Ereignisse wie Anzahl des Verbindungsaufbaus oder Anzahl der Verbindungen beschreiben. Verkehrstheoretisch bedeutet dies, dass das Verkehrsverhalten auf einer anderen Zeitskala (z.B. pro Tag) betrachtet wird. Die Einflussfaktoren, die für die zeitliche Varianz von Ereignissen bzw. Kenngrößen verantwortlich sind, liegen nicht nur im deterministischen, sondern größtenteils im *nicht*-deterministischen, also im zufallsbedingten Bereich. Etliche Modellbetrachtungen haben versucht, dieses Verhalten nachzuvollziehen und daraus zu lernen. Teilweise wiederkehrende Muster können mit speziellen Mustererkennungsverfahren behandelt werden. Für eine pragmatische Planung spielen sie allerdings keine Rolle.

Das dynamische Verkehrsverhalten des neuen VPN kann bei der Planung durch den Erwartungswert, den so genannten Mittelwert berücksichtigt werden, indem in einem recht verkehrsintensiven Zeitfenster (Hauptverkehrsstunde) gemessen wird. Die Hauptverkehrsstunde spielt beispielsweise in der Sprachnetzplanung eine herausragende Rolle. Ähnliche Ansätze werden bei der Planung von Datennetzen verfolgt, indem neben dem Mittelwert des Datenvolumens der Spitzenwert und die Burstiness als Merkmale des Nachrichtenverkehrs berücksichtigt werden. Mittelwert und Spitzenwert des Datenvolumens werden in den oben genannten Maßeinheiten angegeben. Die Burstiness – das Verhältnis aus Spitzenwert und Mittelwert – kann als Maß für die Kontinuität des Informationsflusses innerhalb des betrachteten Zeitintervalls definiert werden. Bei der Frame-Relay-Behandlung in Abschn. 8.3 ist bereits auf diesen Aspekt hingewiesen worden. Abb. 8.10 zeigt das Verhalten zwischen Burst und normaler Last, und Gleichung 8.3 liefert eine Größenordnungsbetrachtung.

Leistungskenngrößen

Leistungskenngrößen setzen die Parameter eines VPN in Bezug zu den geforderten und benötigten Eigenschaften fest. Vom Endnutzer wird oftmals das Netz oder VPN als solches nicht wahrgenommen; normalerweise bemerkt er Antwortzeiten, Einwahlverfahren und die Reaktion der benutzten Applikation. Oftmals werden ungünstige Antwortzeiten dem Netz zugeschrieben, rühren je-

doch von einer langsamen Datenbankabfrage oder vom langsamen Endgerät her. Deshalb sind neben quantifizierbaren Größen auch qualifizierbare Messgrößen wünschenswert, die eine objektive Bewertung und Fehlerverfolgung ermöglichen.

Messbar heißt zunächst allgemein, dass das Verhalten für die Dauer eines bestimmten Zeitintervalls $(t_1 - t_2)$ mit geeigneten physikalischen Messverfahren beobachtet und mit einer Metrik quantifiziert werden kann. Messbar ist der Bitstrom an verschiedenen Punkten, z.B. auf den Leitungen, an den Schnittstellen zu Netzelementen oder an den IT-Systemen selbst. Als Leistungskenngrößen zur Beurteilung des Bitstromes sind Bitfehlerrate, Übertragungsrate und -verzögerungen definiert.

Die Bitfehlerrate ist definiert als Quotient der Anzahl fehlerhaft empfangener Bits zur Gesamtzahl empfangener Bits. Die Bitfehlerrate von Glasfasern liegt z.B. in der Größenordnung von 10^{-9} bis 10^{-12}. Die Übertragungsrate ist definiert als die Anzahl der Bits, die pro Zeiteinheit übertragen werden, z.B. kbit/s oder Mbit/s. Die Übertragungsverzögerung[1] gibt die zwischen dem Aussenden und dem Empfangen einer Nachricht verstrichene Zeit an. Sie setzt sich je nach verwendetem Übertragungsverfahren aus verschiedenen Anteilen zusammen. Als Übertragungsverzögerungen lassen sich die drei Größen *Transmission Delay*, *Switching Delay* und *Packetization Delay* definieren:

Transmission Delay ist unabhängig von dem gewählten Übermittlungsverfahren. Die Verzögerung ist abhängig von der Entfernung zwischen Sender und Empfänger. Die Transmission Delay bezeichnet die gesamte Übertragungsdauer einer Informationseinheit über alle Zwischenleitungen.

Switching Delay setzt sich in paketvermittelnden Netzen aus einer konstanten und einer variablen Komponente additiv zusammen. Der konstante Anteil *Fixed Switching Delay* ist implementierungsabhängig und umfasst die gesamte Verarbeitungsdauer in allen an der Nachrichtenübertragung beteiligten Systemen und kann gegenüber dem variablen Anteil *Queuing Delay* vernachlässigt werden. Der variable Anteil wird durch die Zwischenspeicherung der Informationseinheiten (Warteschlangenverhalten) in den Kommunikationssystemen hervorgerufen (Abb. 2.14). Queuing Delay ist somit eine Folge der Verkehrslast.

Packetization Delay tritt beim Erzeugen der Protokolldateneinheiten (PDU) auf (Abschn. 2.2.3 oder auch Abb. 2.3). Generell sollte eine Verzögerung deutlich unter 30 ms liegen. Die Packetization Delay steht im direkten Zusammenhang

[1] In paketorientierten Netzen kommt es generell zu umsetzungs- und netzspezifischen Verzögerungen. Im Audio-Codec und der Paketierung im Sender kann die Verzögerung zwischen 20 ms und 25 ms betragen. Für die Zwischenspeicherung im Netzbereich können weiterhin Verzögerungen bis zu 700 ms auftreten und bei der Synchronisierung, Depaketierung und Decodierung nochmals bis zu 150 ms. Bei der Übertragung von graphischen Informationen in Echtzeit liegt der akzeptable Wert bei 30 ms. Im Weitverkehrsbereich sollte die Verzögerungszeit 100 ms nicht überschreiten, im LAN sollte sie unter 30 ms liegen.

mit der Leistungsfähigkeit der CPU. Je geringer ein Delay ist, um so höher muss die Frame-Rate sein und damit die CPU-Leistung.

Neben den oben genannten Kenngrößen können nach Auswertung der logischen Struktur eines Bitstromes weitere Leistungskennzeichen, wie die Verlustwahrscheinlichkeit von Zellen, Rahmen oder Paketen aus deren Verzögerungen abgeleitet werden. Mit diesen Information kann die Leistungsfähigkeit eines VPN abgerundet werden. Wichtig für eine Abschätzung ist der Zusammenhang zwischen den direkten physikalischen Kenngrößen und den protokollspezifischen Leistungskenngrößen.

Eine weitere Kenngröße, der Durchsatz, sagt aus, wie viele Informationseinheiten in der betrachteten Zeiteinheit von einem Netz verarbeitet werden können. Der Durchsatz wird üblicherweise in Bit/s angegeben, und zwar nach eingesetzter Technologie in Zellen/Zeiteinheit, Rahmen/Zeiteinheit oder Paketen/Zeiteinheit. Eines der Ziele, die in der Konzeption verfolgt werden müssen, ist es, den Durchsatz eines VPN zu maximieren.

Außerdem ist die Auslastung eines VPN interessant, da diese oftmals einen direkten Bezug zu den Kosten hat. Die Auslastung gibt an, zu welchem Prozentsatz – bezogen auf ein festgelegtes Beobachtungszeitintervall – das VPN beschäftigt ist, also aktiv im Beobachtungsintervall Daten überträgt oder verarbeitet. Beim Netzentwurf wird versucht, eine Auslastung von 75 - 80 % zu erreichen; dieser Richtwert gilt natürlich auch für ein VPN. Wird er später im operationellen Betrieb eingehalten, wird dieses Netz in einem optimalen wirtschaftlichen Verhältnis genutzt.

Eine kennzeichnende Eigenschaft für VPN der ersten Generation ist, die auf paketorientierte Übermittlungsverfahren (z.B. Frame Relay, oder ATM) basieren (Abschn. 8.3 bzw. 8.4), dass mit zunehmender Auslastung die zeitliche Verzögerung der Datenübertragung und -verarbeitung ansteigt. Denn die vorhandenen Ressourcen werden den Anwendern im Multiplex zur Verfügung gestellt. Damit nimmt die Wahrscheinlichkeit, dass eine zur Übertragung oder Verarbeitung anstehende Nachricht ein nicht beschäftigtes Netz vorfindet und sofort bedient werden kann, mit steigender Auslastung ab. Folglich steigt die Wartezeit bei der Übertragung oder Verarbeitung mit zunehmender Auslastung an.

Ein weiterer wichtiger Leistungsparameter eines VPN ist die Zuverlässigkeit, häufig auch als Verfügbarkeit bezeichnet. Im Wesentlichen wird die Robustheit des Systems gegenüber Ausfällen beschrieben. Für geschäftskritische Anwendungen, die eine hohe Verfügbarkeit erfordern, kann diese durch Redundanz erhöht werden. Die Verfügbarkeit gibt jene Wahrscheinlichkeit an, die ein System, z.B. ein VPN, als Ganzes oder in Teilen, in einem Beobachtungszeitraum im Zustand der Funktionstüchtigkeit vorfindet. Häufig wird ein Beobachtungszeitraum von 365 Tagen zugrunde gelegt. Die Verfügbarkeit ist nach [Michler 1984] eine relativ komplexe Zuverlässigkeitskenngröße. Sie lässt sich sowohl aus der Ausfallfreiheit eines Systems als auch aus dem Reparatur- sowie dem Wartungsverhalten ableiten. Die Ausfalldauer, d.h. die Dauer vom Zeitpunkt des Ausfalls des Systems bis zu seiner erfolgreichen Wiederinbetriebnahme, beinhaltet drei Einflussgrößen:

- Zeitdauer bis zur Fehlerlokalisierung
- Zeitdauer der Reparatur
- Antrittszeit des Servicetechnikers

Im Gegensatz zu den ersten beiden Einflussgrößen ist die zuletzt genannte über entsprechende Service Level Agreements (SLA) steuerbar. Vereinbart werden diese mit Herstellern, Lieferanten oder Providern (Abschn. 9.2.3).

Die Verfügbarkeit eines Systems oder eines seiner Teilkomponenten kann aus der mittleren vom Hersteller angegebenen, Ausfallzeit *Mean Time Between Failure* (MTBF) und der mittleren erforderlichen Reparaturzeit *Mean Time To Repair* (MTTR), z.B. für einen Router, errechnet werden.

Hersteller geben die mittlere Ausfallzeit MTBF für Systeme und Komponenten oftmals an. Sie ist im Dauerbetrieb unter realistischen Randbedingungen ermittelt worden. Eine andere Möglichkeit besteht darin, die Verfügbarkeit aus mathematischen Modellen abzuleiten.

Die Verfügbarkeit (V) lässt sich dann durch

$$V = \frac{MTBF}{MTBF + MTTR} \tag{10.1}$$

bestimmen. Ebenso kann aus der Verfügbarkeit (V) eines Systems der Umkehrschluss gezogen werden und die Nichtverfügbarkeit ($U = 1 - V$) mit

$$U = 1 - V = \frac{MTTR}{MTBF + MTTR} \tag{10.2}$$

berechnet werden. Die Verfügbarkeit ($V = 1 - U$) eines Systems, z.B. eines VPN oder auch eines Notebooks, hängt von mehreren Komponenten ($i = 1...n$) ab.

Somit lässt sich mit den Einzelverfügbarkeiten der abhängigen Komponenten ($V_i = 1 - U_i$) und mit einer Serienschaltung, (Abb. 10.14)

$$V_{Serie} = V_i \cdot V_{i+1} \cdots V_n, \tag{10.3}$$

sowie durch Einsetzen der mittleren Ausfallzeiten und der mittleren Reparaturzeiten

$$V_{Serie} = \frac{MTBF_i}{MTBF_i + MTTR_i} \cdot \frac{MTBF_{i+1}}{MTBF_{i+1} + MTTR_{i+1}} \cdots \frac{MTBF_n}{MTBF_n + MTTR_n} \tag{10.4}$$

die Gesamtverfügbarkeit des Systems bestimmen. Abb. 10.14 zeigt eine Serienschaltung mit den Verfügbarkeiten (V_1, V_2) zweier Teilkomponenten im oberen Abschnitt der Grafik.

Wird die Verfügbarkeit durch eine redundante Auslegung von Teilkomponenten erhöht, wie im unteren Abschnitt der Grafik dargestellt, entsteht ein Parallel-

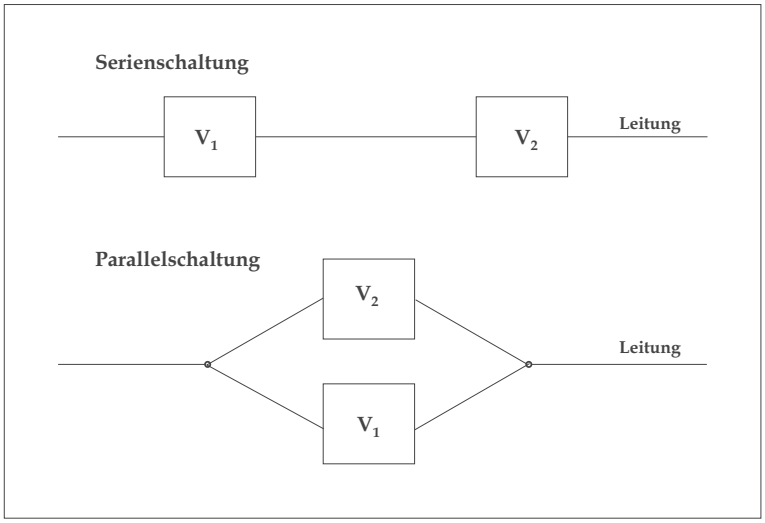


Abb. 10.14: Betrachtung der Verfügbarkeit bei Serien- und Parallelschaltung [Spohn 1993]

system, das gut durch eine Parallelschaltung hinsichtlich seiner Verfügbarkeit beschrieben werden kann.

Die Verfügbarkeit des Parallelsystems (Abb. 10.14) kann einfach über die Nichtverfügbarkeit U

$$U_{parallel} = U_1 \cdot U_2 = (1 - V_1) \cdot (1 - V_2) = 1 - V_1 - V_2 + V_1 \cdot V_2, \tag{10.5}$$

bestimmt werden. Die Verfügbarkeit ergibt sich dann mittels der parallelen Teilkomponenten zu

$$V_{parallel} = (1 - U_{parallel}) = V_1 + V_2 - V_1 \cdot V_2. \tag{10.6}$$

Wird die Gleichung (10.3) mit der Gleichung (10.6) verglichen, wird schnell deutlich, dass in einer Serienschaltung beim Ausfall einer Komponente die gesamte Schaltung funktionsuntüchtig wird, da alle Komponenten multiplikativ miteinander verknüpft sind.

Anders verhält es sich bei einer Parallelschaltung, bei der eine additive Verknüpfung der Komponenten vorliegt. Hier liegt die Gesamtverfügbarkeit deutlich über der einer Serienschaltung. Nachteilig ist, dass ein Parallelsystem wesentlich kostenintensiver ist, so dass es sich nur an bestimmten neuralgischen Punkten wirtschaftlich rechnet. Hier wäre eine gezielte Risikoanalyse (Abbschn. 3.2.1) angebracht. Durch sukzessive Anwendung von Serien- und Parallelschaltung lässt sich die Verfügbarkeit von komplexen Systemen formal berechnen.

Soll neben der Verfügbarkeit auch die Zuverlässigkeit R eines Systems berechnet werden, muss die Wahrscheinlichkeit, dass das System nicht vor Ablauf von t

Stunden ausfällt, bestimmt werden. Eine einfache Näherungsformel, die für Systeme mit Markow'schem Ausfallverhalten gilt, lautet:

$$R = e^{-\frac{t}{MTBF}}. \tag{10.7}$$

Aus dieser Gleichung kann die Zuverlässigkeit (R) eines Systems einfach abgeleitet werden. Gilt beispielsweise eine MTBF von 10 000 Stunden, betrachtet über ein Jahr – t entspricht 8760 Stunden –, ergibt sich eine Zuverlässigkeit von R = 41,64%.

Auch wenn die theoretischen Ausführungen über Markow-Ketten bzw. Ausfallzeiten und Zuverlässigkeitsbetrachtungen in der Praxis kaum verwendet werden, sollte doch eine grobe Abschätzung bei einer VPN-Planung vorgenommen werden. Je zeit- und geschäftskritischer die Applikationen sind, die über ein VPN geführt werden sollen, um so genauer sollten die obigen Berechnungen angestellt werden.

In einem pragmatischen Ansatz sollten die in Abb. 10.10 skizzierten Punkte behandelt werden. Zur Minimalbetrachtung sollten zumindest die in Tab. 10.4 aufgeführten Punkte analysiert werden.

Nach Abschluss der Analyse sollten alle Daten als Grundlage für eine darauf aufbauende Konzeption vorliegen. Alles, was in der Analyse nicht behandelt wurde, kann auch nicht in der Konzeption berücksichtigt werden.

10.4.2 Konzeption

Die Konzeptionsphase baut auf die Analysephase auf und setzt die gesammelten Informationen in unterschiedliche Konzepte um. Es werden unter anderem das Mengengerüst, die Randbedingungen und die Eckwerte für den Investitionsschutz berücksichtigt, die als Ergebnis aus der Analyse hervorgegangen sind. Die Konzeption gliedert sich in mehrere Arbeitsschritte auf, die in der Abb. 10.15 beschrieben sind. Die Arbeitsschritte in der Konzeptionsphase legen zwar eine zeitliche Abfolge nahe, die jedoch nicht als verbindlich anzusehen ist. Im Grobkonzept könnte jeweils eine Alternative – einmal CPE-basierend und einmal Netzbasierend – erarbeitet werden. Dies gilt jedoch nur für ein Intranet-VPN (Site-to-Site) und ein Extranet-VPN (End-to-End).

Für ein Access-VPN ist es fast zwingend, ein ISP zu berücksichtigen, falls Kosten eingespart werden sollen. Die VPN-Sicherheitspolicy wiederum ist der allgemeinen Sicherheitspolicy unterzuordnen. Diese kann in Anlehnung an Abschn. 3.2.6 erfolgen. Zeitgleich sollte das Netz-Design und die Sicherheitsarchitektur unter Berücksichtigung des Mengengerüstes durchgeführt werden. Damit liegen – bis auf das VPN-Betriebskonzept – im Wesentlichen alle Elemente in zweifacher Ausführung vor. Bei der Planung müssen eine CPE-basierte und eine Netz-basierte Lösung entwickelt werden, wenn zur Entscheidungsfindung beide Lösungen diskutiert werden sollen. Sprechen triftige Gründe für eine der beiden

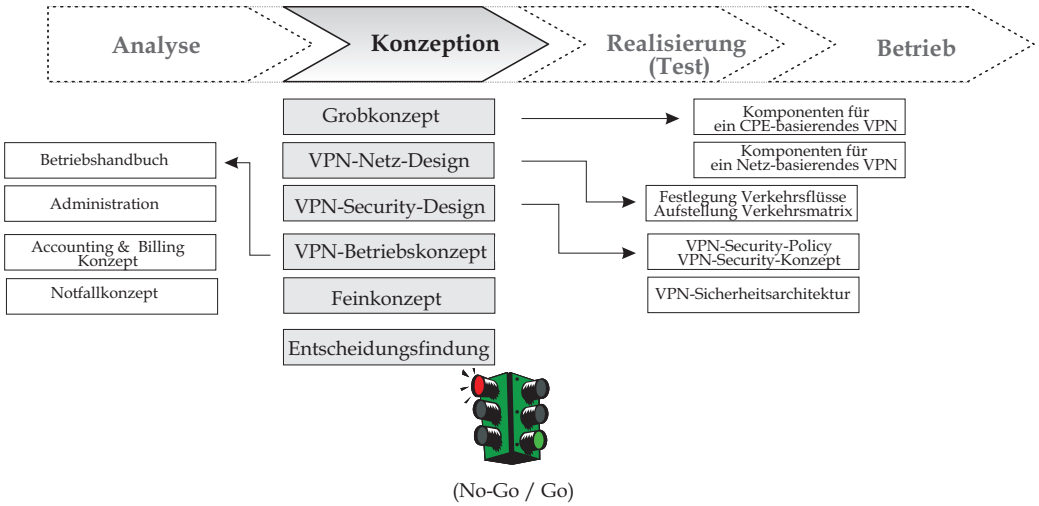


Abb. 10.15: Arbeitsschritte der Konzeption mit (No-Go/Go) Meilenstein

Lösungen, kann eine Entscheidung bereits im Vorfeld gefallen sein. Um eine fundierte und kostengünstige Entscheidung zu treffen, sollten beide Lösungen betrachtet werden.

Das Betriebshandbuch (Abb. 10.15) und die dazu gehörigen Arbeitsschritte gelten in erster Linie für eine CPE-basierte VPN-Lösung. Für ein Unternehmen, das ein Netz-basiertes VPN plant, sind dagegen nur einige Elemente relevant. Im Schritt Administration wird festgehalten, wie das VPN und wie die Benutzer verwaltet werden (Berechtigungskonzept). Weiterhin wird in einer Systemkonfiguration der Anfangszustand des VPN, der sich im Lauf der Zeit ändern kann, festgeschrieben. Ebenso ist der Arbeitsschritt Accounting und Billing von Bedeutung. Hier wird festgehalten, was wann welcher Abteilung bzw. dem Endnutzer verursachergerecht an Datenaufkommen erfasst und in Rechnung gestellt werden soll.

Im anschließenden Feinkonzept werden alle logischen Netzkomponenten und Netzkonfigurationen des zukünftigen VPN vorbereitet. Weiterhin sollte eine Einordnung gemäß Abb. 9.3 erfolgen, welche die Konsequenzen zwischen Eigen- und Fremdrealisierung aufzeigt. In diesem Arbeitsschritt wird auch der Unterschied zwischen den beiden im Grobkonzept vorgeschlagenen Lösungsvarianten deutlich. Ist das Feinkonzept bis zu einer bestimmten Fertigungstiefe herangereift, liegen alle zu einer Entscheidungsfindung notwendigen Komponenten vor. Je nach Grad der Eigenrealisierung fallen Liefer- und Leistungsbedingungen (SLA) an. Die in Abschn. 9.2.3 angestellten Überlegungen sind hierbei hilfreich.

Nachdem sich die Kosten neuer Netze, Teilnetze oder Architekturen sowie einer komplexen Netzerweiterung oder -umbaus in der Planungsphase nicht immer

genau beziffern lassen, wird häufig zunächst für die Analyse- und Planungsphase ein Budget bereitgestellt, das oftmals auch Beraterhonorare einschließt. Liegt dann dem Entscheidungsgremium ein ausgearbeitetes Feinkonzept vor, kann ein Investitionsantrag für die zu beschaffenden Komponenten gestellt werden.

10.4.3 Realisierung

Die Realisierungsphase, die auch als *Build* bezeichnet wird, unterscheidet sich deutlich von der Analyse und Konzeption. Waren die ersten beiden Phasen vor allem durch theoretische Ausarbeitungen geprägt, sind die Phasen Realisierung und anschließender Betrieb vornehmlich durch praktische Aktivitäten gekennzeichnet. Die Realisierung besteht im Wesentlichen aus drei Hauptarbeitsschritten, die sich in weitere Schritte verzweigen (Abb. 10.16). Nach dem Aufbau der VPN-Komponenten und Einrichtung der VPN-Absicherungen wird in einem Testnetz an Hand von typischen Szenarien geprüft, in wie weit die die gesetzten Anforderungen erfüllt werden (*Proof of Concept*). Hauptanliegen der Realisierung ist jedoch die Pilotierung, aus der wertvolle Erkenntnisse für den späteren Betrieb gezogen werden. Die Pilotierung bietet die letztmalige Chance, Erkentnisse

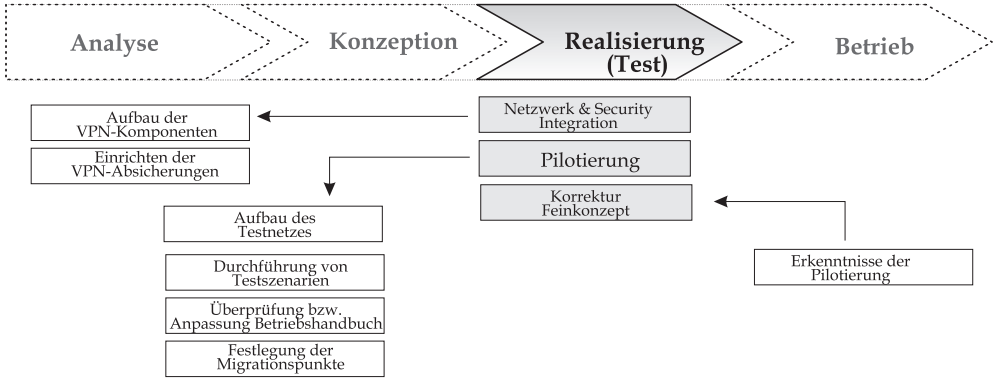


Abb. 10.16: Haupt- und Nebenarbeitsschritte der Realisierung

die in den Testszenarien gewonnen wurden, in das Feinkonzept korrigierend einzupflegen. Diese Korrektur ist immer noch kostengünstiger, als im Betrieb Korrekturen vornehmen zu müssen. Als Szeanrio kann der Rückruf aller Laptops mit fehlerhaften IPSec-Clients bei einem Remote-Access-VPN betrachtet werden. Sind schon etliche tausend Laptops mit fehlerhaften Clients ausgeliefert, erfordert dies einen erheblichen Aufwand und Mehrkosten.

10.4.4 Betrieb

Die Betriebsphase oder auch als *Run* bezeichnet, ist bei der Planung und Umsetzung eines VPN-Projektes die entscheidende Phase. Denn nun wird aufbauend auf der Konzeption und Realisierung der operative Betrieb (Wirkbetrieb) aufgenommen und die neuen Dienste werden bereitgestellt. Die Ausfallzeiten beschränken sich auf die Wartungsfenster. Abb. 10.17 zeigt die Betriebsphase und die einzelnen Arbeitsschritte bis zur Inbetriebnahme. Vorgelagert ist die Migration, und zwar mit zwei Arbeitsschritten. Zum einen muss aufbauend auf den Erkenntnissen der Pilotierung, die für die Migration relevant sind zum anderen muss ein Migrationsfahrplan erstellt werden. Dieser enthält Angaben darüber, wann wo welche Komponenten ausgetauscht werden, sowie über Rückfallszenarien für technische Probleme, die größer als erwartet sind.

Der betriebliche Aufwand für den Unterhalt eines CPE-basierten IP-VPN unterscheidet sich vom Unterhalt eines Netz-basierten IP-VPN erheblich. Bei einem Netz-basierten VPN werden Kundenschnittstellen eingerichtet, so dass vom Kunden Informationen zur Überprüfung der Liefer- und Leistungsbegingungen (SLA)gesammelt werden können.

Für Netz-basierte IP-VPN existieren mittlerweile komplette Management-Center, die eine Verwaltung umfangreicher VPN erheblich erleichtern. Bietet ein Service-Provider zusätzlich zum IP-VPN eine solche Überwachungs- und Steuerungsmöglichkeit an, genießt der Kunde einige nicht zu unterschätzende Vorteile.

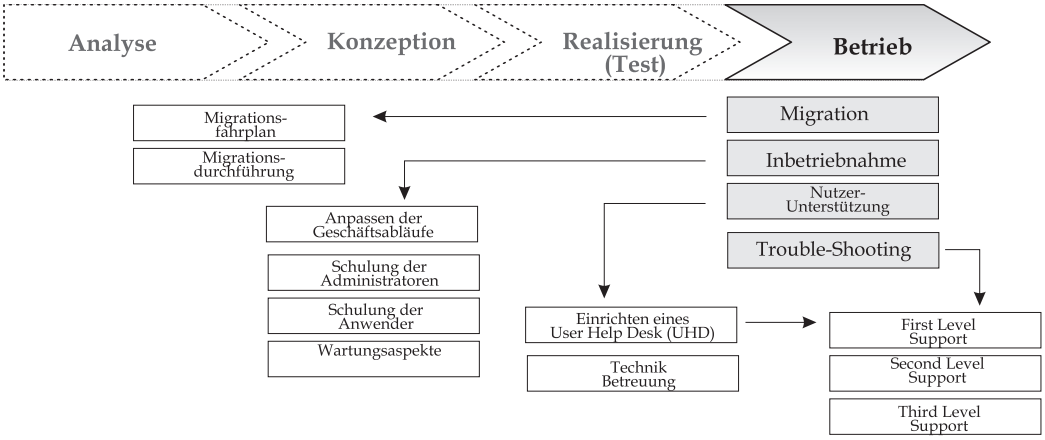


Abb. 10.17: Arbeitsschritte des VPN-Betriebs mit Migration

10.5 Schlussbemerkung

Derzeit befindet sich der VPN-Markt (Abb. 10.1) nicht mehr im Stadium der frühen Mehrheit (Early Majority), wie die Marktanalysen deutlich machen. Alle bedeutenden Wirtschaftsanalysten sind sich über die weitere Entwicklung der VPN einig. Die VPN-Technologie ist im *Mainstream* angekommen und bietet großen wie auch kleinen Unternehmen eine kostengünstige Möglichkeit, den Zugriff auf die Unternehmensressourcen flexibel zu gestalten. Weiterhin wird sich die Flexibilität, d.h. einen ortsunabhängigen Zugang zu haben, weiter durchsetzen.

Bei den Netz-basierten VPN-Lösungen zeichnet sich deutlich ab, dass MPLS mehr und mehr auf der Layer-2 die VPN-Technologie beherrschen wird. Allerdings werden künftig die optischen Netze eine größere Rolle spielen. Trotz etlicher ungelöster Probleme wird demnächst mit dem *Wavelength Division Multiplexing* (WDM) ein Übertragungsverfahren zur Verfügung stehen, das für eine hohe Transportkapazität in Glasfasernetzen sorgt.

Für die CPE-basierten VPN, die sich nach Aussagen der Analysten in den nächsten Jahren reduzieren werden, wird eine Vereinfachung in Planung und Implementierung allein schon durch die Migration zu IPv6 erreicht werden. IP wird das Protokoll sein, das die Kommunikationsverbindungen beherrschen wird. Dies gilt für den LAN- wie für den WAN-Bereich.

Veränderungen wird es weiterhin in den mobilen Verbindungen (Mobil-IP) geben, die ebenfalls mit einer VPN-Technologie ausgestattet werden, falls Dienstgüten und Absicherungsmechanismen sowie Skalierbarkeit und Managementaspekte eine Rolle spielen sollen. Dies gilt auch für die aufkommende Wireless-LAN- und die Bluetooth-Technologie. Die „Luftschnittstelle“bzw. die kabelfreie Informationsübertragung, sofern diese sicher sein soll, ist hinsichtlich der Datenabsicherung, Vertraulichkeit und Integrität mittels VPN-Technologie zu begegnen. Ferner müssen geeignete Roaming-Verfahren wie z.B. DIAMETER etabliert sein. Aber auch der Schlüsselaustausch und die eingesetzten Verfahren müssen in der Handhabung für den Endnutzer einfacher gestaltet werden, um für einen Massenmarkt geeignet zu sein. Der begonnene Wandel der Netzwerk- und Telekommunikationsstruktur ist bedeutender denn je. Die Beherrschung der „Luftschnittstelle“ wird dabei eine entscheidende Rolle für die IuK spielen. Viele Unternehmen müssen die Architektur ihrer Netzwerke umgestalten. Gerade die neuen Entwicklungen im Bereich Sprach-Datenintegration (Voice-over-IP, VoIP) werden neben den Anforderungen zur Mobilität zum Wandel noch verstärken.

Die Entwicklungen im Bereich DIAMETER, Mobil IP und UMTS – auch wenn diese sich nur zögerlich durchsetzen – geben die Richtung mit ihren technischen Möglichkeiten vor. Unterbrechungsfreie, providerübergreifende gesicherte Verbindungen (VPN), erhöhen die Mobilität. Das noch theoretische Szenario, das ein Nutzer beim Weg vom Büro nach Hause einen ständigen VPN-Tunnel und damit eine unterbrechungsfreie Session (Seamless Session) unterhält; dabei jedoch verschiedene Provider und unterschiedliche Netze (UMTS, WLAN) kreuzt, wird in

naher Zukunft zum Alltagsbild gehören.

10.6 Übungen

1. Was ist unter einem genesteten VPN-Tunnel zu verstehen?
2. Skizzieren Sie die Kernaufgaben des Vier-Phasen-Modells.
3. Worin liegen die Unterschiede zwischen dem *Plan-Build-Run*-Modell und dem Vier-Phasen-Modell?
4. Entwerfen Sie unter Anwendung des Vier-Phasen-Modells ein IPSec-VPN, das die Möglichkeit zulässt, sich von einem beliebigen Standort in die Firmenzentrale einzuwählen. Es soll für 500 Mitarbeiter ausgelegt sein. Davon sollen ca. 300 Sessions parallel und ohne Performance-Verluste betrieben werden können.
5. Welches sind die IT-Sicherheitsmerkmale von VPN der zweiten Generation?
6. Was wird unter einem Produktlebenszyklus in Bezug auf die VPN-Technologie verstanden?
7. Was ist eine DUT?
8. Entwickeln Sie einen Messaufbau in Anlehnung zur Abb. 10.7, um die Tunnelaufbauphase *(Setup Rate and Time)* zeitlich messen zu können.
9. Entwickeln Sie einen Prozessansatz nach ITIL für die Betriebsphase eines VPN.
10. Errechnen Sie nach dem Markow'schen Ausfallverhalten die prozentuale Zuverlässigkeit (R) eines IPSec-Gateways, wenn dies einer MTBF von 35 000 Stunden unterliegt.
11. An welchen Punkten im Netz ist es sinnvoll hinsichtlich der Verfügbarkeit ein Parallelsystem einzusetzen?

Literaturverzeichnis

[Aurand 2001] Aurand, A.: Sicherheit in Cisco- und Windows-2000-Netzwerken, Installation und Troubleshooting von IPSec in der Praxis. Addison-Wesley, München, 2001, ISBN 3-8273-1930-7.

[AF56-96] The ATM-Forum Technical Committee: Private Network-Network Interface Specification Version 1.0 (PNNI 1.0), [af.pnni.55], March 1996.

[Becker 1998] Becker, J.: Marketing-Konzeption, Grundlagen des strategischen und operativen Marketing-Managements, 6. vollständig bearbeitete und erweiterte Auflage, Verlag Franz Vahlen, München, 1998, ISBN 3-8006-2116-9.

[Beckett 1988] Beckett, B.: Introduction to Cryptology, Blackwell Scientific Publication, Oxford, 1988, pp. 73-76.

[Bellovin 1989] Bellovin, S.: Security Problems in the TCP/IP Protocol Suite, Computer Communications Review 2:19, April 1989, pp. 32-48.

[BSI 2004a] BSI: IT-Grundschutzhandbuch 2004, Bundesamt für Sicherheit in der Informationstechnik, Schriftenreihe zur IT-Sicherheit, Band 3, Bundesanzeiger, Bonn, 2004, ISBN-3-88784-915-9.

[BSI 2004b] BSI: Risikoanalyse auf der Basis von IT-Grundschutz, Version 1.0, interne Veröffentlichung, BSI Newsletter, Ausgabe 01/2004, 15. März 2004.

[Biaz und Vaidya 1999] Biaz, S.; Vaidya, N. H.: Is the round-trip time correlated with the number of packets in flight? Technical Report 99-006, Department of Computer Science, Texas A&M University, March 1999.

[Biham und Shamir 1993] Biham, E.; Shamir, A.: Differential Cryptanalysis of the Data Encryption Standard, Springer Verlag, New York, 1993.

[Buchmann 2001] Buchmann, J.: Einführung in die Kryptographie, 2., erweiterte Auflage, Springer Verlag Berlin, Heidelberg, 2001, ISBN 3-540-41283-2.

[Bon 2002] Bon, J.v. et al.: IT Service Management, eine Einführung [Version 1.0], Van Haren Publishing, Niederlande, 2002, ISBN 90-806713-5-5.

[Böhmer 1998b] Böhmer, W.: Sicherheitsanalyse in der Unternehmenskommunikation, Handbuch der Telekommunikation, Fachverlag Deutscher Wirtschaftsdienst GmbH, Köln, 1998, ISBN 3-87156-096-0.

[Böhmer 2000] Böhmer, W.: Enterprise Security Management (ESM), Danet Nachrichten, Danet Group, Ausgabe Nr. 1, 2000.

[Böhmer und Knöpfle 2001] Böhmer, W.; Knöpfle, K.: AES und die Zukunft der Privatsphäre im Internet. Tagungsband 7. Deutscher IT-Sicherheitskongress des BSI, SecuMedia Verlag, Ingelheim, 2001, ISBN 3-922746-36-5.

[Böhmer 2001-b] Böhmer, W.: Die IT-Security-ScoreCard als Überprüfungsinstrument zur unternehmensweiten IT-Sicherheit, unveröffentlichtes Manuskript, Darmstadt, November 2001.

[Böhmer 2004-a] Böhmer, W.: Die „erwachsene“ IT-Sicherheitsorganisation, submitted paper, 9. Deutscher IT-Sicherheitskongress „IT-Sicherheit geht alle an! “, Bad Godesberg, 10.-12. Mai 2005

[Böhmer 2004-b] Böhmer, W.: Einstufung der IT-Unternehmensicherheit mittels quasi-objektiver Methode, submitted paper, 2. Jahrestagung des Fachbereichs „Sicherheit - Schutz und Zuverlässigkeit “der Gesellschaft für Informatik e.V. (GI), Universität Regensburg, 5.-8. April 2005

[Cahners In-Stat Group 2001] Cahners In-Stat Group: IP-VPN Market Opportunities: An End-User Survey, Study: TX0103EU, pub. date: May 2001.

[Campo und Pohlman 2001] Campus M.; Pohlman, N.: Virtual Private Networks, mitp-Verlag, Bonn, 2001, ISBN 3-8266-4060-8.

[Chadwick 1999] Chadwick, D.: Understanding X.500 - The Directory (online-version), International Thomson Computer Press, 1996, ISBN 1-85032-281-3.

[Comer 1995] Comer, D.: Internetworking with TCP/IP Vol I: Principles, Protocols and Architecture. 3rd. ed., Prentice-Hall International, 1995, ISBN 0-13-216987-8.

[Crypto-Gram 03-2000] Schneier, B.: Crypto-Gram Newsletter March 15, 2000, http://www.counterpane.com

[Crypto-Gram 04-2000] Schneier, B.: Crypto-Gram Newsletter April 15, 2000, http://www.counterpane.com

[Crypto-Gram 05-2000] Schneier, B.: Crypto-Gram Newsletter June 15, 2000, http://www.counterpane.com

[Crypto-Gram 06-2000] Schneier, B.: Crypto-Gram Newsletter July 15, 2000, http://www.counterpane.com

[Daemen und Rijmen, 1999] Daemen, J.; Rijmen, V.: AES Proposal: Rijndael, Vers. 2.0, 1999, http://csrc.nist.gov/encryption/aes/round2/AESAlgs/-Rijndael.pdf

[Deming 1998] Deming, W. Edwards: Out of the Crisis, MIT, 1989.

[Denning 1983] Denning, D., E.: Cryptography and Data Security, reprinted with corrections, Addison-Wesley, 1983, ISBN 0-201-10150-5.

[Detken und Eren 2001] Detken, K.-O.; Eren, E.: Extranet. VPN-Technik zum Aufbau sicherer Unternehmensnetze, Addison-Wesley, München, 2001, ISBN 3-8273-1674-X.

[Diffie und Hellman 1976] Diffie, W.; Hellman, M. E.: New Direction in Cryptography. IEEE Transactions on Information Theory, 6, November 1976, pp. 644-654.

[Dierstein 2002] Dierstein, R.: IT-Sicherheit und ihre Besonderheiten - Duale Sicherheit, Vorlesungsmanuskript, Technische Universität München, 2002 ff., 22 S.

[DIN IEC 1998] DIN IEC 56/581/CD, Leifaden zur Gefährdungs- und Betreibbarkeitsuntersuchung (HAZOP), Janur 1998 (Entwurf).

[DIN IEC 2001] DIN IEC 60812, Analysetechniken für die Funktionsfähigkeit von Systemen – Verfahren für die Fehlzustandsart- und -auswirkungsanalyse (FMEA), Oktober 2001.

[DIN VDE 3100-2 1987] DIN VDE 3100, Allgemeine Leitsätze für das sicherheitsgerechte Gestalten technischer Erzeugnisse, Teil 2, Begriffe der Sicherheitstechnik, Dezember 1987.

[Eckert 2004] Eckert, C.: IT-Sicherheit, Konzepte – Verfahren – Protokolle, 3., überarbeitete und erweiterte Auflage, Oldenburg Verlag, München, 2004, ISBN 3-486-20000-3.

[ELGamal 1985] ELGamal, T.: A Public Key Cryptosystem and a Signature Scheme based on Diskrete Logarithms. IEEE Transaction on Information Theory, Vol. IT-31, 1985, pp. 469-472.

[Ellison und Schneier, 2000] Ellision, E.; Schneier, B.: Ten Risks of PKI: What You‘re not being told about Public Key Infrastructure, Computer Security Journal, Volume XVI, Number 1, 2000.

[Federal Information Processing 1977] Data Encryption Standard (DES): Standards Publication Nr. 46, National Technical Information Service, Springfield, VA April 1977. Federal Register, March 17, 1975 und August 1, 1975.

[Feistel 1973] Feistel, H.: Cryptography and Computer Privacy, Scientific American, May 1973.

[Ferguson und Schneier 1999] Ferguson, N.; Schneier, B.: A Cryptographic Evaluation of IPsec, Counterpane Internet Security, Inc. 3031 Tisch Way, Suite 100PE, San Jose, CA 95128, http://www.counterpane.com/ipsec.html

[Fishman 1978] Fishman, G.: Principles of Discrete Event Simulation, John Wiley & Sons, New York, Brisbane, Chichster, Toronto, 1978, ISBN 0-471-04395-8.

[Fluhrer et al. 2001] Fluhrer, S.; Mantin, I.; Shamir, A.: Weaknesses in the Keyscheduling Algorithm of RC4, SAC 2001.

[Frank 1999] Frank, M.; Martini, P.: Eine Erweiterung der Transportebene zur Bandbreitenregelung auf Ende-zu-Ende Basis, PIK 22, Saur Verlag (1/1999), S. 11-21.

[Frost & Sullivan 2003] Frost & Sullivan: Debate of where the true value lies in Europe's IP VPN Service Market; Report B190, Rubrik: Markt/Studien, Froet & Sullivan, Clemenststr. 9, 60487 Frankfurt am Main, 2003.

[Füser 1997] Füser, K.: Modernes Management, Beck-Wirtschaftsberater im dtv, ISBN 3432508094.

[Gilbert 2000] Gilbert, H., Minier, M.: A Collision Attack on 7 Rounds of Rijndael, Proceedings of the 3rd AES Candidate Conference, S. 230, NY, USA, April 2000, http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

[Goldberg 2001] Goldberg, I. et al.: Interception Mobile Commuications: The Insecurity of 802.11, accepted paper, on the 4th ACM International Workshop on Modeling, Analysis and Simulation of Wireless and Mobile Systems, July 21, 2001 Rome Italy, a satellite workshop of the 7th Annual Internatiuonal Conference on Mobile Computing an Networking.

[Halpern et al. 2004] Halpern, J.; Covery, S.; Saville, R.: SAFE, VPN IPSec Virtual Private Networks in Depth, within CCSP Self-Study: Cisco Secure Virtual Private Networks (CSVPN), 2nd Edition, Cisco Press, ISBN: 1587051451; published: May 19, 2004.

[Hasslinger 1999] Hasslinger, G.; Klein, T.: Breitband-ISDN und ATM, Multimediale (Tele-)Kommunikation mit garantierter

Übertragungsqualität, Teubner-Verlag, Stuttgart 1999, ISBN 3-519-06251-8.

[HP 2004] HP Admin Guide: HP-UX IPSec Performance and Sizing, HP-UX IPsec version A.02.00 Administrator's Guide, HP, 2004, J4256-90014,12/2004.

[Huitema 1998] Huitema, Ch.: IPv6: The New Internet Protocol, 2nd. Ed., Prentice Hall, 1998, ISBN 0138505055.

[IEEE] IEEE 802.3 Working Group Standards, siehe www.ieee.org.

[IEEE 802.2] IEEE 802.2 Logical Link Control.

[IEEE 802.3] IEEE 802.3 Carrier Sense Multiple Access / Collision Detection.

[IEEE 802.11] IEEE 802.11 Carrier Sense Multiple Access / Collision Avoidance.

[ISO 7498-2:1989] Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture, International Standard, Genf, 1989.

[ISO 8326:1987] ISO 8326: Information Processing Systems - Open Systems Interconnection - Basic Connection Oriented Session Service Definition, Technical Report 8326, ISO, 1987.

[ISO 8327:1987] ISO 8327: Information Processing Systems - Open Systems Interconnection - Basic Connection Oriented Session Protocol Specification, Technical Report 8327, ISO, 1987.

[ISO 9594:1994] CCITT X.500 Series (1994); ISO/IEC 9594,1-9:1994, Information Technology - Open Systems Interconnection - The Directory, 1994.

[ISO 9594-1:1994] CCITT Rec. X.500 (1994); ISO/IEC 9594-1:1994, Information Technology - Open Systems Interconnection - The Directory: Overview of Concepts, Models and Services.

[ISO 9594-8:1994] CCITT Rec. X.509 (1994); ISO/IEC 9594-8: Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, 1994.

[ISO 15408:1999] CC 2.0; ISO/IEC 15408: Common Criteria (CC), Allgemeines Modell.

[I.362] ITU-T Recommendation I.362: B-ISDN ATM Adaptation Layer (AAL) Functional Description, Helsinki, März 1993.

[Kauffels 1994] Kauffels, F.-J.: Moderne Datenkommunikation, DATACOM-Verlag, 1994, ISBN 3-89238-096-1.

[Kosiur 1998] Kosiur, D.: Building and Managing Virtual Private Networks, Wiley Computer Publishing, John Wiley & Sons, Inc., New-York, Chichester, Weinheim, Brisbane, Singapore, Toronto, 1998, ISBN 0-471-29526-4.

[Koblas 1992] Koblas, D.; Koblas, M.: SOCKS, Proceedings, UNIX Security Symposium III, September 1992.

[Kurtz et al. 2001] Kurtz, G.; McClure, S.; Scambry, J.: Das Anti-Hacker-Buch, zweite aktualisierte und erweiterte Auflage, mitp-Verlag, Bonn, 2001, ISBN 3-8266-0670-1.

[Kreiszig 1982] Kreiszig, E.: Statistische Methoden und ihre Anwendungen; Nachdr. der 7 Auflage; Vandenhoeck & Ruprecht, Göttingen, 1982, ISBN 3-525-40717-3.

[Lakshman 1998] Lakshman, T. V.; Kumar, V. P. (Hrsg.): Gigabit Networking: Issues and Trends in Router Design; Beyond Best Effort: Router Architectures for the Differentiated Services of Tomorrow's Internet; Evolution of MPLS, IEEE Communications Magazine (5/1998), S.144-173.

[Landau 2000] Landau, S.: Standing the Test of Time: The Data Encryption Standard; Journal of Mathematics Society, Notice of AMS, Volume 47, No.3, 2000.

[Lampe 1993] Lampe, U.: Erfahrungen mit dem IT-Sicherheitshandbuch in Behörden, Tagungsband 3. Deutscher IT-Sicherheitskongreß des BSI 1993, SecuMedia Verlags-GmbH, Ingelheim, 1994, S.491-498, ISBN 3-922746-23-3.

[Lamport 1981] Lamport, L.: Password Authentication with Insecure Communication; Communications of the ACM 24.11, November 1981, pp. 770-772.

[Lipmaa 2000] Lipmaa, H.: AES Candidates: A Survey of Implementations, http:// www.tml.hut.fi/ helger/aes/

[Lucks 2000] Lucks, S.: Attacking Seven Rounds of Rijndael under 192- and 256-bit Keys, Proceedings of the 3rd AES Candidate Conference, S. 215, NY, USA, April 2000.

[Mankin 1998] Mankin, A.: The IETF Christmas Campaign on Quality of Service, IEEE Network (1/1998), pp. 6-13.

[Meta Group 2001] Meta Group: VPN and VPN Services in Germany; Market Research Report, 1 Nov. 2001, META Group AG, Oskar-Messterstr. 24, 85737 Ismaning, 2001.

[Meyer 1982] Meyer, C. H.; Matyas, S. M.: Cryptography: A New Dimension in Computer Data Security, A Guide for the Design and

Implementation of Secure Systems, Cryptography Competency Center, IBM Corporation, Kingston, New York, John Wiley & Sons, Inc., 1982, ISBN 0-471-04892-5.

[Michler 1984] Michler, E.: Grundlagen der Theorie der Zuverlässigkeit, Lehrbriefe für das Hochschulstudium, Technische Universität Dresden, 1984.

[Mock 2003] Mock, R.: Risiko, Sicherheit und Zuverlässigkeit, Analysemethoden in der „Information and Communication Technology“?, Informatik Spektrum, Hauptbeitrag im Band 26, Heft 3, Juni 2003.

[NBS 77] National Bureau of Standards: Data Encryption Standard, PUB Nr. 46.

[Nett 2001] Nett E. et. al.: Das drahtlose Ethernet. Der IEE 802.11 Standard: Grundlagen und Anwendung. Addison Wesley, ein Imprint der Pearson Education Deutschland GmbH, München, 2001, ISBN 3-8272-1741-X.

[Newton 1998] Newton, David, E.: Encyclopedia of Cryptology, ABC-CLIO Ltd., OXFORD OX2 6AT, England, 1998, ISBN 1-851093230.

[Pfitzmann 1998] Pfitzmann, A.: Datensicherheit und Kryptographie, Vorlesungsskript Wintersemester 98/99, Technische Universität Dresden.

[Press et al. 1990] Press, W. A. et al.: Numerical Recipes, The Art of Sientific Computing (Fortran Version) Cambridge University Press, 1989, ISBN 0-521-38330-7.

[Q.922 1988] ITU-T Recommendation Q.922: ISDN Data Link Layer Specification for Frame Mode Bearer Services, ITU, Geneva, 1988.

[Raasch 1992] Raasch, J.: Systementwicklung mit sturkturierten Methoden; Carl Hanser Verlag, München, 2. Auflage, 1992, ISBN 3-446-17263-7.

[Rannenberg et al. 1996] Rannenberg, K.; Pfitzmann, A.; Müller, G.: Sicherheit, insbesondere mehrseitige IT-Sicherheit, it+ti Informationstechnik und technische Informatik, 38. Jahrgang 1996, Heft 4, Oldenbourg Verlag, München, S.5 und S. 10

[Romanow 1995] Romanow, A.; Floyd, S.: Dynamics of TCP Traffic over ATM networks, IEEE JSAC (1995) S.633-641.

[RSA 1978] Rivest, R.; Shamir, A.; Adleman, L.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of ACM, 1978, pp. 120-126.

[Schneier 1996] Schneier, B.: Applied Cryptography, Protocols, Algorithms and Source Code, Second Edition, Wiley and Sons., Inc., 1996, ISBN 0-471-12845-7 oder 0-471-11709-9.

[Schneier 2000] Schneier, B.: Secrets and Lies: Digital Security in a Networked World. Wiley and Sons., Inc., 2000, ISBN 0-471-25311-1.

[Schneier et al. 1999] Schneier, B.; Mudge, P.: Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2), CQRE '99, Springer-Verlag, 1999, pp. 192-203.

[Scott et al. 1998] Scott, C.; Wolfe, P.; Erwin, M.: Virtual Private Networks, O'Reilly & Associates, Inc., First Edition, 1998, ISBN 1-56592-319-7.

[Selke 2000] Selke, G.: Kryptographie, O'Reilly-Verlag, 2000, ISBN 3-89721-155-6.

[Shannon 1949] Shannon, C.: Communication Theory of Secrecy Systems, Bell Systems Technical Journal, No.4, 1949.

[Siegmund 1999] Siegmund, G.: Technik der Netze, 4., neubearb. und erw. Aufl., Hüthig Verlag, 1999, ISBN 3-7785-2637-5.

[Singh 1998] Singh, S.: Fermats letzter Satz, Carl Hanser Verlag, München, 1998, ISBN 3-446-19313-8.

[Singh 1999] Singh, S.: Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet, Carl Hanser Verlag, München, 1999, ISBN 3-446-19873-3.

[Spengenberg 2004] Spengenberg, R.: VPN mit Linux. Grundlagen und Anwendung Virtuelle Privater Netzwerke mit Open Source-Tools, Addision-Wesley Verlag, München, 2004, ISBN 3-8273-2114-X.

[Spohn 1993] Spohn, D. L.: Data Network Design, McGraw-Hill Series on Computer Communications, New York, 1993, ISBN 0-07-060360-X.

[Stallings 1998] Stallings, W.: Crypthography and Network Security. Principles and Practice, 2nd ed., Prentice-Hall International (UK) Limited, London, 1998, ISBN 0-13-869017-0.

[Steffen 2002a] Steffen, A.: Den Ausweis bitte Sicherer Zugang zum LAN via Virtual Private Network, c't, Magazin für Computer technik, 5/2002, Seite 216, ISSN 0724-8679.

[Steffen 2002b] Steffen, A.: Eigener Schlüsseldienst. VPNs und Zertifikate im Eigenbau, c't, Magazin für Computer technik, 5/2002, Seite 220, ISSN 0724-8679

[Steeman 1993] Steeman, D.: X.500 - The Directory Standard and its Application (Online Version) Technology Appraisals 1993, ISBN 1-871802-24-5.

[Stevens 1994] Stevens, R.: TCP/IP Illustrated, Volume I, The Protocols, Addison Wesley, 1994, ISBN-0201633469.

[Stubblefield et al. 2001] Stubblefield, A.; Ioannidis, J.; Rubin, A.: Using the Fluhrer, Mantin and Shamir Attack to break WEP., AT&T Labs Technical Report TD-4ZCPZZ.

[Tanenbaum 2000] Tanenbaum, A.: Computernetzwerke, 3. revidierte Auflage, Pearson Studium, ein Imprint der Pearson Education Deutschland GmbH, Martin-Kollar-Straße 10-12, München, 2000, ISBN 3-8273-7011-6.

[TeleChoice 2001] TeleChoice and Celox: IP-VPNs and Land Run for New Revenue, Whitepaper, preapared for Celox Networks, Apr. 2001, TeleChoice, Inc. 1307 S. Boulder Ave., Suite 120, Tulsa OK 74119.

[Ventura 2002] Ventura H.: Diameter next generation's AAA protocol, Master Thesis in Information Theory at Linköpings Tekniska Högskola, Linköping University, ISRN LITH-ISY-EX-3232-2002.

[Xiao 1999] Xiao, X.; Ni, L. M.: Internet QoS: A big picture, IEEE Network (2/1999), pp. 8-18.

[X.200 1994] ITU-T Recommendation X.200: Data networks and open system communications, Open Systems Interconnection - Model and notation, Version 7, Genf, 1994.

[X.509 1994] ITU-T Recommendation X.509: Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, 1994.

[Y.1311.1 2000] ITU-T Draft Recommendation Y.1311.1: Network Based IP VPN over MPLS Architecture, November 2000.

Stichwortverzeichnis

N-Entity, 24
n^2-Problem, 302
Überlast, 45
Übertragungsrate, 400
Übertragungsverzögerung, 400
öffentlicher Schlüssel, 126

Ack, 214
AES, 116
AP, 279
Application Layer, 23
Asynchroner Transfer Modus (ATM), 320
ATM, 10
  Stream Merging, 333
ATM-Dienstgüten, 325
ATM-Dienstgütenparameter
  Maximum Burst Size (MBS), 326
  Peak Cell Rate (PCR), 326
  Sustainable Cell Rate (SCR), 326
ATM-Header
  virtuell channel (VC), 322
  virtuell path (VP), 322
ATM-Referenzmodell, 329
Attribute Value Pair (AVP), 220
Auslastung, 401
Authentication Header, 230
Authentifizierung, 145
  einfache, 147
  geschützte, 150
  ungeschützte, 148
Authentikation
  starke, 152

B2B, 175
B2C, 175, 205
Best Effort, 42, 198
Bitfehlerrate, 400
Blockchiffre mit Blockverkettung (CBC), 103
BSI, 136
Burstiness, 399

Cäsars Verschlüsselung, 90
CA, 275
CAHP, 212
CE, 348, 349
Certificate Authority, 135
Certificate Authority, 273
Certificate Revocation List, 135
CHAP, 164
Chipkarten, 159
Circuit Emulation, 326
Class of Service (CoS), 42, 43, 53
Classless Internet Domain Routing, 30
Client-initiiert, 191
Closed User Group, 5
CMC, 274
CMP, 274
CNMS, 376
Common Criteria (CC), 72, 73
Compulsory Mode, 11
Compulsory Tunnel, 216
Controlled Load Service, 49
CoS, 31
CoS – Class of Service, 42
CPE, 373
CRAMM, 67

CRL, 137, 278
CTCPEC, 73
Customer Premise Equipment (CPE), 355
Cut-Through-Switching, 18

Data Encryption Standard, 111
Data-Link-Layer, 23
Daten, 19
Dateneinheiten, 19
Datenendeinheit (DEE), 25
Decapsulation, 207
Demultiplexen, 24
Denial-of-Service, 124
Denial-of-Service-Attacken, 63
DES, 111
DHCP, 30, 33, 245
DialIn, 222
DialOut, 223
DIAMETER, 172
  Basisprotokoll, 172
  CMS Security Module, 172
Dienstgüte, 42
Differentiated Services (DiffServ), 52
Diffie-Hellman-Schlüsselaustausch, 120
DiffServ
  Assured Forwarding (AF), 53
  Default Forwarding (DF), 53
  Expedited Forwarding (EF), 53
  Per-Hop-Behavior (PHB), 53
DoS, 63, 384
Drei-Wege-Authentifizierung, 155
DSSS, 278
Durchsatz, 401
DUT, 384

EFQM, 355
Ein-Wege-Authentifizierung, 153
Einmal-Passwort, 150
Einweg-Hash-Funktion, 129
Elektronisches Codebuch (ECB), 102
Encapsulating Security Payload, 236
Encapsulation, 206, 211
Encapsulation Security Payload, 230
Endliche Automaten, 27
Enterprise Security Management, 83
Enterprise Network, 4
ENX, 13
Ergebnisrückführung (OFB), 107

Fast-Packet-Switching (FPS), 314
  Data-Link-Control (DLC), 314
  Fast-Packet-Adaption (FPA), 314
  Fast-Packet-Relay (FPR), 314
FDDI, 26
FHSS, 278
Frame Relay, 10, 315
  Fast-Packet-Switching, 316
  FH, 315
  FRAD, 315
  Permanent Virtual Connections (PVC), 316
  statistisches Multiplexing, 316
  Switched Virtual Connections (SVC), 316
Frame-Header, 319
  BECN, 319
  DLCI, 319
  FECBN, 319

General Routing Encapsulation (GRE), 207
GPOA, 391
GPRS, 172
GRE, 195, 345
Guaranteed Service, 48

Hash, 129
Hauptverkehrsstunde, 399
HAZOP, 67
HDLC, 26
hotspots, 172

IANA, 233
ICMP, 37
IDEA, 115
IDS, 83, 186
IETF, VIII, 30
Informationsübermittlung, 18
  Nachrichtenübertragung, 18
  Nachrichtenvermittlung, 18

Information, 19
ingress device, 302
Inhalte, 19
Initialisierungsvektor, 103, 283
Insourcing, 342
integrierte Dienste, 47
Integrität, 395
Intermediate system to Intermediate system (IS-IS), 299
International Organization for Standardization (ISO), 21
Internet Scale VPN, 348
Internet-Protokoll (IP), 10, 17, 28, 399
IntServ
  Controlled Load Service, 48
  Guaranteed Service, 48
IP, 20
IP-Datagramm, 10
IPPM, 355
IPSec, 227
  AH, 234
  ESP, 236
  IKEv1, 243, 248, 250
  IKEv1-Phase-1, 251
  IKEv1-Phase-2, 256
  IKEv2, 262
  IKEv2-EAP, 268
  IKEv2-QoS, 268
  IKEv2-rekeying, 268
  ISAKMP, 249, 257
  KAME, 249
  Oakley, 260
  over L2TP, 248
  Racoon, 249
  Remote Access, 245
  SA, 232, 241, 260
  Transportmodus, 238
  Tunnelmodus, 239
  Ziel, 229
IPv4, 28
IPv5, 30
IPv6, 28, 29
ISDN, VII
ISMS, 358
ISP, 11, 339
IT-Security Scorecard-Verfahren, 84
ITSEC, 73
ITU-*T*, 152
IuK-Schutzziele, 228
IuK-Sicherheit, 61

Jitter, 44

KDC, 175
Kerberos, 174
KMU, 337, 361, 371
Kryptoanalyse, 89
Kryptographie, 89
Kryptologie, 89

L2Sec, 225
L2TP, 217
  Header, 221
  IPSec, 224
  LAC, 220
  LNS, 220
Label Switching, 298
Label-Stack, 303
  Last-in-First-out, 303
LAC, 221
LAN, 210
Latenzzeit, 44
Layer-2 Forwarding (L2F), 210
Layer-2-Tunnel (L2TP), 208
LDAP, 138
Lightweight Directory Access Protocol (LDAP), 56
LLC, 26
LNS, 221
logische Verbindung, 5

Maßeinheiten für Daten, 398
Man-in-the-middle-Attack, 124
Managed VPN, 337
Medium Access Control (MAC), 27
MobIKE, 231, 269
Mobile-IP, 172
MPLS
  Autonomes System, 307
MPLS-FEC
  Stream Merging, 305

MPLS-VPN, 304
MPPE, 212
MS-CHAP, 212
MSS – Maximum Segment Size, 40
MTBF, 402
MTTR, 361, 402
Multi Stage Exchange Networks, 325
Multiplexen, 24
Multiprotocol Label Switching
  MPLS, 298
Multiprotocol Lambda Switching
  optical transport network (OTN), 312

Nachrichtenvermittlung
  Leitungsvermittlung(Circuit Switching), 18
  Paketvermittlung(Packet Switching), 19
  Speichervermittlung (Message Switching), 18
Nachrichten, 19
NAP, 339
NAS, 345
NAT, 30, 208, 252, 268
NB-VPN, 350
Network Access Point (NAP), 339
Network Layer, 23
Netze planen, 369
  Leistungskenngrößen, 399
  Verkehrscharakteristiken, 397
Next-Generation-VPN (NG-VPN), 347
NIC, 269
NIST, 229
NMS, 352
NSP, VII, 11, 338

OLA, 356
Open Shortest Path First(OSPF), 299
OSI-Referenzmodell, 21
  Die Dienste, 24
  Die Protokolle, 25
  Die Schichten, 22
OSI-Sicherheitsarchitektur, 76
OSI-Sicherheitsdienste, 77
OSPF, 17
OTP, 148
Overlay-Netz, 9

Packetization Delay, 400
Paketvermittlung, 314
  Datagrammdienst, 315
  Virtual Circuit, 315
PAP, 164, 212
PDCA, 358
PDU, 398
Peer-N-Instanz, 24
Physical Layer, 22
PKC, 274
PKCS, 152
PKI, 83, 135, 274
PKIX, 152, 275
Plattform, 4
Playfair Algorithmus, 94
PNS, 213
Point-to-Point Protocol (PPP), 162
Point-to-Point-Protokoll (PPP), 208
PoP, 210, 213
PPP, 210
  PoP, 217
PPP-Frame, 214
PPTP, 210, 211
  NAS, 217
Pre-shared Keys (PSK), 254
Presentation Layer, 23
Primitive, 24
privater Schlüssel, 126
Public-Key-Kryptographie, 119
PVC, 305
PVC – *Permanent Virtual Circuit*, 20

QoS, 198, 208
QoS – Quality of Service, 42
Quality of Service (QoS)
  Dienstgüte, 319

RA, 275
RADIUS, 168
Rail Fence Chiffrierung, 97
RDP, 14
Resequencing, 20
RED – Random Early Discard, 42
Registration Authority, 135

Resource Reservation Protocol (RSVP), 47
RIP – *Routing Information Protocol*, 299
RIP – *Routing Information Protocol*
  Exterior Gateway Protocol, 299
  Interior Gateway Protocol, 299
Risiko, 67
  Bedrohung, 70
  Risikoszenarien, 71
  Schwachstelle, 70
RSN, 280
RSVP – Resource Reservation Protocol, 47
RTP – Real Time Transport Protocol, 38

SAD, 243
SBM, 44
SCEP, 274
Schlüsseltextrückführung (CFB), 105
Schutzziele
  Integrität, 71
  Verfügbarkeit, 71
  Vertraulichkeit, 71
SCTP, 173
SDU – *Service Data Unit*, 24
Security Association – (SA), 232
Security Associations
  Security Association Database, 234
  Security Policy Database, 234
Server (NAS)-initiiert, 192
Service Access Point (SAP), 24
Service Level Agreement, 402
Service Vereinbarungen (SLA), 358
Session Layer, 23
Signalisierung
  RSVP, 47
simplex-Verbindung, 233
SIP, 29
Site-to-Site, 187
SKIP, 281
SLA, 198, 225, 337, 341, 407
SLA – Service Level Agreement, 43
Sliding Window, 40
SNMP, 353
Socket, 38
soft state, 51
SPD, 243, 272
SSL, 152, 185
SSL-VPN, 282
  SSL-Handshake-Protokoll, 286
  SSL-Record-Protokoll, 285
  Verbindungsabschluss, 291
  Verbindungsaufbau, 287
  Verbindungsclient-Identifizierung, 290
  Verbindungsserveridentifizierung, 289
Store-and-Forward-Switching, 18
Stromchiffren, 100
SVC – *Switched Virtual Circuit*, 20
Switching Delay, 400
Synchronous Digital Hierarchy (SDH), 297

TACACS, 170
TCP, 20
TCP – Transmission Control Protocol, 38
TFTP - Trivial File Transfer Protocol, 32
Time Division Multiplexing (TDM), 322
Token Card, 156
TOS, 46
TOS – Type of Service, 52
Traffic Control, 49
Traffic Engineering, 304
  Constraint Based Routed Label Distribution Protocol, 304
  Label Distributed Protocol (LDP, 304
  Ressource-Reservation Protocol (RSVP-TE), 304
Transmission Delay, 400
Transport Layer, 23
Trojaner, 192
Trust Center, 134, 152
Trusted Third Party, 152
TSEC, 73
TT, 353
TTP – Trusted Third Party, 152
TTS, 353
Tunnel, 10
Tunneling, 206
  GRE, 208

Tunnel-Header, 206

UDP – User Datagram Protocol, 38
UMTS, 172

VC, 20
verbindungslose Daten, 32
Verfügbarkeit, 395, 401
Verlustwahrscheinlichkeit
für Pakete, 401
für Rahmen, 401
für Zellen, 401
Verschlüsselung
Reversibilität, 89
Verschlüsselungstechniken, 90
Substitutionstechnik, 90
Transpositionstechnik, 97
Vertraulichkeit, 395
VFI, 351
VIPR, 11
Virtual Circuit, 346
Virtual Private Trunking, 11
virtuelle Verbindung, 5, 20

WAN, VII
WDM, 408
Weitverkehrsnetze (WAN), 297
WEP, 279
WLAN, 278
WRED – Weighted Random Early Discard, 42

X.500, 136, 138
X.509 v3, 137
XOR-Operation, 96

ZDA, 136
Zuverlässigkeit, 403
Zwei-Wege-Authentifizierung, 154